INFORME DE INVESTIGACIÓN CIJUL

TEMA: DELITOS INFORMÁTICOS

RESUMEN: Informe general acerca de los elementos básicos que intervienen en el tema de los Delitos Informáticos. Un tema relativamente novedoso y de constante evolución doctrinaria, normativa y jurisprudencial tanto a nivel nacional como internacional.

SUMARIO:

x. **Compras por INTERNET**
xi. **Sabotaje**
xii. **Espionaje**
xiii. **Divulgación de Imágenes e Información**
xiv. **Violación a la Intimidad**
xv. **Homicidio**

2. **NORMATIVA**
   a. **Código Penal**
   b. **Ley de Derechos de Autor y Derechos Conexos**[1]
   c. **Ley de Procedimientos de Observancia de Derechos de Propiedad Intelectual**[2]
   d. **Código de Normas y Procedimientos Tributarios (Código Tributario)**[3]
   e. **Ley General de Aduanas**[4]
   f. **Administración Financiera de la República y Presupuestos Públicos**[5]
3. **JURISPRUDENCIA**
   a. **Concepto en sentido amplio y distinción entre el fraude informático y el sabotaje informático**
   b. **Comunidad virtual" que ofrece por medio de internet servicios de índole sexual que involucra a menores**

DESARROLLO

1. CRITERIOS DOCTRINALES

a. Definición

"En efecto, podemos definir al delito informático como; la acción que se realiza con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de las máquinas –hardware- o programas –software-."[6]

b. Clasificación

"Julio Tellez Valdés clasifica los delitos informáticos en atención a dos criterios: como instrumento o medio, o como fin u objetivo.

i) Como instrumento o medio. En esta categoría tenemos a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc).

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude,etc).

d) "Robo" de tiempo de computadora.

e) Lectura, sustracción o copiado de información confidencial.

f) Modificación de datos tanto en la entrada como en la salida.

g) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto se le conoce en el medio como el método del "Caballo de Troya").

h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la "técnica de salami".

i) Uso no autorizado de programas de cómputo.

j) Introducción de instrucciones que "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, tales como consulta a su distribuidor.

k) Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles virus informáticos.

ii) Como fin u objetivo. En esta categoría se enmarcan las conductas criminales que van dirigidas en contra de la computadora , accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etc.).

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate, etc.).”[7]

c. Elementos Subjetivos

i. Sujeto Activo

“Los sujetos activos no son delincuentes comunes. Por ello, presentan una particulares características, veamos:
1. Poseen importantes conocimientos de informática.
2. Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible. Por ello, se les ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema.
3. A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.
4. Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, pues algunos consideran que el nivel educacional a nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico. Para una respetable parte de la doctrina, acerca del delincuente informático se ha

realizado toda una caracterización mítica, donde se han servido como base los primeros casos de jóvenes norteamericanos que han procedido a vulnerarlos sistemas de seguridad de grandes sistemas informáticos, como lo son, aquellos de la NASA y el Departamento de Defensa de los Estados Unidos de América. Esa imagen del adolescente de clase media, inofensivo, el cual no tiene conciencia de que actúa mal, inmerso muchas veces en el "síndrome de Robín Hood", y con un coeficiente intelectual alto, permanece latente en el recuerdo de muchos. No obstante, estudios posteriores a esas primeras intromisiones no autorizadas a bases de datos, donde se han verificado graves consecuencias, han sido efectuadas por sujetos que laboran en el medio de la informática, de una edad superior a aquellos jóvenes y no tan inteligentes.
5. Estos delitos se han calificado de "cuello blanco", porque el sujeto que comete el delito es una persona de cierto status socioeconómico. El término "delitos de cuello blanco" fue acuñada por Sutherland en el año 1934."[8]

ii. Sujeto Pasivo

"El sujeto pasivo se encuentra representado por la persona o entidad sobre el cual recae la conducta que realiza el sujeto activo. Este sujeto ocupa una especial posición, debido a que en la mayoría de los casos, donde ha resultado económicamente perjudicado por la comisión de delitos informáticos en su contra, no denuncia esta situación y permanece en silencio, como lo dijimos, por no hacer más gravosa su posición y evitar la pérdida de confianza de sus clientes (especialmente en el caso de entidades bancarias, caso del Citibank citado líneas atrás) Muchas de las veces resulta de menor impacto la pérdida económica sufrida, que las posibles consecuencias del conocimiento, por parte de los clientes, de la vulneración de las bases de datos del sujeto (empresa) pasivo de la delincuencia informática."[9]

d. Características

"Según el mexicano Julio Tellez Valdez, los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.

- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

- Provocan serias pérdidas económicas, ya que casi siempre producen «beneficios» de más de cinco cifras a aquellos que las realizan.

- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

- Son muy sofisticados y relativamente frecuentes en el ámbito militar.

- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley."[10]

e. Tipos

i. Hacking y Cracking

1. Hacker

"Individuo que sin derecho penetra un sistema informático sólo por gusto o para probar sus habilidades. Usualmente no tiene fines delictivos graves este tipo de intrusión.

Sin embargo, ellos mismos se definen como: 1. Una persona que disfruta el explorar detalles de sistemas programables y cómo maximizar sus capacidades; 2. Alguien que programa entusiastamente; 3. Una persona que es buena programando rápidamente; 4. Un experto en un programa particular, como un "hacker de Unix"; 5. De manera despectiva, un intruso malicioso que trata de descubrir información sensible merodeando. Según ellos, el término correcto para esta definición despectiva es "cracker"."[11]

2. Cracker

"Derivado del hacking. Persona que sin derecho penetra un sistema informático con el fin de robar o destruir información valiosa, realizar transacciones ilícitas, o impedir el buen funcionamiento de redes informáticas o computadoras. Alguien que viola la

seguridad en un sistema. Este término fue acuñado por los hackers para defenderse del mal uso periodístico del término "hacker". El término "cracker" refleja la gran revulsión a los actos de robo y vandalismo perpetrados por los círculos de criminales conocidos como crackers."[12]

ii. Phreaking

"Penetrar ilícitamente sistemas telefónicos o de telecomunicaciones con el fin de obtener beneficios o causar perjuicios a terceros. Esta es una de las prácticas más antiguas en la historia del cibercrimen, la cual inicia en 1971 cuando un veterano de Vietnam, John Draper alias "Capitán Crunch", descubrió como un silbato podía reproducir el tono de 2600 hertz de los sistemas telefónicos.

También se puede definir como el arte y ciencia de crackear una red telefónica (para, por ejemplo, hacer llamadas de larga distancia gratuitas). Por extensión, la violación de la seguridad en cualquier otro contexto, especialmente en redes de comunicaciones."[13]

iii. CiberTerrorismo

"Aprovechamiento de las redes informáticas (Internet) para obtener información, fomentar o cometer actos de terrorismo. Los grupos extremistas, milicias y guerrillas pueden intentar ciberasaltos masivos contra el gobierno e infraestructura crítica de un país, como el transporte (aeropuertos, puertos marinos), la energía eléctrica, gas y servicios de emergencia."[14]

iv. Hacktivismo

"Derivado del *hacking.* Uso de la red por grupos activistas de cualquier tipo (políticos, religiosos, pro-derechos humanos, ambientalistas, etc.) para promover ciber-desobediencia civil o ataques en contra del gobierno.

La diferencia entre *ciberterrorismo* y *hacktivismo* es muy fina. En términos generales podemos decir que el fin último del *ciberterrorismo* es la destrucción física y/o electrónica de la infraestructura de un gobierno y su nación, y la motivación del *hacktivismo* es la protesta enérgica en contra del gobierno, la cual puede estar caracterizada por actos de "violencia electrónica"."[15]

v. CiberAcoso

"Acosar, hostigar, molestar, intimidar o amenazar personas o

entidades usando medios informáticos. El CiberAcoso puede ser definido como la conducta amenazante o aproximaciones no deseadas dirigidas a otra persona usando el Internet y otras formas de comunicación "en línea".”[16]

f. Delitos Informáticos e Internet actualmente

“El ciberespacio es un mundo virtual en el cual los defectos y actos ilegales del ser humano se reproducen con la misma facilidad que sus virtudes y negocios legales. Con el uso de las nuevas tecnologías, la masificación de las computadoras y la creciente difusión de Internet, las posibilidades de comisión de delitos informáticos y de actos de criminalidad computarizada se acrecientan. Por lo cual, creemos que un acercamiento al tema de los delitos informáticos en el contexto de internet es necesario, buscando dar una visión general sobre esta problemática.

En Europa, se considera a Internet y a su más conocida aplicación World Wide Web, como una de las principales piezas de infraestructura mundial de la información y un estímulo fundamental de la sociedad de información en Europa. En una comunicación de la Comisión Europea “se advierte del riesgo que supone la transmisión a través de la “web” de ciertos contenidos potencialmente nocivos, ilícitos o la utilización de la red como vehículo de actividades delictivas”. La Comisión, para evitar los perjuicios que pudieran provocarse considera que es necesario adoptar medidas para una acción inmediata, las que incluyen la cooperación de los estados miembros a fin de homogenizar los criterios europeos sobre los contenidos delictivos, la responsabilidad de los suministradores de acceso y los suministradores de servicio de ordenador central. Entre las conductas de criminalidad informática en Internet podemos mencionar: acceso no autorizado, destrucción de datos, infracción de los derechos de autor. Interceptación de correo electrónico, estafas electrónicas, transferencias de fondos indebidas.

Frente a estos problemas debe plantearse en Sudamérica y otros países del mundo, la solución de problemas como el de la Jurisdicción y competencia en Internet, la armonización de legislaciones y de tipos penales que permitan una represión penal efectiva, dado el ámbito territorial de las normas.

Por ejemplo en Uruguay se ha propuesto la tipificación del delito de fraude informático por una parte y el delito de hurto informático por otra. Se define en un proyecto de ley uruguayo por delito de Fraude Informático “el que con intención de procurarse a sí mismo o a un tercero un beneficio patrimonial, indebido, o

causare un patrimonio de otro, operando un proceso de datos incorrecto, configurando incorrectamente un programa de software, empleando adrede datos falsos, incorrectos o incompletos, o a través de cualquier otra intervención o manipulación ilegítima, sin la debida autorización o excediéndose de la misma, será castigado con pena de dos a seis años de penitenciaría". En este mismo proyecto de ley uruguayo se define por hurto informático "el que utilizando un sistema de computación, soporte lógico o "software" adecuado, sin la debida autorización, o excediéndose del marco de la misma, se apoderare de valores intangibles o incorporales ajenos, como depósitos monetarios, transferencias electrónica de fondos, créditos, información o secretos industriales o comerciales ; sustrayéndolos a su tenedor, para aprovecharse o que otro se aproveche de ella, será castigado con tres meses de prisión a tres años de penitenciaría". En Chile se ha promulgado recientemente la ley 19223 que tipifica figuras penales relativas a la informática. En otros países iberoamericanos también hay iniciativas de legislar sobre el tema.

En el Perú, como hemos mencionado, está tipificado el delito de hurto agravado por transferencia electrónica de fondos, uso de la telemática y vulneración de claves secretas. En la Segunda Reunión de Ministros de Justicia de las Américas realizada en Lima, del 01 al 03 de Marzo de 1999 se recomendó "el establecimiento de un grupo de expertos gubernamentales en el marco de la Organización de Estados Americanos (OEA) con la finalidad de hacer un diagnóstico de la actividad delictiva vinculada a las computadoras como medio para cometer un delito y hacer un diagnóstico de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad".

Por otra parte, también en el Perú, en forma reciente en Agosto de 1999, se ha presentado el Proyecto de Ley Nº 5071, en el Congreso Peruano sobre Delitos Informáticos en el cual se sostiene que "los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido, el presente proyecto se dirige a la regulación penal de las posibles medidas preventivas de carácter penal que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de delitos, alcance en el país los niveles de peligrosidad que se han dado en otros países". Este Proyecto de Ley está aún en proceso de discusión, lo que demuestra la actualidad de este tema en nuestro país. Para la discusión de este tema consideramos necesario tener en cuenta el contenido de este artículo, escrito por el autor, y que fue presentado como Ponencia Peruana en la

Segunda Reunión de Ministros de Justicia de las Américas . Con la finalidad de contribuir en la discusión de este proyecto es que publicamos el presente artículo, además de los otros objetivos señalados anteriormente.

Consideramos, asimismo que es necesario a nivel iberoamericano, armonizar legislaciones y los tipos penales que sancionan conductas criminales informáticas, teniendo en cuenta el acceso a Internet y la adopción cada vez más generalizada de las nuevas tecnologías."[17]

g. Algunas figuras delictivas a través de la Informática

i. Proxenetismo

"En la Red, el proxenetismo ha encontrado toda una gama de posibilidades para desarrollarse al margen de la ley, y nuestro país no se encuentra alejado de esta realidad. Costa Rica es promocionada en muchas páginas de Internet como un "paraíso sexual"; bajo "slogans" como "erotic vacation" (vacaciones eróticas), "World Sex Guide" (el mundo homosexual), o "sexual vacation" (vacaciones sexuales), así, se promocionan lugares dentro de nuestro país, donde se puede disponer de servicios sexuales, sin que pueda llegar a configurarse una conducta delictiva, salvo en el caso que se trate de menores.

Tal vez, tal y como lo indicamos anteriormente, la debilidad de la regulación de este ilícito lo encontramos, en primer lugar, en la competencia jurisdiccional para juzgar la responsabilidad del proxeneta que promueve, ahora por medio de la Red los servicios de sus víctimas. Si el proxeneta reside en nuestro país, aunque la página se encuentre en un servidor extranjero no consideramos que se perjudique la competencia y creemos que puede ser cesado con nuestra legislación.

(…)

Entendemos, entonces, que esta conducta resulta impune, por el problema que indicamos supra sobre la extradición de ciudadanos extranjeros, aunado al hecho que no estamos frente a un delito internacional. Incluso, si ese mismo holandés tiene un grupo de varones a los que prostituye, enviándolos de un país a otro para satisfacer a sus dientas (es), no podríamos decir que se configura un delito internacional, al menos partiendo desde la perspectiva de nuestro Código Penal vigente, y tampoco se relaciona de la trata de blancas (que sí es un delito internacional), pues este se refiere a mujeres o niños, excluyendo a los varones mayores de edad."[18]

ii. Pornografía

"La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. Durante los pasados cinco años, el

número de condenas por transmisión o posesión de pornografía infantil ha aumentado de 100 a 400 al año en un país norteamericano. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material «ofensivo» que se transmita o archive."[19]

"Existen en la red una serie de programas que podrían introducir un nivel problema de la regulación, éstos se caracterizan por seleccionar la formación a la que tiene acceso un computador específico y restringir algunas consultas, algunos de ellos son Safe surf, Nanny, Cyberpatrol, etc.
La situación en Internet no es la mejor, aunque existan mil leyes estatales que prohíban la pornografía, siempre habrá lugares en el mundo donde no existan «fricciones al respecto (caso de Holanda); de manera que se trata de un problema i el ámbito mundial, lo cual nos lleva a pensar en la necesidad de una regulación procedo internacionales, con el fin de evitar los delitos transfronterizos.
(…)
Es evidente que el problema de la regulación de la pornografía es sumamente complejo. No estamos frente a unas cuantas empresas de revistas, o boletines sexuales, se trata de la red de la información, de miles de páginas en decenas de países que contienen material de este tipo.
Ahora, son varias las aristas del problema:
a.- la definición de pornografía, que no resulta nada fácil;
b.- el debido respeto a la libertad de expresión, aunque ésta puede ser jada debe respetarse y no eliminarla y;
c.- la elaboración de una norma o conjunto de éstas que representen la preocupación mundial sobre este tema."[20]

iii. Manipulación en el ingreso de datos

"Cuando hablamos de la manipulación en el ingreso de los datos, estamos ante un verdadero fraude informático, al cual se le conoce como sustracción de datos. Esta conducta resulta ser el delito informático más común, de fácil comisión y difícil descubrir.
Este delito no requiere que el sujeto activo posea especiales conocimientos informáticos, sino que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La introducción y el almacenamiento de datos, corresponde al paso inicial del procesamiento de los mismos por medio de la computadora. Una vez ingresada la información, la misma computadora, con aplicación de los programas que posee, procede a

ordenarla, para posteriormente ser utilizada.
Como ejemplo, podemos citar en Costa Rica, el caso en el cual una empleada que tenia bajo su control el ingreso de los datos relativos a la planilla del Poder Judicial," incluyó como funcionario (juez) a su compañero, sin que el mismo nunca realizara labor alguna y fuera nombrado en el cargo, recibiendo el salario respectivo que le correspondía conforme la función que, supuestamente, tenía asignada según los datos que fueron ingresados fraudulentamente al sistema de planillas."[21]

iv. Manipulación de datos ingresados

"En este supuesto, el autor manipula los datos de la computadora. Por ejemplo manipula la información de la cuenta de impuestos de un contribuyente, de manera tal que obligue a la Administración Tributaria a pagarle al contribuyente (devolución de los impuestos pagados), así se genera un beneficio para quien se encuentra obligado al pago de tributos. La manipulación se puede hacer al menos de dos formas, introduciendo información falsa a la computadora (ya tratado en el caso anterior) o bien, alterando los datos una vez que éstos han sido correctamente introducidos al sistema o bien eliminando información. En ninguno de estos supuestos se puede hablar de daños, por el contrario, la hipótesis se asemeja más a la estafa, con la salvedad ya apuntada de ausencia de agente pasivo (conducta atípica en nuestro sistema). Tampoco se podría hablar en sentido estricto de falsificación de documento art. 357 y siguiente del CP, pues el documento en sentido penal se define como "una Idea aclaratoria incorporada, esto es, unida con una cosa, en general o así entendida, en sentido humano, apropiada y determinada, para dar seguridad en el tráfico y que deja reconocer a quien lo emite". En este sentido, el documento como tal está compuesto por un elemento subjetivo, concepto o "idea aclaratoria" y un elemento material, "papel, cartón, etc." que permite transmitir la idea, más aún, pareciera que la posibilidad de conocer al emisor es un elemento constitutivo del documento, con lo cual un anónimo estaría fuera del concepto. De esta forma, no podría admitirse que la base de datos de una computadora, pueda encajar dentro de la idea de documento. De tal forma, la manipulación de los datos ingresados a la computadora, no podría sancionarse como daños en sentido estricto, aún y cuando en realidad produzca un daño en términos económicos, pues en realidad la base de datos sigue intacta, solo que contiene datos alterados. Por otra parte, los datos contenidos en la base, encajan en el concepto de cosa contenido en el del art. 228 del CP."[22]

v. Manipulación en los datos que salen de la Computadora (Caballo de Troya)

"Cuando los datos se transfieren a otra computadora, en los programas de impresión (output), o en programas de actualización, es decir, una vez que los datos son ingresados, ordenados y los procesos de cálculo elaborados, la información final, por lo general se imprime y almacena. Es posible manipular la información que se imprime y almacena, de manera tal que la alteración no pueda detectarse, durante el procesamiento de datos. Esta forma de comisión es una de las más complejas de detectar, pues por lo general se realiza en la etapa final de proceso. En programas de contabilidad, para citar un ejemplo, una vez que los datos del período son procesados, revisados contra los comprobantes y verificados, los mismos pasan a un proceso de actualización de saldos de cuentas, con lo cual se borran los movimientos del período y los saldos al final del período anterior se acumulan con los movimientos de ese período, generando un saldo inicial para el período siguiente. Esto es lo que se denomina feedback o retroalimentación, que es cuando la computadora asume, y aprovecha los resultados de un proceso, como fuente de información paro otro nuevo tratamiento. Si el programa es alterado en el momento en que los datos se actualizan, es muy difícil determinar la alteración, pues en la práctica se parte de la base, de que los cálculos de la computadora son los correctos y que el cuidado debe tenerse, precisamente cuando se introducen los datos al mismo. Esta forma de manipulación es prácticamente impensable en condiciones normales de trabajo y por eso suele pasar inadvertida, por lo general se descubre mediante la realización de un procedimiento de auditoría, por lo demás caro, lento, complejo y muchas veces tardío."[23]

"Un método común utilizado por personas que tienen conocimientos especializados en programación informática es el denominado "Caballo de Troya", que consiste en insertar instrucciones de computadora en forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. El nombre se debe al episodio de la Iliada de Homero, Ulises diseñó una estratagema mediante la cual regala a los troyanos un gran caballo de madera, que en el interior ocultaba soldados, con lo cual hacía creer que el ejército griego abandonaba el sitio de la ciudad. Confiando los troyanos que efectivamente se trataba de un regalo de los vencidos en guerra, ingresaron el caballo en el recinto amurallado de Troya y, aprovechando la noche y confianza de los habitantes, los guerreros ocultos hicieron entrar a las tropas griegas que aguardaban en las puertas de la ciudad, la cual invadieron.

Conforme lo expuesto, un "Caballo de Troya" es un programa legítimo que contiene una sección de "código oculto", a simple vista parece inofensivo, pero cuando se procesa, se activa el mismo y provoca graves distorsiones a los sistemas informáticos.
(…)
El ejemplo que más se presenta en esta etapa, corresponde al que se realiza en los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Inicialmente dichos fraudes se ejecutaban con tarjetas bancarias robadas, pero actualmente se utilizan equipos y programas especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito"[24]

vi. Técnica del Salami o manipulación de Programas

"En este caso, el autor no manipula ni altera los datos de la computadora, sino que por el contrario, la manipulación y/o alteración se genera en el programa. Un ejemplo de este caso, relativamente sencillo es el del empleado bancario, que altera el programa de cálculo de intereses de las cuentas de ahorro, de manera tal que solo los dos primeros dígitos de los decimales, se tomen como intereses y los restantes dígitos se transfieran a una cuenta, por él controlada. De esta manera tan simple, es posible obtener grandes sumas de dinero, puestos cuentahabientes no lo pueden detectar. Por otra parte, se puede aplicar a programas de redondeo, pensiones, amortizaciones, etc., es decir, se presenta para el inescrupuloso, una gama de posibilidades muy amplias."[25]

"Como ejemplo, tenemos el caso de un empleado de puesto de bolsa que altera el programa de cálculo de intereses de las cuentas de inversión, resultando que si los ingresos por intereses de cada título supera cierta cantidad y contiene además centavos de dólar, estos últimos sean desviados a una cuenta suya en el extranjero. Por este medio se han obtenido importantes cantidades de dinero, como ha sucedido en Estados Unidos, resultando difícil su detección."[26]

vii. Intromisión de base de datos

"Otra hipótesis de criminalidad electrónica, constituye en la mera intromisión en bases de datos, las cuales contienen información no disponible al público, por ejemplo archivos médicos, criminales, de bancos, etc. Este tipo de información en manos de personas inescrupulosas genera, un alto riesgo pues con ella se pueden cometer una gran cantidad de conductas criminales. Piénsese solo en un caso: un delincuente o un banda de delincuentes, logra accesar

la base dé datos de un banco, por medio de la cual determina la frecuencia de los depósitos en la cuenta corriente de una empresa, de igual forma determina qué porcentaje de dichos depósitos se realiza en efectivo y qué porcentaje en otros valores, determina la hora del depósito y la agencia bancaria en la que los mismos se realizan. Con todos esos datos, solo requerirán identificar al depositante y con seguridad darán un buen golpe. El simple acceso a la base de datos no genera por sí solo, un daño, pues más bien, las bases de datos están diseñadas para ser accesadas, con lo cual se requiere de tipos penales específicos que sancionen la conducta."[27]

"Como ejemplo podemos citar el caso donde una banda criminal ingrese a la base de datos de un banco, logra determinar la frecuencia de los depósitos en la cuenta corriente de una empresa, así como el porcentaje de depósitos que se realizan en dinero efectivo y en otros valores, se determina la hura de los depósitos y hasta la agencia bancaria en la que los mismos se realizan. Con estos datos, sólo quedará identificar físicamente al depositante y consumar el ilícito."[28]

viii. Estafa

"…podemos clasificar este tipo de delitos (estafas electrónicas) como manipulaciones a distancia. Estas se caracterizan principalmente por ser realizadas desde fuera del lugar en que se encuentra el ordenador afectado, incluso puede ser desde otra parte del mundo. Los problemas de este delito son bifásicos (al igual que los demás de esta investigación). Por un lado nos enfrentamos a la atipicidad respecto del engaño y el error al que no es susceptible el ordenador, y por otro al aspecto de territorialidad, pues la red permite a sus usuarios ir de un lugar a otro del globo, aún sin darse cuenta. Así, una maniobra realizada por un ruso desde su país contra el Banco Nacional de Costa Rica, podría ser descubierta, pero sin una norma de carácter internacional que permita el juzgamiento en el exterior, o bien podría ocurrir que no pueda llevarse a cabo la extradición, por lo que el hecho quedaría impune.

No queda duda de la atipicidad de las manipulaciones por medio de un computador, y mucho menos aún de aquellas que son realizadas por Internet y permiten generar delitos a miles de kilómetros del lugar en el que se inicia la acción.

La necesidad de crear un tipo específico es inminente, nuestro ordenamiento e incluso los proyectos de ley son omisos en cuanto a las manipulaciones. Algunos países europeos han legislado en este campo, de manera que podamos aprender del derecho comparado y reconocer las deficiencias de nuestro

sistema."[29]

ix. Falsificación de datos

"Tanto la falsificación de datos en Internet como en cualquier medio informático encuentra una serie de problemas para ser comprendidos dentro de la figura tradicional de la falsificación de documentos de nuestro Código Penal.

Son tres las principales vertientes del problema en cuanto a la Internet. Primero, la materialidad del documento, segundo, el concepto de documento en la doctrina y tercero la manifestación de voluntad en el documento.

La materialidad es uno de los requisitos del "documento", en los delitos de falsificaciones (del art 357 a 362 de nuestro Código Penal vigente). Según Juan Bustos Ramírez, es "una concepción muy restringida de los documentos que ya no obedecen a las formas modernas de las relaciones jurídico-sociales.

(...)

Así, la materialidad entendida como atributos visuales o legibles hace que los documentos informáticos no formen parte del concepto de documentos tal y como se entiende actualmente.

(…)

La otra arista del problema de la falsificación de datos es la manifestación de voluntad que contiene el documento. Para Romeo Casabona deben distinguirse dos situaciones, las manipulaciones de entrada (input) y salida (output) de datos, y las manipulaciones de programa.

En las manipulaciones input la situación de la manifestación de voluntad no es problema. Se trata de los casos en los que se introducen al computador pero resultan falsos o alterados, verbigracia, el sujeto que introduce en el registro de la delincuencia características distintas para no ser atrapado, o el que por el contrario borra cualquier referencia de juicios anteriores. Estaríamos frente a una verdadera falsificación informática, pero, ampliado el concepto de documento para los datos informáticos; ésto al menos mientras no se imprima el documento, lo que le daría la materialidad a la acción y no daría problemas para insertarlo en el tipo tradicional.

La segunda posibilidad a la que se refiere Romeo Casabona es la falsificación de datos de un programa, según el cual "un programa no encara en sí mismo un pensamiento o una declaración de voluntad concretos de una persona determinada en el sentido expuesto, sino que, como es sabido, constituye un instrumento de trabajo para, valga la expresión, tratar informáticamente -es decir, mediante ciertos procedimientos técnicos más o menos sofisticados- el pensamiento humano(p. Ej. Un estado de

cuentas, una cartera de clientes, los salarios de los trabajadores, multitudes de textos epistores".
Precisamente muchas de las defraudaciones se realizan a través de falsificaciones en las operaciones que ejecuta un programa, a la hora de procesar los datos, como por ejemplo, insertar alguna orden al programa para que saque de salario una suma y la ponga en una cuenta aparte. Se está frente a una falsificación, pues, por un lado se crea un dato informático falso (la nueva cuenta), y por otro se alteran varias cuentas existentes (que podrían se planillas de alguna institución del Estado)."[30]

x. Compras por INTERNET

"Hoy día existe en la Red Internet, una gama muy amplia de posibilidades de adquirir bienes y servicios, los cuales por lo general se pagan a través de tarjetas de crédito. Para pagar y ordenar el servicio, quienes ofrecen servicios o bienes por este medio, solicitan únicamente los datos del tarjetahabiente, nombre, número de tarjeta, fecha de vencimiento y tipo de tarjeta, si todos esos datos coinciden, por lo general, sin ninguna otra verificación el producto se adquiere o se despacha. Desde luego el tarjetahabiente no advierte el hecho, sino hasta que el estado de cuenta es recibido y aparece el cargo hecho por la compañía administradora de la tarjeta. La situación se dificulta aún más, cuando existen tarjetas adicionales, o bien, el estado de cuenta es recibido por una persona distinta del tenedor de la tarjeta, pues muchas veces escapan al control, sobre todo cuanto el monto de los cargos no es muy elevado como por ejemplo suscripciones a revistas, periódicos, programas de cómputo (software), etc."[31]

xi. Sabotaje

"En 1973 en Estados Unidos de Norteamérica, cerca del 18% de los casos de criminalidad por computadora se encontraba en esta categoría. Esta forma de criminalidad tiene por objeto la afectación o destrucción tanto del programa, como de los datos almacenados en la computadora, bien puede provocarse un daño al hardware o disco duro (en cuyo caso se podría hablar de daños en sentido del art. 228 del CP), pero la forma más común de comisión es a través del deterioro de los datos almacenados y los programas. En ausencia de archivos de respaldo y programas para la reinstalación y restitución del sistema, este tipo de criminalidad genera pérdidas enormes tanto para particulares, como para empresas o instituciones. La forma de comisión más común es la intromisión del hardware y/o programas de la computadora y que se encargan de

destruir la información, inutilizarla o bien producir daños al mismo disco duro, que lo hacen inaccesible y/o inservible. Normalmente consisten estos virus en rutinas, instrucciones o partes de programas que se introducen a través de un soporte físico que los contiene, o a través de la red de comunicaciones, que pueden actuar en el momento o incluso con efecto retardado."[32]

xii. Espionaje

"Las posibilidades de cometer un acto de espionaje en la Red son variadas, incluso podría llamar a problemas de concursos con otros delitos ya estudiados durante esta investigación. Verbigracia el acceso a un sistema con una clave falsa podría sancionarse como acceso no autorizado, empero, habría que hacer la diferencia en cuanto al dolo que exigen ambas figuras. La primera se refiere al acceso no autorizado o con clave falsa, pero el espionaje implica una intención, la de imponerse de secretos industriales, comerciales, políticos económicos o militares ya sea de una empresa o el estado. La diferencia la ha hecho también el derecho español que establece un delito de espionaje en su artículo 278. Sobre el punto indica el Lic. Álvaro Burgos "Es claro, que el tipo subjetivo solamente admite la comisión por dolo de parte de quién realiza la acción, y se incorpora dentro del artículo 278 del código penal español la finalidad que debe tener el sujeto activo del ilícito de querer "...descubrir un secreto de la empresa...", por lo que el mero descubrimiento no doloso, causal o culposo sería atípico de no darse el dolo específico del tipo aludido". Como vemos el dolo puede hacer la diferencia entre esta y otras figuras específicas, empero es un problema resuelto para legislaciones que si tienen estos delitos y no como nuestro país que tiene una norma muy específica de acceso no autorizado y ninguna de espionaje industrial o personal.

(…)

Nuestro ordenamiento no tiene una figura relativa a este tipo de acción delictiva, diferente al caso de España y Alemania, y el proyecto de Código Penal no contiene ninguna figura que dé una esperanza para cubrir esta lamentable laguna del ordenamiento. Si bien es cierto el citado proyecto contiene un delito de espionaje y un capítulo dedicado a violación de datos personales, no contiene una norma que regule el problema planteado, incluso de la interpretación del delito de espionaje y de los artículos del título IV delitos contra el ámbito de intimidad, capítulo I violación de datos personales y comunicaciones, no se podría sancionar la sustracción de secretos de una empresa por un particular."[33]

xiii. Divulgación de Imágenes e Información

"En este caso, no se trata del daño o intromisión en bases de datos privadas, sino por el contrario, la utilización de bases de datos abiertas con fines criminales. Por esa vía se pueden hacer circular a nivel mundial datos e imágenes, sin autorización de quien legítimamente puede darla, o bien como ha sucedido y que recientemente ha sido objeto de persecución policial a nivel mundial, se hace circular pornografía. Desde luego en este caso, quedan a salvo los derechos de las víctimas en relación con los delitos contra el honor, sin embargo, es claro que la pena establecida en el CP es mínima en relación con el daño que se puede causar."[34]

xiv. Violación a la Intimidad

"La intimidad o privacidad es un área restringida, de la cual surge el derecho a tener una vida privada sin intromisión, curiosidad, vigilancia y espionaje. Este delito informático consiste en la violación de la intimidad de la vida personal y familiar, sea observando, escuchando o registrando hechos, palabras, escritos o imágenes, valiéndose de instrumentos, procesos técnicos u otros medios.

También se podría tipificar como delito el que organiza, proporciona o emplea indebidamente un archivo que tenga datos referentes a las convicciones religiosas, políticas o a la vida íntima de las personas.

Con el desarrollo de la informática y su utilización masiva, el instrumento más efectivo para lograr controlar la difusión de cierta información personal que pueda causar graves perjuicios es, indudablemente, el hábeas data. Este brinda la posibilidad a cualquier persona, de acceder a la información contenida en las bases de datos, para lograr la supresión en caso de ser errónea, así como modificándola y/o actualizándola cuando fuera necesario o cuando fuera discriminatoria.

Por medio del hábeas data se garantiza el acceso a los bancos de datos donde se encuentra registrados o almacenados la información acerca de la persona. En caso de falsedad de los datos, se podrá;

- exigir su supresión; lo cual implica la eliminación del registro,
- exigir la rectificación; conduce ala modificación o cambio de la información existente por la aportada, ella seguirá existiendo, pero adecuada al aporte efectuado,
- exigir la actualización; se encuentra íntimamente ligada con la rectificación, pues aquí se persigue una modificación del registro de datos, debido a que son antiguos, han perdido vigencia o interés.

La vía del hábeas data puede resumirse como el derecho de acceso,

control y remedio para los datos personales almacenados en diferentes sistemas computarizados."[35]

xv. Homicidio

"Aunque no parezca creíble es posible cometer homicidio por computadora. Se daría en los casos en que a un paciente que está recibiendo un determinado tratamiento, se modifican las instrucciones en la computadora, que puede hacerse incluso desde una terminar remota."[36]

2. NORMATIVA

a. Código Penal[37]

Artículo 196 bis.- Violación de comunicaciones electrónicas

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

(Así adicionado por Ley N° 8148 de 24 de octubre del 2001)

Artículo 217 bis.- Fraude informático

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

(Así adicionado por Ley N° 8148 de 24 de octubre del 2001)

b. Ley de Derechos de Autor y Derechos Conexos[38]

ARTICULO 1º.- Las producciones intelectuales originales confieren a sus autores los derechos referidos en esta ley. La protección del derecho de autor abarcará las expresiones, pero no las ideas, los

procedimientos, métodos de operación ni los conceptos matemáticos en sí. Los autores son los titulares de los derechos patrimoniales y morales sobre sus obras literarias o artísticas.

(Así reformado por Ley N° 7979 del 6 de enero del 2000)
Por "obras literarias y artísticas" deben entenderse todas las producciones en los campos literario y artístico, cualquiera sea la forma de expresión, tales como: libros, folletos, cartas y otros escritos; además, los programas de cómputo dentro de los cuales se incluyen sus versiones sucesivas y los programas derivados; también las conferencias, las alocuciones, los sermones y otras obras de similar naturaleza, así como las obras dramático musicales, las coreográficas, las pantomimas; las composiciones musicales, con o sin ella y las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía, las obras de dibujo, pintura, arquitectura, escultura, grabado y litografía, las obras fotográficas y las expresadas por procedimiento análogo a la fotografía; las de artes aplicadas; tales como ilustraciones, mapas, planos, croquis y las obras plásticas relativas a la geografía, la topografía, la arquitectura o las ciencias y las obras derivadas como las adaptaciones, las traducciones y otras transformaciones de obras originarias que, sin pertenecer al dominio público, hayan sido autorizadas por sus autores.
(Así reformado por el artículo 1º de la ley Nº 7397 de 3 de mayo de 1994)

c. Ley de Procedimientos de Observancia de Derechos de Propiedad Intelectual[39]

Delitos contra derechos de autor y derechos Conexos

Artículo 51.—Representación o comunicación pública sin autorización de obras literarias o artísticas. Será sancionado con prisión de uno a tres años quien represente o comunique al público obras literarias o artísticas protegidas, sin autorización del autor, el titular o el representante del derecho.

Artículo 52.—Comunicación de fonogramas, videogramas o emisiones sin autorización. Será sancionado con prisión de uno a tres años quien comunique al público fonogramas, videogramas o emisiones, incluidas las satelitales, protegidas por la Ley de derechos de autor y derechos conexos, N° 6683, de 14 de octubre de 1982, y sus reformas, sin autorización del autor, el titular o el representante del derecho, de modo que pueda resultar perjuicio.

Artículo 53.—Inscripción registral de derechos de autor ajenos. Será sancionado con prisión de uno a tres años quien inscriba como suyos, en el Registro Nacional de Derechos de Autor y Derechos Conexos, obras literarias o artísticas, fonogramas o videogramas, interpretaciones o ejecuciones fijadas o no, o emisiones, incluidas las satelitales, protegidas en la Ley de derechos de autor y derechos conexos, N° 6683, de 14 de octubre de 1982, y sus reformas, siendo derechos ajenos.

Artículo 54.—Reproducción no autorizada de obras literarias o artísticas, fonogramas o videogramas. Será sancionado con prisión de uno a tres años quien fije y reproduzca obras literarias o artísticas, fonogramas o videogramas protegidos, sin autorización del autor, el titular o el representante del derecho, de modo que pueda resultar perjuicio.

Artículo 55.—Fijación, reproducción y transmisión de ejecuciones e interpretaciones protegidas. Será sancionado con prisión de uno a tres años quien fije y reproduzca o transmita interpretaciones o ejecuciones protegidas, sin autorización del titular, de modo que pueda resultar perjuicio.
La misma pena se aplicará a quien fije, reproduzca o retransmita emisiones protegidas, incluidas las satelitales, sin autorización del autor, el titular o el representante del derecho, de modo que pueda resultar perjuicio.

Artículo 56.—Impresión de un número superior de ejemplares de una obra. Será sancionado con prisión de uno a tres años el editor o impresor que reproduzca un número de ejemplares superior al número convenido con el autor de la obra, de modo que pueda resultar perjuicio.

Artículo 57.—Publicación como propias de obras ajenas. Será sancionado con prisión de uno a tres años quien publique como propias o como de otro autor, obras ajenas protegidas, a las cuales se les haya cambiado o suprimido el título o se les haya alterado el texto, de modo que pueda resultar perjuicio.

Artículo 58.—Adaptación, traducción, modificación y compendio sin autorización de obras literarias o artísticas. Será sancionado con prisión de uno a tres años quien adapte, transforme, traduzca, modifique o compile obras literarias o artísticas protegidas, sin

autorización del titular, de modo que pueda resultar perjuicio. No serán punibles los compendios de obras literarias o de artículos de revista científicos o técnicos que tengan fin didáctico, siempre y cuando hayan sido elaborados sin fines de lucro e indiquen la fuente de donde se extrajo la información.

Artículo 59.—Venta, ofrecimiento, almacenamiento, depósito y distribución de ejemplares fraudulentos. Será sancionado con prisión de uno a tres años quien venda, ofrezca para la venta, almacene, distribuya, guarde en depósito, importe o exporte, ejemplares fraudulentos de una obra literaria o artística, fonograma o videograma, de modo que se afecten los derechos que la Ley de derechos de autor y derechos conexos, Nº 6683, de 14 de octubre de 1982, y sus reformas, confiere al titular.

Artículo 60.—Arrendamiento de obras literarias o artísticas, fonogramas o videogramas sin autorización del autor. Será sancionado con prisión de uno a tres años quien alquile o dé en arrendamiento obras literarias o artísticas, fonogramas o videogramas, sin autorización del autor, el titular o el representante del derecho, de modo que pueda resultar perjuicio.

Artículo 61.—Fabricación, importación, venta y alquiler de aparatos o mecanismos descodificadores. Será sancionado con prisión de uno a tres años quien fabrique, importe, venda u ofrezca para la venta, dé en arrendamiento o facilite un dispositivo o sistema útil para descifrar una señal de satélite portadora de programas, sin autorización del distribuidor legítimo de esta señal, de modo que pueda resultar perjuicio a los derechos del distribuidor.

Artículo 62.—Alteración, supresión, modificación o deterioro de las defensas tecnológicas contra la reproducción de obras o la puesta a disposición del público. Será sancionado con prisión de uno a tres años quien, en cualquier forma, altere, suprima, modifique o deteriore los mecanismos de protección electrónica o las señales codificadas de cualquier naturaleza que los titulares de derechos de autor, artistas, intérpretes o ejecutantes, o productores de fonogramas hayan introducido en las copias de sus obras, interpretaciones o fonogramas, con la finalidad de restringir su comunicación al público, reproducción o puesta a disposición del público.

Artículo 63.—Alteración de información electrónica colocada para proteger derechos patrimoniales del titular. Será sancionado con prisión de uno a tres años quien altere o suprima, sin autorización, la información electrónica colocada por los titulares de los derechos de autor o conexos, para posibilitar la gestión de sus derechos patrimoniales y morales, de modo que puedan perjudicarse estos derechos.
La misma pena se aplicará a quien distribuya, importe con fines de distribución, emita o comunique al público, sin autorización, ejemplares de obras, interpretaciones o fonogramas, sabiendo que la información electrónica, colocada por los titulares de derechos de autor o conexos, ha sido suprimida o alterada sin autorización.

Delitos contra derechos de patentes de invención, dibujos y modelos industriales y modelos de utilidad

Artículo 64.—Violación de productos patentados o protegidos. Será sancionado con prisión de uno a tres años quien haga aparecer como productos patentados o protegidos por modelos de utilidad, los que no lo están, de modo que pueda resultar perjuicio al legítimo titular del derecho.

Para los efectos de la interpretación del presente artículo, se utilizarán los conceptos de productos patentados o protegidos y el de modelos de utilidad contenidos en la Ley de patentes de invención, dibujos y modelos industriales y modelos de utilidad, Nº 6867, de 25 de abril de 1983.

Artículo 65.—Invocación frente a terceros de derechos en calidad de titular. Será sancionado con prisión de uno a tres años quien, sin ser titular de una patente ni de un modelo de utilidad o sin gozar ya de estos privilegios, los invoque ante terceros como si los disfrutara, de modo que pueda causar daño al legítimo titular del derecho.
Queda a salvo el derecho que posee el creador de utilizar su invención o modelo de utilidad una vez iniciado el trámite de registro de esa patente de invención o modelo de utilidad.

Artículo 66.—Violación de derechos derivados de patentes o modelos de utilidad registrados en Costa Rica. Será sancionado con prisión de uno a tres años quien fabrique productos patentados y registrados en Costa Rica por modelos de utilidad, emplee

procedimientos patentados y registrados en Costa Rica sin el consentimiento de su titular, o actúe sin licencia ni autorización, de modo que pueda resultar daño al legítimo titular del derecho.

Artículo 67.—Reproducción ilícita de modelos o dibujos industriales. Será sancionado con prisión de uno a tres años quien reproduzca modelos o dibujos industriales protegidos y registrados en Costa Rica, sin el consentimiento de su titular, sin la licencia ni la autorización correspondiente, de modo que pueda resultar daño al legítimo titular del derecho.

Artículo 68.—Venta, almacenamiento, distribución, depósito, exportación o importación de ejemplares fraudulentos. Será sancionado con prisión de uno a tres años quien venda, ofrezca para la venta, almacene, distribuya, guarde en depósito, importe o exporte ejemplares fraudulentos de modo que se pueda causar daño a los derechos conferidos en la Ley de patentes de invención, dibujos y modelos industriales y modelos de utilidad, Nº 6867, de 25 de abril de 1983.

d. Código de Normas y Procedimientos Tributarios (Código Tributario)[40]

ARTÍCULO 94.- Acceso desautorizado a la información Será sancionado con prisión de uno a tres años quien, por cualquier medio tecnológico, acceda a los sistemas de información o bases de datos de la Administración Tributaria, sin la autorización correspondiente.

(Así reformado por el artículo 2º de la ley No.7900 de 3 de agosto de 1999)

ARTÍCULO 95.- Manejo indebido de programas de cómputo Será sancionado con pena de tres a diez años de prisión, quien sin autorización de la Administración Tributaria, se apodere de cualquier programa de cómputo, utilizado por ella para administrar la información tributaria y sus bases de datos, lo copie, destruya, inutilice, altere, transfiera, o lo conserve en su poder, siempre que la Administración Tributaria los haya declarado de uso restringido, mediante resolución.

(Así reformado por el artículo 2º de la ley No.7900 de 3 de agosto

de 1999)

ARTÍCULO 96.- Facilitación del código y la clave de acceso Será sancionado con prisión de tres a cinco años, quien facilite su código y clave de acceso, asignados para ingresar a los sistemas de información tributarios, para que otra persona los use.

(Así reformado por el artículo 2º de la ley No.7900 de 3 de agosto de 1999)

ARTÍCULO 97.- Préstamo de código y clave de acceso Será sancionado con prisión de seis meses a un año quien, culposamente, permita que su código o clave de acceso, asignados para ingresar a los sistemas de información tributarios, sean utilizados por otra persona.

(Así reformado por el artículo 2º de la ley No.7900 de 3 de agosto de 1999)

e. Ley General de Aduanas[41]

ARTÍCULO 221.- Delitos informáticos

Será reprimido con prisión de uno a tres años quien:

a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas.

b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad.
c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona.
d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente.

ARTICULO 222.- Agravante

La pena será de tres a cinco años cuando, en alguna de las causales del artículo anterior, concurra una de las siguientes

circunstancias:

a) Intervengan en el hecho tres o más personas, en calidad de autoras.

b) Intervenga, en calidad de autor, instigador o cómplice, un funcionario público en ejercicio de sus funciones, con ocasión de ellas o con abuso de su cargo.

f. Administración Financiera de la República y Presupuestos Públicos[42]

ARTÍCULO 111.- Delito informático

Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:

a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.

b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.

c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.

d) Utilizar las facilidades del Sistema para beneficio propio o de terceros.

3. JURISPRUDENCIA

a. Concepto en sentido amplio y distinción entre el fraude informático y el sabotaje informático

“Dos son los aspectos que la recurrente reclama: que se está en presencia de delitos informáticos y que estos concurren materialmente, por lo que no se trata de un delito continuado. A)

Sobre el delito de fraude informático: Esta Sala considera que tal acción no es configurativa de dicho ilícito. La norma citada describe: *"Se impondrá prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema"*. En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal). *"Por una parte, el National Center for computer Crime Data indica que "el delito informático incluye todos los delitos perpetrados por medio del uso de ordenadores y todos los delitos en que se dañe a los ordenadores o a sus componentes". De igual forma, y siempre con ese carácter de generalidad y amplitud, la Organización para la Cooperación y Desarrollo Económico (OCDE) explica que el "delito informático es toda conducta ilegal, no ética o no autorizada, que involucra un proceso automático de datos y/o la transmisión de datos". Asimismo, William Cashion – estadounidense experto en informática – señala que el "delito informático es cualquier acto inicuo que no puede ser cometido sin un ordenador o que no existiría sin un ordenador o su tecnología"* (Delitos informáticos, Carlos Chinchilla Sandí, Farben, 2004, página 27). Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en **influir** en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de **incidir** en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso. El usuario aparece al final de ese proceso, y en términos generales, no lo puede modificar. Para hacerlo, requiere el ingreso al sistema, y usualmente debe poseer ciertos conocimientos. Las personas que cometen delitos

informáticos presentan algunas características que no tiene el común de las personas, como la destreza en el manejo de los sistemas informáticos, o una posición estratégica que le facilita el manejo de información restringida, o, en muchos casos, ambas ventajas. Por estos aspectos son considerados "delitos de cuello blanco". Esto por cuanto, además de la tecnicidad en el manejo de los sistemas, éstos se encuentran protegidos por mecanismos de defensa cuya vulneración requiere, usualmente, de conocimientos técnicos: *"Esta predisposición de medios defensivos en forma general y la limitación que se puso a los delitos electrónicos nos permite inducir en forma clara que para ingresar a cualquier sistema sin la debida autorización (para el caso la simple intrusión resultaría el delito subsidiario de otros más graves como hacking o robo de información, por citar algunos) implica necesariamente vencer una resistencia predispuesta del sistema colocada allí expresamente por razones de seguridad, - según expresan los programadores y constructores -."* (Derecho Penal Informático, Gabriel Cámpoli, Investigaciones Jurídicas S.A., 2003, página 28). Según indica el doctor Chinchilla Sandí, dentro de esas conductas destacan la **manipulación de los datos de entrada:** conocido también como sustracción de datos, es el más común en vista de la facilidad para la comisión y la dificultad en el descubrimiento. No requiere de conocimientos técnicos en informática y puede realizarlo cualquier persona que tenga acceso al procesamiento de datos en su fase de adquisición; **manipulación de programas:** difícil de descubrir pues el sujeto activo ha de tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en introducir nuevos programas o nuevas rutinas. Un método muy usado es el denominado "Caballo de Troya", el cual consiste en implantar instrucciones de computadora en forma subrepticia en un programa informático para que realice una función no autorizada al mismo tiempo que la normal; **manipulación de los datos de salida:** se lleva a cabo fijando un objetivo al funcionamiento del sistema informático, como el fraude a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos, lo que se hacía con tarjetas bancarias robadas. Ahora se usa equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y en las tarjetas de crédito. Como se observa, la conducta implica cierto manejo de los datos, los programas, que incide en el proceso de los datos del sistema. Por su parte, la conducta tenida por acreditada en este caso, es el uso ilegítimo de la tarjeta original, por medio de un ordenador (cajero automático), pero sin modificación ni

alteración de la información que éste contenía, que indujera a error en el procesamiento o el resultado de los datos del sistema, así como el uso en diversos establecimientos, de la tarjeta verdadera, por parte de quienes la habían sustraído, haciéndose pasar la co-imputada, por su titular, lo que hizo incurrir en error a los vendedores, quienes hicieron entrega de los bienes que de esa forma se adquirieron. Por tanto, la conducta tenida por cierta no se adecua al tipo en referencia."[43]

b. Comunidad virtual" que ofrece por medio de internet servicios de índole sexual que involucra a menores

"**V.-** [...]. Con respecto a la utilización de mensajes enviados por medio del correo electrónico, aportados por un particular como elementos de convicción, que proporcionan indicios suficientes para iniciar una investigación penal, debe apuntarse que el acceso al correo electrónico de las personas, al igual que otros medios de comunicación, están amparados por el derecho constitucional a la intimidad (artículo 24 de la Carta Magna). Dicha afirmación cobra mayor relevancia, si se tiene en cuenta el creciente volumen de correspondencia que circula de esa manera y las también progresivas capacidades de los particulares y del Estado, para seguir y controlar el texto o contenido enviado por ese medio. Empero, ello no significa que la tutela de la autodeterminación informativa sea irrestricta, pues en circunstancias excepcionales el titular de los datos puede consentir en que se difundan a terceros. Establecido este principio general, adicionalmente debe tomarse en cuenta, que cuando se ofrece una dirección de correos por Internet, dirigida indiscriminadamente a cualquier persona que desee tener contacto con otras personas, se parte del hecho de que se podrá acceder a ella en cualquier momento, desde cualquier lugar y con cualquier objetivo, incluso aquel para el que originalmente se decidió poner esa dirección en la amplia red mundial denominada Internet. Desde esta última perspectiva, quien haga esto acepta la posibilidad de que a dicha dirección pueden llegar mensajes de cualquier criterio, tema y calidad y por supuesto, correos provenientes de quienes investigan sucesos delictivos. Es el titular de la cuenta electrónica quien decide, caso por caso, si opta por responder o no mensajes de procedencia desconocida y eventualmente, iniciar comunicación con otras personas. Con ello, voluntariamente asume el riesgo de que, por las condiciones de anonimato facilitadas por la citada red, la persona con la que se comunique pueda ser o no, quien dice ser. Al dar inicio al intercambio de opiniones, textos, fotografías, vídeos y otros documentos, igual que como sucede con la correspondencia tradicional, quien los remite puede

representarse como posible que el destinatario no lo reserve, máxime si como sucedió en la especie, las comunicaciones versaban sobre la estructura organizativa de un grupo criminal encaminado a corromper sexualmente a menores de edad y a intercambiar material pornográfico prohibido. En la especie sometida a examen, no existió una imposición indebida de las comunicaciones privadas de parte de los funcionarios encargados de realizar la investigación penal, pues es cierto que la correspondencia electrónica fue agregada a la denuncia, por la persona que había creado la cuenta virtual de correo. Llegado a este punto, conviene tener presente que en el ámbito de la doctrina y la jurisprudencia comparadas, se ha expuesto la denominada **"teoría del riesgo"** como excepción a la regla de los **"frutos del árbol envenenado"**, teoría ésta que como es sabido tiene aplicación, cuando para obtener el material probatorio se violenten derechos fundamentales de forma tan decisiva, que contaminen con la misma invalidez los actos probatorios o procesales derivados de la infracción procesal originaria (regla de exclusión probatoria). Esta teoría del riesgo, que impide considerar como ilícita la prueba obtenida, se fundamenta en que en todas las actividades cotidianas de comunicación entre dos o más personas, quien hace revelaciones extraprocesales y voluntarias ante un particular, respecto a un ilícito o realiza actividades relacionadas con éste, asume el riesgo de que el interlocutor lo delate, de forma que ese conocimiento pueda aprovecharse en las investigaciones originadas o que pueda respaldar. Sí debe aclararse, que carecen de valor probatorio las manifestaciones vertidas por quien conoció los datos, en virtud de habérseles confiado por existir un deber de secreto profesional o en caso de que un funcionario omita cumplir una serie de garantías procesales de rango constitucional, estatuidas a favor de los justiciables (por ejemplo, una confesión policial sin contar con la presencia de abogado defensor, constituiría una prueba ilegítima). La teoría del riesgo se sustenta en el principio genérico de libertad probatoria y en el consentimiento tácito de quien puede prever que sus expresiones sean conocidas por otros, aunque no sean sus destinatarios originales. Es así como se ha afirmado, que: "..."*El Tribunal Supremo español entiende que en esta hipótesis, el derecho a la intimidad es renunciado por el propio ciudadano que exteriorizó sus pensamientos sin coacción. Asimismo, que el derecho no podría prohibir que la exteriorización de propósitos delictivos sea mantenida en reserva por el destinatario de la charla, pues la ley no garantiza el secreto que una persona dice a otra, ya que nada impide que éste revele lo que hablaron, siendo irrelevante la forma en que se documenta ese diálogo..."* (Sentencia 11/5/94, citada por Torres Morato: La prueba ilícita penal. Citado por

Hairabedián, Maximiliano: **Eficacia de la prueba ilícita y sus derivadas en el proceso penal**, Editorial Ad-hoc, Argentina, 2.002, pág. 106-107). Así, si en el caso conocido en esta sede se comprobó que los acusados formaron parte de una "comunidad virtual" interesada en intercambiar información con cualquier persona que accediera a la página o los contactara vía correo electrónico (documentos e imágenes), para realizar actividades relativas a la instrumentalización de menores de edad, como parte de material pornográfico o como meros objetos para satisfacer sexualmente al grupo. Se autodenominaron incluso, como "boys lovers" y en los mensajes de correo electrónico aportados, se identificaron expresamente como "pedófilos". Como parte de sus funciones en la organización no gubernamental (O.N.G.), denominada "Casa Alianza", la funcionaria María del Rocío Rodríguez García localizó una página virtual del grupo identificado como "Comunidad Paidos" [...]. a la que pertenecían los imputados, estableció comunicación con ellos con el exclusivo interés de verificar que estaban implicados en actividades delictivas de contenido sexual, en detrimento de personas menores de edad. Tal como señala el Tribunal, a folio 81 de la sentencia: *"... dado que dentro de esta página, la cual está abierta al público, aparecen todos los requisitos para suscribirse con el fin de intercambiar correspondencia con otros boylovers, la señora Rodríguez, se inscribe, identificándose como Roger Morales, pañameño, residente en Estados Unidos, de 43 años y de profesión Contador, y creó para tal fin, la cuenta de correo electrónico* [...]*..."*. Fue así como recibió un primer mensaje de Cristian Araya Monge, quien se identificó como "boylover" o "pedófilo", quien a partir de ahí le narró quiénes integraban la agrupación, remitiéndole una serie de documentos para que aprendiera: *"... el arte de abusar sexualmente a las personas menores de edad..."*, a la vez que le envió fotografías pornográficas de menores de edad, en donde aparecen adultos abusando sexualmente de niños entre los 3 o 4 años de edad aproximadamente y otras en las que figuran el propio Araya Monge y el menor de edad O.M., segundo apellido ignorado. (ver folio 82). Con esta información en su poder, María del Rocío interpuso la denuncia penal correspondiente y anexó la documentación indicada. Como dijo el Tribunal de instancia entre folios 130 a 134, no existió una intromisión indebida en las comunicaciones de parte de las autoridades, pues quedó demostrado que uno de los partícipes de la comunicación, a saber, la funcionaria Rodríguez García del grupo privado de cita, proporcionó los mensajes que a través del correo electrónico se habían dirigido a la cuenta creada por ella. Como queda expuesto en esta sentencia, los encartados asumieron - bajo su propio riesgo - la posibilidad de ser descubiertos al manifestar sus acciones delictivas. No lleva

razón quien recurre, al argumentar que el proceso penal se impuso de aspectos íntimos de los acusados, pues lo cierto es que al establecer contacto con terceros, aquellos renunciaron a la tutela que ellos mismos podían desplegar en su ámbito de privacidad. Tal como lo ha indicado la jurisprudencia de esta Sala, resulta válido que una persona a quien se dirige una comunicación la aporte al proceso judicial, para que en él se la considere como un elemento de convicción. Así, se ha señalado que:*"... El numeral 29 de la Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones establece en su párrafo segundo lo siguiente: "Cuando el destinatario de una comunicación, mediante la cual se está cometiendo un delito tipificado por la Ley, la registre o la conserve, ésta podrá ser presentada, ante las autoridades judiciales o policiales, para la investigación correspondiente". Como puede apreciarse, se extrae que el "propietario", por decirlo de alguna forma, de una comunicación es quien la recibe. Sobre él pesa la responsabilidad de presentarla como elemento para una investigación. Claro está que si la presenta, se convierte en un elemento probatorio que debe ser discutido y al cual debe dársele el valor que corresponda luego de apreciarlo conforme a las máximas del correcto entendimiento humano. Asimismo, contrario a lo que estima el Tribunal, este derecho de registrar la comunicación que ostenta su destinatario no se restringe a los casos en que se investiguen delitos de Narcotráfico y de Secuestro Extorsivo, que son los mencionados en la Ley 7425. Si en ese párrafo se permite el registro en relación con "un delito tipificado por la Ley" y si la ley mencionada no tipifica delitos, entonces debe entenderse que se refiere a todos los delitos descritos y sancionados (es decir, tipificados) en las leyes penales, sea el Código Penal o cualquiera de las especiales ..."*. (Sentencia número 48-2.001, de 11:00 horas del 12 de enero de 2.001). **(ii) Utilización de agentes encubiertos y grabaciones de vídeo en delitos de índole sexual:** En otro orden de ideas, no existe infracción al debido proceso por utilizar a un agente encubierto para descubrir la forma en que se verificaron las infracciones, por no existir impedimento legal alguno para acudir a esta técnica, máxime cuando resulta útil para esclarecer hechos ejecutados en la clandestinidad, como los que aquí se comprobaron. Luego, si los responsables de la pesquisa determinaron que la reunión ("fiesta") concertada debía realizarse en un apartamento perteneciente a "Casa Alianza", al que llegarían los acusados en compañía del agente encubierto y de menores de edad, con el objeto de filmar los actos que ejecutarían utilizando un equipo de vídeo-grabación del que disponía el oficial encubierto, Jonathan Abarca Segura, debe acotarse que no existe ilegalidad alguna que

reprochar. Cabe recordar, que para el caso no era necesario efectuar un registro previo del domicilio, de manera que se pudiera verificar la no existencia de droga en el sitio - como bien resolvió el sentenciador – quedando demostrado que los acusados fueron quienes llevaron y suministraron las sustancias ilícitas (confrontar folios 131 a 132). Ahora bien, esta forma de perpetuar las comunicaciones mediante su grabación, se conoce como ***"grabación ex-professo"*** o predeterminada, que son: *".... aquellas que se disponen como registro documental periodístico o de investigación, o como mecanismo de prevención y seguridad, o cuando existen, previamente, indicios serios y fundados que permiten sospechar que en un lugar determinado va a ser cometido o se está cometiendo un hecho delictivo, a los efectos de su registro a través de la imagen y de ser posible también de su sonido, para su posterior introducción al proceso penal como medio de acreditación de la plataforma fáctica delictual.(...) Las que derivan de las cámaras ocultas son aquellas que se han provisto de antemano para captar intencionalmente también hechos delictivos, rastros o circunstancias vinculados a él, que pueden ser operadas por particulares (ciudadanos o prensa) o por el propio Estado (fuerzas de seguridad) sin autorización legitimante del órgano judicial, ya sea que la cámara se oculte materialmente en un espacio público del Estado (por ej: en una plaza) o de particulares abierto al público (por ej: restaurant) o en un ámbito privado (morada), o en el cuerpo o efectos del propio cameraman situado en cualquiera de estos lugares...".* (Pascua, Francisco Javier: **Escuchas telefónicas, grabaciones de audio subrepticias y filmaciones**, Ediciones Jurídicas Cuyo, Argentina, 2.002, págs. 141 a 142). En el caso que ahora se resuelve, la actividad de investigación se limitó a registrar la conducta planificada de antemano por los acusados y ejecutada por ellos con pleno dominio del acontecimiento, sin que pueda sostenerse que las autoridades instigaron la comisión del ilícito o que toleraran la lesión de bienes jurídicos de los menores perjudicados. En realidad, la intervención policial, ejecutando la orden de allanamiento previamente dictada y contando con presencia de juez, fiscal y defensores designados al efecto, se efectuó para impedir que los sucesos llegaran a consecuencias dañosas ulteriores. Obsérvese, que la argumentación del impugnante se torna contradictoria, al afirmar que no existió infracción alguna porque los menores – aún desconociéndolo - contaban con respaldo policial, pero a su vez sostiene, que los responsables fueron los funcionarios que consintieron en que se realizara el convivio. Con cualquiera de las dos opciones, lo que se pretende es exonerar de responsabilidad a los encartados. Sin embargo, esa posición carece de mérito, porque fueron los propios implicados

quienes con sus conductas individuales y con planeamiento de grupo, realizaron los hechos reprochados en el fallo de mérito, sin que en ningún momento se les indujera a cometerlos. Bajo esta tesitura, tampoco existe irrespeto alguno a las garantías de los menores relacionados ("interés superior del niño"), ya que la acción policial se encaminó a documentar en vídeo lo que acontecía, cuidando evidentemente que no se ejecutaran actos contrarios a la voluntad de los menores asistentes al evento."[44]

FUENTES CITADAS

[1] Ley de Derechos de Autor y Derechos Conexos. Ley N° 6683. Costa Rica, 14 de octubre de 1982.

[2] Ley de Procedimientos de Observancia de Derechos de Propiedad Intelectual. Ley N° 8039. Costa Rica, 12 de Octubre de 2000.

[3] Código de Normas y Procedimientos Tributarios (Código Tributario) Ley N° 4755. Costa Rica, 03 de mayo de 1971.

[4] Ley General de Aduanas Ley N° 7557. Costa Rica, 20 de octubre de 1995.

[5] Administración Financiera de la República y Presupuestos Públicos. Ley N° 8131. Costa Rica, 18 de setiembre de 2001.

[6] CHINCHILLA Sandí, Carlos. Delitos Informáticos. 1ª ed. San José, C.R.: IJSA, 2002. p. 26. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 343.2 Ch539d).

[7] NUÑEZ Ponce, Julio. Los delitos informáticos. Revista de Derecho Informático. [en línea]. Octubre 1999, N° 015. [fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=343
ISSN: 1681-5726

[8] GUTIÉRREZ Francés citado por CHINCHILLA Sandí, Carlos. Delitos Informáticos. 1ª ed. San José, C.R.: IJSA, 2002. pp. 32 a 34. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 343.2 Ch539d).

[9] CHINCHILLA Sandí, Carlos. Delitos Informáticos. 1ª ed. San José, C.R.: IJSA, 2002. pp. 35-36. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 343.2 Ch539d).

[10] SOTO Campos, José Galileo. Delitos Informáticos.. MailxMail.com. [en línea]. 29 de Agosto, 2004. {fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo6.htm

[11] Hacking y Cracking. [en línea]. 2002-2005. [fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.delitosinformaticos.com.mx/hacking.htm

[12] Hacking y Cracking. [en línea]. 2002-2005. [fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.delitosinformaticos.com.mx/hacking.htm

[13] Phreaking (Hacking o Cracking Telefónico). [en línea]. 2002-2005. [fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.delitosinformaticos.com.mx/phreaking.htm

[14] CiberTerrorismo y Activismo. [en línea]. 2002-2005. [fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.delitosinformaticos.com.mx/ciberterrorismo.htm

[15] CiberTerrorismo y Activismo. [en línea]. 2002-2005. [fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.delitosinformaticos.com.mx/ciberterrorismo.htm

[16] CiberAcoso (CyberStalking). [en línea]. 2002-2005. [fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.delitosinformaticos.com.mx/ciberacoso.htm

[17] NUÑEZ Ponce, Julio. Los delitos informáticos. Revista de Derecho Informático. [en línea]. Octubre 1999, N° 015. [fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=343
ISSN: 1681-5726

[18] SALAS Arroyo, Jessica Paola y SÁNCHEZ Delgado, José Daniel. Algunas figuras delictivas en Internet. Tesis de grado para optar por el grado de Licenciadas en Derecho. San José: Universidad de Costa Rica, 1999. pp. 151-152. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 3550).

[19] SOTO Campos, José Galileo. Delitos Informáticos. MailxMail.com. [en línea]. 29 de Agosto, 2004. {fecha de consulta: 4 de agosto de 2006]. Disponible en: http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo15

.htm

[20] SALAS Arroyo, Jessica Paola y SÁNCHEZ Delgado, José Daniel. Algunas figuras delictivas en Internet. Tesis de grado para optar por el grado de Licenciadas en Derecho. San José: Universidad de Costa Rica, 1999. pp. 176 y 182. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 3550).

[21] SIEBER y VIEGA citados por CHINCHILLA Sandí, Carlos. Delitos Informáticos. 1ª ed. San José, C.R.: IJSA, 2002. p. 26. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 343.2 Ch539d).

[22] SALAZAR Rodríguez, Alonso. Delito Informático (análisis comparativo con el delito de daños y otros tipos del Código Penal Costarricense). Revista Judicial. N° 79, junio 2001. p. 120. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 340 R).

[23] SALAZAR Rodríguez, Alonso. Delito Informático (análisis comparativo con el delito de daños y otros tipos del Código Penal Costarricense). Revista Judicial. N° 79, junio 2001. p. 121. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 340 R).

[24] CHINCHILLA Sandí, Carlos. Delitos Informáticos. 1ª ed. San José, C.R.: IJSA, 2002. pp. 42-43. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 343.2 Ch539d).

[25] SALAZAR Rodríguez, Alonso. Delito Informático (análisis comparativo con el delito de daños y otros tipos del Código Penal Costarricense). Revista Judicial. N° 79, junio 2001. p. 120. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 340 R).

[26] CHINCHILLA Sandí, Carlos. Delitos Informáticos. 1ª ed. San José, C.R.: IJSA, 2002. p. 44. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 343.2 Ch539d).

[27] SALAZAR Rodríguez, Alonso. Delito Informático (análisis comparativo con el delito de daños y otros tipos del Código Penal Costarricense). Revista Judicial. N° 79, junio 2001. p. 121. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 340 R).

[28] CHINCHILLA Sandí, Carlos. Delitos Informáticos. 1ª ed. San José, C.R.: IJSA, 2002. p. 45. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 343.2 Ch539d).

[29] SALAS Arroyo, Jessica Paola y SÁNCHEZ Delgado, José Daniel. Algunas figuras delictivas en Internet. Tesis de grado para optar por el grado de Licenciadas en Derecho. San José: Universidad de Costa Rica, 1999. pp. 202-203. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 3550).

[30] SALAS Arroyo, Jessica Paola y SÁNCHEZ Delgado, José Daniel. Algunas figuras delictivas en Internet. Tesis de grado para optar por el grado de Licenciadas en Derecho. San José: Universidad de Costa Rica, 1999. pp. 240, 241 y 246-247. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 3550).

[31] SALAZAR Rodríguez, Alonso. Delito Informático (análisis comparativo con el delito de daños y otros tipos del Código Penal Costarricense). Revista Judicial. N° 79, junio 2001. p. 123. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 340 R).

[32] SALAZAR Rodríguez, Alonso. Delito Informático (análisis comparativo con el delito de daños y otros tipos del Código Penal Costarricense). Revista Judicial. N° 79, junio 2001. pp. 121-122. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 340 R).

[33] SALAS Arroyo, Jessica Paola y SÁNCHEZ Delgado, José Daniel. Algunas figuras delictivas en Internet. Tesis de grado para optar por el grado de Licenciadas en Derecho. San José: Universidad de Costa Rica, 1999. pp. 356-357 y 364. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 3550).

[34] SALAZAR Rodríguez, Alonso. Delito Informático (análisis comparativo con el delito de daños y otros tipos del Código Penal Costarricense). Revista Judicial. N° 79, junio 2001. p. 124. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 340 R).

[35] NOUGRERES, VIEGA [ET AL] citados por CHINCHILLA Sandí, Carlos. Delitos Informáticos. 1ª ed. San José, C.R.: IJSA, 2002. pp. 57 a 59. (Localizado en la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica, signatura 343.2 Ch539d).

[36] VIEGA Rodríguez, María José. Un nuevo desafío jurídico: Los Delitos Informáticos. [en línea]. {fecha de consulta: 4 de agosto de 2006]. Disponible en: **http://www.viegasociados.com/publicac/DelitosInformaticos.pdf**

[37] Código Penal. Ley N° 4573. Costa Rica, 4 de abril de 1970.

[38] Ley de Derechos de Autor y Derechos Conexos. Ley N° 6683. Costa Rica, 14 de octubre de 1982.

[39] Ley de Procedimientos de Observancia de Derechos de Propiedad Intelectual. Ley N° 8039. Costa Rica, 12 de Octubre de 2000.

[40] Código de Normas y Procedimientos Tributarios (Código Tributario) Ley N° 4755. Costa Rica, 03 de mayo de 1971.

[41] Ley General de Aduanas Ley N° 7557. Costa Rica, 20 de octubre de 1995.

[42] Administración Financiera de la República y Presupuestos Públicos. Ley N° 8131. Costa Rica, 18 de setiembre de 2001.

[43] SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. Resolución N° 2006-00148 de las nueve horas del veinticuatro de febrero de dos mil seis.

[44] SALA TERCERA DE LA CORTE SUPREMA DE JUSTICIA. Resolución N° 2003-00457 de las quince horas con veinte minutos del cinco de junio del año dos mil tres.