INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"IMPLICACIONES LEGALES EN MATERIA DE PROPIEDAD INTELECTUAL EN MÉXICO EN CASO DE LA ADOPCIÓN DEL CONVENIO DE BUDAPEST."

SOLUCIÓN ESTRATÉGICA EMPRESARIAL
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.

Presenta:

Lino Alberto Almazán Monroy.

Asesor:

Dr. Alberto Nava Garcés.

Ciudad de México, a 21 de mayo de 2018.

Autorización de Impresión

C4

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 27 de julio de 2018

La Gerencia de Capital Humano/ Gerencia de Investigación hacen constar que el proyecto terminal titulado:

"Implicaciones legales en materia de propiedad intelectual en México en caso de la adopción del convenio de Budapest"

Desarrollada por el alumno

Nombre: **Lino Alberto**

Apellido paterno: **Almazán**

Apellido materno: **Monroy**

Desarrollado bajo la asesoría del:

Dr. Alberto Enrique Nava Garcés

Ha sido revisado y aprobado por miembro del Núcleo Académico Básico (NAB).

Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

Mtra. Patricia Ávila Muñoz
Gerencia de Capital Humano

***Anexar a la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.**

Tabla de contenido

Siglas y abreviaturas

ADPIC: Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual
ATA: Anti-terrorism Act (Ley Anti-terrorismo).
CDPC: European Committee on Crime Problems (Comité Europeo para Asuntos Delictivos).
CFAA: Computer Fraud and Abuse Act (Ley contra abuso y fraude por computadoras).
C-PROC: Cybercrime Programme Office (Oficina de Programa sobre Cibercrimen).
CSS: Content Scrambling Systems (Sistemas de Aleatorización de Contenidos).
DRM: Digital Right Management (Gestión de Derechos Digitales).
ERMI: Electronic Resource Management Iniciative (Gestión de Información de Derechos Electrónicos).
GLACY: Global Action on Cybercrime (Proyecto Global en contra del Cibercrimen).
HTML: HyperText Markup Language (Lenguaje de Marcas de Hipertexto).
ICANN: Internet Corporation for Assigned Names and Numbers (Corporación de Internet para la Asignación de Nombres y Números).
IP: Internet Protocol (Protocolo de Internet).
ITU: International Telecommunication Union (Unión Internacional de Telecomunicaciones).
LFDA: Ley Federal del Derecho de Autor.
LPI: Ley de la Propiedad Industrial.
OMPI: Organización Mundial de la Propiedad Intelectual.
P2P: Peer-to-peer (Red de pares).
RMI: Rights Management Information (Información de Gestión de Derechos).
TLCAN: Tratado de Libre Comercio de América del Norte.
TPM's: Technological Protection Measures (Medidas de Protección Tecnológica).
TPP: Trans-Pacific Partnership (Acuerdo Transpacífico de Cooperación Económica).
UDRP: Uniform Domain-Name Dispute-Resolution Policy (Política Uniforme de Resolución de Disputas de Nombre de Dominio).
WCT: World Intellectual Property Organization Copyright Treaty (Tratado de la **OMPI** sobre Derechos de Autor).
WPPT: World Intellectual Property Organization Performances and Phonograms Treaty (Tratado de la **OMPI** sobre Interpretación o Ejecución y Fonogramas).

Capítulo 1

Internet y la propiedad intelectual

Capítulo 1: Internet y la propiedad intelectual

Bajo el concepto de propiedad intelectual se tutela a las obras literarias, artísticas, musicales, cinematográficas, fotográficas, arquitectónicas, programas de computo, entre otras (propiedad intelectual), así como lo relativo a las patentes, certificados de invención, marcas para productos o servicios, dibujos o modelos industriales y la competencia desleal (propiedad industrial). [1]

En cuestión de legislación, hay países que homogenizan su legislación interna para establecer normas concretas entre los países y asegurar la protección y defensa de derechos de Propiedad Intelectual en el territorio de tales países. Como ejemplo está la celebración del TLCAN entre México, Estados Unidos y Canadá. Otro ejemplo corresponde al Acuerdo Transpacífico de Cooperación Económica (TPP por sus siglas en inglés: Trans-Pacific Partnership)[2] el cual en uno de sus apartados homogeniza el tema de propiedad intelectual entre los países miembros.

Sin embargo, esto no conlleva a erradicar las infracciones en materia de propiedad intelectual. El atentado más común contra la propiedad intelectual e industrial es el que afecta el derecho de reproducción y su distribución a escala comercial. Esta reproducción ocasiona no solamente daños al derecho moral de los autores, que consiste en la creación, divulgación, publicación, corrección, modificación, o destrucción de su obra; sino también el derecho patrimonial de los autores, que consiste en la reproducción, disposición, plusvalía, o por el uso de su obra, etc.

En el plano internacional, existen dos instrumentos encaminados a proteger el Derecho de Autor y Derechos Conexos en el ámbito digital. Estos son el Tratado de la OMPI sobre Derechos de Autor (WCT), y el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT). El WCT confiere

[1] Organización Mundial de la Propiedad Intelectual, ¿Qué es la propiedad intelectual?, Publicación 450(S) disponible en http://www.wipo.int/edocs/pubdocs/es/intproperty/450/wipo_pub_450.pdf Consultado el 1-mayo-2017.

[2] Tratado Amplio y Progresista de Asociación Transpacífico (CPTPP) disponible en: http://www.gob.mx/tratado-de-asociacion-transpacifico Consultado el 1-mayo-2017.

derechos a los autores respecto: al derecho de distribución, el derecho de alquiler y un derecho más amplio de comunicación al público[3]. Además, respecto a las limitaciones y excepciones, en el artículo 10 del WCT se incorpora la llamada "regla de los tres pasos" para la determinación de las limitaciones y excepciones con arreglo a lo dispuesto en el párrafo 2 del artículo 9 del Convenio de Berna, que extiende su aplicación a todos los derechos y pueden hacerse extensivas al entorno digital.

Respecto al WPPT[4] se contemplan los derechos de propiedad intelectual de dos categorías de beneficiarios, especialmente en el entorno digital: i) los artistas intérpretes o ejecutantes (actores, cantantes, músicos, etc.) y ii) los productores de fonogramas (personas físicas o jurídicas que toman la iniciativa y tienen la responsabilidad de la fijación de los sonidos de la interpretación o ejecución).

Con lo anterior, si bien los derechos de autor están contemplados en la red, las obras sufren vulnerabilidades considerables. Por ejemplo, el compartir música a través de programas o aplicaciones en Internet sin remunerar al titular de los derechos patrimoniales.

México es un país rico en la creación intelectual y la calidad de las obras de sus artistas, creadores e inventores que han trascendido las fronteras, alcanzando un merecido reconocimiento internacional. Sin embargo, las sociedades autorales y organizaciones empresariales enfrentan graves problemas por la reproducción ilegal de obras y productos protegidos por el derecho autoral, afectando con ello además del orden jurídico a la economía del país.

En materia de marcas, su territorialidad se ve cuestionada por el uso frecuente y constante en diferentes lugares al mismo tiempo sin autorización del titular.

1.1 Delitos que involucran infracciones de la propiedad intelectual

[3] http://www.wipo.int/treaties/es/ip/wct/summary_wct.html Consultado el 1-mayo-2017.
[4] http://www.wipo.int/treaties/es/ip/wppt/ Consultado el 1-mayo-2017.

De las figuras comprendidas en la propiedad intelectual, los derechos de autor y las marcas presentan más vulneraciones a los derechos que protegen por el uso de Internet, debido en una parte a que la información fluye con facilidad a través de la red y, por otra parte, a que las legislaciones en materia de propiedad intelectual en el entorno digital no son lo suficientemente robustas, ni homogéneas para permitir atender las vulneraciones cometidas a los derecho de autor o marcas.

1.1.1 Derechos de autor

En cuestión de derechos de autor, el Internet permite a los usuarios copiar, descargar, distribuir y compartir obras audiovisuales, literarias y otras, sin pedir autorización del autor para realizar dichas acciones. Dado que la digitalización de contenido permite mantener la calidad de las copias intacta en comparación con la fuente original, resulta atractivo para el infractor y consumidores el mantener prácticas ilegales que violan a los derechos de autor. Las acciones más comunes a los derechos de autor contemplan las siguientes:

- Intercambiar archivos a través de sistemas para tal fin.
- Elusión de los sistemas de gestión de derechos en el ámbito digital inadvertida o intencionalmente.

El intercambio de archivos por medio de los servicios de la red hace posible compartir los archivos entre un número muy grande de usuarios. Para esto es necesario contar con un software (código de programación) que permite la búsqueda e intercambio de archivos por medio de intercambio directo entre usuarios, en vez de requerir el soporte de un servidor centralizado. Las aplicaciones de intercambio de archivos pueden clasificarse como: De comunicación y colaboración, Computación distribuida, Soporte de servicio de Internet, Sistemas de bases de datos y Distribución de Contenido. Siendo ésta última clasificación la que implica las actividades de violación de derechos de

autor[5], toda vez que se permite compartir contenidos entre los usuarios sin tomar en cuenta los derechos de autor asociados a los mismos.

Respecto a la elusión de los sistemas de gestión de derechos en el ámbito digital, cabe mencionar que dentro del argot legal y técnico se ha adoptado el término DRM Digital Right Management; no obstante, éste término no se menciona en los textos de los tratados internacionales tales como el WCT, WPPT o en las Directivas Europeas, ni tampoco en las leyes nacionales que implementan a dichos tratados.

Los términos que se utilizan en los tratados internacionales son Medidas de Protección Tecnológicas (Technological Protection Measures TPMs por sus siglas en inglés) y también Información de Gestión de Derechos (Rights Management Information RMI, por sus siglas en inglés). La implementación de TPMs implica una práctica de hacer condicional el acceso a una obra por medio de una remuneración razonable, ya sea económica o por medio de otra especie[6].

Los TPMs son medidas de restricción técnicas tales como passwords, códigos de acceso o datos encriptados que previenen el acceso o reproducción de la obra protegida bajo derechos de autor a los usuarios.

Los DRM[7] son diseñados por empresas y tienen por objetivos: detectar y reportar al proveedor el acceso a una obra por parte del usuario; y autorizar o denegar el acceso a la obra conforme a las condiciones preestablecidas por el proveedor.

Otro término utilizado es Gestión de Información de Derechos Electrónicos (Electronic Resource Management Iniciative, ERMI por sus siglas en inglés) y se refiere a la información anexada o embebida en un archivo o material electrónico, por ejemplo, una firma digital o marca de agua. Un ERMI puede consistir de

---

[5] Stephanos Androutsellis-Theotokis and **Diomidis Spinellis**. A survey of peer-to-peer content distribution technologies. *ACM Computing Surveys*, 36(4):335–371, December 2004. (doi:10.1145/1041680.1041681) Consultado el 2-agosto-2014.

[6] *Sub-regional Seminar on the Protection of Computer Software and Databases organized by the World Intellectual Property Organization (WIPO), the Romanian Copyright Office (ORDA), and the State Office for Inventions and Trademarks (OSIM). Mangalia, Romania, August 25 to 27, 2010. TOPIC 12:DIGITAL RIGHTS MANAGEMENT (DRM) AND ITS CO-EXISTENCE WITH COPYRIGHT EXCEPTIONS. Dr. Mihály Ficsor, Chairman. Central and Eastern European Copyright Alliance (CEECA). Budapest. www.wipo.int/edocs/mdocs/.../wipo_ip_mng_10_ref_t12.pptx* Consultado el 2-agosto-2014.

[7] http://www.monash.edu.au/ Consultado el 12-abril-2014.

información como: el nombre del autor o del archivo, o nombre del autor y del propietario de los derechos de autor, o los datos para contactar a estos últimos o la información que indique la forma correcta de uso de la obra. Asimismo, se anexan los términos de licencia al archivo, un ejemplo es una licencia Creative Commons.

Finalmente, los sistemas de aleatorización de contenido CSS (Content Scrambling Systems) son otra tecnología que encripta los datos e impide la copia de contenidos de obras en DVD.

A pesar de los diversos tipos de tecnologías de protección para obras audiovisuales, literarias y otras, los delincuentes informáticos han utilizado herramientas para su elusión. Una vez vulnerada la tecnología de protección, es posible hacer copias y reproducción de una obra y ponerla a disposición del público en Internet de forma gratuita o a precios muy por debajo del precio comercial lo que ocasiona la violación de los derechos de autor con su respectiva pérdida económica.

1.1.2 Marcas

En cuestión de marcas, actividades como la piratería[8] y la falsificación afectan a autores y empresas debido a que es factible utilizar la imagen de una marca, el diseño de algún logotipo original e incluso registrar un nombre de dominio haciendo uso del nombre de una marca sin autorización.

Los delitos referentes a la infracción de marcas son:

- El uso de las marcas en actividades delictivas para inducir el engaño de las víctimas; y

[8] El Acuerdo Nacional contra la Piratería, en el que señala que por piratería debe entenderse toda aquella producción, reproducción, importación, comercialización, venta, almacenamiento, transportación, arrendamiento, distribución y puesta a disposición de bienes o productos en contravención a lo establecido en la Ley Federal del Derecho de Autor y en la Ley de la Propiedad Industrial. http://www.pgr.gob.mx/Unidades-Especializadas/ueiddapi/Paginas/default.aspx Consultado el 2-mayo-2017.

[9] La UDRP establece los términos y condiciones relacionados cuando surge una disputa entre el propietario del nombre de domino y un tercero (registrar). https://www.icann.org/resources/pages/udrp-2012-02-25-en Consultado el 2-mayo-2017.

[10] Persona física o moral, acreditada para distribuir y ofrecer servicios de administración de Nombres de Dominio. https://www.akky.mx/static/docs/PoliticasGeneralesDeNombresDeDominioAkky.pdf Consultado

- El uso de la marca indebidamente para el registro de nombre de dominio.

Respecto al uso de marcas para inducir al engaño con fines delictivos, el delincuente se aprovecha de la reputación de la marca para generar nombres similares o idénticos a la marca. Por medio del envío de correo electrónico es posible que el usuario confíe en el enlace que lo direccionará a un sitio web fraudulento en el cual se comprometerá la seguridad de los datos personales del usuario.

En referencia a las violaciones de marcas a través del registro de nombres de dominio, una práctica conocida es la ciberocupación (*cybersquatting*) en la cual se registra un nombre de dominio bajo el nombre de una marca de la cual no se tiene titularidad. El propósito puede ser el obtener ventaja de la reputación de la marca para atraer la atención del usuario y desviar el tráfico de consultas de los usuarios hacia una página distinta de la marca, o bien ofrecer la transferencia del nombre de dominio al titular de la marca a cambio de un precio excesivo.

En consecuencia de la práctica de ciberocupación, la ICANN elaboró la Política Uniforme de Resolución de Disputas de Nombre de Dominio[9] (UDRP) para establecer mecanismos arbitrales que permitan la resolución de disputas de nombres de dominio a través de acuerdos, órdenes de la corte o un proceso de arbitraje ante el Registrar[10] para cancelar, suspender o transferir el nombre de dominio.

Otra práctica que genera infracción de marca por medio de nombres de dominio es la apropiación indebida del dominio o registro de nombres de dominio que han caducado y el titular por descuido no procedió con la renovación.

1.2 Nombres de Dominio

[9] La UDRP establece los términos y condiciones relacionados cuando surge una disputa entre el propietario del nombre de domino y un tercero (registrar). https://www.icann.org/resources/pages/udrp-2012-02-25-en Consultado el 2-mayo-2017.

[10] Persona física o moral, acreditada para distribuir y ofrecer servicios de administración de Nombres de Dominio. https://www.akky.mx/static/docs/PoliticasGeneralesDeNombresDeDominioAkky.pdf Consultado el 2-diciembre-2014.

Los nombres de dominio atribuyen una especie de identidad dentro de la red y sirven como una ruta para que se transmita la información. Están diseñados para permitir a los usuarios localizar fácilmente un sitio web en Internet ya que asocian una cadena de letras conocidas para el usuario con una dirección IP la cual está comprendida por una serie de números.

El nombre de dominio puede permanecer sin cambios, a pesar de que el sitio web se traslade a un equipo o servidor host distinto.

1.3 Delincuentes informáticos

Muchas de las actividades realizadas en Internet que vulneran la seguridad de los sistemas informáticos y comprometen el contenido de la información contenida en ellos son realizadas por personas con conocimiento variado en el uso de Internet y sus deficiencias presentes. Tales personas se califican como delincuentes informáticos.

Los delincuentes informáticos cometen los delitos a través de tecnologías como: banda ancha; conexiones inalámbricas; informática móvil y acceso remoto; tecnologías web como Java, ActiveX; correo electrónico que admite HTML y programación de scripts; correo electrónico y banca en línea; mensajes de texto instantáneos; y nuevos sistemas operativos.

En relación a la clasificación de delincuentes en materia de delitos informáticos, se tiene la siguiente[11]:

A) Hacker: Son personas que acceden al sistema informático sin autorización. A veces buscando información para ellos mismos o por “pedido” de terceros. En otras oportunidades sin un objeto preciso, con la solafinalidad de desafiar los sistemas de seguridad y tratar de demostrar que no existen barreras para su ingreso al sistema, cuando ese es su propósito. Para el hacker constituye una afrenta no poder entrar a un sistema o a un sitio que se proponga.

[11] Luz Clara, Bibiana, *Manual de Derecho informático*, 1ª ed., Argentina. Editorial Nova tesis Editorial Jurídica, 2001, pp. 118-119. Consultado en diciembre de 2017.

B) Cracker: Aquí se inutilizan los sistemas de protección de aplicaciones informáticas mediante programas elaborados para tal fin. A diferencia del hacker el cracker tiene la intención precisa de provocar un daño.

C) Phreaker: Son quienes utilizan técnicas de fraude en telefonía ya sea esta digital o analógica.

D) Virucker[12]: Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

E) Pirata informático: Es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor.

[12] http://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap5.htm#5_1 Consultado en diciembre de 2014.

Capítulo 2

Ciberseguridad

Capítulo 2: Ciberseguridad

El término “ciber espacio” se utilizó por primera vez en la obra *Neuromencer* de 1984 escrita por William Gibson[13]. Dicho término definía el mundo virtual de las computadoras. Sin embargo, en la actualidad el término “ciber espacio” se asocia con Internet, aunque cabe señalar que el “ciber espacio” se refiere a la World Wide Web (www). La www es un conjunto de servicios basados en hipermedios ofrecidos en todo el mundo a través de Internet[14].

Dado que la tecnología se ha vuelto cada vez más amigable con el púbico usuario, a su vez, se ha abierto la puerta a los delincuentes informáticos para que realicen actividades criminales que antes no eran conocidas, ni siquiera concebibles. Con las herramientas tecnológicas digitales de hoy en día, los delincuentes informáticos pueden afectar a individuos, compañías y gobiernos. Las leyes en la actualidad, fueron realizadas sin tener en mente el fenómeno de la ciberdelincuencia ya que no se contemplaba el hecho de que pudieran realizarse delitos a través del uso de Internet. Así, resulta relevante determinar qué reformas son necesarias a estas leyes para confrontar la ciberdelincuencia. Como un intento para controlar las conductas de los delincuentes informáticos, diversas naciones han reformado sus leyes. Una hipótesis referida a la solución de este fenómeno, consiste en la adopción de una legislación penal que sea clara y transparente[15], es decir, no deben crearse leyes nuevas para afrentar el problema de la ciberdelincuencia. Además, debido a que la ciberdelincuencia se realiza sin considerar las fronteras, en donde cualquier persona, sistema y organización es vulnerable, debe implementarse la colaboración internacional en la aplicación de la ley de las agencias especializadas y la armonización de las leyes en distintos países.

---

[13] Gibson, William. 1984. *Neuromancer*. U.S. Ace Books. http://cmap.javeriana.edu.co/servlet/SBReadResourceServlet?rid=1LQ8S8P5H-VJTDCY-2GW Consultado en diciembre de 2014.

[14] Téllez Valdés, Julio. *Derecho Informático*. 4ta ed. México. Ed. McGraw Hill. 2009. Pp. 101.

[15] Karake Shalhub, Zeinab. *Cyber Law and Cyber Security in Developing and Emerging Economies*. UK. Edward Elgar Publishing Limited. 2010.

La hipótesis antes citada, va en línea con cambios de paradigma en la ciencia del derecho, que implican que ahora los fenómenos que involucran el uso de las tecnologías de información y comunicación, deben abordarse desde un punto de vista sistémico y no territorial. Como consecuencia, se considera que los países están dentro de un sistema (global y no territorial) en el cual las acciones de un determinado fenómeno, por ejemplo la ciberdelincuencia, provoca cambios en partes específicas del sistema que afectan o hacen reaccionar a las mismas, y a su vez, afectan o hacen reaccionar otras partes del sistema en una medida distinta.

Aunado a lo anterior, en el plano nacional se considera conveniente legislar debidamente a los delitos informáticos y resolver el problema de comprobarlos. Además de unificar las leyes penales. En el caso de México, se debería federalizar la legislación penal para evitar el problema de no poder dar seguimiento a un delito informático determinado entre un estado de la república y otro debido a la falta de tipificación en la legislación estatal.

Aun así, debe tenerse en cuenta que Internet es difícil de regular debido a que no hay una autoridad centralizada independiente con jurisdicción en el ámbito internacional, aunado a que la legislación aún en países desarrollados ha tenido problemas para solventar este fenómeno, ya que el avance de la tecnología supera al del derecho.

Una de las características de las ciberamenazas es que pueden realizarse por diferentes tipos de actores, su costo es mínimo y su seguimiento en Internet llega a ser difícil. Como ejemplo de amenazas cibernéticas están: el espionaje, robo, sabotaje de servicios, terrorismo informático y operaciones para comprometer información contenida en sistemas informáticos. Por ello, debe ser obligación de cualquier Estado proteger su infraestructura de telecomunicaciones a fin de proteger a los ciudadanos, organizaciones gubernamentales y al sector privado.

Para asegurar el ciberespacio y tener medios de defensa y ataque contra ciberamenazas, los gobiernos implementan estrategias nacionales con el esfuerzo combinado de sociedad, gobierno, sector privado y académico. Con ello, se

salvaguardan las estructuras críticas de un país contra cualquier ciberamenaza. Como estructuras críticas de un país se contemplan a los sectores financiero, transporte y distribución, energía, salud, comunicaciones y administraciones públicas.

La implementación de una estrategia nacional contiene 5 prioridades fundamentales:

1) Un sistema de respuesta y seguridad nacional del Ciberespacio. Permite la identificación, el intercambio de información y la rápida acción para atenuar el daño causado por la actividad maliciosa en el Ciberespacio.
2) Un programa de reducción de vulnerabilidades y amenazas a la seguridad del Ciberespacio. Tiene por objetivo identificar y prevenir ataques organizados que puedan poner en peligro la seguridad de infraestructuras críticas de la nación.
3) Un programa de formación y concientización sobre seguridad en el Ciberespacio. Su objetivo es identificar las insuficiencias presentes en el país que complican la tarea de tratar la ciberseguridad. Se capacita a usuarios, administradores de sistemas, se provee de personal entrenado y se dan certificaciones a los profesionales en el tema de ciberseguridad.
4) Un programa de seguridad para gobierno en línea. Identifica acciones para desarrollar el gobierno como líder de seguridad en el ciberespacio y promotor del uso de las tecnologías de la información y comunicación.
5) Un programa de cooperación internacional en temas de Ciberseguridad. Establecen esquemas para participar ordenadamente en los sistemas de cooperación internacional para reducir vulnerabilidades existentes en las infraestructuras críticas de la nación y facilitar que se comparta la información relevante con otros gobiernos respecto a los ataques.

En cuestión de ciberseguridad, se tienen 4 principios que son necesarios para cualquier compromiso confiable en el ciberespacio[16]. Estos principios son:

i) Principio de confidencialidad. Los datos transmitidos o almacenados deben ser privados y ser visibles solamente por personal autorizado.

ii) Principio de integridad. Los datos transmitidos o almacenados deben ser auténticos, libres de errores que pudieran cometerse durante su almacenamiento o durante su transmisión.

iii) Principio de disponibilidad. Los datos transmitidos o almacenados deben ser accesibles a todo personal autorizado.

iv) Principio de no repudio. Los datos transmitidos o almacenados son de autenticidad indiscutible, especialmente cuando se respaldan por certificados digitales aceptables, firmas digitales u cualquier otro identificador explícito.

Además, el desarrollo expansivo de Internet también amenaza al sector público y privado en el sentido de que el capital intelectual ha pasado a formar parte de una preocupación prioritaria.

Antes de la llegada de la era digital, la legislación en materia de propiedad intelectual, en específico el derecho de autor y el copyright, habían sido capaces de responder a los cambios tecnológicos. Por ejemplo, la aparición de la imprenta suscitó una necesidad por reforzar la protección del derecho de autor. Antes de la posibilidad de que la información pudiera ser almacenada en formato digital, la copia de obras era posible pero a un costo considerable y con la inversión de mucho tiempo. En el caso de la copia de música, las copias por lo general no mantenían la calidad de la copia original, salvo que el usuario decidiera comprar equipo costoso y especializado para ello.

No obstante, con el incremento de la información en forma digital, los titulares de derechos de propiedad intelectual han presentado dificultades para proteger sus derechos. Esto es porque la información que está en soporte digital puede ser copiada y distribuida fácilmente, sin involucrar un costo considerable.

[16] Kostopoulos, George K. *Cyberspace and Cybersecurity.* U.S. CRC Press. 2013. pp. Xiv.

Actualmente, las redes Peer-to-Peer (P2P)[17] permiten compartir archivos protegidos por derechos de autor, sin la necesidad de solicitar la autorización al autor o titular de derechos, realizando con ello una vulneración a los derechos patrimoniales.

De manera similar, la digitalización de información posibilita que se vulneren secretos industriales. Anterior a la era digital, quien decidiera robar información protegida por un secreto industrial tenía que robar necesariamente el documento físico y arriesgarse a fotocopiarlo involucrando con ello un tiempo considerable en función del tamaño del documento. Sin embargo, ahora si la información se encuentra digitalizada y sin medidas de protección, entonces prácticamente cualquier persona puede hacerse de dicha información de manera instantánea y distribuirla además a través de Internet.

Dado que los bienes intangibles protegidos por la propiedad intelectual son la base económica de muchos países, la criminalización de violaciones a derechos de propiedad intelectual y mal uso de sistemas informáticos deben establecerse para imponer responsabilidad criminal, prevenir fraudes, aplicar honestidad en el comercio, castigar el robo de propiedad intelectual, y mejorar la confianza en el comercio[18].

En el plano internacional como medidas para hacer frente al fenómeno de ciberdelincuencia, en 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define el **Delito Informático**. Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la

[17] Una red informática P2P se refiere a una red que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red. Este modelo contrasta con el modelo cliente-servidor tradicionalmente empleado en las aplicaciones de Internet. González, Abel Santín, *Peer 2 Peer,* Sistemas Operativos Distribuidos. Disponible en: http://www.dit.upm.es/~joaquin/so/p2p/p2p.pdf Consultado en noviembre de 2014.

[18] Toren, Peter. *Intellectual Property and Computer Crimes*. U.S. ALM Properties Inc. 2005. Pp. 1-1.

intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

Por otra parte, en 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad"[19].

Asimismo, es importante considerar que en 2007 la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés) lanzó la Agenda Global de Ciberseguridad[20]. Dicha Agenda es un marco de trabajo para la cooperación internacional dirigida a mejorar la confidencialidad y seguridad de la sociedad de la información. La Agenda Global de Ciberseguridad está diseñada para lograr la cooperación y eficiencia, además de alentar la colaboración con y entre todos los participantes relevantes a fin de construir y evitar, con base en iniciativas existentes, que se dupliquen esfuerzos. Desde su lanzamiento, la Agenda Global de Ciberseguridad ha atraído el apoyo y reconocimiento de diversos líderes y expertos en ciberseguridad de todo el mundo.

Ahora bien, es precisamente que en materia de ciberseguridad surge el Convenio sobre la Ciberdelincuencia[21], que es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Dicho convenio contempla en su Título 4 a los delitos relacionados con infracciones de propiedad intelectual y de los derechos afines.

---

[19] Breve reseña histórica del delito informático de la Revista del Instituto de la Judicatura Federal, No. 28, año 2009: *Delitos informáticos en México*, Cassou Ruiz, Jorge Esteban.

[20] http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx Consultado en agosto 2014.

[21] https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf Consultado en noviembre de 2014.

Capítulo 3

El convenio sobre la ciberdelincuencia

Capítulo 3: El convenio sobre la ciberdelincuencia

En 1996 el Comité Europeo para Asuntos Delictivos (CDPC) decidió establecer un Comité de Expertos para abordar el ciberdelito, a partir de cual se preparó la redacción de un Convenio. El proyecto del Convenio fue adoptado por el Pleno en 2001. El proyecto de Convenio se presentó para su aprobación al CDPC y ulteriormente el texto de dicho Proyecto se trasladó al Comité de Ministros con miras a su adopción. La firma del Convenio se abrió en Budapest el 23 de noviembre de 2001 en la cual 30 países lo firmaron (incluidos cuatro Estados no miembros del Consejo de Europa: Canadá, Estados Unidos, Japón y Sudáfrica, que habían participado en las negociaciones)[22]. El Convenio entró en vigor el 1 de julio de 2004.

El Convenio de ciberseguridad es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la ciberdelincuencia.

En abril de 2001 el Consejo Europeo publicó el proyecto destinado a armonizar las legislaciones en los estados miembros (47 miembros y 8 observadores) y abierta a otros países como Australia, Japón, Canadá, Sudáfrica y los Estados Unidos en noviembre de 2001. Actualmente países como Argentina (que ha basado su ley de delitos informáticos en este convenio) y Ecuador están analizando adherirse.

Por ende, este convenio es el único que se encarga de la seguridad de la información y trata los delitos contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos.

El Convenio sobre la Ciberdelincuencia consta de 48 artículos y un preámbulo inicial. Están divididos en cuatro capítulos, divididos a su vez en secciones y títulos. El primer capítulo comprende un precepto, referido a la terminología usada en el texto. El segundo capítulo Titulado “Medidas que

[22] Ver página 106 del documento: *El Ciberdelito: Guía para los Países en Desarrollo*. Proyecto de abril de 2009.

deberán adoptarse a nivel nacional", incluye elementos tanto de Derecho material (responsabilidad penal, tentativa, complicidad, etc.) como Derecho procesal (procedimiento, salvaguardas, datos, registros, jurisdicción, etc.). En el tercer capítulo se introduce directamente en la cooperación internacional. Abarca cuestiones como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el establecimiento de una red 24/7. El último capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

No obstante, el Convenio sobre la Ciberdelincuencia como tal en lo que respecta a los preceptos de aplicación material, puede resumirse, conceptualmente, en dos partes bien diferenciadas: Derecho Penal Internacional, constituido por las disposiciones 2 a 13, y Derecho Procesal Penal Internacional, en los artículos 14 a 35.

México es país observador[23] del Consejo de Europa desde 1999, y fue invitado a convertirse en Estado Parte del citado convenio que ya han ratificado 32 de los 47 estados miembros, además de Estados Unidos, Canadá, Japón y Sudáfrica. La adhesión de México al mismo aún no ha sido ratificada.

Cabe señalar que diversas publicaciones en el país[24] consideran que la ratificación a dicho Convenio traería ventajas en la labor de reforzar políticas, definir estrategias, establecer una legislación adecuada y aplicar medidas prácticas sobre el cibercrimen y la seguridad cibernética en el país. Dichas ventajas se sustentan en el hecho de que el Convenio sobre la Ciberdelincuencia es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia –derecho penal, derecho procesal, propiedad intelectual y cooperación internacional– y trata con carácter prioritario una política penal contra la ciberdelincuencia en cada uno de los países miembros. Y uno de los problemas presentes para los investigadores digitales en muchos casos es,

[23] *Proceedings of a workshop on deterring cyberattacks*. National Research Council of The National Academies. U.S. pp. 207.

[24] http://www.mattica.com/2012/09/mexico-deberia-incorporarse-al-convenio-de-budapest/ Consultado en noviembre de 2014.

precisamente, el de la trasnacionalidad de los delitos informáticos y la falta de tratados internacionales que nos permitan traspasar fronteras al perseguir a los delincuentes.

Al respecto, el Consejo de Europa realiza la Conferencia Octopus de Cooperación contra el Cibercrimen. En la pasada conferencia del 2012 en Estrasburgo, Francia, se reunieron 280 expertos en cibercrimen de 80 países, 15 organizaciones e iniciativas internacionales, y 30 participantes del sector privado y académico para mejorar la cooperación contra el cibercrimen en todos los niveles. En dicha conferencia se discutió también el vincular la protección de datos personales con las estrategias contra el cibercrimen que se establezcan en cada país, debido a la alta incidencia del robo de información personal con fines delictivos a nivel mundial.

Como resultado a dicha Conferencia del 2012[25], se concluyó que las estrategias contra el cibercrimen están ligadas a derechos humanos, la regulación de la ley y la protección de datos personales, por lo que deben ser parte de políticas amplias que se dirijan a oportunidades y retos del ciberespacio. La cooperación entre multi-sectores permanece esencial. Se fomenta la adopción en la legislación e implementación del Convenio en los Estados que aún no son parte. El control y prevención del cibercrimen se lograran a través de compartir información pública y privada teniendo en cuenta estándares de protección de datos. La adopción de legislación en línea con las Convenciones de Lanzarote[26] y Budapest permitirá mayores acciones de justicia criminal a nivel internacional para identificar y proteger a las víctimas de explotación sexual a través de Internet. Implementar la observancia de leyes transfronterizas para el acceso a datos y evidencia digital.

---

25 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Octopus2012/2571_Octo_key_messages_V5.pdf Consultado en noviembre de 2014.

26 También conocido como Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual. Tiene por objetivo prevenir delitos sexuales contra menores, la persecución penal de sus autores y la protección de los niños víctimas de aquellos. Para lo cual el Convenio pide a los Estados Parte Medidas Preventivas, Medidas de Protección, Medidas de Derecho Penal, Procedimientos de investigación y judiciales adecuados a los menores y Seguimiento.
http://www.coe.int/t/dg3/children/pdf/ConventionSexualAbuse_sp.pdf Consultado en diciembre de 2014.

En dicha Conferencia del 2012, si bien se trataron temas importantes referentes a la adopción del Convenio de Ciberdelincuencia, de acuerdo a documento “Octopus 2012 - Key Messages”, no se hizo hincapié en materia de Propiedad Intelectual.

En 2013, la Conferencia Octopus de Cooperación contra el Cibercrimen se llevó a cabo del 4 al 6 de Diciembre de 2013 en la ciudad de Estrasburgo[27]. Para esta conferencia, se contó con la asistencia de un mayor número de expertos en cibercrimen ya que la cifra ascendió a 300 asistentes de más de 80 naciones, 17 organizaciones internacionales e iniciativas y 45 del sector privado, sociedad civil y académico. La conferencia se enfocó primordialmente en analizar los siguientes temas divididos en seis talleres: (1) iniciativas internacionales; (2) legislación sobre cibercrimen en la región Asia-Pacifico; (3) fortalecimiento de la capacidad en contra del cibercrimen y evidencias electrónicas; (4) acceso transfronterizo a datos y jurisdicción; (5) protección de los menores en contra de la explotación sexual en línea; y (vi) cooperación internacional y preservación de datos.

Para esta Conferencia del 2013, se obtuvieron como resultados[28] la implementación de pasos para prevenir y hacer frente a las amenazas del cibercrimen las cuales están en constante crecimiento. La obligación de los gobiernos para proteger a los ciudadanos contra el crimen. Deben distinguirse las medidas de justicia criminal sobre el cibercrimen contra las medidas de seguridad nacional en la legislación para evitar cualquier duda al momento de ejercer cualquier derecho fundamental. Es esencial que las organizaciones internacionales cooperen entre ellas para brindar mejores servicios a la sociedad. Se fomenta la armonización de la legislación en África, América, Asia y Europa de acuerdo a los estándares marcados en el Convenio. Se establece una Oficina de Programa sobre Cibercrimen (C-PROC) en Bucarest, Rumania para atender específicamente las buenas prácticas y capacidad de establecer proyectos entre los Estados Parte como consecuencia de las reformas legislativas efectuadas. Se

[27] http://www.protecciondedatos.org.mx/2013/11/conferencia-octopus-2013-cooperacin-ciberdelito-consejo-europa/ Consultado en diciembre de 2014.

[28] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571Octo2013_keymessages_v3short.pdf Consultado en diciembre de 2014.

puntualiza la necesidad contar en mayor medida con la participación de mujeres contra el cibercrimen. Se vuelve a reiterar la protección de los niños contra el abuso sexual.

A su vez, durante la conferencia hubo tres grupos de trabajo; el primero dedicado a analizar los avances sobre legislación de ciberdelito en Latinoamérica; el segundo sobre la actualización de la guía sobre evidencias electrónicas y materiales para entrenamiento y apoyo y; el tercer grupo estará enfocado a analizar planes y directrices del Proyecto Global en contra del Cibercrimen (**GLACY**) de la Unión Europea y el Consejo de Europa.

En esta Conferencia y de acuerdo al documento “Octopus 2013 - Key Messages”, nuevamente no se hizo hincapié en materia de Propiedad Intelectual.

3.1 Aspectos de propiedad intelectual contemplados en el Convenio

El Convenio en su Título 4, hace mención a los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Dicho Título consta de un solo Artículo, el 10 que consiste de 3 párrafos y establece lo siguiente:

Título 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado

de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo.

De acuerdo a dicho Artículo 10, en el párrafo 1 se menciona que las Partes adoptaran las medidas necesarias para tipificar como delito las infracciones de la propiedad intelectual cuando tales actos se cometan deliberadamente a escala comercial y por medio de un sistema informático, de conformidad con las obligaciones que hayan contraído en la aplicación del Acta de París de 24 de julio de 1971. En dicho párrafo se hace referencia al Convenio de Berna, los ADPIC, y el Tratado de la OMPI sobre Derechos de Autor.

El párrafo 2 establece que cada Parte adoptará las medidas legislativas para tipificar como delito las infracciones de derechos afines definidas en su legislación cuando tales actos se cometan deliberadamente a escala comercial y por medio de un sistema informático, de conformidad con las obligaciones que hayan contraído en aplicación de la Convención Internacional sobre la protección de los Artistas Intérpretes o Ejecutantes, los productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), de los ADPIC y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas.

Finalmente, el párrafo 3 establece que toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del citado Artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales en la aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2.

3. 2 Estados parte del Convenio

A la fecha, los Estados Parte al convenio son los siguientes: Albania, Alemania, Armenia, Australia, Austria, Azerbaiyán, Bélgica, Bosnia y Herzegovina, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos de América, Estonia, Finlandia, Francia, Georgia, Hungría, Islandia, Italia, Japón, Letonia, Lituania, Macedonia, Malta, Mauricio, Moldavia, Montenegro, Noruega, Países Bajos, Panamá, Portugal, Reino Unido, República Checa, República Dominicana, Rumania, Serbia, Suiza y Ucrania.

Capítulo 4

Legislaciones de algunos estados parte al convenio del continente americano sobre delitos informáticos

Capítulo 4: Legislaciones de algunos estados parte al convenio del continente americano sobre delitos informáticos

Como referencia respecto a legislaciones en materia de delios informáticos se mencionan a continuación un listado de leyes existentes en algunos países del continente americano tomando en cuenta que dichas legislaciones pudieran ser consideradas como fuente de consulta para reformas de leyes mexicanas.

4.1 Estados Unidos

En relación a delitos informáticos, Estados Unidos cuenta con las siguientes legislaciones:

1. Fraud and related activity in connection with computer – 18 USC 1030 (The Computer Fraud and Abuse Act), y
2. Anti-terrorism Act "ATA", CAM SPAM, 1-1-04.

El Computer Fraud and Abuse Act (CFAA) es un instrumento jurídico que se generó en el año de 1984 como una demanda para regular el Internet en Estados Unidos. Su alcance se dirige a los delitos por computadora y fraude a través del uso de las computadoras. Para este efecto, cubre tres áreas: (1) acceso a computadoras para obtener información de defensa o extranjera clasificada para dañar a los Estados Unidos o conseguir ventaja de una nación extranjera; (2) acceso a computadoras para obtener registros financieros a través de instituciones financieras o información de consumidores a través de agencias; y (3) modificar, destruir, o describir información de manera que afecte el uso que da el gobierno a las computadoras[29].

[29] 1996. *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*. Jo-Ann M. Adams. Santa Clara High Technology Law Journal. Consultado en enero de 2015. (http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1206&context=chtlj&sei-redir=1&referer=http%3A%2F%2Fscholar.google.com.mx%2Fscholar%3Fq%3DComputer%2BFraud%2Band%2BAbuse%2BAct%2Bcomments%26hl%3Des%26as_sdt%3D0%26as_vis%3D1%26oi%3Dscholart%26sa%3DX

En materia de propiedad intelectual, la obtención de información a través de Internet (downloading) por medio de un acceso no autorizado en una computadora con medios de protección puede violar el párrafo 1030(a)(2) y constituir una infracción de derechos de autor[30].

En referencia al Anti-terrorism Act "ATA", CAM SPAM, 1-1-04, dicho instrumento se creó con el propósito de combatir al terrorismo y defender a la nación contra actos terroristas. Como objetivos, tiene el enmendar la Ley de Terrorismo de 2000; adopta disposiciones complementarias sobre el terrorismo y la seguridad; prevé la congelación de los activos; establece disposiciones sobre la inmigración y el asilo; modifica o extiende el derecho penal y las competencias de la prevención del delito y la aplicación de la ley; establece disposiciones sobre el control de los patógenos y las toxinas; prevé la retención de datos de comunicaciones.

En el ámbito digital, el ATA tiene como una de sus misiones el permitir a los proveedores de servicios de comunicaciones la retención de datos, para asegurar el acceso a los mismos a través de las agencias que investigan el terrorismo o actividades delictivas.

4.2 Panamá

En el caso de Panamá, su Código Penal busca proteger los bienes jurídicos tutelados y los valores significativos de la sociedad de conformidad con la política criminal del Estado a través de la tipificación de conductas y comportamientos.

El Código Penal de Panamá trata en su capítulo III los delitos contra la inviolabilidad del Secreto y el Derecho a la Intimidad. Así, el Artículo 164 castiga el apoderamiento o información indebidas del contenido de una carta, mensaje de correo electrónico, pliego despacho cablegráfico o de otra naturaleza.

%26ei%3D5Re_U6n8JeHJ8AHql4HgAw%26ved%3D0CBoQgQMwAA#search=%22Computer%20Fraud%20Abuse%20Act%20comments%22)

[30] *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Charles Doyle. Senior Specialist in American Public Law. December 27, 2010. http://fas.org/sgp/crs/misc/97-1025.pdf Consultado en enero de 2015.

En el Artículo 165 se tipifican como delitos la sustracción, destrucción, sustitución, ocultación, extravío, intercepción o bloqueo de una carta, mensaje de correo electrónico, pliego despacho cablegráfico o de otra naturaleza.

Por su parte, el Artículo 220 condena el engaño de un provecho ilícito en perjuicio de otro. La sanción se aumenta en un tercio cuando se realice a través de un medio cibernético o informático.

En el Capitulo VI de dicho Código, se contemplan los delitos contra la Propiedad Intelectual.

El Artículo 262 impone penas a la comunicación pública por cualquier forma o procedimiento de una obra protegida por el derecho de autor. Asimismo, condena la retransmisión, por cualquier medio alámbrico o inalámbrico, de las emisiones de radiodifusión de cable o satélite.

Cabe hacer mención especial al Artículo 266 que contempla las sanciones para la fabricación, ensamble, modificación, importación, venta arrendamiento o puesta en circulación de decodificadores o cualquier otro artefacto, equipo, dispositivo o sistema diseñado exclusivamente para conectar, recibir, eliminar impedir, desactivar, o eludir los dispositivos técnicos que los distribuidores o concesionarios autorizados de las señales portadoras de programas, sonidos, imágenes, datos o cualesquiera combinación de ellos, tengan o hallan instalado para la protección o recepción de los mismos.

En cuestión de marcas, si bien no se hace mención explicita a delitos relativos a los nombres de dominio o a la actividad de ciberocupación, el Articulo 283 condena la divulgación de información falsa o alterada sobre un competidor o uso de cualquier método fraudulento para desviar en favor propio o de un tercero la clientela ajena, siempre que cause perjuicio.

El Título VIII, Capítulo I se refiere a los Delitos contra la Seguridad Informática, en los cuales se condenan las conductas como el ingreso, uso, apoderamiento, copia, modificación, interferencia, intercepción, obstaculización o impedimento de transmisión de una base de datos, red o sistema informático.

4.3 República Dominicana

El gobierno de la República Dominicana emitió la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. En uno de sus motivos se expone la necesidad de prever los crímenes y delitos relacionados con las tecnologías de información y comunicación en la legislación penal dominicana a fin de poder sancionar a los autores de tales acciones. Con lo cual es necesaria la tipificación y adopción de mecanismos para el combate de tales crímenes, facilitando la cooperación entre el Estado y el sector privado en términos de detección, investigación y sanción a nivel nacional de este tipo de crímenes, estableciendo además disposiciones que permitan una cooperación internacional fiable y rápida.

En dicha Ley, se tomó en cuenta, entre otras leyes y tratados internacionales, el Convenio sobre la Ciberdelincuencia del Consejo de Europa.

En términos de propiedad intelectual, el Capítulo III trata sobre esta materia y en su Artículo 25 menciona lo siguiente:

CAPÍTULO III
DELITOS DE PROPIEDAD INTELECTUAL Y AFINES

> *Artículo 25.- Delitos Relacionados a la Propiedad Intelectual y Afines. Cuando las infracciones establecidas en la Ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la Ley No.65-00, del 21 de agosto del año 2000, sobre Derecho de Autor, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones para estos actos ilícitos.*

Con esto, la Ley dominicana cumplió con lo establecido en el Artículo 10, párrafos 1 y 2 del Convenio sobre la Ciberdelincuencia ya que como Estado Parte, adoptó las medidas legislativas para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina la legislación de conformidad con las obligaciones que haya contraído en aplicación del Acta de París, los ADPIC, del Tratado de la OMPI sobre Derecho de Autor y de la Convención de Roma.

La Ley No. 20-00 en el Título V, Capítulo único trata sobre las Infracciones, Procedimiento, Sanciones y Prescripción de los Derechos de Propiedad Industrial.

El Artículo 166 trata sobre las sanciones que son las siguientes:

Artículo 166.- De las sanciones.
Incurren en prisión correccional de tres meses a dos años y multa de diez a cincuenta salarios mínimos o ambas penas quienes intencionalmente:
a) Sin el consentimiento del titular de un signo distintivo use en el comercio un signo idéntico o una marca registrada, o una copia servil o una imitación fraudulenta de esa marca, en relación a los productos o servicios que ella distingue, o a productos o servicios relacionados;
b) Sin el consentimiento del titular de un signo distintivo realice respecto a un nombre comercial, un rótulo o un emblema con las siguientes actuaciones:
i) Use en el comercio un signo distintivo idéntico, para un negocio idéntico o relacionado;
ii) Use en el comercio un signo distintivo parecido, cuando ello fuese susceptible de crear confusión;
c) Use en el comercio, con relación a un producto o a un servicio, una indicación geográfica falsa o susceptible de engañar al público sobre la procedencia de ese producto o servicio o sobre la identidad del productor, fabricante o comerciante del producto o servicio;
d) Use en el comercio, con relación a un producto, una denominación de origen falsa o engañosa o la imitación de una denominación de origen, aun cuando se indique el verdadero origen de producto, se emplee una tradición de la denominación de origen o se use la denominación de origen acompañada de expresiones como "tipo", "género", "manera", "incautación" y otras calificaciones análogas;
e) Continúe usando una marca no registrada parecida en grado de confusión a otra registrada o después de que la sanción administrativa impuesta por esta razón sea definitiva;
f) Ofrezca en venta o ponga en circulación los productos o prestar los servicios con las marcas a que se refiere la infracción anterior;
g) Fabrique o elabore productos amparados por una patente de invención o modelo de utilidad, sin consentimiento de su titular o sin la licencia respectiva;
h) Ofrezca en venta o ponga en circulación productos amparados por una patente de invención o modelo de utilidad, a sabiendas de

que fueron fabricados o elaborados sin consentimiento del titular de la patente o registro o sin la licencia respectiva;

i) Utilice procesos patentados, sin el consentimiento del titular de la patente o sin la licencia respectiva;

j) Ofrezca en venta, venda o utilice, importe o almacene productos que sean resultado directo de la utilización de procesos patentados, a sabiendas de que fueron utilizados sin el consentimiento del titular de la patente o de quien tuviera una licencia de explotación;

k) Reproduzca o imite diseños industriales protegidos por un registro, sin consentimiento de su titular o sin la licencia respectiva;

l) Sin ser titular de una patente o modelo de utilidad o no gozando ya de los derechos conferidos por los mismos, se sirve en sus productos o en su propaganda de denominaciones susceptibles de inducir al público en error en cuanto a la existencia de ellos;

ll) Oculte o suministre falsa información a la Oficina Nacional de la Propiedad Industrial con el objetivo de obtener una patente que no cumple con los requisitos de patentabilidad.

No obstante, en el Título V de la Ley No. 20-00 no se mencionan infracciones a través de medio electrónicos.

Por otra Parte, la Ley No.65-00 de Derecho de Autor en su Título XIII trata sobre las Violaciones al Derecho de Autor y Derechos Afines y como sanciones menciona las siguientes:

DE LAS SANCIONES

Art. 169.- Incurre en prisión correccional de tres meses a tres años y multa de cincuenta a mil salarios mínimos, quien:

1) *En relación con una obra literaria, artística o científica, interpretación o ejecución artística, producción fonográfica o emisión de radiodifusión, la inscriba en el registro o la difunda por cualquier medio como propia, en todo o en parte, textualmente o tratando de disimularla mediante alteraciones o supresiones, atribuyéndose o atribuyendo a otro la autoría o la titularidad ajena;*
2) *En relación con una obra literaria, artística o científica, interpretación o ejecución artística, producción fonográfica o emisión de radiodifusión, y sin autorización expresa:*

a) La modifique, total o parcialmente;

b) La reproduzca, en forma total o parcial, por cualquier medio o en cualquier forma;

c) La distribuya mediante venta, alquiler o de cualquier otra manera;

d) La comunique o difunda, por cualesquiera de los medios de comunicación pública reservados al titular del respectivo derecho;

e) La reproduzca, distribuya o comunique en mayor número que el autorizado en forma expresa;

f) Conociendo el origen ilícito de la copia o reproducción, la distribuya al público, o la almacene, oculte, introduzca en el país o la saque de éste; o,

g) La reproduzca, distribuya o comunique por cualquier medio, después de vencido el término de la cesión o la licencia concedida;

3) Dé a conocer una obra inédita o no divulgada, que haya recibido en confianza del autor o su causahabiente, o de alguien en su nombre, sin la autorización para la divulgación otorgada por el titular del derecho;

4) En relación con una obra literaria, artística o científica, interpretación o ejecución artística, producción fonográfica o emisión de radiodifusión, se atribuya falsamente la cualidad de titular, originario o derivado, de cualesquiera de los derechos reconocidos en la presente ley y, con esa indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación o ejecución, producción;

5) Comunique, reproduzca o distribuya la obra, interpretación o ejecución artística, producción fonográfica o emisión de radiodifusión, por cualquier medio o procedimiento, suprimiendo o alterando el nombre o seudónimo del autor, del artista intérprete o ejecutante, del productor fonográfico o del organismo de radiodifusión, según los casos;

6) Comunique, reproduzca o distribuya la obra, interpretación o ejecución artística, producción fonográfica o emisión de radiodifusión, por cualquier medio o procedimiento, con alteraciones o supresiones capaces de atentar contra el decoro de la misma o contra la reputación de su respectivo titular;

7) Presente declaraciones falsas en cuanto a certificaciones de ingresos; asistencia de público; repertorio utilizado; identificación de los autores o artistas intérpretes o ejecutantes; autorización obtenida; número de ejemplares reproducidos o distribuidos; o toda adulteración de datos susceptibles de causar perjuicio a cualesquiera de los titulares de derechos reconocidos por la presente ley;

8) Fabrique, ensamble, importe, modifique, venda o ponga de cualquier otra manera en circulación, dispositivos, sistemas o equipos capaces de soslayar o desactivar otro dispositivo destinado a impedir o restringir la realización de copias de la obra, interpretación o ejecución, producción o emisión, o a menoscabar la calidad de las copias realizadas; o capaz de eludir o desactivar otro dispositivo destinado a impedir o controlar la recepción de programas transmitidos a través de las telecomunicaciones, alámbricas o inalámbricas, o de cualquier otra forma al público, por parte de aquellos no autorizados para esa recepción;

9) Altere, elimine o eluda, de cualquier forma, los dispositivos o medios técnicos introducidos en las obras, interpretaciones o ejecuciones, producciones o emisiones protegidas, que impidan o restrinjan la reproducción o el control de las mismas, o realice cualquiera de dichos actos en relación con las señales codificadas, dirigidas a restringir la comunicación por cualquier medio de las obras, interpretaciones o ejecuciones, producciones o emisiones;

10) Suprima o altere sin autorización cualquier información electrónica sobre la gestión colectiva de los derechos reconocidos en esta ley, o distribuya, importe para su distribución, emita, comunique o ponga a disposición del público, sin autorización, obras, interpretaciones o ejecuciones o producciones, sabiendo que la información electrónica sobre la gestión de los derechos correspondientes ha sido suprimida o alterada sin autorización;

11) Utilice de cualquier otra manera una obra, interpretación o ejecución, producción o emisión, de manera tal que infrinja uno de los derechos patrimoniales exclusivos reconocidos por la presente ley.

En este caso, los párrafos 8 a 10 abarcan sanciones pertinentes aplicables cuando se vulneren las medidas de protección tecnológicas.

4.4 Perú

Perú no es un Estado Parte del Convenio de ciberdelincuencia, sin embargo, cuenta con legislación específica sobre delitos informáticos cuyo objetivo es el prevenir y sancionar las conductas ilícitas que afecten los sistemas informáticos y

otros viene jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de a información o de la comunicación. Con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

En la Ley de Delitos Informáticos de Perú, se contemplan delitos contra datos y sistemas informáticos, delitos informáticos contra la indemnidad y libertad sexuales, delitos informáticos contra la intimidad y el secreto de las comunicaciones, delitos informáticos contra el patrimonio, y delitos informáticos contra la fe pública.

En materia de propiedad intelectual, la Ley de Delitos Informáticos de Perú no menciona explícitamente algún delito en particular. No obstante, el Artículo 10 establece multas por el abuso de mecanismos y dispositivos informáticos. Dicho artículo contempla lo siguiente:

> *"El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días de multa".*

A partir de la lectura del Artículo 10, pudiera inferirse que una persona que vulnere los sistemas de gestión de derechos estaría sujeta a multa.

Por otra parte, y con excepción de lo comentado respecto al Artículo 10, la Ley de Delitos Informáticos de Perú no hace mención a delitos referidos a marcas registradas o derechos de autor a través de medios electrónicos.

4.5 Legislación mexicana en materia de Propiedad Intelectual

En México se cuenta específicamente con la Ley de la Propiedad Industrial (LPI) la cual de acuerdo a su Artículo 2º, Fracción V menciona como uno de sus objetivos el proteger la propiedad industrial mediante la regulación y otorgamiento de

patentes de invención; registros de modelos de utilidad, diseños industriales, marcas, y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen, y regulación de secretos industriales.

La LPI contempla en su Título Séptimo la Inspección, Infracciones y Sanciones Administrativas de los Delitos.

El Artículo 213 considera como infracciones administrativas las siguientes:

I.- Realizar actos contrarios a los buenos usos y costumbres en la industria, comercio y servicios que impliquen competencia desleal y que se relacionen con la materia que esta Ley regula;

II.- Hacer aparecer como productos patentados aquéllos que no lo estén. Si la patente ha caducado o fue declarada nula, se incurrirá en la infracción después de un año de la fecha de caducidad o, en su caso, de la fecha en que haya quedado firme la declaración de nulidad;

III.- Poner a la venta o en circulación productos u ofrecer servicios, indicando que están protegidos por una marca registrada sin que lo estén. Si el registro de marca ha caducado o ha sido declarado nulo o cancelado, se incurrirá en infracción después de un año de la fecha de caducidad o en su caso, de la fecha en que haya quedado firme la declaración correspondiente;

IV.- Usar una marca parecida en grado de confusión a otra registrada, para amparar los mismos o similares productos o servicios que los protegidos por la registrada;

V.- Usar, sin consentimiento de su titular, una marca registrada o semejante en grado de confusión como elemento de un nombre comercial o de una denominación o razón social, o viceversa, siempre que dichos nombres, denominaciones o razones sociales estén relacionados con establecimientos que operen con los productos o servicios protegidos por la marca;

VI.- Usar, dentro de la zona geográfica de la clientela efectiva o en cualquier parte de la República, en el caso previsto por el artículo 105 de esta Ley, un nombre comercial idéntico o semejante en grado de

confusión, con otro que ya esté siendo usado por un tercero, para amparar un establecimiento industrial, comercial o de servicios del mismo o similar giro;

VII.- Usar como marcas las denominaciones, signos, símbolos, siglas o emblemas a que se refiere el artículo 4o. y las fracciones VII, VIII, IX, XII, XIII, XIV y XV del artículo 90 de esta Ley;

VIII.- Usar una marca previamente registrada o semejante en grado de confusión como nombre comercial, denominación o razón social o como partes de éstos, de una persona física o moral cuya actividad sea la producción, importación o comercialización de bienes o servicios iguales o similares a los que se aplica la marca registrada, sin el consentimiento, manifestado por escrito, del titular del registro de marca o de la persona que tenga facultades para ello;

IX.- Efectuar, en el ejercicio de actividades industriales o mercantiles, actos que causen o induzcan al público a confusión, error o engaño, por hacer creer o suponer infundadamente:

a).- La existencia de una relación o asociación entre un establecimiento y el de un tercero;

b).- Que se fabriquen productos bajo especificaciones, licencias o autorización de un tercero;

c).- Que se prestan servicios o se venden productos bajo autorización, licencias o especificaciones de un tercero;

d) Que el producto de que se trate proviene de un territorio, región o localidad distinta al verdadero lugar de origen, de modo que induzca al público a error en cuanto al origen geográfico del producto;

X.- Intentar o lograr el propósito de desprestigiar los productos, los servicios, la actividad industrial o comercial o el establecimiento de otro. No estará comprendida en esta disposición, la comparación de productos o servicios que ampare la marca con el propósito de informar al público, siempre que dicha comparación no sea tendenciosa, falsa o

exagerada en los términos de la Ley Federal de Protección al Consumidor;

XI.- Fabricar o elaborar productos amparados por una patente o por un registro de modelo de utilidad o diseño industrial, sin consentimiento de su titular o sin la licencia respectiva;

XII.- Ofrecer en venta o poner en circulación productos amparados por una patente o por un registro de modelo de utilidad o diseño industrial, a sabiendas de que fueron fabricados o elaborados sin consentimiento del titular de la patente o registro o sin la licencia respectiva;

XIII.- Utilizar procesos patentados, sin consentimiento del titular de la patente o sin la licencia respectiva;

XIV.- Ofrecer en venta o poner en circulación productos que sean resultado de la utilización de procesos patentados, a sabiendas que fueron utilizados sin el consentimiento del titular de la patente o de quien tuviera una licencia de explotación;

XV.- Reproducir o imitar diseños industriales protegidos por un registro, sin el consentimiento de su titular o sin la licencia respectiva;

XVI.- Usar un aviso comercial registrado o uno semejante en grado de confusión, sin el consentimiento de su titular o sin la licencia respectiva para anunciar bienes, servicios o establecimientos iguales o similares a los que se aplique el aviso;

XVII.- Usar un nombre comercial o uno semejante en grado de confusión, sin el consentimiento de su titular o sin la licencia respectiva, para amparar un establecimiento industrial, comercial o de servicios del mismo o similar giro;

XVIII.- Usar una marca registrada, sin el consentimiento de su titular o sin la licencia respectiva, en productos o servicios iguales o similares a los que la marca se aplique;

XIX.- Ofrecer en venta o poner en circulación productos iguales o similares a los que se aplica una marca registrada, a sabiendas de que se usó ésta en los mismos sin consentimiento de su titular;

XX.- Ofrecer en venta o poner en circulación productos a los que se aplica una marca registrada que hayan sido alterados;

XXI.- Ofrecer en venta o poner en circulación productos a los que se aplica una marca registrada, después de haber alterado, sustituido o suprimido parcial o totalmente ésta;

XXII.- Usar sin autorización o licencia correspondiente una denominación de origen;

XXIII.- Reproducir un esquema de trazado protegido, sin la autorización del titular del registro, en su totalidad o cualquier parte que se considere original por sí sola, por incorporación en un circuito integrado o en otra forma;

XXIV. Importar, vender o distribuir en contravención a lo previsto en esta Ley, sin la autorización del titular del registro, en cualquier forma para fines comerciales:

a) Un esquema de trazado protegido;

b) Un circuito integrado en el que esté incorporado un esquema de trazado protegido, o

c) Un bien que incorpore un circuito integrado que a su vez incorpore un esquema de trazado protegido reproducido ilícitamente;

XXV. No proporcionar al franquiciatario la información, a que se refiere el artículo 142 de esta Ley, siempre y cuando haya transcurrido el plazo para ello y haya sido requerida;

XXVI.- Usar la combinación de signos distintivos, elementos operativos y de imagen, que permitan identificar productos o servicios iguales o similares en grado de confusión a otros protegidos por esta Ley y que por su uso causen o induzcan al público a confusión, error o engaño, por hacer creer o suponer la existencia de una relación entre el titular de los derechos protegidos y el usuario no autorizado. El uso de tales elementos operativos y de imagen en la forma indicada constituye competencia desleal en los términos de la fracción I de este mismo artículo;

XXVII. Cuando el titular de una patente o su licenciatario, usuario o distribuidor, inicie procedimientos de infracción en contra de uno o más terceros, una vez que el Instituto haya determinado, en un procedimiento administrativo anterior que haya causado ejecutoria, la inexistencia de la misma infracción;

XXVIII. Impedir el acceso al personal comisionado para practicar visitas de inspección, en términos de lo establecido en el artículo 206 de esta Ley;

XXIX. No proporcionar información, sin causa justificada, y datos al Instituto cuando los requiera en ejercicio de la atribución prevista en la fracción I del artículo 203, y

XXX. Las demás violaciones a las disposiciones de esta Ley que no constituyan delitos.

De lo anterior, puede notarse que el Artículo 213 de la LPI no contempla el uso de medios electrónicos para el engaño como infracción administrativa de marca.

Por otra parte, el Artículo 223 contempla como delitos a las siguientes conductas:

I. Reincidir en las conductas previstas en las fracciones II a XXII del artículo 213 de esta Ley, una vez que la primera sanción administrativa impuesta por esta razón haya quedado firme;

II. Falsificar, en forma dolosa y con fin de especulación comercial, marcas protegidas por esta Ley;

III. Producir, almacenar, transportar, introducir al país, distribuir o vender, en forma dolosa y con fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por esta Ley, así como aportar o proveer de cualquier forma, a sabiendas, materias primas o insumos destinados a la producción de objetos que ostenten falsificaciones de marcas protegidas por esta Ley;

IV. Revelar a un tercero un secreto industrial, que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en virtud del otorgamiento de una licencia para su uso, sin consentimiento de la persona que guarde el secreto industrial, habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto;

V. Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que lo guarde o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o a su usuario autorizado, y

VI. Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o relación de negocios, sin consentimiento de quien lo guarde o de su usuario autorizado, o que le haya sido revelado por un tercero, a sabiendas que éste no contaba para ello con el consentimiento de la persona que guarde el secreto industrial o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o su usuario autorizado.

Los delitos previstos en este artículo se perseguirán por querella de parte ofendida.

Sin embargo, el Artículo 223 no hace mención al uso de marcas por medios electrónicos para inducir al engaño.

Asimismo, la Ley Federal del Derecho de Autor (LFDA) en su Artículo 1º establece que tiene por objeto la salvaguarda y promoción del acervo cultural de la Nación; protección de los derechos de los autores, de los artistas intérpretes o ejecutantes, así como de los editores, de los productores y de los organismos de

radiodifusión, en relación con sus obras literarias o artísticas en todas sus manifestaciones, sus interpretaciones o ejecuciones, sus ediciones, sus fonogramas o videogramas, sus emisiones, así como de los otros derechos de propiedad intelectual.

El Título XII de la LFDA en su Capítulo I menciona las Infracciones en Materia de Derechos de Autor. El Artículo 229 establece las siguientes infracciones:

I. Celebrar el editor, empresario, productor, empleador, organismo de radiodifusión o licenciatario un contrato que tenga por objeto la transmisión de derechos de autor en contravención a lo dispuesto por la presente Ley;

II. Infringir el licenciatario los términos de la licencia obligatoria que se hubiese declarado conforme al artículo 146 la presente Ley;

III. Ostentarse como sociedad de gestión colectiva sin haber obtenido el registro correspondiente ante el Instituto;

IV. No proporcionar, sin causa justificada, al Instituto, siendo administrador de una sociedad de gestión colectiva los informes y documentos a que se refieren los artículos 204 fracción IV y 207 de la presente Ley;

V. No insertar en una obra publicada las menciones a que se refiere el artículo 17 de la presente Ley;

VI. Omitir o insertar con falsedad en una edición los datos a que se refiere el artículo 53 de la presente Ley;

VII. Omitir o insertar con falsedad las menciones a que se refiere el artículo 54 de la presente Ley;

VIII. No insertar en un fonograma las menciones a que se refiere el artículo 132 de la presente Ley;

IX. Publicar una obra, estando autorizado para ello, sin mencionar en los ejemplares de ella el nombre del autor, traductor, compilador, adaptador o arreglista;

X. Publicar una obra, estando autorizado para ello, con menoscabo de la reputación del autor como tal y, en su caso, del traductor, compilador, arreglista o adaptador;

XI. Publicar antes que la Federación, los Estados o los Municipios y sin autorización las obras hechas en el servicio oficial;

XII. Emplear dolosamente en una obra un título que induzca a confusión con otra publicada con anterioridad;

XIII. Fijar, representar, publicar, efectuar alguna comunicación o utilizar en cualquier forma una obra literaria y artística, protegida conforme al capítulo III, del Título VII, de la presente Ley, sin mencionar la comunidad o etnia, o en su caso la región de la República Mexicana de la que es propia, y

XIV. Las demás que se deriven de la interpretación de la presente Ley y sus reglamentos.

No obstante, el Artículo 229 no contempla la elusión de sistemas o medidas de protección tecnológicas.

Además, el mismo Título en su Capítulo II contempla las Infracciones en Materia de comercio en donde el Artículo 231 menciona las siguientes infracciones:

I. Comunicar o utilizar públicamente una obra protegida por cualquier medio, y de cualquier forma sin la autorización previa y expresa del autor, de sus legítimos herederos o del titular del derecho patrimonial de autor;

II. Utilizar la imagen de una persona sin su autorización o la de sus causahabientes;

III. Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros, protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta ley;

IV. Ofrecer en venta, almacenar, transportar o poner en circulación obras protegidas por esta Ley que hayan sido deformadas, modificadas o mutiladas sin autorización del titular del derecho de autor;

V. Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación;

VI. Retransmitir, fijar, reproducir y difundir al público emisiones de organismos de radiodifusión y sin la autorización debida;

VII. Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular;

VIII. Usar o explotar un nombre, título, denominación, características físicas o psicológicas, o características de operación de tal forma que induzcan a error o confusión con una reserva de derechos protegida;

IX. Utilizar las obras literarias y artísticas protegidas por el capítulo III, del Título VII de la presente Ley en contravención a lo dispuesto por el artículo 158 de la misma, y

X. Las demás infracciones a las disposiciones de la Ley que impliquen conducta a escala comercial o industrial relacionada con obras protegidas por esta Ley.

Aunque el artículo 231 en su fracción I pudiera abarcar de manera general el intercambio de archivos ya que establece como infracción el comunicar o utilizar públicamente una obra protegida por cualquier medio, y de cualquier forma sin la autorización previa y expresa del autor, de sus legítimos herederos o del titular del derecho patrimonial de autor, sería conveniente que se hiciera mención explícita del intercambio de archivos como delito referentes a la infracción de derechos de autor.

Capítulo 5

Implicaciones

Capítulo 5: Implicaciones

Como se ha visto con otros países que se han adherido al citado Convenio, a fin de cumplir con lo establecido en el Artículo 10 del mismo, será necesario que en México las infracciones de propiedad intelectual contenidas en la LPI y LFDA sean tipificadas como delito cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

Asimismo, deben tipificarse en la legislación las conductas consideradas como delictivas en materia de derechos de autor y marcas en el ámbito digital.

Como se describió anteriormente, los delitos referentes a la infracción de derechos de autor comprenden el intercambio de archivos a través de sistemas de intercambio de archivos y la elusión de los sistemas de gestión de derechos en el ámbito digital.

En referencia al intercambio de archivos el artículo 229 no hace mención a dicha actividad. No obstante, el artículo 231 en su fracción I pudiera abarcar de manera general el intercambio de archivos ya que establece como infracción el comunicar o utilizar públicamente una obra protegida por cualquier medio, y de cualquier forma sin la autorización previa y expresa del autor, de sus legítimos herederos o del titular del derecho patrimonial de autor.

Sin embargo, sería conveniente incluir de manera explícita los delitos referentes a la infracción de derechos de autor que comprenden el intercambio de archivos.

En materia de elusión de los sistemas de gestión, el artículo 231 en su fracción V hace mención como infracción a: importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Sin embargo, es conveniente que también se incluyan de manera explícita las actividades que vulneren los TPMs.

Por otra parte los delitos referentes a la infracción de marcas comprenden el uso de las marcas en actividades delictivas para inducir engaño a las víctimas; y el uso de la marca para el registro de nombre de dominio.

En cuestión del uso de las marcas para inducir engaño con fines delictivos, el artículo 213 en su fracción IX, contempla el engaño como infracción administrativa de marca. Sin embargo, no se hace mención al uso de medios electrónicos para llevar a cabo ésta actividad.

Considerando que con la adhesión al Convenio los supuestos descritos en el artículo 213 deberán contemplarse también en el ámbito electrónico, esta conducta quedaría cubierta.

Finalmente, el uso de marca para el registro de nombre de dominio, no está contemplado en la legislación en materia de propiedad intelectual. No obstante, la empresa AKKY maneja menciona en sus políticas los procedimientos a seguir en caso de disputas de nombres de dominio de propiedad intelectual.

Capítulo 6. Conclusiones

Capítulo 6. Conclusiones

El Internet ha propiciado grandes avances en el intercambio de información para hacer más eficientes y rápidos los procesos de comunicación.

Sin embargo, el Internet ha permitido que los delincuentes saquen provecho de la falta de legislación en algunos países o de la omisión de ciertas actividades como delitos para llevar a cabo delitos por medios electrónicos que comprometen la información contenida de forma digital. Entre esta información, se encuentra la vulneración de la propiedad intelectual referente a derechos de autor y marcas.

En este sentido, a nivel internacional se han llevado diversas actividades para lograr una armonización legal entre los países, a fin de combatir a los delitos que se comenten por medios electrónicos.

En cuestión de tratados internacionales, el Convenio de Budapest es hasta ahora el único tratado que atiende la problemática de los delitos informáticos y entre los cuales se contemplan los delitos relacionados con infracciones de propiedad intelectual y de los derechos afines.

La adhesión al Convenio supone una mejor cooperación entre los Estados Parte, ya que se tipifican de forma común las actividades delictivas por medios electrónicos, se permite el intercambio de información entre jurisdicciones para localizar a los delincuentes informáticos y se implementan procedimientos para penalizar los delitos cometidos por medios electrónicos.

Si bien México cuenta con legislación en materia de Derechos de Autor y Propiedad Industrial referida a marcas, tal legislación no abarca en su totalidad o de forma explicita la infracción o penalización de actividades que vulneren la propiedad intelectual por medios electrónicos.

Por tanto, la adhesión de México al Convenio de Budapest generaría reformas en la legislación en materia de propiedad intelectual que estarían encaminadas a contemplar los delitos informáticos que vulneren los derechos de propiedad intelectual con su respectiva penalización. De esta manera, se proveería un ambiente de certeza y seguridad tanto a los titulares de derechos de propiedad intelectual como, además, al sector público y privado. Con lo cual se

fomentará en México la innovación, la creación de contenidos, generación de conocimiento y valor agregado, y sobre todo, se asegure un ambiente que propicie el comercio electrónico.

Capítulo 7. Propuesta

Capítulo 7. Propuesta

Los delitos cometidos a través de medios informáticos obligan a que las legislaciones en general se armonicen con el fin de que sea posible dar seguimiento a las conductas delictivas y lo más importante, aprehender a los delincuentes y aplicar las penas respectivas.

En materia de propiedad intelectual, es importante que las legislaciones en la materia contemplen tanto la comisión de delitos referentes a derechos de autor y marcas a través de medios informáticos como también las sanciones a las cuales son sujetas dichas conductas.

Una Ley que contemple estos escenarios, cumpliría por anticipado con una parte de los requerimientos descritos en el Convenio de Ciberdelincuencia. Como supuestos adicionales a la armonización, la legislación debe contemplar la afirmación de la jurisdicción del Estado respecto de cualquier delito y la cooperación internacional con otros países para que sea posible realizar las investigaciones o procedimientos relativos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

Por lo anterior, la adhesión al Convenio de Ciberdelincuencia sirve como un medio para facilitar la reforma de las legislaciones de manera que se contemple la tipificación de conductas delictivas por medios informáticos y se permita tener un medio para realizar las investigaciones y procedimientos relativos. En cuestión de propiedad intelectual en México, si bien las reformas pertinentes a la Ley de Propiedad Industrial y Ley Federal de Derechos de Autor pueden realizarse sin la necesidad de adhesión al Convenio de Ciberdelincuencia, cabe mencionar que dicha adhesión obligaría al Estado Mexicano a realizar tales reformas. Esto significaría un beneficio hacia la sociedad e incuso hacia el gobierno toda vez que México contaría con un sistema legal armonizado que le permita hacer frente a las amenazas cibernéticas que afectan hoy en día a muchos ciudadanos y empresas privadas.

Bibliografía

Becerra, Manuel. 2004. *La Propiedad Intelectual en Transformación*. México. UNAM, Instituto de Investigaciones Jurídicas.

Chamizo García, Juan Manuel, *et al.* 2006. *Servicios electrónicos para la sociedad de la información: Desarrollo de grandes aplicaciones distribuidas sobre Internet*. España. Publicaciones Universidad de Alicante.

Coughlan, Steve, *et.al.*, June 23, 2006. *Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization*, Canada. Dalhousie Law School.

El Ciberdelito: *Guía para los Países en Desarrollo*. Proyecto de Abril de 2009. UIT.

Díaz Barrado, Cástor M. 2004. *El derecho internacional del tiempo presente*. Madrid. Dykinson S.L.

Esteve González, Lydia. 2006. *Aspectos internacionales de las infracciones de derechos de autor en Internet*. In: Colección Ciencia jurídica y derecho internacional. Granada. Editorial Comares.

Gibson, William. 1984. *Neuromancer*. U.S. Ace Books.

Karake Shalhub, Zeinab. 2010. *Cyber Law and Cyber Security in Developing and Emerging Economies*. UK. Edward Elgar Publishing Limited.

Kostopoulos, George K. 2013. *Cyberspace and Cybersecurity*. U.S. CRC Press.

Nava Garcés, Alberto. 2007. *Delitos Informáticos*. 2ª. ed. México. Porrúa.

Nava Garcés, Alberto. 2011. *La prueba electrónica en materia Penal*. 1ª. ed. México. Porrúa.

Téllez Valdés, Julio. 2009. *Derecho Informático*. 4ª. ed. México. Mc Graw Hill.

Toren, Peter. 2005. *Intellectual Property and Computer Crimes*. U.S. ALM Properties Inc.

ARTÍCULOS

Cassou Ruiz, Jorge Esteban. 2009. Delitos informáticos en México. Revista del Instituto de la Judicatura Federal, No. 28.

De Sola Quintero, René, *Delitos Informáticos*. Disponible en: http://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

Doyle, Charles. December 27, 2010. *Senior Specialist in American Public Law*. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Disponible en: http://fas.org/sgp/crs/misc/97-1025.pdf

Jo-Ann M. Adams. 1996. *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 Santa Clara High Tech. L.J. 403. Disponible en: http://digitalcommons.law.scu.edu/chtlj/vol12/iss2/5

Kleinrock, Leonard. January-February 2002. *Creating a mathematical theory of computer networks*, Operations Research, Vol. 50, No. 1.

Rodríguez Bernal, Antonio Pedro. Septiembre de 2006. *Los cibercrímenes en el espacio de libertad, seguridad y justicia*. Disponible en: http://www.alfa-redi.org/sites/default/files/articles/files/rodriguez.pdf

Stephanos Androutsellis-Theotokis and Diomidis Spinellis. December 2004. A survey of peer-to-peer content distribution technologies. *ACM Computing Surveys*, 36(4):335–371.

LEGISLACIONES

Estados Unidos:
Anti-terrorism Act “ATA”, CAM SPAM, 1-1-04.
Fraud and related activity in connection with computer – 18 USC 1030 (The Computer Fraud and Abuse Act).

México:
Ley de la Propiedad Industrial.
Ley Federal del Derecho de Autor.

Panamá:

Código Penal de Panamá.

Perú:
Ley de Delitos Informáticos de Perú.

República Dominicana:
Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología.
Ley No. 20-00.
Ley No.65-00 de Derecho de Autor.

CONVENIOS INTERNACIONALES
Convenio de Lanzarote.
Convenio sobre la Ciberdelincuencia.
Convenio de Berna para la Protección de las Obras Literarias y Artísticas.
Tratado de la OMPI sobre Derecho de Autor.
Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas.