Cuestiones Jurídicas
Revista de Ciencias Jurídicas
de la Universidad Rafael Urdaneta
Vol. V N° 1 (Enero - Junio 2011)
ISSN 1856-6073

Tres tipos penales informáticos *

Michelle Azuaje Pirela**
Salvador Leal Wilhelm ***

Resumen

El incremento en el uso de Internet ha traído consigo nuevos delitos, que utilizan como medio o se cometen en contra de sistemas de información. Se examinan tres tipos penales contenidos en la Ley especial venezolana contra los delitos informáticos; el acceso indebido, el sabotaje o daño a sistemas y la exhibición de material pornográfico. Partiendo de una concepción analítica y recurriendo al método comparatista se toman como referencia algunos tipos tradicionales consagrados para analizar la tipificación de estos delitos, con la finalidad, de distinguir los delitos tradicionales de esta nueva clase de delitos que para su consumación utilizan medios informáticos ya sea por ser medio o por ser el objeto de ataque, la tipificación de estos delitos permite mayor protección a los usuarios de las tecnologías de la información, e impulsar su uso.

*Palabras Clave***:** acceso indebido, sabotaje, tecnologías de información, material pornográfico.

* Recibido: 10/03/2011 Aceptado: 28/06/2011

** Abogada. Máster en Derecho de la Empresa, Universidad de Alcalá. España.

*** Abogado. Profesor de Derecho Constitucional y de Procedimientos Contencioso Administrativos de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia. Doctor en Derecho**.**

**** Abreviaturas Utilizadas: CRBV: Constitución de la República Bolivariana de Venezuela. CP: Código Penal. LECDI: Ley especial contra delitos informáticos. Las traducciones son todas de los autores.

Three computer crimes standards

Abstract

The increase in Internet use has brought new crimes, those that use as means or are committed against information systems. Next, three types of crimes contained the Special Venezuelan Law against computer crimes were examined: The illegal access, the sabotage or damage to systems; and the exhibition or diffusion of pornographic material. Using an analytical conception and resorting to the comparative method, some type of traditional crimes directed to analyze crimes are taken as a reference, with the purpose of identifying them with consecrated traditional types and to distinguish them from the new type of felonies committed with computers, the classification of these crimes allow a better protection to computer systems users and to motivate or promote its use.

Key words: illegal access, sabotage, information systems, pornographic material

Introducción

En el mes de febrero del año 2000 los usuarios de sitios como Amazon, Hotmail, Yahoo o CNN se consiguieron con un mensaje de página no disponible. Los sitios eran víctimas de un ataque de denegación de servicio (DoS)[1] (Abreu, 2001) resultado de miles de solicitudes enviadas por computadoras "zombis" capturadas por un *hacker*[2], inundaron los servidores impidiendo a los legítimos usuarios el acceso.

Todos los días se reciben en cuentas de *email* mensajes de bancos pidiendo actualizar información o comunicando que la persona ganó la lotería, es lo que se conoce como "*phishing"* es una forma de obtener datos sobre cuentas bancarias o tarjetas de crédito, el nombre "*phishing*" viene de la semejanza con la pesca, se lanza una red, millones de personas reciben el *email* y alguna caerá. Un par de bancos venezolanos han sido víctimas de este tipo de ataque. (Asociación de Internautas, 2007)

---

[1] DoS: un *ataque de denegación de servicio*, también llamado ataque *DoS* (de las siglas en inglés *Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos." (Wikipedia,2011)

[2] Hacker: persona que se dedica a la entrada ilegal en sistemas informáticos

Si se introduce la palabra *sex* en G*oogle,* se obtienen 737 millones de páginas en español y 739 millones en inglés, los primeros veinte resultados incluyen una noticia sobre matrimonios entre personas del mismo sexo, la página de Wikipedia junto a tres *links* hacia pornografía. Al usar el filtro de contenidos se obtienen 491 millones en inglés y el mismo número en español, esta vez incluye links a páginas con videos de *Hollywood,* la página de Wikipedia sobre el tema, los *Sex Pistols*, etc. El sesenta por ciento (60%) de las páginas son consideradas seguras, es decir, no incluyen contenidos sexuales explícitos ni textuales ni imágenes, pero, eso no impide que se considere a toda la *World Wide Web* como un lugar de solo sexo. Obviando que a diferencia de las revistas en los quioscos, las películas en el cable o en la televisión abierta, en la WWW, no lo conseguirá si no lo está buscando.

En el mundo virtual, el delito es real, pero así como la Internet facilita el delito, también lo hace más visible pues siempre quedan huellas que permiten la persecución, pero los problemas de jurisdicción la dificultan. Ante esto, los Estados reaccionan con nuevas leyes ante los "nuevos" delitos pero estos no son tales, en su mayoría son delitos tradicionales con nuevos métodos. Una estafa es una estafa, sin importar si se usa un boleto de lotería en papel o un *email* con los números ganadores, de la misma manera que un robo es un robo con un puñal o con una pistola.

En este artículo, partiendo de la concepción analítica del delito se estudiarán tres tipos delictivos: uno propiamente informático, uno tradicional pero cometido sobre computadoras y con consecuencias mucho más graves y uno contra la moralidad. Para esto se recurrirá al método comparatista. Se tomarán como referencias los modelos de Estados Unidos, con la ley especial más antigua y que ha generado más jurisprudencia: Italia cuyo Código de 1889, derogado en 1930, fue el modelo del Código Penal venezolano, lo que significa que la ley sobre el tema responde a una filosofía semejante a la venezolana y finalmente la convención de Bucarest, la ley internacional sobre el tema.

1. Acceso Indebido

El Artículo 6 de la Ley Especial Contra los Delitos Informáticos (LECDI) establece:

> **"**Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que

> utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias".

Este es uno de los pocos sino el único delito informático sin paralelo en el derecho penal tradicional. Si bien en el Código Penal Italiano (Pecorella, 2005: 307), se le iguala a la violación de domicilio (Art. 183 y 184 del Código Penal venezolano), posición que requiere forzar en exceso el concepto de domicilio.

La norma venezolana al igual que la italiana castiga el solo hecho de acceder indebidamente, sin importar que se obtenga información o se tenga a la vista, tal como en principio exige la norma equiparable en los Estados Unidos (Kerr, 2006: 29). La Convención de Bucarest sobre el ciberdelito del Consejo de Europa, también exige castigar el acceso indebido *per se* sin exigir otro condicionante (Council of Europe, 2001a). Si bien se teme la posibilidad de sobre-criminalizar, pues se estaría castigando la tentativa con la pena plena, (Deutscher Bundestag Cit. en Pecorella, 2005: 306) la norma debe ser amplia para incluir la mayoría de los accesos violatorios que son motivados por la vanidad, que son sólo muestras de poder hacerlo.

1.1. El Acceso

El Diccionario de la Real Academia de la Lengua Española (Real Academia Española, 2001) define acceso como: acceso.

(Del lat. *accessus*).

1. m. Acción de llegar o acercarse.

3. m. Entrada o paso.

4. m. Entrada al trato o comunicación con alguien

Obviamente, quien "accede" a una computadora no entra en ella, "acercarse" físicamente a ella no puede considerarse entrar en ella, sólo el cuarto significado se corresponde con el acceso a sistemas informáticos, es comunicarse con ella, en definitiva, el usar una computadora (Kerr, 2003). En el texto explicativo de la Convención de Bucarest se consideró acceso el "ingreso" en un sistema excluyendo el envío de *email* o archivos a otra computadora (Council Of Europe, 2001b), esto último excluiría el envío de virus a otras computadoras.

La Ley incluye como acciones punibles el uso del sistema por lo que acceso debería ser entendido como interacción exitosa con una computadora (Kerr, 2006: 42), entendiéndose como uso: "el envío de un comando

pidiendo información en respuesta y la computadora responde enviando información de vuelta al usuario". (Kerr, 2006: 42)

La LECDI agrega interceptar e interferir, lo cual crea un concurso ideal con el artículo 21 de violación de la privacidad y el artículo 7 que castiga el sabotaje de sistemas que en la Convención de Bucarest, esas conductas se corresponden con los delitos de intercepción ilegal que se corresponde a su vez con sabotaje y con espionaje (Council Of Europe, 2001b: 12) o con la violación de la correspondencia.

El acceso puede ser hecho con cualquier medio, sea a través de Internet, sea situándose frente a la computadora y tecleando, el *login* y el *password* (Pecorella, 2005: 308), lo importante es que el acceso sea sin autorización o excediendo la autorización concedida. Uno de los casos más comunes es el *hacking*, técnica que permite la entrada a un sistema informático sin la correspondiente autorización de su propietario, caso en el que la doctrina enfatiza, se trata de un acceso no autorizado pero, sin fines nocivos (Rico, 2006: 62), siguiendo la romántica visión creada por los medios de comunicación, que en una clara apología del delito ha idealizado al intruso.

1.1.1 Sin autorización o excediéndola

Las normas que otorgan autorización son de tres tipos: código, contractuales y sociales (Kerr, 2006: 42) y si al margen de esas normas, por ejemplo, si se utiliza un programa, un caballo de Troya para obtener el *password* o si se obtiene a través de *phishing,* el *password* el equivalente de una llave falsa se trata de un acceso prohibido por el código programado.

Cuando se contrata con un proveedor de Internet, se suscriben ciertas cláusulas sobre la forma de acceder, asimismo los usos sociales también pueden impedir o permitir el acceso. Al menos en Venezuela nadie criticaría a un padre preocupado que revise la computadora de un niño para saber que hace en la WWW.

1.1.2. Excediendo la autorización que se hubiere obtenido

Un empleador autoriza el uso de una computadora a sus empleados y alguno la utiliza para leer su *email* personal, otro para chatear en *Messenger* y otro para actualizar su *Facebook*, o bajar canciones de un sitio de intercambio ¿Son hechos punibles penalmente? La doctrina extranjera ha dado una respuesta negativa (Pecorella, 2005: 346) el sistema penal es una medida de *extrema ratio* no puede ser utilizado como medio de garantizar

obligaciones laborales. Siendo distinto el caso cuando se trata de funcionarios públicos y el acceso es a información sensible como más adelante se verá (Lloyd, 2000: 235). La norma del USCode una de las pocas que utiliza la distinción que la LECDI hace, lo define como "el acceso a un computador con autorización y usar ese acceso para obtener o alterar información que el accedente no tiene derecho a obtener". (Computer Crime And Intellectual Property Section – Ccips- Of The United States Deparment Of Justice, 2007). Y en la discusión de la Ley de los Estados Unidos se dejó claro que el acceso excediendo la autorización sólo sería penado si se hubiera causado un daño (Computer Crime And Intellectual Property Section – Ccips- Of The United States Deparment Of Justice, 2007), precisión que la Ley venezolana no hace.

1.1.3. Acceso a un sistema que utilice tecnologías de información

La LECDI, define como sistema:

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

Y como tecnología de información:

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

La definición es extremadamente amplia por lo que incluye sin distinción computadoras de escritorio, *laptops,* PDAs (*personal digital assistant*), un *I-Phone* por su capacidad para enviar *emails* y manejar archivos, una intranet, la Internet, etc. pero también un *I- Pod,* el *GPS* de un vehículo y hasta un equipo de video juego son sistemas que utilizan tecnología de información. En el caso de una página *web* el acceso es al *host*[1]*,* la computadora que la

[1] Host: servidor. Computadora en las que se almacenan las páginas web . y las pone a disposición de los usuarios.

almacena no a la página, si bien como en ese caso, la amplísima definición de la LECDI la incluiría.

1.1.4. Acceso a sistemas protegidos

El artículo 9 establece una calificante del delito que se hace aplicable cuando

> " (…) los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas."

La norma tiene antecedente en el USCode 1030 que establece el castigo para quien obtenga información que por "ley o reglamento" exija protección contra revelación no autorizada por razones de defensa nacional o relaciones internacionales.

Una segunda norma del USCode menciona las computadoras protegidas para referirse a las computadoras del gobierno o de instituciones financieras, en definitiva, es un "término técnico legal" que no tiene nada que ver con la seguridad de un computador (Computer Crime And Intellectual Property Section – Ccips- Of The United States Deparment Of Justice, 2007). Éste es el significado también en Venezuela, como lo confirma la continuación de la norma que a similitud del Código Penal italiano que califica el delito cuando la información está afectada a un uso de interés público (Pecorella, 2005: 347)

Entonces, se trataría de acceso a aquellos sistemas que utilicen o almacenen información que requiere protección especial por contener información cuya divulgación afectaría la seguridad y defensa, el funcionamiento del Estado o los derechos de personas y empresas. La Constitución venezolana (Arts. 143 y 326) da potestad al Estado para declarar la confidencialidad de aquella información que afecte la seguridad y defensa. Asimismo, el artículo 143 *ejusdem* prohíbe el acceso a archivos y registros que contengan informaciones sensibles, cuya divulgación violaría el derecho a la intimidad (Art. 60 CRBV) así como ordena regular el uso de la informática para garantizarla, es lo que se conoce como derecho a la autodeterminación informativa, extendiendo ésta a la información patrimonial que frente al Estado, no frente a terceros, no está protegida por la intimidad y la perteneciente a las personas jurídicas cuya información goza de protección sobre la base del derecho de propiedad y no de la intimidad.

A todo esto agrega la información de uso del Estado que no es ni confidencial ni reservada (Art. 143 CRBV), autoriza el acceso a ella por vías regulares, sino en razón de la necesidad de garantizar la eficiencia de la Administración (Art. 141 CRBV).

1.2 Culpabilidad

El acto se castiga sólo en caso de dolo, dado que no hay referencia a la culpa y al ser el castigo de la culpa excepcional debería hacerse referencia expresa a ella. Debe probarse que el imputado sabía que no tenía autorización de acceder o que ésta era insuficiente. La consumación del delito no exige que se adquiera información ni siquiera que se la vea, sólo que se entre al sistema (Computer Crime And Intellectual Property Section (CCIPS) Of The United States Department Of Justice, 2007); es un delito de peligro (Pecorella, 2006: 350), el cual supone su consumación con la mera puesta en peligro del bien jurídico tutelado. Si se obtiene información con el fin de obtener beneficios económicos, se configura el delito de hurto (Art. 13 LECDI), pero si se compromete la confidencialidad de los datos es de espionaje informático, tipificado en el Art. 11 LECDI o los varios tipos de delitos de violación de la privacidad (Art. 20 al 23).

Una pregunta que podría hacerse y no es hipotética, es si se accede sin derecho a la computadora de un delincuente o si se hace para fines académicos legítimos, ¿sigue siendo delito? Un estudio sobre la efectividad del *spam* [1]se basó en información obtenida ingresando ilegalmente en una red de *spam*, "secuestrándola" y enviando *spam* falso (BBC News, 2008).

1.3. Pena

Las penas son de uno a cinco años para el tipo simple y ésta se aumenta de una tercera parte a la mitad en el caso calificado. Se impondrá además un multa de 10 a 50 unidades tributarias.

2.- Sabotaje o daño a sistemas

El artículo 7 LECDI establece lo siguiente:

> "Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los compo-

[1] Spam: correo no solicitado, enviado de forma masiva que contiene normalmente publicidad engañosa.

> nentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo".

Este delito, en principio, no es sino una forma del delito de daños castigado por el artículo 473 del Código Penal venezolano que castiga lo que tradicionalmente se ha considerado un delito menor, pues, sus actores no buscan beneficio material sino sólo causar daño (Mendoza, 1980:595) castigando lo que comúnmente se conoce como vandalismo. El Código Penal además dedica un título completo a regular el castigo de aquellos daños que exponen a las personas o cosas a graves peligros, (Mendoza, 1965: 319) que tienen carácter catastrófico. La norma sobre el daño menor ciertamente es aplicable a la destrucción física de la computadora, al *hardware,* pero por lo general ese no es el tipo de daño que se inflige o exige o se busca infligir. Lo que es común es que se busque inhabilitar las funciones del computador o forzarla a que realice una actividad distinta de aquella que su dueño desea que realice, lo que se ataca es el *software* "el componente técnico del sistema" (Pecorella, 2006: 168) haciendo inaplicable la norma de daño genérico o mínimo.

Por otra parte, si bien el daño puede limitarse a una computadora aislada, lo cual por muy grave que sea, especialmente si no se posee respaldo de la información, palidece ante la magnitud de los ataques que a través de Internet puede afectar no a miles sino a millones de computadores. Tales como los ataques distribuidos de denegación de servicio (DDOS) que se dirigen contra redes enteras, que son de tal magnitud que han sido empleados como arma de guerra (Markoff, 2008) haciendo necesaria una nueva tipificación, que se ajuste la norma al nuevo objeto de delito a la magnitud del daño.

2.1. El que destruya, dañe o modifique cualquier acto que altere el funcionamiento o inutilice un sistema o uno de sus componentes

La norma sigue casi al pie de la letra, a la norma italiana que es la única en el mundo aparte de la venezolana que contempla el daño al *hardware*, lo que ya castiga el Código Penal en su artículo 473. Por lo que, el destruir y

dañar deben entenderse en primer lugar como daño físico a la computadora o sus componentes, lo que abarcaría tanto los internos como discos duros, tarjeta madre, memoria como aquellos exteriores a ella tales como el modem o cualquier otro periférico. Igualmente, en caso de una red incluiría los equipos de interconexión como ruteadores que permiten la conexión entre las computadoras, incluso un *pen drive* estaría protegido por la norma dado que para funcionar usa un software interno. No es necesaria su destrucción total, bastan actos que impidan su normal funcionamiento sin llegar a su destrucción, como por ejemplo, desconectar las partes internas (Pecorella, 2006: 194)

El hardware puede ser inutilizado por medio de programas tales como los *bots*, estos son programas que realizan tareas para quien los introduce en la computadora, convirtiendo la máquina en un *zombi* (Symantec, 2008a). Pueden ser utilizados incluso en una serie de computadoras, se le llama entonces un *botnet*[1] que puede por ejemplo, enviar *spam*, correo basura, o realizar un ataque distribuido de denegación de servicio, DDOS (Markoff, 2008) sin que el dueño lo sepa, reduciendo su capacidad de computo (Wilson, 2008) incluso llevar la computadora a navegar por su cuenta por Internet, bajando archivos ilegales (Romm, 2008) utilizando capacidad de procesamiento y ancho de banda que dificultan el uso de la computadora. Normalmente, para instalarlos se utiliza un caballo de Troya, un programa que a diferencia de un virus no se auto reproduce y que luego baja programas como *bots*. (Koerner, 2003)

En materia de daños genéricos, el bien tiene que ser ajeno, pero la norma venezolana de la LECDI, a diferencia de la italiana no lo dice. Si el dueño de un servidor de Internet "una computadora que provee, uno o más servicios en una red de computadoras, típicamente a través de una rutina de pedido-respuesta" (Wikipedia, 2008) la daña haciendo inaccesibles las páginas web de terceros, sería punible.

2.2. Daño, destrucción, modificación de los datos y la información

Lo primero que debe notarse es que los programas no aparecen mencionados por lo que sólo podría entenderse incluidos en componentes del sistema con grave riesgo de la seguridad jurídica. El daño a la información

[1] *Botnet*: programa malicioso que convierte la computadora en una especia de robot que ejecuta instrucciones provistas por un tercero distinto del usuario autorizado

en cambio, está erróneamente incluido porque "la información no es una cosa, sino un proceso o una relación entre la mente de una persona y cualquier estímulo." (Piragoff Cit. En Pecorella, 2005: 202)

La data en cambio, si es susceptible de ser objeto del delito, cuando se trata de data, la destrucción será el borrado, supresión. La modificación se causará cuando se comprometa la integridad: "La confiabilidad de la data… y es usualmente descrita como la prevención de cambios impropia o sin autorización. La integridad incluye, integridad de la data…y de la metadata[1] o integridad de origen[2]". (Bishoff Cit. En Kerr, 2006: 86)

El daño ocurrirá cuando sin llegar a suprimirla, se hace inutilizable por estar comprometida su integridad y la información ya no es accesible, tales como los ataques de denegación de servicio que inundan la computadora de peticiones impidiéndole que provea la data a quien tiene derecho a ella.

2.3. Agravante

Cuando el sabotaje se haga a través de un virus o programa análogo se aumentará la pena. Un virus es un programa que se introduce dentro de otro programa y luego se auto replica (Koerner, 2003), usualmente se transmite usando un caballo de Troya. Los gusanos, a diferencia del virus, son programas que no necesitan un receptor para reproducirse (Koerner, 2003).

2.4. Culpabilidad

El delito se castiga a título doloso o culposo. Es necesario entonces, probar la intención de dañar bien el sistema, bien la data. El delito culposo es castigado por el artículo 8, siendo de los supuestos de culpa, la negligencia es la hipótesis más común, así cuando la persona se conecta a Internet sin un antivirus o sin actualizarlo, corre el riesgo de que su computadora se convierta en el difusor del virus, si la copia del antivirus es ilegal, "pirata" en el lenguaje coloquial, estaríamos en presencia de una negligencia grave, pues un programa ilegalmente utilizado no es actualizable y por lo tanto no estará en capacidad de detectar nuevas amenazas.

---

[1] Metadata:"Encabezamientos, documentos adjuntos, fecha y hora, nombre de dominio, metadatos en el sistema de archivos puede proveer información sobre tamaño y versión de los archivos…. Y los documentos creados por programas populares como… pueden revelar información sobre cambios, borrados y número de revisiones"(EDRM PROJECT TEAM ,2010)

[2] Integridad de origen: certeza sobre la autoría y la no modificación de la información

La imprudencia, el actuar sin tomar en cuenta las consecuencias, es ejemplificada por el histórico caso Morris de los EE UU. Morris un estudiante del Phd en Cornell, programó el gusano "Internet" para demostrar la vulnerabilidad del sistema de la Universidad. El gusano estaba supuesto a desaparecer al apagar la computadora pero el gusano se reprodujo a una velocidad muy superior a la que él estimó, dañando computadoras a lo ancho y largo de E.E.U.U. si bien dado que en aquel entonces sólo las Universidades y el Pentágono estaban en la red no se produjo un daño aun mayor (Kerr, 2006: 42).

El segundo supuesto, la impericia, en este caso crea el riesgo de una sobre-criminalización puesto que hay centenares de millones de usuarios de Internet y la mayoría no son expertos y están expuestos a causar daños sin tener idea de que lo están haciendo.

2.5. Pena

Como se ha dicho, conforme al artículo 7 LECDI la pena será de prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias, en los casos de daño, destrucción, modificación o alteración de sistemas o sus componentes y de inutilización de la data o información. Por otra parte, la pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados, se realizan mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo. Finalmente, si se trata del tipo culposo la sanción se reducirá entre la mitad y dos tercios (Art. 8 LECDI).

3. Difusión o exhibición de material pornográfico

En ventas de periódicos, en los periódicos, en las revistas dominicales, al hacer *zapping*[1] en el cable o en la televisión de señal abierta pueden verse imágenes de contenido sexual pero en el caso de la televisión de señal abierta por su carácter invasivo se ha justificado la censura (Corte Suprema De Justicia Cit. En Brewer-Carías, Ortíz-Álvarez, 2007: 604) .En EE UU, en la sentencia FCC vs Pacifica Foundation, la Corte Suprema de Justicia consideró que la "televisión se introduce en la privacidad del hogar y es imposible evitarlo." (U.S. Supreme Court, 1978).Ese criterio fue

[1] Zapping: el cambiar de un canal a otro con el control remoto sin fijarse en un programa específico

asumido por la entonces Corte Suprema de Justicia en el caso "RCTV- La Escuelita":

> "(…)en cuanto a los medios de radiodifusión, instrumentos poderosísimos de influjo en la opinión pública y cuyo mensaje llega al público aun sin proponerse oírlo, si resulta admisible en un estado democrático que puedan establecerse monopolios estatales precisamente para custodiar la libertad de pensamiento. (Corte Suprema De Justicia Cit En Brewer-Carías, Ortíz-Álvarez, 2007: 604) "

Pero, ese no es el caso de la WWW, en ella no se consigue sino lo que se busca, y aun así eso es difícil, de allí que los buscadores sean una de las más exitosas empresas de la Internet, no obstante, se ha desarrollado un celo, una paranoia sobre el sexo en la WWW, alimentado por el ludismo y por los intentos de los MSM, los medios tradicionales, de detener el avance de la WWW. Esta ha hecho caer la circulación de los MSM, y los ha hecho perder credibilidad y sobre todo influencia y en su intento por defender el negocio, falsifican la realidad con noticias que buscan crear pánico en la opinión pública. En 1995, mucho antes de que la WWW se convirtiera en una amenaza, la revista Time se hizo eco de un estudio falso sobre la pornografía a la que estaban expuestos los niños, el estudio se basaba en el uso de una BBS, un tablero electrónico de los tiempos previos a la WWW, por estudiantes de una Universidad (Godwin, 2003: 259).

A partir de allí, se iniciaron los intentos, fallidos en los EE UU, de regular el acceso de niños a la WWW, obviamente, si se hace en nombre de los niños, nadie se opondrá. El resultado, el uso de filtros que se justifican con la protección de la niñez pero se termina incluyendo temas no relacionados como la pretensión de censurar los sitios que defienden ideas polémicas o las opiniones políticas de oposición (Funnel, 2008).

3.1. El tipo

El artículo 23 LECDI establece:

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

Esta norma, actualiza el medio de comunicación y aumenta la pena del delito castigado por el Art. 382 del Código Penal, si bien, limitando

su alcance, pues el 382 castiga el delito incluso si se dirige la actividad a personas adultas, mientras, la LECDI sólo castiga si se trata de niños y adolescentes. Las acciones incluyen exhibirlos, exponerlos a la vista de niños y adolescentes, así cuando las imágenes sean visibles en una página web; difundirlos, distribuirlos bien a través del *email*, bien a través de sitios de *file sharing*[1] o redes *peer to peer*[2], sitios que permiten el intercambio de archivos, o bien ponerlos a disposición para bajarlos a una página *web* aunque no sean visibles o las imágenes de muestra están censuradas si el archivo a bajar no lo está. Igualmente transmitirlos, permite castigar el sólo hecho de enviarlas a través de la red aun si no llegan a ser vistas solo con ser puestas a disposición de la persona. En la interpretación de la norma equivalente del Código Penal que castiga no la venta sino la oferta en venta, se ha defendido la precisión de que debe ser una venta masiva. (Mendoza, 1965: 279) pero no es el caso aquí, pues la norma no menciona el extremo.

3.1.1. Material Pornográfico o reservado a personas adultas

En el caso RCTV- La Juventud, la entonces Corte Suprema de Justicia tuvo oportunidad de pronunciarse sobre qué debe entenderse por ofensas a la moral pública en el contexto de la regulación de la televisión y se precisó qué imágenes se corresponderían con lo que debe entenderse por pornografía a la que considera "torpe, despreciable y repudiable" y después de señalar que la moral pública es un concepto jurídico indeterminado, especifica que la determinación de la regla depende de la concepción que se tenga en cada tiempo y cada cultura. Y se destaca que un desnudo per se no constituye pornografía, y esto ocurrió en 1982, inclusive se considera "signo de evolución cultural "el que se acepte el desnudo en el arte, la ciencia, en los medios de comunicación bien como entretenimiento, bien como información. De hecho, en el caso particular la transmisión fue en horas de la tarde en un programa dirigido a jóvenes. (Corte Suprema De Justicia Cit. En Brewer-Carías, Ortíz-Álvarez, 2007: 596). Lo que es pornografía y ofende a la moral pública debe establecerse de acuerdo con el estándar vigente en la colectividad, se trata de un concepto jurídico indeterminado

---

[1] File sharing: intercambio de archivos. Puede realizarse descargando archivos desde páginas web dedicadas a ello como la famosa Napster o directamente entre computadoras o peer to peer.

[2] Peer to peer: red de computadoras que permite el intercambio de archivos entre computadoras de manera directa (Wikipedia, 2011b)

de allí que se l excluye los simples desnudos, pero, ¿qué es pornografía? En los EE UU, donde la respuesta se da de acuerdo con el estándar vigente en la comunidad, tal como estableció en Venezuela la Corte Suprema de Justicia se considera tal:

a) La exhibición evidentemente ofensiva o descripción de las relaciones sexuales, normales o pervertidas, reales o simuladas.
b) Representaciones patentemente ofensivas de masturbación, funciones excretorias, o groseras exhibiciones de genitales. (U.S. Supreme Court, 1973)

Salvo que haya un valor real, redimente, de carácter científico, literario, artístico o político (U.S. Supreme Court, 1973).

3.1.2. Sin advertir al usuario para que se restrinja el acceso a niños y adolescentes

La LECDI, a diferencia de la *Communication Decency Act* de los EE UU, anulada por la Corte Suprema de los EE UU en 1997, (U.S. Supreme Court,1997) que exigía un sistema basado en tarjetas de crédito para permitir el acceso, ha convertido en obligación legal la página de advertencia que contienen el común de los sitios para adultos e incluso, los sitios de museos y similares que distribuyen material que en modo alguno constituye pornografía. Debido a la anulación de la Ley muchos sitios que transmiten lo que se define como pornografía en los EE UU ya no la tienen. Por demás, dependiendo del diseño de sitios si se llega a través de un *link* es posible que la persona acceda a los contenidos sexuales sin ver la página de advertencia mientras que algunos sitios sólo permiten la entrada a través de la página de advertencia.

La página no impide entrar sólo hace la advertencia, para que los padres, representantes o responsables, por sí mismos o a través de filtros impidan el acceso que los proveedores de Internet ISP deben poner a disposición de los padres y que los ciber-cafés deben instalar, según el artículo 10 de la Ley para la Protección de Niños y Adolescentes en Internet.

3.2. Culpabilidad

El delito se castiga a título de dolo. Debe haber la intención de exhibir o distribuir el material y no haberse hecho la advertencia y si la advertencia no es vista porque la página *web* permite el acceso sin pasar forzosamente por la advertencia habría culpa gravísima equiparable al dolo. En cambio, si

la advertencia es ignorada o la computadora no dispone de filtros no habrá delito. Si los padres autorizan el acceso al material, lo cual es legítimo pues la exposición a ese tipo de material coadyuva en el proceso de maduración de un adolescente (Heins, 2002: 258), el legislador no puede interferir. A final de cuentas, ya es un lugar común observar que la exposición continua a la violencia es aceptada más no así al sexo.

3.3. Pena

De conformidad con el artículo 23 LECDI este delito será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Conclusiones

Como se ha visto, el desarrollo tecnológico, ha obligado a las legislaciones a replantear algunas figuras tradicionales de delitos, e incluso a crear nuevos tipos delictivos a fin de proteger los derechos y libertades ciudadanas. Se habla en la actualidad de delitos informáticos, en su mayoría delitos de peligro, los cuales se ven facilitados con el uso de Internet, y se distinguen de los tradicionales por utilizar medios informáticos para su consumación, o por atacar precisamente dichos sistemas o sus soportes, si bien, en la mayoría de los casos se trata de delitos tradicionales con una nueva plataforma que con la promulgación de una nueva ley penal en la actualidad, los viene a calificar como especiales.

El acceso indebido, es uno de los pocos delitos informáticos propiamente dichos ya que no encuentra su equivalente en la legislación penal tradicional venezolana y de igual forma, viene a ser uno de los más comunes gracias a la proliferación de la utilización de técnicas de *hacking,* que en la mayoría de los casos simplemente se ven motivadas en la vanidad. Por otra parte, en aras de garantizar aun más la seguridad en el uso de las nuevas tecnologías, se extiende la protección a regular no sólo el acceso sino además otros usos que se hagan de ellas y dada la importancia de las tecnologías de la información en la sociedad actual, al tipificar el delito de sabotaje que sanciona la destrucción, daño, inutilización o modificación de sistemas o sus componentes, tradicionalmente sancionado en el Código Penal, se crea un tipo especial que puede decirse castiga ahora el "vandalismo cibernético".

Finalmente, en virtud del innegable y vertiginoso avance de las comunicaciones por Internet, se hizo necesario, o al menos así se percibe, regular la difusión o exhibición de imágenes de contenido sexual en la *web,* a fin

de proteger a los niños y adolescentes; lo cual se reduce básicamente a la colocación de una advertencia sobre su contenido indicando el acceso restringido para los mismos, norma que simplemente actualiza el medio de comunicación y agrava la pena del tipo tradicional contenido en el Código Penal. En definitiva, con la tipificación de estos delitos, se trata de brindar mayor seguridad a fin de proteger y estimular el uso de las nuevas tecnologías de la información.

Referencias Bibliográficas

ABREU, Elinor. 2001. **"U.S. Security Site Back From Attack". Original Industry Standard Archive.** En *http://www.thestandard.com/article/0,1902,24725,00.html*. Fecha de consulta 13 de noviembre de 2008

ASAMBLEA NACIONAL. 2001. **Ley Especial contra los Delitos Informáticos**. Gaceta Oficial Nro. 37313, del 30 de octubre de 2001. Imprenta Nacional. Caracas.

ASAMBLEA NACIONAL. 2005. **Ley de Reforma Parcial del Código Penal**. Gaceta Oficial Nro. 5768 del 13 de abril de 2005. Imprenta Nacional. Caracas.

ASAMBLEA NACIONAL. 2006. **Ley para la Protección de Niños, Niñas y Adolescentes en Sala de Uso de Internet, Videojuegos y otros Multimedias**. Gaceta Oficial Nro. 38529 del 25 de septiembre de 2006. Imprenta Nacional. Caracas

ASAMBLEA NACIONAL CONSTITUYENTE. 2009. "**Constitución de la República Bolivariana de Venezuela, con la Enmienda Nº 1 aprobada por el Pueblo Soberano, mediante Referendo Constitucional, a los quince días del mes de febrero de dos mil nueve. Año 198º de la Independencia, 149º de la Federación y 11º de la Revolución Bolivariana**". Gaceta Oficial Extraordinaria Nº**.** 5.908 de 19 de febrero de 2009. Imprenta Nacional. Caracas

ASOCIACIÓN DE INTERNAUTAS. 2007. "**Los casos de "phishing" han aumentado un 320 por ciento en tres meses, según la Asociación de Internautas**". En *http://www.europapress.net/Default.aspx?opcion=sociedad&fechor=20070515104846.* Fecha de consulta 13 de noviembre de 2008

BBC NEWS. 2008. "**Study shows how spammers cash in**". En *http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/7719281.stm*. Fecha de consulta 13 de noviembre de 2008.

BREWER-CARÍAS, Allan R.; ORTIZ-ÁLVAREZ, Luis A. 2007. **Las Grandes Decisiones de la Jurisprudencia Contencioso-administrativa, (1961 - 1996).** Editorial Jurídica Venezolana. Caracas.

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION (CCIPS) OF THE UNITED STATES DEPARTMENT OF JUSTICE. 2007. **Prosecuting**

Computer Crimes. En *http://www.cybercrime.gov/ccmanual/index.html.* Fecha de consulta 13 de noviembre de 2008

COUNCIL OF EUROPE. 2001a. "**Convention on Cybercrime".** En *http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.* Fecha de consulta 13 de noviembre de 2008.

COUNCIL OF EUROPE. 2001b. **"Convention on Cybercrime. Explanatory Report"**. En *http://conventions.coe.int/Treaty/en/Reports/Html/185.htm*. Fecha de consulta 13 de noviembre de 2008.

EDRM PROJECT TEAM.2010." **E-Discover Road**" en: *http.//www.law.com/jsp/legaltechnology/roadmap*. Fecha de consulta 10 de noviembre 2010.

FUNNEL, Antony. 2008. **"The Great Firewall of Australia**". En Media Report *http://www.abc.net.au/rn/mediareport/stories/2008/2405376.htm.* Fecha de Consulta 13 e noviembre de 2008.

GODWIN, Mike , 2003. "**Cyber Rights: Defending Free Speech in the Digital Age"**. MIT Press. Cambridge.

HEINS, Marjorie. 2002. **Not in Front of the Children: "Indecency," Censorship and the Innocence of Youth.** Farrar, Straus and Giroux. Nueva York

KERR, Orin. 2006. **Computer Crime Law**. Thomson West, St. Paul, MN

KERR,Orin. 2003. **"Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes" New York University Law Review**. En *http://ssrn.com/abstract=399740.* Fecha de consulta 18 de octubre de 2007.

KOERNER, Brendan. 2003. **"What's Worse, a Virus or a Worm? Slate.** En *http://www.slate.com/id/2083292/.* Fecha de consulta 13 de noviembre de 2008.

LLOYD, Ian. 2000. **Information Technology Law**. Butterworths. Londres.

MARKOFF, John. 2008. **"Internet Attacks Grow More Potent"** New York Times. En *http://www.nytimes.com/pages/national/index.html.* Fecha de consulta 13 de noviembre de 2008.

MENDOZA, José Rafael. 1965. **Curso de Derecho Penal Venezolano**. Tomo V. Letras. Madrid

MENDOZA, José Rafael. 1980. **Curso de Derecho Penal Venezolano**. **Compendio de Parte Especial.** Destino. Caracas

PECORELLA, Claudia. 2005. **Il Diritto Penale dell'Informatica**. Cedam. Bologna.

REAL ACADEMIA ESPAÑOLA. 2001. Diccionario de la Lengua Española. Vigésima Segunda ediciòn.En *http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA= acceso.* Fecha de consulta 13 de noviembre de 2008.

RICO, Marilena. 2006. **Comercio Electrónico Internet y Derecho.** Legis. Caracas.

ROMM, Tony. 2008. **"Why Would a Virus Look at Kiddie Porn? Malicious code that makes your computer visit illegal Web sites"**. **Slate**. En *http://www.slate.com/id/2175823/*. Fecha de consulta 13 de noviembre de 2008.

SYMANTEC. 2008a. **"Cybercrime. Crimeware: Bots"**. En *http://www.symantec.com /norton/cybercrime/bots.jsp.* Fecha de consulta 13 de noviembre de 2008.

SYMANTEC. 2008b. **"Cybercrime. Crimeware: Trojans & Spyware"**. En *http://www.symantec.com/norton/cybercrime/trojansspyware.jsp*. Fecha de consulta 13 de noviembre de 2008.

U.S. SUPREME COURT. 1997. "**RENO V. AMERICAN CIVIL LIBERTIES UNION, 117 S.CT. 2329, 138 L.ED.2D 874 (1997) [Opinion]".** En: *http://supct.law.cornell.edu/supct/search/display.html?terms=cda&url=/supct/html/96-511.ZO.html.* Fecha de consulta 13 de noviembre de 2008.

U.S. SUPREME COURT. 1973. **"MILLER v. CALIFORNIA, 413 U.S. 15"**. En *http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=413&invol=15*. . Fecha de consulta 13 de noviembre de 2008.

U.S. SUPREME COURT. 1978. **"FCC v. PACIFICA FOUNDATION, 438 U.S. 726"**. En 36 *http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=438&invol=726.* Fecha de consulta 13 de noviembre de 2008.

WIKIPEDIA. 2008. **"Server (computing)"**. En *http://en.wikipedia.org/wiki/ Server_(computing).* Fecha de consulta 13 de noviembre de 2008.

WIKIPEDIA, 2011. **"Ataque de denegación de servicio".** En: *http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio*. Fecha de consulta 22 de julio de 2011

WIKIPEDIA, 2011b **"Peer to peer".** En: *http://es.wikipedia.org/wiki/Peer-to-peer.* Fecha de consulta 22 de julio de 2011.

WILSON, Chris. 2008. **"What's a Botnet? An army of infected computers that can send out 100 billion spam e-mails a day"**. **Slate.** En *http://www.slate.com/id/2190275/*. Fecha de consulta 13 de noviembre de 2008.