



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

**LA APLICACIÓN E IMPORTANCIA DEL DERECHO
INFORMÁTICO EN MÉXICO**

TESIS PROFESIONAL

MAYRA GUADALUPE ROJO SÁNCHEZ

VIRIDIANA ZAMORA BOLAÑOS



MÉXICO, D.F.

2013



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

**LA APLICACIÓN E IMPORTANCIA DEL DERECHO
INFORMÁTICO EN MÉXICO**

**TESIS PROFESIONAL
QUE PARA OBTENER EL TÍTULO DE:**

LICENCIADO EN INFORMÁTICA

PRESENTA:

MAYRA GUADALUPE ROJO SÁNCHEZ

VIRIDIANA ZAMORA BOLAÑOS

ASESORA:

DRA. GRACIELA BRIBIESCA CORREA



MÉXICO, D.F.

2013

AGRADECIMIENTOS

Agradecemos infinitamente a Dios por dejarnos llegar a este punto de nuestra vida y realización personal.

A los maestros, que con sus bases nos alimentaron el espíritu de superación y amor a nuestra profesión.

A la Dra. Graciela, por ser una excelente persona y maestra, sin su apoyo y afecto esta meta no habría sido lograda, de igual manera que con su paciencia nos alentó a seguir a adelante.

A la Universidad Nacional Autónoma de México, por darnos la oportunidad de adquirir nuevos conocimientos además de gozar como alumnas a esta Institución

Simplemente... Gracias.

INDICE

INTRODUCCIÓN.....	8
MATRIZ DE CONGRUENCIA	12
METODOLOGIA	13
PLANTEAMIENTO DEL PROBLEMA.....	13
PREGUNTA DE INVESTIGACIÓN.....	13
DESARROLLO	13
OBJETIVO.....	14
ALCANCE.....	14
RESULTADOS	14
CAPITULO 1. MARCO TEÓRICO	15
1.1 DERECHO INFORMÁTICO	15
1.1.1 CONCEPTO DE DERECHO INFORMÁTICO	15
1.1.2 VERTIENTES DEL DERECHO INFORMÁTICO	17
1.1.2.1 Informática Jurídica.....	17
1.1.2.1.1 Informática jurídica documental	18
1.1.2.1.2 Informática jurídica de gestión	19
1.1.2.1.3 Informática jurídica metadecisional.....	19
1.1.2.2 Derecho de la Informática.....	21
1.1.2.2.1 La protección jurídica de la información personal	21
1.1.2.2.2 La protección jurídica del software	22
1.1.2.2.3 El flujo de datos transfrontera	23
1.1.2.2.4 Los convenios o contratos informáticos.....	23
1.1.2.2.5 Los delitos informáticos	24
1.1.2.2.6 Valor probatorio del documento electromagnético	25
1.2 DERECHO INFORMÁTICO EN MÉXICO.....	26
1.2.1 ACUERDOS INTERNACIONALES SUSCRITOS POR MÉXICO	26
1.2.1.1 El Tratado de Libre Comercio de América del Norte (TLCAN o NAFTA). 27	
1.2.1.2 Acuerdo de Propiedad Intelectual en relación con el Comercio o ADPIC	27
1.2.1.3 Ley de derechos de autor o de copyright de cada país.....	28
1.2.1.4 CONVENIOS	30
1.2.1.4.1 El Convenio de Berna para la Protección de las Obras Literarias y	
Artísticas 31	
1.2.1.4.2 El Convenio que establece la Organización Mundial de la Propiedad	
Intelectual (OMPI).....	31

1.2.1.4.3	Convenio de París para la Protección Industrial del 20 de marzo de 1883	32
1.2.2	TRATADOS INTERNACIONALES CON LA PARTICIPACIÓN DE MÉXICO.....	32
1.2.2.1	El Tratado de la OMPI sobre Derecho de Autor (WCT).....	32
1.2.2.2	Tratado de cooperación en materia de patentes	33
1.2.2.3	Tratado de Singapur sobre el Derecho de Marcas.....	33
1.2.2.4	El Tratado de Libre Comercio de América del Norte (TLCAN o NAFTA).	34
APORTACIONES		35
CAPÍTULO 2. DELITOS INFORMÁTICOS EN GENERAL		38
2.1	CONCEPTO DE FRAUDE Y DELITO.....	38
2.2	CONCEPTO DE DELITO INFORMÁTICO	39
2.2.1	Efectos de los Delitos Informáticos en la Sociedad.....	40
2.2.2	Efectos de los Delitos Informáticos en la Economía	40
2.3	CARACTERÍSTICAS DEL DELITO INFORMÁTICO	41
2.3.1	Caracterización de los sujetos.....	43
2.3.1.1	Sujeto Activo	44
2.3.1.2	Sujeto Pasivo	45
2.4	CLASIFICACIÓN DE DELITO INFORMÁTICO.....	46
2.4.1	Legislación comparada sobre delitos informáticos.....	47
2.4.2	Regulación Nacional de los delitos informáticos	48
2.5	TIPOS DE DELITO INFORMÁTICO.....	48
2.6	PIRATAS INFORMÁTICOS.....	52
2.6.1	Hackers.....	54
2.6.2	Crackers.....	54
2.6.3	Lamers.....	54
2.6.4	Copyhackers	55
2.6.5	Bucaneros.....	55
2.6.6	Phreaker	55
2.6.7	Newbie	55
2.6.8	Script Kiddie	55
2.6.9	Casos de Hackers famosos a nivel mundial.....	56
2.7	PREVENCIÓN FRENTE A LOS DELITOS INFORMÁTICOS	60
2.7.1	Piratería Informática	60
2.7.2	Contratos informáticos	62

2.7.2.1	Tipos de contratos.....	63
	APORTACIONES.....	65
	CAPÍTULO 3. LEGISLACIÓN ACTUAL EN MÉXICO EN RELACIÓN AL DERECHO INFORMÁTICO	
	66
3.1	LEGISLACIÓN FEDERAL.....	66
3.1.1	CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.....	66
3.1.2	CÓDIGO PENAL FEDERAL.....	69
3.1.3	CÓDIGO CIVIL FEDERAL.....	75
3.1.4	CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES.....	78
3.1.5	CÓDIGO DE COMERCIO.....	79
3.1.6	LEY FEDERAL DEL PROCEDIMIENTO ADMINISTRATIVO.....	84
3.1.7	LEY FEDERAL DEL DERECHO DE AUTOR.....	86
3.1.8	LEY FEDERAL DE TELECOMUNICACIONES.....	92
3.1.9	LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.....	93
3.1.10	LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR.....	96
3.1.11	LEY DE LA PROPIEDAD INDUSTRIAL.....	99
3.1.12	LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES.....	100
3.2	LEGISLACIÓN ESTATAL.....	106
	CAPÍTULO 4. LA IMPORTANCIA DEL DERECHO INFORMÁTICO EN MÉXICO Y SU EVOLUCIÓN.....	129
4.1	PROBLEMÁTICA A NIVEL INTERNACIONAL.....	129
4.1.1	Tecnología y trabajo.....	131
4.1.2	Ética en la Informática.....	132
4.2	TENDENCIAS INTERNACIONALES DE LA INFORMÁTICA Y EL DERECHO.....	134
4.2.1	Tendencia Inicial o Básica:.....	134
4.2.2	Tendencia Creciente o Progresiva:.....	134
4.2.3	Tendencia Avanzada o Próspera.....	134
4.2.4	Tendencia Culminante o Innovadora.....	134
4.3	TENDENCIAS DE LA INFORMÁTICA Y EL DERECHO EN EL DERECHO COMPARADO	
	135	
4.3.1	Países con Tendencia Inicial-Creciente:.....	135
4.3.2	Países con Tendencia Avanzada o Próspera:.....	136
4.3.3	Países con Tendencias Culminante o Innovadora:.....	136

4.4	CASOS INTERNACIONALES	137
4.4.1	SOPA.....	137
4.4.2	ACTA	137
4.4.3	PIPA	138
4.5	EVOLUCIÓN DEL DERECHO INFORMÁTICO EN MÉXICO.....	138
4.5.1	Delitos informáticos en el ámbito Federal:.....	139
4.5.2	Delitos informáticos en el ámbito Local:.....	140
4.5.3	Policía cibernética en México.....	140
4.5.4	Gobierno Electrónico	141
4.5.5	Evolución del valor probatorio del documento electrónico	142
4.5.6	La Firma electrónica	143
4.5.7	El voto electrónico	145
4.5.8	Comercio electrónico	146
4.6	DERECHO INFORMÁTICO COMO MATERIA DE EDUCACIÓN EN MÉXICO	147
4.6.1	Primeros avances de Informática Jurídica en México.....	148
4.7	SITUACIÓN ACTUAL Y POSIBLES DIRECCIONES	149
	APORTACIONES	152
	CONCLUSIONES Y RECOMENDACIONES.....	153
	ANEXO	156
	BIBLIOGRAFIA GENERAL.....	164

INTRODUCCIÓN

El acelerado crecimiento tecnológico dio lugar a que la informática hoy en día sea necesaria para la sociedad; sin embargo, el desvío de su uso correcto y eficaz, conlleva a una serie de acciones jurídicas que tratan de reglamentarse mediante leyes y sanciones. Es aquí donde el Derecho Informático nace como una rama joven, fundamental y muy prometedora para un equilibrio social, cultural, y tecnológico.

El Derecho Informático ha tomado un nuevo rumbo para establecerse, consolidarse y actuar sobre actos ilícitos en referencia al uso de la tecnología en la sociedad. Esta nueva rama del Derecho, ha causado impacto a nivel social, económico y legislativo.

El Derecho ya no se aprecia como una ciencia tradicional, sino que ha tenido que adaptarse a la evolución tecnológica de hoy en día. Se busca que esta evolución tecnológica no afecte de manera directa la integridad de la sociedad en general, puesto que como se ha establecido, la tecnología existe en beneficio de la sociedad, mas no para su afectación, ni para un aprovechamiento ilícito y negativo hacia ambas partes.

En México existen actualmente 40 millones de usuarios de internet¹ y día con día esta cifra se ha ido incrementando. Retos, apenas ayer inexistentes que no requerían de una consideración jurídica, ahora son una realidad y que conllevan una serie de consecuencias; es decir, una trascendencia individual y social que no puede pasarse por alto.

Diversos fenómenos mundiales como las redes sociales, compras en línea o mejor llamado comercio electrónico, el trabajo a distancia, transferencias electrónicas y un sinfín de acciones a través de la tecnología que ayer se creían difíciles de alcanzar, hoy son ya una realidad, son hechos que nos obligan a mejorar paso a paso y firmemente la legislación informática en México y tener mejor comprensión del Derecho Informático. Países como Estados Unidos, Alemania, Argentina y Francia; entre otros, y en su mayoría europeos, han rebasado fronteras por impulsar un mejor uso de la tecnología por parte de la sociedad y que en caso contrario, sea lo suficientemente penado por quien lo comete. Ejemplos como esos son los que nos impulsan como estudiantes a analizar un tema en el que para México es apenas reconocible para la población y poco apoyado por las autoridades.

En el caso de México a través de los años, hemos visto que las acciones negativas e ilícitas ya sea beneficiándose de la tecnología o contra ella, se han visto rebasadas, dando como resultado que el mal manejo de la información sea una amenaza para la sociedad. Esas acciones negativas a

¹ INEGI, *Usuarios de Internet en México*, consultado en Marzo 20 del 2013 en <http://www.inegi.gob.mx/est/contenidos/espanol/temas/Sociodem/notatinf212.asp>

las que nos referimos son los llamados delitos informáticos, los cuales se han incrementado notablemente a nivel nacional e internacional; en México son delitos de los que en términos legislativos no se encuentran tipificados correctamente², o sencillamente no son lo suficientemente penados en el país. Ante la ausencia de una debida implementación en ley sobre delitos informáticos, se comprende el hecho de que México como país en vías de desarrollo no regule a la perfección las leyes tecnológicas; es entendible el rezago que existe debido a que el impacto de las TIC pasa por las decisiones de los gobiernos e impulsan su aplicación, lo que ha llevado a que estos procesos de decisión se transformen en un mecanismo lento y difícil³, por lo que, si las propias autoridades no desarrollan las suficientes iniciativas, no queda otra alternativa para la sociedad más que exigir los derechos como principales causantes de que la tecnología esté cada vez más relacionada a nuestra vida cotidiana. Los mexicanos como involucrados en los avances tecnológicos, deben estar preparados para una eficaz y correcta implementación de la información y sus herramientas informáticas principalmente a nivel social, y que en caso contrario, sean capaces de reconocer las acciones a implementar en términos jurídicos.

Como se mencionó anteriormente, la consecuencia de la falta de una ley en delitos informáticos, así mismo el poco seguimiento de normas y leyes en apoyo al Derecho Informático en México, han llevado a que la delincuencia cibernética sea astuta, difícil de castigar e imposibilita su persecución. Aunado a esto existe poca cultura de las buenas prácticas del usuario respecto al uso y aplicación de la tecnología informática; además de que algunas de las autoridades no poseen el nivel de experiencia requerido para las áreas tecnológicas⁴. Pese a esto, poco a poco se han establecido leyes en cuanto a tecnología e informática se refiere, protegiendo derechos y estableciendo obligaciones para quienes hacen uso de esta herramienta ya sea en términos laborales o personales. En mayo 17 de 1999⁵ por primera vez aparecieron en el Diario Oficial de la Federación aspectos relacionados con los delitos informáticos en México, se ha ido avanzando en forma lenta y superficial con la creación y reformas a las leyes en aspectos informáticos.

En años recientes se han elaborado leyes como la Ley Federal de Protección de Datos Personales, reformas constitucionales en materia informática, reformas al Código Penal Federal y Código Civil Federal en materia informática, Ley de Transparencia y Acceso a la Información Pública

² El Universal, *Rezagos en la tipificación y persecución de delitos informáticos*, Consultado en Marzo 20 del 2013 en <http://www.eluniversal.com.mx/cultura/69843.html>

³ Gamba Jacopo, *Panorama del derecho informático en América Latina y el Caribe*, CEPAL, Chile, 2010, p.6.

⁴ Aguilar Castillo, Gildardo, *Ética y Legislación Informática*, Universidad Veracruzana, p 1.

⁵ Landa Durán, Graciela M., *Los delitos informáticos en el Derecho penal de México y España*, España, 2007.

y la Ley Federal de Telecomunicaciones⁶; sin embargo no son suficientes mientras no se apliquen eficazmente, o no sean lo suficientemente penados por la ley; por lo que se espera que México tome las riendas para un correcto análisis de las diversas modificaciones necesarias en la legislación informática y las implementaciones necesarias a la misma, y que una vez implementadas, garanticen una continuidad, vigencia y sobre todo, un total entendimiento por quienes deben aplicarla.

Una correcta legislación requiere de un análisis profundo al impacto social, económico y educativo, para entonces determinar las necesidades, modificaciones, o en su caso, la creación de la misma para controlar aquellos factores que causan efectos negativos y se impulse a los positivos. Algunos de esos factores son considerados en **este trabajo de investigación**, con base en legislaciones, sus problemáticas y soluciones.

Existen diversos rubros que deben tomarse en cuenta para la correcta determinación en la legislación mexicana. No se debe indagar a fondo para saber que el surgimiento de la poca privacidad de información en las redes sociales, los ahora ya comunes fraudes informáticos, las grandes redes de pornografía infantil ahora también difundidas por medios informáticos, la nula atención a los aspectos laborales informáticos, las débiles propuestas de leyes informáticas, la falta de consideración en cuanto al valor probatorio de los documentos electrónicos, la regulación del comercio electrónico, la ausencia de neutralidad en la red, entre otros problemas que se pueden seguir enlistando, son día a día desafíos con los que el usuario debe enfrentarse para no ser víctima de éstos delitos informáticos, desafíos que pueden prevenirse informándose correctamente, en conjunto con los esfuerzos de los Estados e Instituciones que propicien una evolución en legislación informática, evitando una mayor propagación en delitos informáticos.⁷

Es por eso que en **este trabajo de investigación** se da un panorama del Derecho Informático en México, analizando desde su concepto, delitos, legislación, aplicación, evolución y su posible futuro, con base en la información existente, que aunque escasa; ya comienza a vislumbrarse. Se presenta una introducción de lo que significa el Derecho Informático a nivel nacional e internacional y su importancia, además de plasmar la actual legislación informática de México, en la que actualmente siguen existiendo deficiencias.

El objetivo en **este trabajo de investigación** es mostrar las deficiencias en Derecho Informático principalmente a nivel nacional; aportar a la sociedad

⁶ Informática jurídica.com, *Legislación de Derecho Informático*, consultado en Marzo 20 del 2013, en <http://www.informatica-juridica.com/legislacion/mexico.asp>

⁷ Cassou Ruiz, Jorge Esteban, *Delitos informáticos en México*, Revista del Instituto de la Judicatura Federal Núm. 28, 2009, p.210.

que el Derecho Informático llegó para solucionar problemas como el mal uso de la información, la poca privacidad de la misma en las redes sociales, los fraudes informáticos, la pornografía infantil ahora también difundida en medios informáticos, las débiles propuestas de leyes relacionadas con la informática, la falta de consideración en cuanto al valor probatorio de los documentos electrónicos, la regulación del comercio electrónico, entre otros, que recientemente aqueja y amenaza tanto a la sociedad en México.

Se tiene como reto evitar que todos los problemas anteriormente mencionados puedan convertirse en una amenaza constante, que se cometan infracciones sin las debidas sanciones o por malas decisiones de acciones jurídicas. Desafortunadamente la delincuencia cibernética está más segura que nunca de cometer éste tipo de delitos sin la preocupación que representa un delito físico o tangible, es decir, la mayoría de las veces sus acciones malintencionadas son difícilmente detectadas a tiempo, sus sanciones son lentas en los procesos jurídicos y no existe la suficiente prevención para estos actos.

No podemos permitir que la tecnología, la información y sus herramientas, se transformen en un aspecto negativo y sin expectativas de mejorar a la sociedad. El potencial de una computadora sobre el humano no es lo que preocupa, sino la utilización que hace en realidad el hombre sobre la información que se procesa en los sistemas de cómputo en forma deshonesto y poco ética⁸. Esta es la principal problemática a la que se enfrenta el Derecho Informático y que forma este trabajo de investigación, donde se plasma su situación actual en México.

⁸ Aguilar Castillo, Gildardo, *Ética y Legislación Informática*, Universidad Veracruzana, p.1.

MATRIZ DE CONGRUENCIA

Título	Pregunta de Investigación	Hipótesis	Objetivo	Desarrollo	Conclusiones y Resultados
<p style="text-align: center;">LA APLICACIÓN E IMPORTANCIA DEL DERECHO INFORMÁTICO EN MÉXICO</p>	<p style="text-align: center;">¿Qué importancia tiene el Derecho Informático en México?</p>	<p style="text-align: center;">En este trabajo de titulación se realizará una investigación en donde se plasmen y analicen las vertientes del Derecho Informático en México así como su impacto en la sociedad.</p>	<p style="text-align: center;">Mostrar y describir las deficiencias del Derecho Informático en México.</p>	<p style="text-align: center;">Se lleva a cabo una investigación bibliográfica y digital en la cual se analiza la situación actual del Derecho Informático en México, su evolución e importancia.</p>	<p style="text-align: center;">Obtener una investigación bibliográfica en la que se exponga el nivel de importancia y evolución del Derecho Informático en México, en relación a su análisis y aplicación.</p>

METODOLOGIA

PLANTEAMIENTO DEL PROBLEMA

Es lamentable que actualmente en nuestro país no se le dé la debida importancia al tema del Derecho Informático y sus consecuentes delitos, e incluso se desconozcan y no se consideren. Es comprensible que México como país en vías de desarrollo no pueda implementar las leyes tecnológicas suficientes, teniendo problemas que se consideran más importantes. El rezago en este tema existe debido a que las autoridades competentes no desarrollan las suficientes iniciativas; esto puede generar que la aplicación del Derecho Informático no evolucione conforme lo exigen las necesidades actuales. Por consecuencia las autoridades mexicanas tienen el deber de implementar leyes y reformas que una vez entrando en vigor, garanticen una actualización constante y sobre todo total entendimiento e importancia por quienes la aplican.

Actualmente existen diversas problemáticas que no se tratan a fondo por el desconocimiento de información que se tiene respecto a la correcta aplicación del Derecho Informático, lo que deriva en una ignorancia del tema para la mayoría de la población. El Derecho Informático les resulta “novedoso” a pesar de la brecha que se ha abierto para el desarrollo y uso de los sistemas de información, entre ellos la web, la cual día a día está presente en nuestras vidas. Esta desactualización y desconocimiento da como consecuencia incurrir en delitos que generalmente no podríamos tipificarlos como tal y que incluso pueden resultar delitos comunes, pero cuando se analizan a fondo, se vuelven más recurrentes y peligrosos de lo que se imagina.

PREGUNTA DE INVESTIGACIÓN

¿Qué importancia tiene el Derecho Informático en México?

DESARROLLO

En este trabajo de titulación se realizará una investigación en donde se analiza y explica la importancia sobre el Derecho Informático en México, así como sus diversas problemáticas, impacto e interés.

Por consecuencia se investigará la actual legislación mexicana en relación a temas informáticos, haciendo mención de diversas leyes que han sido elaboradas conforme a las necesidades y avance de la tecnología.

OBJETIVO

Obtener una investigación bibliográfica en la que se exponga la importancia del Derecho Informático en México, determinando su aplicación e impacto en la sociedad.

ALCANCE

Este trabajo de titulación es una investigación bibliográfica que explica la importancia del Derecho Informático en México, su evolución y su legislación actual. Se busca exponer los diversos problemas en su aplicación, para así ampliar el conocimiento del tema en general y crear consciencia de la importancia de implementar soluciones eficaces a los rezagos que existen en función a la aplicación de las leyes sobre el Derecho Informático.

RESULTADOS

La investigación bibliográfica hecha en este trabajo plasma la deficiente aplicación de las leyes en el tema del Derecho Informático, así como los diferentes casos en los que se infringen a las mencionadas leyes.

CAPITULO 1. MARCO TEÓRICO

1.1 DERECHO INFORMÁTICO

“El Derecho es el conjunto de normas que imponen deberes y normas que confieren facultades, que establecen las bases de convivencia social y cuyo fin es dotar a todos los miembros de la sociedad de los mínimos de seguridad, certeza, igualdad, libertad y justicia”.⁹

El Derecho, como en su origen latín *directum* lo afirma: “lo que está hecho conforme a la regla”¹⁰, ha evolucionado de tal forma que conforme al paso del tiempo ha dado surgimiento a una rama que se apega a unas nuevas reglas que han surgido por el avance tecnológico de los últimos tiempos. Ésta rama de la que se hablará se trata del Derecho Informático.

Todos los avances tecnológicos traen consigo cambios en diferentes ramas, en particular modificaciones en el sistema jurídico, ya que en ella se basan y regulan diferentes conductas de nuestras acciones al igual que sus consecuencias.

La aparición de las computadoras y la constante evolución tecnológica han ido rebasando varias disciplinas, al igual que han facilitado el trabajo de las mismas, pero al tratar la información que combinada con la conducta ilícita del ser humano, surgen varias limitantes y cuestiones que dan surgimiento a diferentes leyes que regulan el tratamiento de la información mediante las computadoras y los dispositivos tecnológicos en relación a la sociedad.

1.1.1 CONCEPTO DE DERECHO INFORMÁTICO

Desde el surgimiento de herramientas como las computadoras y el Internet, han pasado a ser de alguna u otra forma parte esencial de la vida de las personas, ayudando a una mayor difusión y tratamiento de la diversa información. Cuando lamentablemente la sociedad hace mal uso de ello, el Derecho debe actuar ante esas malas acciones que se cometen y debe adaptarse a las nuevas costumbres y necesidades tecnológicas. Es aquí cuando surge el Derecho Informático a partir de esas necesidades y acciones.

Al surgir todo este tipo de necesidades, diferentes autores han realizado y compartido definiciones para esta rama. Sus antecedentes se remontan a partir del año 1949 cuando Norbert Wiener el fundador de la cibernética, fue el primero en interrelacionar estos dos temas (Derecho y comunicaciones),

⁹ Pereznieto y Castro Leonel, Ledesma Mondragón Abel, *Introducción al estudio del Derecho*, 2ª. ed., Harla, p. 9

¹⁰ Villoro Toranzo, Miguel, *Introducción al Estudio del Derecho*, México, Porrúa, 2000, p.4.

en donde expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.¹¹

El Derecho Informático es el sector normativo de los sistemas, dirigido a la regulación de las nuevas tecnologías de la información y la comunicación. Asimismo integran el Derecho Informático las proposiciones normativas, es decir, los razonamientos de los teóricos del derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y las telecomunicaciones.¹²

Hay diversos puntos de vista para definir el concepto de Derecho Informático, en donde como un primer concepto global, es considerado como el conjunto de principios y normas que regulan los efectos jurídicos a partir de la relación sujeto-informática y sus derivaciones, especialmente en el área denominada *tecnología de la información*, la cual ha tenido mucho auge ya que utilizamos múltiples medios para almacenar, procesar y difundir todo tipo de información por medio de las computadoras o diferentes dispositivos electrónicos.

Para Julio Tellez¹³ el Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática tanto como instrumento (informática jurídica) como objeto de estudio (derecho de la informática) y se define como un conjunto de leyes, normas y principios aplicables a los hechos y actos derivados a la informática.

Emilio Suñe¹⁴ lo define como el conjunto de normas reguladoras del objeto informático o de problemas directamente relacionados con el mismo.

El Derecho Informático es la aplicación del Derecho a la Informática permitiendo que se adopten o creen soluciones jurídicas a los problemas que surgen en torno al fenómeno informático.¹⁵

Así que se puede definir al Derecho Informático como un conjunto de normas, las cuales regulan acciones y procesos de la informática que resulta del manejo de fuentes de información y tecnologías de información.

El Derecho Informático comprende entonces la relación entre las TIC (Tecnologías de la Información y Comunicación) y el Derecho, de donde surgen aspectos tales como la propiedad intelectual de intangibles electrónicos o digitalizables, el comercio electrónico, la protección de datos

¹¹ Tellez, Julio, *Derecho Informático*, 2ª ed., México, McGraw-Hill, 1996, p.21.

¹² Pérez Luño, Antonio-Enrique, *Manual de informática y derecho*, Madrid, Ariel, 1996, p.18.

¹³ Tellez, Julio, *Derecho Informático*, 2ª ed., México, McGraw-Hill, 1996, p.22.

¹⁴ Suñe, Emilio, "Introducción a la informática jurídica y al derecho de la Informática", Revista de la Facultad de Derecho de la Universidad Complutense, Informática y Derecho, Monográfico 12, Madrid, septiembre de 1986, p.77.

¹⁵ Núñez Ponce, Julio, *Derecho Informático*, Marsol, Perú, 1996, p.22.

personales, el tratamiento jurídico de los delitos informáticos, los aspectos tecnológicos que impactan en el ámbito laboral y social, entre otros.

La Informática es el objeto regulado por el Derecho y algunos países miembros de la OCDE (Organización para la Cooperación y el Desarrollo Económico) como Francia, Alemania, Austria, Canadá, Dinamarca, Estados Unidos, Luxemburgo, Noruega y Suecia, han colocado al Derecho Informático como un derecho público general mediante leyes especiales e importantes, por ejemplo, en la protección de datos personales, en lo cual México ya se ha sumado.

A pesar de que actualmente varios países, incluyendo México, denotan un rezago en sus leyes en cuestión de tecnología, debe ser un derecho de la sociedad que exista de manera urgente regulaciones legislativas, pues la innovación y el avance tecnológico no reconocen fronteras.

1.1.2 VERTIENTES DEL DERECHO INFORMÁTICO

El Derecho Informático, como se ha definido anteriormente, estudia las transformaciones producidas en el Derecho, a partir de la relación e incorporación de las TIC (Tecnologías de la Información y Comunicación), principalmente en Instituciones Jurídicas, en el Estado y en la sociedad, partiendo de nuevas normatividades que regularán la forma de ver al Derecho, es por ello la importancia que ha surgido de estudiar dicha rama desde dos perspectivas.

Derecho e Informática, abarcan dos aspectos; los normativos del uso de la Informática desarrollados bajo el derecho de la informática, y la aplicación de la informática en el tratamiento de la información jurídica, que es conocida, como la informática jurídica.¹⁶

El Derecho Informático se clasifica en:

- 1 Informática Jurídica.
- 2 Derecho de la Informática.

1.1.2.1 Informática Jurídica

Ésta disciplina surge en 1949, puesto que en el mundo jurídico, se comenzó a hablar de computadoras a partir del nacimiento de la cibernética de Norbert Wiener en 1948.¹⁷

Julio Téllez señala que:

¹⁶ Ríos Estavullo Juan José, *Derecho e Informática en México. Informática Jurídica y Derecho de la Informática*, 1ª ed., Instituto de Investigaciones Jurídicas-UNAM, México, 1997, p. 45.

¹⁷ Téllez, Julio, *Derecho Informático*, 2ª ed., México, McGraw-Hill, 1996, p.21.

“La informática jurídica es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación.”¹⁸

Es decir, creación y recuperación de toda información que contenga datos de interés jurídicos, pero, no sólo información, sino verdaderos actos jurídicos, como programas estudiados expresamente.

En cambio, Emilio Suñé define por informática jurídica como “la aplicación de los ordenadores electrónicos orientada a la resolución de problemas jurídicos”.¹⁹

La informática jurídica analiza, reestructura, amplía y formaliza términos cibernéticos-informáticos al propio derecho.²⁰ En general, la informática jurídica es resultado de la aplicación de la informática a los procesos y conocimientos del Derecho. La informática jurídica está dividida en:

- a) Informática jurídica documental.
- b) Informática jurídica de control y/o gestión y/o administración.
- c) Informática jurídica de ayuda a la decisión y/o metadocumental y/o metadecisional.

1.1.2.1.1 Informática jurídica documental

Se maneja el análisis de la información contenida en documentos jurídicos, formándose así bases de datos documentales.

Como rama de la informática jurídica, la informática jurídica documental es la aplicación de técnicas informáticas a la documentación jurídica en aspectos de análisis, archivo y recuperación de información contenida en la legislación, jurisprudencia, doctrina o cualquier otro documento con contenido jurídico relevante.²¹

Se consideran 3 características importantes en la informática jurídica documental:²²

- a) Aplicación técnico-jurídica: Se ajusta a una metodología especial de análisis de unidades de información, donde se habla de sistemas de

¹⁸ *Ibidem*, p.26.

¹⁹ Suñé, Emilio, “Introducción a la informática jurídica y al derecho de la Informática”, Revista de la Facultad de Derecho de la Universidad Complutense, Informática y Derecho, Monográfico 12, Madrid, septiembre de 1986, p.65.

²⁰ Ríos Estavillo Juan José, *Derecho e Informática en México. Informática Jurídica y Derecho de la Informática*, 1ª ed., Instituto de Investigaciones Jurídicas-UNAM, México, 1997, p. 50.

²¹ Guerrero M. María Fernanda, *La inteligencia artificial aplicada al derecho*, Revista uno y cero, Milán, pp.10 y ss.

²² Ríos Estavillo Juan José, *Derecho e Informática en México. Informática Jurídica y Derecho de la Informática*, 1ª ed., Instituto de Investigaciones Jurídicas-UNAM, México, 1997, p. 59.

tratamiento y recuperación de la información jurídica, éstos sistemas son.²³

-Indexación, consiste en una lista de descriptores, en la que dependiendo de la información manejada, se individualiza la información por medio de palabras clave;

-Full-text (texto completo), se trata del almacenamiento del texto íntegro en la computadora, para posteriormente recuperar esa información;

-Abstract, consiste en extraer y concretar las características fundamentales del documento, logrando su recuperación.

- b) La formación de bases de datos, ya sean archivos mensuales o sistematizados.
- c) La utilización de lenguajes o mecanismos de recuperación de información, apoyándose de herramientas lingüísticas.

1.1.2.1.2 Informática jurídica de gestión

También conocida como de administración y/o control, ésta rama organiza y controla toda la información jurídica de documentos, expedientes, etcétera, mediante la aplicación de programas de administración, para llevar un control y seguimiento de trámites y procesos, para así mantener la información actualizada.²⁴

Miguel López Muñoz Goñi establece que la informática jurídica de gestión, se divide en:²⁵

- a) Registral: manejo de todo tipo de registros, públicos o privados, con el objetivo de facilitar rápidamente los datos a los distintos usuarios en los registros oficiales.
- b) Operacional: facilita la actualización de datos en las oficinas públicas y privadas relacionadas en Derecho, en donde la computadora lleve un control de asuntos.
- c) Decisional: se utiliza en la actividad administrativa que lleva todo órgano jurisdiccional, con modelos predefinidos para soluciones de casos concretos.

1.1.2.1.3 Informática jurídica metadecisional

Se conforma por bases de conocimiento jurídico, donde más allá de obtener, recuperar y reproducir la información a través de aplicaciones informáticas,

²³ Véase *El sistema UNAM-JURE un banco de datos legislativos*, pp. 33-42.

²⁴ Ríos Estavillo Juan José, *Derecho e Informática en México. Informática Jurídica y Derecho de la Informática*, 1ª ed., Instituto de Investigaciones Jurídicas-UNAM, México, 1997, p. 60.

²⁵ López Muñoz Goñi, Miguel, *Informática jurídica documental*, Madrid, Díaz de Santos, 1984, pp.10 y ss.

se pretende que la máquina resuelva por sí misma, o auxilie a problemas de tipo jurídicos, contribuyendo al avance de la teoría jurídica.²⁶

Ésta rama se subdivide en:

- a) Sistemas expertos legales;
- b) Sistemas de enseñanza del derecho asistidos por computadora.

Sistemas expertos legales

Los sistemas expertos legales, son la estructuración de conocimientos especializados que, acoplados a un mecanismo de inferencia, saca conclusiones a partir de la información que se le suministra en forma de preguntas y respuestas.²⁷

Es decir, que estos sistemas, al asignarles una tarea dada con la debida explotación de conocimientos, puedan hacer una simulación de evaluar por sí mismas un resultado o toma de decisión como lo haría un ser humano, a través del estudio de una situación y que la misma se dé en campos o áreas muy específicas al derecho.

Sistemas de enseñanza del derecho asistidos por computadora

Los sistemas de enseñanza del derecho asistidos por computadora, interactúan directamente con las materias de pedagogía del derecho, psicología educativa, lingüística y comunicación, cuyo objetivo es la creación de sistemas de enseñanza en donde su realización se aplique en la utilización de un instrumento computacional y en las bases de conocimiento para representar, organizar, analizar y estructurar la información jurídica, para finalmente evaluar la formación del proceso enseñanza-aprendizaje previsto en el sistema.²⁸

Para el desarrollo de éstos sistemas se deben considerar ciertos aspectos, como la determinación de nivel educacional, determinar el medio informático que cubra los elementos pedagógicos indispensables, adoptar el método de diseño instruccional más conveniente para un buen aprendizaje y finalmente, elaborar el sistema de enseñanza asistido por computadora en conjunto con los alumnos, para que se prevean todo tipo de preguntas y respuestas en lo que se refiere a la interfase con el alumno, todo esto conjunto es para que éstos sistemas no sustituyan el invaluable esfuerzo de un maestro en su enseñanza, sino que, pretendan ser una valiosa herramienta para permitir una mayor difusión y obtener una mejor efectividad en la labor docente.

²⁶ Fix Fierro, Héctor, *Informática y documentación jurídica*, p. 57 y 58.

²⁷ *Ídem*.

²⁸ Ríos Estavillo Juan José, *Derecho e Informática en México. Informática Jurídica y Derecho de la Informática*, 1ª ed., Instituto de Investigaciones Jurídicas-UNAM, México, 1997, p. 65.

1.1.2.2 Derecho de la Informática

Julio Téllez define el concepto de derecho de la informática: “es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática”.²⁹

Existe un error muy común en el que se confunde como un mismo elemento al Derecho Informático y al derecho de la informática, pues es importante destacar que tanto la informática jurídica como el derecho de la Informática, son elementos de estudio y se catalogan bajo la relación “derecho e informática”.

Porque, como señala Vittorio Frosini:

“el binomio informática y derecho indica con claridad la interacción entre dos ciencias, de la cual surge un campo fecundo del saber, por una parte, la computadora se considera un instrumento utilizado por el jurista para la creación de bases de datos jurídicas y facilitar la administración de justicia, y por otra, recurrir a la computadora plantea una serie de problemas que deben ser regulados por la ley.”³⁰

El derecho de la informática se define como el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma, en las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas.³¹

En resumen, se señala a la informática como objeto de regulación jurídica, y que con el conjunto de normas jurídicas, da origen al derecho de la informática.

Dentro del derecho de la informática se estudian diversos puntos, los cuales son:

- La protección jurídica de la información personal;
- La protección jurídica del *software*;
- El flujo de datos transfrontera;
- Los convenios o contratos informáticos
- Los delitos informáticos
- El valor probatorio de los documentos electromagnéticos.

1.1.2.2.1 La protección jurídica de la información personal

Muchas actividades que ahora son fundamentales, como por ejemplo, la tramitación de una credencial electoral, una apertura de cuenta bancaria, el

²⁹ Téllez, Valdés, Julio, *Derecho Informático*, 2ª. Ed., McGraw-Hill, México, 1996.

³⁰ Frosini, Vittorio, *Informática y derecho*, Colombia, Temis, 1998, p. 135.

³¹ Ríos Estavillo, Juan José, *Derecho e Informática en México, Informática jurídica y derecho de la informática*, UNAM, México, 1997, p. 73.

uso del correo electrónico, etcétera, es decir, con todo este avance tecnológico y el manejo de la información, los diversos entes tanto públicos como privados, se han visto en la necesidad de modificar sus medios de archivar su información, recurriendo al uso de las computadoras y la automatización de la información.

Cierta desconfianza genera el uso de la información personal como datos, pues se juega una intimidad personal. La intimidad se distingue de la vida o círculo privado, debido a que “íntimo” pierde su condición cuando uno o pocos lo conocen, por lo que, se destruye al ser divulgado. En México la vida privada “es aquella parte de la vida que no está consagrada a una actividad pública, y en donde los terceros no tienen acceso alguno, con el objeto de asegurar a la persona el secreto y la tranquilidad a la que tiene derecho absoluto, de modo que el derecho a la información de que goza el ciudadano en general tendría esa limitante”.³²

En el derecho interno de los Estados Unidos de América, se hace la distinción entre cuatro categorías de posibles violaciones al derecho a la vida privada o íntima.³³

- La injerencia en la intimidad del individuo.
- La divulgación al público de hechos concretos de la vida privada.
- La presentación de un individuo al público en general bajo una falsa luz.
- La apropiación de ciertos elementos de la personalidad del individuo con fines de lucro, como nombre, imagen, voz, etcétera.

Una protección efectiva de la intimidad en esta sociedad moderna, no sólo dependerá de la protección jurídica de la información personal, sino también del manejo del usuario en cuanto a la circulación de su información.

1.1.2.2.2 La protección jurídica del software

La protección de la propiedad intelectual en el mercado mundial ha tomado una creciente importancia en los últimos años. Diversos países, principalmente EE.UU. se han preocupado en demasía por la obtención de un régimen legal de propiedad intelectual lo suficientemente fuerte y uniforme, con el propósito de un tratamiento equitativo en el comercio.

Todo éste interés de propiedad intelectual surge como una oportunidad de incorporación a la protección jurídica, debido a la dimensión económica de los intereses que están en juego, en donde destaca una preservación de la

³² Gómez-Robledo Verduzco, Alonso, citado por Castrillón y Luna, Víctor Manuel. “*La protección Constitucional de los Derechos Humanos*”, Ed. Porrúa, México, 2006, p. 100.

³³ Gómez-Robledo Verduzco, Alonso, *El derecho a la intimidad y el derecho a la libertad de expresión: derechos humanos fundamentales*, Ars Iuris, Revista del Instituto de Documentación e Investigación Jurídica de la Facultad de Derecho de la Universidad Panamericana, vol. 14, 1995, p 81.

industria nacional frente a una competencia extranjera y en la protección de un producto que requirió esfuerzos de gran inversión, investigaciones y difusión.

1.1.2.2.3 El flujo de datos transfrontera

Según el Consejo Económico de la Organización de las Naciones Unidas, el Flujo de Datos Transfronterizos (FDT) es la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación.³⁴

La cuestión de la protección de los datos surge cuando estos mismos pasan fronteras de un país e ingresan a otro, usando un medio de transporte digital de información, a través de una red global de distribución, pero en diversas ocasiones el flujo de la información a través de las fronteras de otros países puede crear problemas políticos, económicos y jurídicos.

El capítulo XIII del Tratado Trilateral de Libre Comercio de América del Norte (TLC)³⁵ contiene disposiciones relacionadas al tema del FDT, en los términos siguientes:

- El acceso y el uso de redes o servicios públicos de telecomunicaciones por personas de otra parte;
- El acceso y uso que dichas personas harán cuando operen redes privadas;
- La prestación de servicios mejorados por personas de otra parte, en territorio de la primera o por medio de sus fronteras;
- La normalización respecto de la conexión de equipo terminal u otro equipo a las redes públicas de telecomunicaciones.

1.1.2.2.4 Los convenios o contratos informáticos

Primeramente se debe definir la diferencia entre convenio y contrato. El actual Código Civil, señala en el artículo 1,792 que convenio es un acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones; mientras que el artículo 1,793 apunta al contrato, que es un convenio que producen o transfieren las obligaciones y derechos.³⁶ En referencia al término de contrato informático, Téllez señala que:

“El contrato informático es como todo acuerdo de partes en virtud del cual se crean, conservan, modifican o extinguen obligaciones relativas a los

³⁴ Citado por Téllez Valdés, Julio, *Derecho Informático*, p. 77.

³⁵ Diario Oficial de la Federación, 20 de septiembre de 1993, en vigor a partir del 1º de enero de 1994.

³⁶ Cámara de Diputados del H. Congreso de la Unión. *Código Civil Federal*. Consultado en Marzo 8 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/2.pdf>

sistemas, subsistemas o elementos destinados al tratamiento sistematizado de la información”.³⁷

Carlos Ghersi define a los contratos informáticos como “aquéllos que establecen relaciones jurídicas respecto de prestaciones consistentes en transferir la propiedad o el uso y goce de bienes, o prestar servicios, ambos informáticos”.³⁸ Los bienes y servicios forman parte de un sistema y se vinculan por un objetivo común.

El sistema de los contratos informáticos se constituye:³⁹

- a) El soporte físico o material, es decir, técnicamente lo que se conoce como *hardware*.
- b) El soporte lógico o inmaterial, lo que no se aprecia físicamente, siendo el caso a lo que se nombra *software*.
- c) El elemento humano
- d) La documentación inherente a los bienes o servicios.
- e) La asistencia técnica.

Dada la naturaleza del fin del contrato como de los bienes que están sujetos al mismo, se ha determinado que los contratos informáticos deben cumplir en señalar las obligaciones del proveedor, así como también de quien adquiere.

1.1.2.2.5 Los delitos informáticos

Se puede considerar a los delitos informáticos como un aspecto negativo a la evolución de la informática, en este caso, acrecentando las conductas delictivas. Hoy en día las computadoras ofrecen diversas formas de infringir la ley, por lo tanto se cometen delitos tradicionales, pero ahora de una manera sofisticada.

La Organización para la Cooperación Económica y el Desarrollo (OCDE) da una definición del delito informático: “cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos”.⁴⁰

La clasificación, así como una definición detallada, se dará en el segundo capítulo de este trabajo de investigación.

³⁷ Téllez, Julio, *Contratos Informáticos*, México, UNAM, 1989, p. 17.

³⁸ Ghersi, Carlos Alberto, *Contratos civiles y comerciales*, 2ª, ed., Buenos Aires, Depalma, 1992, t II, p 306.

³⁹ Flores Salgado Lucerito, *Derecho Informático*, Grupo Editorial Patria, México, 2009, p. 119.

⁴⁰ Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

1.1.2.2.6 Valor probatorio del documento electromagnético

El uso del documento electrónico o electromagnético se ha ido incorporando con frecuencia en la vida cotidiana, por lo que también se ha comenzado a admitir como un soporte válido en soportes electrónicos e informáticos ya sea magnético, óptico o impreso. Un documento informático constituye una manera electrónica del acto de escribir.

Hablando en términos jurídicos, un documento electrónico como prueba de los delitos informáticos no se ha considerado fácilmente como tal, debido a la facilidad de la modificación y/o destrucción de los mismos. La problemática de la prueba viene del hecho que se asimila como una prueba escrita, en donde un documento informático no constituye una información escrita, pues contiene llaves de acceso que se pueden modificar y no permiten diferencias entre una copia y su original, a diferencia de los documentos escritos en papel.

El concepto de documento, no se debe restringir a su naturaleza como un soporte informático, ni al escrito como único elemento material, lo que caracteriza a un documento informático es su propia desmaterialización, aunque no deja de ser concreto, visible y perceptible, pues siempre habrá un soporte material como un disco magnético, disco óptico, o listado de impresor.⁴¹

Existen 3 mecanismos que permiten a través de la apertura y transcurso de una conexión, conocer la identidad de las partes:⁴²

- Código secreto: combinación o números y/o letras que el sujeto digita sobre el teclado del sistema que utiliza.
- La criptografía: codificación del texto que se transmite, con ayuda de claves y algoritmos, incomprensibles generalmente.
- Sistema biométrico: Toma como elementos de identificación los rasgos y características físicas del ser humano.

Actualmente, las nuevas tecnologías de la información se basan en el peritaje como medio de búsqueda atribuible al juez, pero con ciertas dudas de su eficacia, pues es posible que no siempre el juez tenga profundos conocimientos informáticos.

⁴¹ Rios Estavillo, Juan José, *Derecho e Informática en México, Informática jurídica y derecho de la informática*, UNAM, México, 1997, p. 131.

⁴² *Ibidem*, p. 132.

1.2 DERECHO INFORMÁTICO EN MÉXICO

Como se ha definido, el Derecho regula la conducta y los diversos fenómenos sociales a través de la creación de leyes. El proceso de esa creación e inserción de las mismas (en el caso de México: municipio, estado, país) la mayoría de las veces es largo y lento, especialmente en el Sistema Jurídico Latino.

En los últimos años, las Tecnologías de la Información y Comunicación (TIC) han revolucionado a la humanidad en diversos aspectos: científicos, laborales, profesionales, comerciales, económicos y educativos. Ciertamente resulta complicado que el Derecho vaya a la par que la tecnología, regulando cuanto fenómeno o conducta ilícita surja en el tema jurídico, pues es evidente que estos fenómenos y conductas deben manifestarse primero, ya que las leyes no pueden regular lo que aún no existe. Si a esto le añadimos el carácter formal y escrito del sistema jurídico, las particularidades de cada proceso legislativo, además de la necesidad de que personas con formación de abogados comprendan lo necesario y fundamental sobre tecnología e informática, resulta que en especial el Derecho Mexicano, que es el que nos ocupa e interesa, se ha rezagado en una adecuada regulación.

1.2.1 ACUERDOS INTERNACIONALES SUSCRITOS POR MÉXICO

Cuando nos referimos a acuerdos puede ser entendido como un punto de encuentro entre las partes que toman lugar en el acto, entiéndase que las partes interesadas pueden ser entidades, instituciones, países o regiones que tienen diversos intereses sociales o económicos. Según la Real Academia Española (RAE) un acuerdo es la resolución que se toma en los tribunales, sociedades, comunidades u órganos colegiados, y es un convenio entre dos o más partes.⁴³

En los acuerdos se exponen diferentes ideas, objetivos o propuestas, las cuales se analizan y se debaten para llegar a una decisión en común entre los interesados, pueden ser formales que estén regidos por leyes, o informales donde en este tipo de acuerdo lo que vale es la palabra y el honor de una persona o entidad en su compromiso por cumplirlo.

Cuando el acuerdo toma lugar de modo escrito y a través de los parámetros legales, es más difícil deshacerlo y no respetarlo, este tipo de acuerdo puede ser entendido como un contrato que tiene que ser respetado por las partes firmantes de cualquier modo bajo pena de algún tipo de castigo o sanción en el caso de no hacerlo o cumplirlo.

⁴³ Véase *Real Academia Española*.

De entre los acuerdos firmados por México relativos a la reglamentación del uso de los medios electrónicos y otros relacionados están:

- El Tratado de Libre Comercio de América del Norte (TLCAN o NAFTA), firmado entre Canadá, México y EUA en el que se incluye un capítulo sobre la propiedad intelectual.
- Acuerdo de Propiedad Intelectual en relación con el Comercio o ADPIC, de la Organización Mundial del Comercio.
- Ley de derechos de autor o de copyright de cada país.⁴⁴

1.2.1.1 El Tratado de Libre Comercio de América del Norte (TLCAN o NAFTA)

Éste tratado, en su capítulo XVII, aborda el tema de la propiedad intelectual, en donde se señala en el artículo 1,721 que los “derechos de propiedad intelectual se refiere a derechos de autor y derechos conexos, derechos de marcas, derechos de patente, derechos de esquema de trazado de circuitos integrados, derechos de secretos industriales o de negocios, derechos de los obtentores de vegetales, derechos de las indicaciones Geográficas y derechos de diseños industriales”.⁴⁵ Fue firmado el 17 de diciembre de 1992, y vigente en nuestro país desde el 1 de enero de 1994.

1.2.1.2 Acuerdo de Propiedad Intelectual en relación con el Comercio o ADPIC

Los derechos de propiedad intelectual son aquellos que se confieren a las personas sobre las creaciones de su mente, en donde comúnmente se dan derechos exclusivos sobre el uso de su obra por un determinado tiempo.⁴⁶ El Acuerdo sobre los aspectos de la Propiedad Intelectual relacionado con el Comercio, fue aprobado el 15 de abril de 1994.

El Acuerdo ADPIC confirma que los programas computacionales (*software*) deben estar protegidos mediante el derecho de autor y que se aplicarán también a ellos las disposiciones del Convenio de Berna aplicables a las obras literarias. También se establece que las compilaciones de datos serán protegidas como creaciones originales siempre que respondan a los criterios de originalidad en razón de la disposición de sus contenidos, independientemente de que la compilación exista en forma legible por máquina o de otra forma y sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales en sí mismos. El acuerdo prevé

⁴⁴ Flores Salgado Lucerito, *Derecho Informático*, Grupo Editorial Patria, México, 2009, p. 165.

⁴⁵ Montalvo Romero, María Teresa, *El marco jurídico de la propiedad intelectual en México*, consultado en Marzo 15 del 2012 en <http://www.letrasjuridicas.com/Volumenes/15/tmontalvo15.pdf>

⁴⁶ Organización Mundial del Comercio, *¿Qué se entiende por ADPIC?*, consultado en Marzo 15 del 2012 en http://www.wto.org/spanish/tratop_s/trips_s/intel1_s.htm

un derecho de arrendamiento comercial de copias de programas (*software*) u obras audiovisuales.

1.2.1.3 Ley de derechos de autor o de copyright de cada país⁴⁷

La legislación sobre los derechos de autor difiere de un país a otro. Las leyes de cada país se caracterizan en lo siguiente:

- Tipo de material sujeto a derecho de autor.
- Plazo de protección, en donde en la mayoría de los países no expira más de 70 años tras la muerte del autor.
- Situación de las obras del Estado, en casi todos los países, los documentos publicados por el Estado para uso oficial son de dominio público.

Alemania

Según la ley de éste país, los documentos están en el dominio público, si han sido publicados como parte de una ley, o si son publicados como un anuncio oficial o información pública. La ley más relevante señala: “Las leyes, las regulaciones, los decretos oficiales y las proclamaciones así como decisiones y principios de guía oficialmente escrito a las decisiones no gozan de la protección del copyright.”

Antigua Unión Soviética

Toda obra publicada por la URSS antes del 27 de mayo de 1973, no se encuentra protegidas por las Convenciones Internacionales sobre Derechos de Autor y por lo tanto, quedan para dominio público.

Argentina

El derecho de autor está señalado por el artículo 17 de la Constitución que expresa que todo autor es propietario exclusivo de su obra, por el término que acuerde la ley. La Ley 11723 que regula la propiedad intelectual, su artículo 5 dice que la propiedad intelectual sobre sus obras corresponde a los autores durante toda su vida y a sus herederos hasta 70 años contados a partir del 1 de Enero del año consecutivo al de la muerte del autor.

Bolivia

La Ley 1322 sobre derechos de autor título IV, capítulo III, artículo 18 establece que la duración de la protección concedida por la presente Ley será por toda la vida del autor y por 50 años después de su muerte, a favor

⁴⁷ Aprende en línea, *¿Qué es copyright?*, Programa Integración de Tecnologías a la Docencia, Universidad de Antioquia, consultado en Marzo 16 del 2012 en <http://aprendeonline.udea.edu.co/lms/moodle/mod/resource/view.php?inpopup=true&id=55823>

de sus herederos. Dicho plazo de 50 años se fija desde el 1 de Enero de año siguiente al de la muerte o de la publicación.

Brasil

Actualmente esta materia se regula por la Ley N. 9.6102, de 19 de febrero de 1998. La ley brasileña contiene la denominación de derecho de autor, como los derechos conexos. Los sucesores del autor de la obra pierden los derechos adquiridos después de 70 años de la muerte del mismo, como lo indica el artículo 41 de la Ley N. 9.6103.

Canadá

Con la ley de derecho de autor, como se ha mencionado anteriormente, los derechos de autor están vigentes toda la vida del autor, y 50 años después de su muerte. Si la obra es seudónima o anónima, entonces los derechos de autor abarcan 50 años tras la publicación o 75 años tras la realización de la obra.

Chile

El derecho de autor está regulado por la Ley N. 17.336 de 1970, sobre propiedad intelectual. De acuerdo a ésta ley, por el hecho de creación de una obra por un chileno o extranjeros que habitan en este país, adquiere una serie de derechos patrimoniales y morales, resguardan el aprovechamiento e integridad de la obra. Los tipos de obra protegidas son de tipo literario, literario-científica y artística.

Colombia

Conforme a la Ley de derechos de autor de 1982, los derechos se disfrutan durante la vida del autor y 80 años después de su muerte. Este plazo es válido igualmente para obras anónimas y colectivas. En el caso de obras donde el autor es una persona jurídica o de derecho público está vigente solamente 30 años a partir de su publicación.

Dinamarca

Según la Ley Refundida de Derechos de Autor de 2003, los derechos de autor sobre imágenes fotográficas expiran 50 años después de la creación de dicha imagen; sin embargo, para obras de fotografía, los derechos de autor expiran 70 años después de su muerte.

España

Aquí los derechos de autor se conocen como "propiedad intelectual". La vigente Ley de Propiedad Intelectual tiene origen desde el 11 de noviembre de 1987.

La Ley de Propiedad Intelectual menciona explícitamente en el artículo 31 el derecho a la “copia privada”, es decir, el derecho a hacer copias privadas sin permiso del autor, siempre que no existan fines de lucro y la obra sea pública. Una excepción a la copia privada es el caso del software, donde sólo se pueden hacer copias de seguridad, es decir, es necesario ser dueño del original para que entonces, la copia sea legal.

India

En la legislación de la India sobre derechos de autor, solamente se establece que todas las imágenes publicadas de hace más de 60 años están en el dominio público.

México

En la Ley Federal del Derecho de Autor, los derechos patrimoniales de autor son vigentes toda la vida, y 100 años después de la muerte del autor más joven o de su fecha de publicación en caso de gobierno municipal, estatal y federal. Sin embargo, hay una excepción para las obras que ingresaron al dominio público antes de la reforma del 23 de julio del 2003 (obras creadas por alguien que murió antes de la fecha mencionada) pues éstas sólo tendrán vigencia hasta 75 años después de su muerte.

Uruguay

La Ley 17.616 de derechos de autor que entró en vigor el 10 de enero de 2003, establece en su artículo 14, que el autor conserva su derecho de propiedad durante toda su vida, y sus herederos por el término de 50 años a partir del fallecimiento del causante. En el artículo 40, nos dice que, terminado el plazo de 50 años, la obra entra en dominio público.

1.2.1.4 CONVENIOS

Los pactos o convenios son convenciones suscritas de buena fe por representantes de dos o más estados, carecen de forma legal, por lo que sólo se le imponen moralmente a quienes lo firman, por lo que no se puede hacer uso de la fuerza para su ejecución.⁴⁸

Los convenios en que México ha participado en materia del Derecho Informático son:

- El Convenio de Berna para la Protección de las Obras Literarias y Artísticas, establecido en 1886 y conocido como el Convenio de Berlín, la versión vigente del Convenio de Berna data de 1971, misma que se llevó a cabo en París con la participación y firma de México,

⁴⁸ Apipilhuasco Ramírez José Antonio, *Derecho Internacional Privado*, Instituto de Investigaciones Jurídicas, UNAM, México, 2007.

entre otros países, para 1973 el Congreso lo aprobó y entró en vigor en 1974.

- El Convenio que establece la Organización Mundial de la Propiedad Intelectual (OMPI).
- El Convenio de París para la Protección Industrial del 20 de marzo de 1883.

1.2.1.4.1 El Convenio de Berna para la Protección de las Obras Literarias y Artísticas

Surge en 1886 y hasta la fecha ampara a nivel internacional el derecho de los autores, con el fin de que tengan el privilegio de controlar el uso sobre sus obras artísticas, científicas o literarias, así como también recibir una compensación por su utilización. Para obtener la protección del Convenio, un autor debe ser originario de uno de los países pertenecientes del mismo, haber publicado su creación por primera vez en algún otro país también miembro de la Unión. Una vez obtenida la protección al autor, permanece durante toda su vida y por cincuenta años después de su muerte. Las producciones que están protegidas por el Convenio se hallan en el campo de la literatura, la ciencia y el arte, en cualquiera de sus formas de expresión. México firmó su adhesión el 24 de julio de 1971, la cual fue ratificada el 11 de septiembre de 1974 y entró en vigor el 17 de diciembre de 1974.⁴⁹

1.2.1.4.2 El Convenio que establece la Organización Mundial de la Propiedad Intelectual (OMPI)

En éste convenio no se define la propiedad intelectual, pero en él se define una lista de objetos que se prestan a la protección por medio de los derechos de propiedad intelectual, que son:⁵⁰

- Protección contra la competencia desleal
- Descubrimientos científicos
- Invenciones en todos los campos de la actividad humana
- Obras literarias artísticas y científicas
- Marcas de fábrica, comercio, servicios y nombres de denominaciones comerciales
- Diseños industriales
- Y todos los demás derechos que conciernen a toda actividad intelectual en aspectos industriales, literarios, artísticos y científicos.

⁴⁹ OMPI, *Reseñas de los Convenios, Tratados y Acuerdos administrados por la OMPI*, México, 2011.

⁵⁰ OMPI, *Convenio que establece la Organización Mundial de la Propiedad Intelectual*, consultado en Marzo 20 del 2012 en http://www.wipo.int/treaties/es/convention/trtdocs_wo029.html#P38_1300

1.2.1.4.3 Convenio de París para la Protección Industrial del 20 de marzo de 1883

Su instrumento de protección son las patentes, además de una preocupación por la competencia desleal. El convenio aplica a la propiedad industrial en su acepción más amplia, con inclusión de las patentes, marcas, dibujos y modelos industriales, modelos de utilidad (una especie de “pequeña patente” establecida en leyes de algunos países), nombres comerciales, procedencias de los mismos y represión de la competencia desleal.⁵¹

1.2.2 TRATADOS INTERNACIONALES CON LA PARTICIPACIÓN DE MÉXICO

Los tratados son hechos entre diferentes sujetos ya sean Estados u Organizaciones Internacionales, y que se encuentran regidos por diferentes instrumentos jurídicos en los cuales pueden establecerse normas o leyes.

Para Carrillo Salcedo el “Tratado es todo acuerdo de voluntades entre dos o más sujetos de Derecho Internacional destinado a producir efectos jurídicos regulados por el Derecho Internacional”⁵² Al referirse a sujetos de derecho internacional no se habla sólo de Estados, sino también de organismos internacionales gubernamentales, o aquellos que se reconozcan capaces de celebrar tratados.

La negociación de los tratados es largo, ya que puede durar varios años realizar un texto definitivo que satisfaga a las partes. Durante ésta fase deben determinarse el objeto, fin y contenido del tratado, y también la redacción del mismo, sobre todo en los tratados entre estados internacionales.

El grado de formalidad de un tratado es más importante que el de un convenio ya que se realizan por escrito, la Organización Mundial de la Propiedad Intelectual (OMPI) administra varios tratados multilaterales entre ellos:

1.2.2.1 El Tratado de la OMPI sobre Derecho de Autor (WCT)⁵³

Este tratado fue adoptado en Ginebra el 20 de diciembre de 1996, reconociendo el impacto que han tenido el desarrollo y la convergencia de las tecnologías de información y comunicación en la creación y utilización de las obras literarias y artísticas.

⁵¹ OMPI, *Reseñas de los Convenios, Tratados y Acuerdos administrados por la OMPI*, México, 2011.

⁵² Carrillo Salcedo, Juan Antonio, *Curso de Derecho Internacional Público: Introducción a su estructura, Dinámica y Funciones*. Peruvian Book Central S.R.L. 1992. p. 103.

⁵³ OMPI, *Tratado de la OMPI sobre Derecho de Autor (WCT)*, 1996, consultado en Marzo 21 del 2012 en http://www.wipo.int/treaties/es/ip/wct/trtdocs_wo033.html

Es desarrollado para mantener la protección de los derechos de los autores a partir de la necesidad de introducir nuevas normas internacionales y clarificar la interpretación de ciertas normas vigentes con la finalidad de proporcionar soluciones adecuadas a las interrogantes planteadas por diferentes acontecimientos ya sea económico, social, cultural y tecnológico.

En su Artículo 4 habla de los programas computacionales, los cuales están protegidos como obras literarias y se aplica en cualquiera que sea su modo o forma de expresión, esta parte de la protección se encuentra en el marco de lo dispuesto en el Artículo 2 del Convenio de Berna antes mencionado.

El Artículo 5 trata sobre compilaciones de datos (bases de datos). Las compilaciones de datos o de otros materiales, en cualquier forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, están protegidas como tales. Esa protección no abarca los datos o materiales en sí mismos y se entiende sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales contenidos en la compilación.

1.2.2.2 Tratado de cooperación en materia de patentes⁵⁴

Elaborado en Washington el 19 de junio de 1970 y modificado el 3 de febrero de 1984 y 3 de octubre de 2001. El tratado permite solicitar simultáneamente en un gran número de países la protección de una invención por patente mediante la presentación de una solicitud “internacional” de patente sin la necesidad de presentar varias solicitudes de patente nacionales o regionales. La concesión de patentes sigue siendo competencia de las Oficinas nacionales de patentes, en lo que se denomina la “fase nacional”.

1.2.2.3 Tratado de Singapur sobre el Derecho de Marcas

El Tratado de Singapur tiene como objetivo crear un marco internacional moderno y dinámico para un mejor ajuste de los trámites administrativos de registro de marcas.⁵⁵ En este tratado las partes contratantes (Países) tienen la libertad para elegir la forma de comunicarse con sus respectivas oficinas (incluidas las comunicaciones en forma electrónica o que se transmiten por medios electrónicos).

También otorga la libertad de elegir la forma y los medios de transmisión de las comunicaciones y se aceptan que estas se presenten en papel, en forma electrónica o en otra forma de transmisión.

⁵⁴ OMPI, *Cómo proteger sus invenciones en otros países: preguntas frecuentes sobre el tratado de cooperación en materia de patentes (PCT)*, consultado en Marzo 21 del 2012 en http://www.wipo.int/export/sites/www/freepublications/es/patents/433/wipo_pub_433.pdf

⁵⁵ OMPI, *Reseñas de los Convenios, Tratados y Acuerdos administrados por la OMPI*, México, 2011.

1.2.2.4 El Tratado de Libre Comercio de América del Norte (TLCAN o NAFTA)

Este tratado, en su capítulo XVII, aborda el tema de la propiedad intelectual, en donde se señala en el artículo 1721 que los “derechos de propiedad intelectual se refiere a derechos de autor y derechos conexos, derechos de marcas, derechos de patente, derechos de esquema de trazado de circuitos integrados, derechos de secretos industriales o de negocios, derechos de los obtentores de vegetales, derechos de las indicaciones Geográficas y derechos de diseños industriales”.⁵⁶ Fue firmado el 17 de diciembre de 1992, y vigente en nuestro país desde el 1 de enero de 1994.

⁵⁶ Montalvo Romero, María Teresa, *El marco jurídico de la propiedad intelectual en México*, consultado en Marzo 21 del 2012 en <http://www.letrasjuridicas.com/Volumenes/15/tmontalvo15.pdf>

APORTACIONES

Finalmente se concluye en este capítulo, que el Derecho Informático como nueva rama del Derecho, surge a partir de las nuevas necesidades a las que el ser humano hoy en día se enfrenta, las cuales tienen mucho que ver con la evolución tecnológica y los actos que se cometan a partir de la misma, todos aquellos actos a los que nos referimos tratan de acciones negativas que tengan repercusión en el uso de la tecnología informática.

La compilación de diversas definiciones y conceptos puede constatar la necesidad de que el Derecho Informático se haga presente a todo momento en que la evolución tecnológica en conjunto con la sociedad lo demande.

En México, el Derecho Informático es un aspecto que desde su origen ha presentado complicaciones en su correcta aplicación, aunado a un mal equilibrio de regulación jurídica a la par con la evolución tecnológica, lo cual suena imposible, pero que puede lograrse.

Como principales esfuerzos en interés de que el Derecho Informático tenga una aplicación adecuada, están los Acuerdos, Tratados y Convenios de los que se hablaron en este capítulo, de los cuales podemos destacar en los que México tuvo participación como lo son el Tratado de Libre Comercio, Acuerdo de Propiedad Intelectual, Leyes de Derecho de Autor en cada país, Convenio de Berna, Convenio de la OMPI, Convenio de París y Tratados sobre Marcas y patentes; en los que se abarcó de lo que tratan y el objeto con los que fueron creados y firmados.

A partir de los conceptos citados, el Derecho Informático presenta las siguientes vertientes: (Mapas de aportación propia)

Informática Jurídica

(Surge en 1949, a partir del nacimiento de la cibernética de Norbert Wiener)

Definición según:
Emilio Suñe
 Es la aplicación de los ordenadores electrónicos orientada a la resolución de problemas jurídicos

Definición según:
Julio Téllez
 Es la técnica interdisciplinaria que tiene como objeto el estudio de los conocimientos de la informática, aplicables a la recuperación de información jurídica

Se divide en:

Informática Jurídica Documental

¿Qué es?

Es la aplicación de técnicas informáticas a la documentación jurídica en aspectos de análisis, archivo y recuperación de información

- Aplicación Técnico-Jurídica
- Indexación Full-text
- Abstract

Características:

Formación de Bases de Datos

Utilización de lenguajes o mecanismos de recuperación de información

Informática Jurídica de Gestión

¿Qué es?

Esta rama organiza y controla toda la información jurídica, mediante la aplicación de programas

- Registral
 - Manejo de los registros
- Operacional
 - Facilita la actualización de datos
- Decisional
 - Modelos predefinidos para soluciones de casos concretos.

Se divide en:

Informática Jurídica Metadecisional

¿Qué es?

Se conforma por bases de conocimiento jurídico, donde pretende que la máquina resuelva por sí misma, o auxilie a problemas de tipo jurídicos

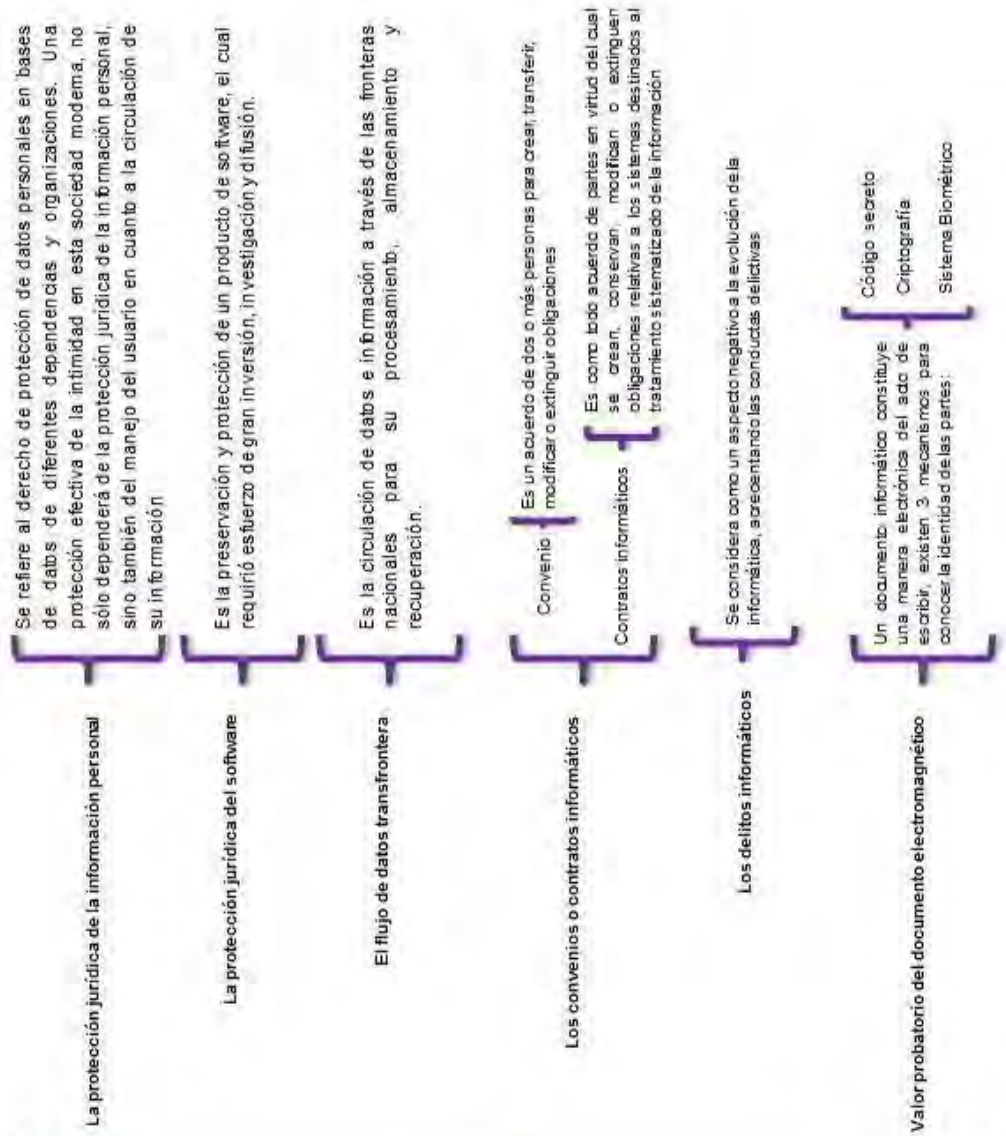
Se subdivide en:

- Sistemas Legales
 - Son la estructuración de conocimientos especializados acoplados a un mecanismo de inferencia, saca conclusiones a partir de la información que se le suministra en forma de preguntas y respuestas
- Sistemas de enseñanza del derecho asistidos por computadora
 - Creación de sistemas de enseñanza que apliquen el uso de un instrumento computacional y bases de conocimiento para representar, organizar, analizar y estructurar la información jurídica

Derecho de la Informática

Julio Téllez

“es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática”.



CAPÍTULO 2. DELITOS INFORMÁTICOS EN GENERAL

A lo largo de la historia, el hombre ha necesitado transmitir y tratar la información de forma continua; sin embargo, con el creciente uso de las computadoras, la revolución del internet que ahora se encuentra al alcance de millones de personas, los delincuentes han encontrado formas de cometer actos ilícitos impunemente.

Todo éste avance tecnológico ha tenido un gran impacto en la sociedad derivado del uso cotidiano de las computadoras, en donde surgen una serie de comportamientos ilícitos llamados “delitos informáticos”, es decir, la tecnología actualmente no es sólo un apoyo al desempeño de nuestras actividades diarias, o como un medio para el manejo de la información, sino que ahora también hay personas cometiendo actos ilícitos a través de éstas herramientas. Todos éstos actos implican actividades criminales que los países han tratado de encuadrar en conductas típicas, como el robo, hurto, fraude, falsificaciones, sabotajes, estafas, etcétera, surgiendo la necesidad de regulación por parte del Derecho.

Como se menciona en el capítulo anterior, los delitos informáticos son un aspecto negativo en la evolución de la informática puesto que, así como resulta ser una herramienta favorable a la sociedad, también se constituye en un instrumento para la realización de actos ilícitos. A consecuencia de ello, poco a poco se han tomado medidas al respecto en nuestro país en materia de regulaciones y sanciones a los delitos informáticos.

2.1 CONCEPTO DE FRAUDE Y DELITO

Fraude se define como engaño, acción contraria a la verdad o a la rectitud. La definición de delito es compleja y han sido muchos los intentos de formular una noción de delito que sirviese para cualquier país, pero esto no ha sido posible, dada la íntima conexión que existe entre vida social y jurídica de cada sociedad y cada siglo.⁵⁷

El artículo 7° del Código Penal Federal dice que: “Son delitos y faltas las acciones u omisiones dolosas o culposas penadas por la ley”.⁵⁸

⁵⁷ Del Peso Navarro Emilio, *Peritajes Informáticos*, 2ª ed., Ediciones Díaz de Santos, España, 2001, p. 161.

⁵⁸ Cámara de Diputados del H. Congreso de la Unión. *Código Penal Federal*. Consultado en Marzo 18 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf>

2.2 CONCEPTO DE DELITO INFORMÁTICO

Por delito informático se entiende como cualquier conducta ilícita cometida por el ser humano y deba ser sancionada por el Derecho penal, consistiendo en el uso indebido de cualquier medio informático, con el fin de un beneficio ilícito. Las acciones indebidas pueden ser como un uso indebido de software, apropiación o comunicación ilícita de datos, interferencias en la banca electrónica y uso de datos ajenos, entre otras conductas antijurídicas relacionadas con la tecnología informática, dichas figuras delictivas tipificadas en el Código Penal u otras leyes.

Organismos internacionales como la OCDE (Organización para la Cooperación y el Desarrollo Económico), lo define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o la transmisión de datos.⁵⁹

Para Julio Téllez Valdez, los delitos informáticos son “aquellas actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).⁶⁰

Los delitos informáticos no constituyen una nueva categoría delictiva, debido a que son los mismos delitos que ya se vienen castigando: delitos contra las personas, contra el honor, la libertad, la seguridad pública o la Nación. Sin embargo, si requieren un espacio y regulación legislativa importante.

Se puede definir que, delincuencia informática es todo acto o conducta ilícita que sea considerada como criminal, con el objetivo de alterar, socavar, destruir o manipular cualquier sistema informático o a sus componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera.⁶¹

En el sistema jurídico de nuestro país, se incluyó a los delitos informáticos con las reformas que se publicaron en el Diario Oficial de la Federación el 17 de mayo de 1999.⁶² Los actos ilícitos se ubicaron dentro de Título Noveno del Código Penal Federal, al que se le denominó “*Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática*”.

El acelerado avance tecnológico hace más difícil descubrir quien realiza el delito, además de las fallas de seguridad en los sistemas y la renuencia a

⁵⁹ Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

⁶⁰ Téllez Valdés, Julio, *Derecho Informático*, 3ª. Ed., México, McGraw-Hill, 2004.

⁶¹ Acurio del Pino Santiago, *Delitos Informáticos: Generalidades*, consultado en Marzo 18 del 2012 en http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

⁶² Landa Durán, Graciela M., *Los delitos informáticos en el Derecho penal de México y España*, España, 2007.

denunciarlos por temor a dañar la imagen y reputación ante los clientes en el caso de víctimas empresariales, entre otros motivos, que contribuyen a la impunidad. Hoy en día los delitos informáticos constituyen una *moderna* forma de delinquir que debe ser regulada.

2.2.1 Efectos de los Delitos Informáticos en la Sociedad

Las perspectivas de la informática no tienen límites previsibles, por ello se ha llegado a afirmar que hoy en día, la Informática es un Poder Social. Las capacidades que pone a disposición de Gobiernos y de particulares con rapidez y por consiguiente, ahorro de tiempo y energía que representan un cuadro de realidades y posibilidades en la aplicación de actos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de nuevas situaciones y de tantas potencialidades en el medio social.⁶³

El constante desarrollo tecnológico y el manejo de la información con las nuevas tecnologías de comunicación, no sólo tiene sus ventajas, sino que también plantea problemas de gran importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, defensa, administración y la sociedad. Debido a ésta relación, el aumento de los delitos informáticos representa una amenaza para un país y para su sociedad en conjunto.

Los autores de los delitos informáticos se consideran a sí mismos “respetables”, siendo objeto de sanciones de carácter económico y no siempre privativos de la libertad. Este nivel de criminalidad se explica por lo difícil que resulta reprimirla en forma internacional, pues hay ocasiones en que los usuarios están en diversos países y en consecuencia, existe una posibilidad muy grande que el agresor y la víctima estén sujetos a leyes nacionales diferentes; aunque los acuerdos y tratados internacionales intentan solucionar algunas de las dificultades ocasionadas por los delitos informáticos, las posibilidades son limitadas.

2.2.2 Efectos de los Delitos Informáticos en la Economía

Sin duda alguna, la Economía es una de las fortalezas del actual modelo social, la existencia de bloques económicos en competencia por acaparar el mercado, hace que se requiera de elementos que favorezcan la obtención de las ganancias planeadas. Es aquí donde la Informática se convierte en un elemento vital para esas aspiraciones.⁶⁴

El fenómeno de la globalización permite el constante manejo de material informático (*hardware* y *software*) en diversos países, generando la reducción de costos y mayor empleo a la sociedad.

⁶³ Instituto Nacional de Estadística e Informática, *Delitos Informáticos*, Lima, 2001, p 70.

⁶⁴ *Ibidem*, p 72.

Son pérdidas económicas millonarias las que generan los delitos informáticos a empresas nacionales e internacionales. De acuerdo con un estudio de *ciberdelito* desarrollado por el Registro de Direcciones de Internet para América Latina y el Caribe (Lacnic), el *phishing* o robo de datos personales significa pérdidas anuales por unos US\$93 mil millones de dólares, en tanto a robos de cuentas de clientes suman otros US\$761 millones de dólares. Cabe mencionar que empresas e instituciones de todo el mundo gastaron 338 mil millones de dólares en 2011, para combatir ataques ciber criminales, dos tercios de los cuales fueron delitos de fraude económico, según cifras durante el Programa de Ciberseguridad y Cibercrimen de la ONU.⁶⁵

En años recientes, se ha notado un incremento en la incidencia delictiva en materia de delitos informáticos, principalmente en México, representando su impacto en términos monetarios un monto considerable respecto de la actividad económica, el patrimonio y la seguridad. Los delitos de mayor incidencia se refieren a los virus informáticos (malware), el de la estafa y el *phishing*. Las pérdidas monetarias para los usuarios causadas por *ciberdelitos* en México son de casi \$2,000 millones de dólares.⁶⁶

México ocupa el tercer lugar en materia de delitos informáticos, siendo el de la pornografía infantil uno de los de mayor incidencia, dado que México se encuentra en tercer lugar de flujo de pornografía infantil.⁶⁷

2.3 CARACTERÍSTICAS DEL DELITO INFORMÁTICO

El delito informático se caracteriza por las dificultades que presenta descubrirlo, probarlo y perseguirlo. Son delitos que en la mayoría de casos no se denuncia, para evitar un desprestigio por un fallo de seguridad o evitar una alarma social, por lo que, las víctimas prefieren sufrir el daño causado e intentar prevenir otro posible ataque, antes que iniciar un procedimiento judicial.

Ésta situación dificulta saber con exactitud el número de delitos que se cometen, además de también dificultar la planificación de una adecuada regulación legislativa.

⁶⁵ DIARIO TI, Delitos Informáticos causan pérdidas millonarias en bancos y empresas. Consultado en Abril, 2, 2012 en http://www.diarioti.com/noticia/Delitos_informaticos_causan_perdidas_millonarias_en_bancos_y_empresas/31409

⁶⁶ Comisión Especial de Acceso digital, *Informe de labores 2010-2012*, Cámara de Diputados, consultado en Abril 2, 2012 en http://archivos.diputados.gob.mx/Programas_anuales/informes/LXI/informe_final_acceso_digital_2012.pdf

⁶⁷ Proceso, *Diputados tipifican delitos cibernéticos como el "ciberfraude"* consultado en Abril 2 del 2012 en <http://www.proceso.com.mx/?p=302516>

Los elementos del tipo penal que se consideran para denominar a un delito como “delito informático” son:⁶⁸

- El bien jurídico tutelado mediante la sanción de los delitos informáticos es la pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
- Elemento objetivo es todo atentado que signifique dañar o desviar el correcto uso de la máquina, con el fin de causar un perjuicio que redunde en un beneficio moral o material para sí o para otro por el uso indebido de una computadora sin la correspondiente autorización.
- El elemento subjetivo debe estar constituido por el dolo o la culpa con que actúa el sujeto activo del delito informático.
- En cuanto a éste sujeto activo se refiere, se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por ejemplo, programadores que violan o inutilizan programas o sistemas, analistas de sistemas que conocen la operación completa de los mismos; personal técnico y de mantenimiento que tienen libre acceso a los centros de cómputo, sistemas operativos y bases de datos, etcétera.
- Sujeto pasivo: entre los sujetos pasivos de los delitos informáticos figuran las entidades bancarias como víctimas frecuentes por la creciente utilización de las transferencias de fondos de forma electrónica, donde se movilizan cantidades importantes de dinero mediante símbolos electrónicos como único tipo de registro.

Para Julio Téllez Valdés⁶⁹, los delitos informáticos presentan las características siguientes:

- Son conductas delictivas de cuello blanco, debido a que sólo un determinado número de personas con ciertos conocimientos técnicos pueden llegar a cometerlas.
- Son acciones ocupacionales, pues muchas veces se realizan cuando el sujeto se encuentra trabajando.
- Son acciones de oportunidad, es decir, se aprovecha una ocasión creada o altamente intensificada en el mundo de las funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas para los afectados, al contrario de los beneficios que les producen a quienes realizan los delitos.

⁶⁸ Salgado Flores, Lucerito. Derecho Informático. Grupo Editorial Patria, 2009.

⁶⁹ Téllez Valdés, Julio. Derecho informático. McGraw-Hill. México, 1996.

- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, todo ello debido a la misma falta de regulación por parte del derecho tanto a nivel internacional, como nacional.
- Son muy sofisticados y frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, debido a su mismo carácter técnico.
- En su mayoría son intencionales, aunque también hay muchos de carácter culposo o imprudencia y en ocasiones van más allá de la intención (preterintencionales).
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienen a proliferar cada vez más, por lo que requieren una urgente regulación jurídica. Por el momento, muchos siguen siendo ilícitos impunes de manera manifiesta ante la ley.

2.3.1 Caracterización de los sujetos

Las personas autoras de delitos informáticos poseen características muy diversas. Aquella persona que “entra” ilegítimamente y en forma remota en un sistema informático sin intenciones delictivas, es muy diferente. En relación a las características personales de aquellos que cometen delitos informáticos, debe tomarse en cuenta lo siguiente:⁷⁰

- En general son personas que no presentan antecedentes delictivos.
- La mayoría son de sexo masculino.
- Actúan en forma individual.
- Poseen una inteligencia brillante y alta capacidad lógica, ansiosos de vencer obstáculos, toman como un deporte el vulnerar la seguridad de los sistemas. Éstas son características comunes en las personas que generalmente se les conoce como *hackers*.
- Son jóvenes con gran habilidad en el manejo de la computadora, con temeridad, coraje y gran confianza en sí mismos.
- También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, han llegado a ser socialmente aceptados.
- En el caso de los *hackers*, realizan sus actividades como una especie de *hobbie* donde el desafío está allí y hay que vencerlo. Aprovecha fallas y deficiencias de seguridad para obtener acceso en los procedimientos del sistema. A menudo, se hacen pasar por usuarios

⁷⁰ De Sola Quintero René, *Delitos Informáticos*, consultado en abril 5 del 2012 en http://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

legítimos del sitio, pues la mayoría de usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.

- Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras y motivadas (es el que siempre está de guardia, el primero en llegar y el último en irse).
- Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos estudiosos de la materia los han catalogado como “delitos de cuello blanco”, (esto se debe a que el sujeto activo que los comete es poseedor de cierto status socio-económico).

2.3.1.1 Sujeto Activo

Aquí no se habla de delincuentes comunes, los sujetos activos tienen como características:⁷¹

- Ocupan puestos estratégicos en las organizaciones, en donde se maneje información de carácter sensible y se nombran *delitos ocupacionales*, pues se cometen por la ocupación y facilidad de acceso al sistema.
- A pesar de las características mencionadas anteriormente, se debe tener presente que puede tratarse de personas muy distintas, pues no es lo mismo el joven que accede a un sistema por curiosidad, investigación o violar el sistema por un desafío personal, a un empleado de una institución financiera que desvíe fondos de las cuentas de sus clientes.
- Las opiniones en cuanto a la tipología del delincuente informático son divididas, pues hay quienes mencionan que el nivel educativo informático no es un indicativo, mientras otros dicen que son personas inteligentes, motivadas y que gustan de desafíos tecnológicos.
- Estos delitos se califican como de “cuello blanco”, pues el delincuente pertenece a un cierto status socio-económico, generalmente alto, como anteriormente se había mencionado.

La cifra negra es muy alta, no es sencillo descubrirlo ni sancionarlo, en razón del poder económico de quienes pueden cometerlos, además de que los daños económicos son altos.

Es una situación controversial que la opinión pública puede no considerar delincuentes como tales a éstos sujetos, pues no los desprecian, marginan o desvalorizan, sino que el autor al realizar el delito a una organización, siente que “hace justicia”, convenciendo a la sociedad de una actitud justiciera.

⁷¹ Acurio del Pino Santiago, *Delitos Informáticos: Generalidades*, consultado en Abril 5 del 2012 en http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

El sujeto activo en cuanto a su cualificación puede no ser un elemento determinante en la delincuencia informática. Sólo algunos delitos como los que cometen los *hackers* se pueden considerar realizados por un sujeto altamente calificado. Los demás delitos no requieren una cualificación, pues, son cometidos por personas que recién se inician en la informática o por adolescentes que están aprendiendo individualmente.

2.3.1.2 Sujeto Pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre el cual recae la conducta típica que realiza el sujeto activo.⁷²

Tenemos que distinguir que la víctima del delito informático o mejor llamado sujeto pasivo es sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo o delincuente, y en este caso las víctimas pueden ser individuos, instituciones crediticias, dependencias gubernamentales, etcétera, que son quienes usan sistemas automatizados de información, generalmente conectados unos a otros.

El sujeto pasivo es un elemento de suma importancia para el estudio de los delitos informáticos, ya que mediante el mismo podemos conocer los diferentes actos ilícitos que cometen los delincuentes informáticos, con el objetivo de prevenir futuros delitos informáticos.

La mayoría de los delitos informáticos no se descubren y se desconoce su magnitud, debido a la falta de denuncia por miedo a un desprestigio, pérdidas económicas y a una falta de preparación y eficacia en algunas autoridades para comprender, investigar y aplicar el tratamiento jurídico que se adecúe a cada situación delictiva, entre otros motivos más, que se unen a la estadística de la llamada “cifra negra”.

Por lo anterior se deduce que para una correcta prevención de la criminalidad informática se requiere, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación y encubrimiento.⁷³

Diversos organismos internacionales han adoptado resoluciones en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de quienes se encargan de aplicar y cumplir la ley y la eficiencia de las

⁷² Acurio del Pino Santiago, *Delitos Informáticos: Generalidades*, consultado en Abril 5 del 2012 en http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

⁷³ *Idem.*

autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.⁷⁴

2.4 CLASIFICACIÓN DE DELITO INFORMÁTICO

Los delitos informáticos han sido objeto de diversas clasificaciones:

María de la Luz Lima⁷⁵ ha clasificado los delitos informáticos en tres categorías:

- Como método: conductas criminales en las cuales los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
- Como medio: conductas criminales en donde para realizar un delito se hace uso de una computadora como medio o símbolo.
- Como fin: conductas criminógenas dirigidas contra la entidad física del objeto, o máquina electrónica o sus componentes con el objeto de dañarla.

Julio Téllez Valdés⁷⁶ por su parte, clasifica a los delitos informáticos en base a dos criterios:

- Como instrumento o medio
- Como fin u objetivo

Como instrumento o medio

Las conductas ilícitas se valen de las computadoras como método, medio o símbolo para cometer el acto, diversos ejemplos se enlistan a continuación:

1. Modificación de datos de entrada o de salida.
2. Uso no autorizado de programas de cómputo.
3. Alteración en el funcionamiento de sistemas mediante los temidos “virus informáticos”.
4. Acceso a áreas informatizadas de forma no autorizada.
5. Introducción de instrucciones que provoquen “interrupciones” en la lógica interna de un software, con el fin de obtener beneficios.
6. Falsificación de documentos.
7. Intervención en las líneas de comunicación de datos.
8. Obtención de información ya sea impresa o en cinta magnética, después de ejecución de trabajos.
9. Lectura, sustracción o copiado de información confidencial.

⁷⁴ *Ídem.*

⁷⁵ Lima de la Luz, María, *Criminalia N° 1-6 año L. Delitos Electrónicos*. Ediciones Porrúa, México, 1984.

⁷⁶ Téllez Valdés, Julio. *Derecho informático*. McGraw-Hill. México, 1996.

10. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria.
11. Violación a aprovechamiento indebido de un código para acceder a un sistema con instrucciones inapropiadas.

Como fin u objetivo

La conducta delictiva se comete en contra de la computadora, accesorios o programas como entidad física. Por ejemplo:

1. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los principales “cerebros” computarizados.
2. Secuestro de soportes magnéticos en los que exista información valiosa con fines de chantaje.
3. Programación de instrucciones con el objetivo de bloquear totalmente el sistema.
4. Atentado físico contra la máquina o sus accesorios.
5. Daño a la memoria
6. Destrucción de programas por cualquier método.

2.4.1 Legislación comparada sobre delitos informáticos

Diversos países y organizaciones internacionales, se han visto en la necesidad de legislar sobre los delitos informáticos debido a los daños y perjuicios que causan a la sociedad. Sin embargo, si bien existe un esfuerzo por tratar de evitarlos, no hay un criterio unificado de cómo deben ser atacados, es por eso que resulta imprescindible que se siga trabajando para llegar a ésa unificación y poder tener una legislación informática coherente, comprometiendo a los países de legislar sobre la materia, basados en los criterios adoptados internacionalmente.

En el manual de las Naciones Unidas para la prevención y Control de Delitos Informáticos, señala que el problema se ha elevado a nivel internacional, debido a que los delitos informáticos constituyen una nueva forma de crímenes transnacionales y su combate requiere de una eficaz unión internacional.⁷⁷ La ONU resume de la siguiente manera los problemas que rodean a la cooperación internacional en materia de delitos informáticos:⁷⁸

- Falta de acuerdos globales, en referencia de qué tipos de conductas se constituyen como delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

⁷⁷ Naciones Unidas. *Octavo Congreso de Las Naciones Unidas sobre prevención del delito y tratamiento del delincuente*. La Habana. 27 de agosto, 7 de septiembre de 1990 (a/conf 144/28/Rev.1) Nueva York, Naciones Unidas, 1991.

⁷⁸ Velázquez Elizarrarás Juan Carlos, *El estudio de caso en las relaciones jurídicas internacionales: modalidades de aplicación del derecho internacional*, UNAM, México, 2007, p. 301.

- Falta de especialización entre las distintas leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de procesos sincronizados que permitan la puesta en vigor de la cooperación internacional.

2.4.2 Regulación Nacional de los delitos informáticos

Existen legislaturas en nuestra nación que castigan algunos de los tipos de delitos informáticos.⁷⁹

- Ley de Protección de la Propiedad Intelectual.
- Código Penal Federal.
- Código Penal para el DF.
- Ley Federal del Derecho de Autor.
- Ley Federal de Protección de datos personales.
- Ley de Propiedad Industrial.
- Código de Comercio.
- Código Federal de Procedimientos Civiles.
- Código Civil Federal.

En meses recientes, se notificó una importante decisión del gobierno mexicano en cuanto a sanciones ante la creciente realización de delitos informáticos, pues en marzo del 2012, la Cámara de Diputados aprobó una serie de modificaciones legales que identifican delitos informáticos como el famoso *hacking*, el uso de engaños para obtener información, tales como contraseñas, obtención y divulgación de información que contengan sistemas informáticos protegidos.⁸⁰

2.5 TIPOS DE DELITO INFORMÁTICO

Las tecnologías de la información y las comunicaciones, están cambiando el entorno social mejorando la productividad, revolucionando los procesos laborales, su eficiencia y economía. Sin embargo, este crecimiento tecnológico también ha desencadenado nuevas formas de delincuencia informática.

⁷⁹ Salgado Flores Lucerito, *Derecho Informático*, Grupo Editorial Patria, 2009, México, p. 138.

⁸⁰ CNN México, *Legisladores definen cuáles son los delitos informáticos y su castigo*. Consultado en Abril 18 del 2012 en <http://mexico.cnn.com/tecnologia/2012/03/29/legisladores-definen-cuales-son-los-delitos-informaticos-y-su-castigo>

Es así que la ONU reconoce como delitos informáticos las siguientes conductas.⁸¹

1. FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS	
Manipulación de los datos de entrada	Esta operación no necesariamente las hacen personas con conocimientos de informática, si no que los puede realizar cualquier persona que tenga acceso a las funciones normales del ordenador. Lo más común es la introducción de datos o movimientos falsos en las transacciones de una empresa.
Manipulación de programas	En este caso deben existir mayores conocimientos en informática, pues se modifican los programas de un ordenador, insertando nuevos programas o nuevas instrucciones. El método más común es el llamado "Caballo de Troya", que consiste en insertar instrucciones computacionales de forma encubierta en un programa informático, para que pueda realizar una función no autorizada a la misma vez que realiza su función normal.
Manipulación de datos de salida	El delito más común en ésta conducta es el fraude, en donde se hace objeto de los cajeros automáticos mediante falsificación de instrucciones para la computadora, en la fase de adquisición de datos.
Fraude efectuado por manipulación informática	También llamado como la "técnica del salami", en la que cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se transfieren a otra; se realiza sin grandes dificultades y es muy difícil de detectar. Un ejemplo es el <i>redondeo hacia abajo</i> , que consiste en una instrucción que se le da al sistema informático para que transfiera a una determinada cuenta los centavos que se descuenten por el redondeo.
2. FALSIFICACIONES INFORMÁTICAS	
Utilizando sistemas informáticos como objetos	Es cuando se modifican documentos computarizados para alterarlos, falsificarlos o su reproducirlos.

⁸¹ INEI, *Delitos Informáticos*. Colección Seguridad de la Información, Lima, 2001.

Utilizando sistemas informáticos como instrumentos	Se produce cuando un equipo es usado para falsificar productos o documentos de uso oficial. Por ejemplo, las fotocopiadoras a color de gran definición permitieron la alteración de documentos no fácilmente identificables.
3. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS	
Sabotaje informático	Consiste en borrar, suprimir o modificar sin autorización funciones o datos de computadora, con intención de obstaculizar el funcionamiento normal del sistema.
Virus	Un virus, es un programa que puede ingresar en un sistema a través de cualquiera de los métodos de acceso de información externa, se instala y se reproduce, causando un daño al mismo.
Gusanos	Se fabrica de forma análoga al virus, se infiltra en los programas ya sea para modificar o destruir los datos, pero se diferencia de los virus porque no pueden regenerarse. Las consecuencias del ataque de un gusano pueden ser considerables.
Bomba lógica o cronológica	Consiste en la introducción de un programa con un conjunto de instrucciones indebidas que actuarán en determinada fecha o circunstancia, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando al mismo.
Acceso no autorizado a sistemas o servicios	Se da por motivos diferentes, desde una simple curiosidad (como en el caso de muchos piratas informáticos), hasta el sabotaje o espionaje informático. Estos ingresos no autorizados comprometen la integridad y la confidencialidad de los datos
Reproducción no autorizada de programas informáticos de protección legal	Entraña una sustancial pérdida económica para los propietarios legítimos. Se refiere de reproducciones no autorizadas a través de la web, piratería y su comercio ilegal, etcétera.

En la anterior clasificación se resalta que *la reproducción no autorizada de programas informáticos de protección legal*, no podría ser considerada en su totalidad como delito informático, pues el bien jurídico a tutelar es la propiedad intelectual. Por lo tanto, el delito contra ésta sólo puede

comprender la defraudación del derecho de autor por su creación científica en el campo del software.⁸²

Otro delito informático es el *homicidio por computadora*⁸³, un ejemplo de este caso es cuando a un paciente que está recibiendo un determinado tratamiento, se modifican las instrucciones en la computadora, que puede hacerse incluso desde una terminal remota, obviamente afectando la salud y arriesgando la vida de un ser humano.

También hay otras prácticas que se sustentan de los sistemas informáticos, convirtiéndose en delitos informáticos y sean un peligro para la sociedad, las cuales son:

Terrorismo

Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional con la ayuda de *hosts* que ocultan la identidad del remitente. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

Narcotráfico

Transmisión de fórmulas para la fabricación de estupefacientes, para el lavado de dinero y para la coordinación de entregas y recolección.

Espionaje

Acceso no autorizado a sistemas informáticos gubernamentales, de empresas e interceptación de correos electrónicos. Se entiende como el apoderamiento indebido de la información y manejo del mismo con fines ilícitos.

Pornografía infantil

Se considera pornografía infantil toda representación visual, gráfica o textual, incluidos dibujos animados o juegos de video que de manera real o simulada, explícita o sugerida, involucren la participación de niños o personas que aparenten serlo, en el desarrollo de actividades sexuales o exhibición de los genitales con fines sexuales.⁸⁴

En la actualidad, la pornografía infantil es impunemente difundida a través de Internet, teléfonos celulares y otros medios en los que sea posible la

⁸² Bramont-Arias Torres Luis Alberto, *Delitos Informáticos*, Revista Peruana de Derecho de la Empresa No. 51, consultado en Marzo 5 del 2013 en

http://perso.unifr.ch/derechopenal/assets/files/obrasportales/op_20130408_02.pdf

⁸³ Viega Rodríguez, María José, *Delitos Informáticos*, REDI Revista Electrónica de Derecho Informático, Núm. 9, 1999.

⁸⁴ UNICEF. *Protocolo Facultativo Convención sobre los Derechos de los Niños relativo a la Venta de Niños, Prostitución infantil y la utilización de Niños en Pornografía* Resolución A/RES/54/263 del 25 de Mayo de 2000.

grabación y reproducción de imágenes o videos, inclusive, se han detectado sitios web y a delincuentes cibernéticos, creando “trampas” hacia los infantes para su secuestro y desaparición. Lamentablemente la sociedad no tiene la suficiente conciencia de lo que implica, ignorando el alcance y el negocio que representa éste delito, convirtiéndolo en algo difícil de erradicar.

Ciberacoso

También llamado *Cyberbullying*, se define como las acciones de acoso realizadas desde plataformas tecnológicas, principalmente internet⁸⁵. Es el uso de información electrónica y medios de comunicación tales como correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, teléfonos móviles, y sitios web difamatorios para acosar a un individuo o grupo, mediante ataques personales u otros medios. Puede constituir un delito penal.

Es un delito voluntarioso e implica un daño recurrente y repetitivo a través del medio del texto electrónico. Según R.B. Standler,⁸⁶ el acoso pretende causar angustia emocional, preocupación, y no tiene propósito legítimo para la elección de comunicaciones. El *ciberacoso* puede ser tan simple como continuar mandando e-mails a alguien que ha dicho que no quiere permanecer en contacto con el remitente. Puede incluir también amenazas, connotaciones sexuales y etiquetas peyorativas.

2.6 PIRATAS INFORMÁTICOS

Para realizar cada delito informático se requieren de personas con conocimientos amplios o de una alta curiosidad.

Los piratas informáticos se aprovechan de la vulnerabilidad de los sistemas informáticos, tal es el caso de la práctica habitual sobre la copia ilegal de software, realizando copias de software en CD, para después comercializar con ellos. Tanto en el terreno doméstico como en el ámbito empresarial, se ha relegado este término a ciertos personajes con alguna capacidad de penetrar en bases de datos y sistemas informáticos, pero que no posee conocimientos, más que para duplicar discos. Sin embargo, el término alude a ésa práctica, no por extendida menos reprochable, que ocasiona cuantiosas pérdidas a la industria informática. A la vez que la tecnología fue avanzando, también lo hizo la piratería informática.

⁸⁵ CNN México, ‘*Cyberbullying: la amenaza constante de la generación ‘hiperconectada’*’, consultado en Abril 25 del 2012 en <http://mexico.cnn.com/salud/2011/08/05/cyberbullying-la-amenaza-constante-de-la-generacion-hiperconectada>

⁸⁶ Standler, Ronald B., *Computer Crime*, 2002, Consultado en Abril 19 del 2012 en <http://www.rbs2.com/ccrime.htm>

Los hackers aparecieron como un instrumento positivo. Cuando el Internet fue creado en los 60's por el gobierno de EE.UU. para uso exclusivamente militar, se vieron en la necesidad de perfeccionar los sistemas de seguridad, por lo que se contrató a genios de la informática para que indagaran en las deficiencias de dichos sistemas con el fin de ir mejorándolos progresivamente, pero el asunto ha terminado por volverse en contra de la red y sistemas de información.

A partir de esto, todo tipo de *hacker* tiene un perfil con amplios conocimientos sobre una tecnología y normalmente conoce todos los terrenos de la tecnología actual. Le dan ansias por saber todo e investiga, y lo que resulta aún más difícil, llega a descifrar ya sea sistemas de cifrado o sistemas de codificación.⁸⁷

Un *hacker* busca, en primer lugar, el entendimiento del sistema, ya sea Hardware o Software y descubre el modo de codificación de las órdenes; en segundo lugar, busca modificar la información para usos propios y de investigación del funcionamiento total del sistema.⁸⁸

Sus conocimientos los difunden, para que otros sepan cómo funciona realmente la tecnología, trata de averiguar temas y situaciones, las cuales aplica en las comunicaciones que existieron antes que los ordenadores.

Ha surgido toda una generación de personajes que difunden el miedo generalmente en la red. Ésta nueva generación de rebeldes de la tecnología aportan sabiduría, enseñanza y difunden el conocimiento, en cambio otros, solamente destrucción y desorden.

Es importante señalar que se debe comprender y saber quién es cada uno de ellos y catalogarlos según sus actos, esto se refiere a que debido a su aportación, es donde se ubican. Podemos visualizar un triángulo: en la punta se encuentran los *hackers*, que son el principio y el nivel más alto de una sociedad, pues poseen más conocimientos que el resto, pero emplean metodologías más agresivas para mostrarlos.

El siguiente nivel de este triángulo, son los *crackers*, en donde éstos son capaces de *crackear* sistemas y romper su seguridad, los más afectados son los programadores y fabricantes de software.

Y por último, los *lamers*, que son auténticos curiosos y poseen mayor influencia en la red a través de WEB's.⁸⁹

⁸⁷ Hernández Claudio, *Hackers. Los piratas del Chip y de Internet*, España, 2001.

⁸⁸ INEI, *Delitos Informáticos*. Colección Seguridad de la Información, Lima, 2001.

⁸⁹ Hernández Claudio, *Hackers: Los Clanes de la RED 2000*, consultado en Abril 19 del 2012 en <http://ucapanama.org/wp-content/uploads/2011/12/Hackers-1-Claudio-Hernandez.pdf>

Pero así como los anteriores, han ido apareciendo diferentes tipos de piratas informáticos que dependiendo de sus actos se han dado a conocer, a continuación explicamos por separado cada uno de ellos.⁹⁰

2.6.1 Hackers

Expertos centrados en sistemas informáticos avanzados; exploran detalles de los sistemas programables y aprenden a usarlos al máximo. Saltan la seguridad de otros ordenadores solo por el hecho de divertirse, es decir, se plantean el pirateo como un reto personal y una vez saltadas éstas barreras, no se llevan nada, ni modifican nada del ordenador atacado.

Es común que los *hackers* sean contratados por alguna empresa de seguridad, el perfil del *hacker* idóneo es el que se interesa por la tecnología y emplea muchas horas delante de la computadora.

2.6.2 Crackers

Son el siguiente peldaño pero los primero rebeldes, se dedican única y exclusivamente a *crackear* sistemas, utilizando sus conocimientos para invadirlos, descifrar claves y contraseñas de programas, algoritmos de encriptación, generan claves de registros falsas para un programa en particular, robar datos personales o cometer otros actos informáticos ilícitos.

Crack es sinónimo de rotura; cubre parte de la programación de software y hardware, deben conocer las dos caras de la tecnología: la programación y la parte física de la electrónica. Existen *crackers* que alteran el contenido de un determinado programa, alterando sus fechas de expiración para hacerlo funcionar como si se tratara de una copia legítima.

2.6.3 Lamers

Tienen mayor número de miembros y gran presencia en la red, carecen de cualquier conocimiento y solo relee toda la información que hay en internet.

Les fascina la posibilidad de entrar a otro sistema remoto, este grupo quizá es el más peligroso de la red, ya que ponen en práctica todo el software de *hackeo* que encuentran en la red. Emplean de forma habitual programas para controlar la red (*sniffers*), interceptan correos electrónicos, para después enviar varios mensajes, con dirección falsa amenazando algún sistema.

⁹⁰ Martínez Alarcón, Benjamín, *La filosofía Hacking & Cracking*, Universidad Autónoma del Estado de Hidalgo, México, 2006.

2.6.4 Copyhackers

Es una sociedad solo conocida en el terreno del *crackeo* de hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago, ellos divagan entre la sombra del verdadero *hacker* y *lamer*.

Poseen conocimientos tecnológicos y se obsesionan por ser superiores, pero no terminan de aceptar su posición. Por ello extraen información del verdadero *hacker* para terminar su trabajo y su principal motivación es el dinero.

2.6.5 Bucaneros

Son peores que los *lamers*, ya que no aprenden nada ni conocen la tecnología, los bucaneros solo buscan el comercio negro de los productos entregados por los *copyhackers*, estos solo tienen cabida fuera de la red, siendo simplemente unos comerciantes y no ven la hora de explotar un producto de *cracking* a nivel masivo.

2.6.6 Phreaker

Es la ciencia de *crackear* la telefonía para obtener beneficios personales. Posee alto conocimiento de los sistemas de telefonía terrestre y móvil. Orientan sus estudios y ocio hacia el aprendizaje del funcionamiento de teléfonos y compañías telefónicas, telecomunicaciones, sistemas que componen una red telefónica y por último, electrónica aplicada a sistemas telefónicos. Su propósito es obtener llamadas gratis, espionaje, o solo romper la seguridad de las líneas.

Un buen *phreaker* debe tener amplios conocimientos sobre informática, pues el control de centrales telefónicas es la parte primordial a tener en cuenta y emplean la informática para su procesamiento.

2.6.7 Newbie

Es un novato, aquel que navega por internet, tropieza con una página de *hacking* y descubre que existe un área de descarga sobre programas de *hackeo*, descarga lo que puede y empieza a trabajar con los programas.

Aprenden el *hacking* siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

2.6.8 Script Kiddie

Se trata de simples usuarios de internet, sin conocimientos sobre *hacking* o *cracking*, son devotos de estos temas, pero no los comprenden. Se limitan a recopilar información de la red, se dedican a buscar programas de *hacking*,

ejecutándolos sin leer primero, con esta acción, sueltan virus, o se fastidian ellos mismos su propio ordenador.

2.6.9 Casos de Hackers famosos a nivel mundial

Es muy sabido que han existido muchos *Hackers* en la historia, por esta razón resulta complicado enumerarlos o enlistarlos por importancia. Muchos de éstos coinciden en que diferentes autores los nombran dándolos a conocer por sus hazañas y que gracias a ello han marcado la historia de la tecnología.

A continuación se enlistan a algunos de estos *Hackers*, los cuales no están numerados por sus proezas o ataques, puesto que cada uno de ellos se desenvuelve en diferentes temas y otros lejos de cometer un acto ilícito premeditado, han ayudado al desarrollo de la Informática.

1. Kevin Mitnick, (“El Cóndor”). El Departamento de Justicia de Estados Unidos lo calificó como “el criminal informático más buscado de la historia” de ese país. Cobró fama en los años 80, cuando logró penetrar sistemas ultra protegidos, como Nokia y Motorola, robar secretos corporativos y hasta *hackear* a otros *hackers*. Fue apresado en 1995, popularizándose entre los medios. Quedó en libertad en el 2002.
2. Kevin Poulson. Famoso en 1990 por *hackear* líneas telefónicas de la radio KIIS-FM de Los Angeles, para asegurarse la llamada número 102 y así ganar un Porsche 944 S2. Fue apresado tras un ataque que realizó a una base de datos del FBI en 1991. En 2006 ayudó a identificar a 744 pedófilos vía MySpace.
3. Adrian Lamo. Nacido en Boston, mundialmente conocido como “*El hacker vagabundo*” pues realizaba sus ataques desde cibercafés y bibliotecas. Su trabajo más famoso fue la inclusión de su nombre en la lista de expertos de New York Times y penetrar en la red de Microsoft. Adquirió fama también por tratar de identificar fallas de seguridad en las redes informáticas de Fortune 500 y después, comunicarles esas fallas encontradas.
4. Stephen Wozniak, quien comenzó su carrera como *hacker* de sistemas telefónicos para realizar llamadas gratis, se dice que hasta llamó al Papa en los años 70. Más tarde formó Apple con su amigo Steve Jobs.
5. Loyd Blankeship (“El Mentor”). Era miembro del grupo hacker *Legion of Doom*, que se enfrentaba a *Masters of Deception*. Es autor del

manifiesto *hacker* “La conciencia de un *hacker*” que escribió en prisión al ser detenido en 1986 y del código para el juego de rol “Ciberpunk”, por esto, gran parte de su fama se debe a su vocación de escritor.

6. Michael Calce. Inició hackeando los sitios web comerciales más grandes del mundo. Después con apenas 15 años de edad, el día de San Valentín en el 2000, lanzó un ataque que afectó a eBay, Amazon y Yahoo!, lo descubrieron por vanagloriarse de su hazaña en varios chats y fue condenado a uso limitado de Internet.
7. Robert Tappan Morris. Creó un virus informático que infectó a cerca de 6 mil grandes máquinas Unix, haciéndolas tan lentas que quedaron inutilizables, causando pérdidas millonarias. El virus realizaba 2 tareas: enviarse a otras máquinas y duplicarse en la máquina infectada. Fue el primer *hacker* en ser procesado por la ley de fraude computacional en Estados Unidos.
8. Masters of Deception. Era un grupo de *hackers* de élite en Nueva York. En los 80's atacaron a más no poder los sistemas telefónicos de Estados Unidos, y su mayor golpe fue entrar al sistema de la compañía AT&T. Varios de ellos terminaron presos en 1992.
9. David L. Smith. Autor del famoso virus Melissa, se propagó por correo electrónico en 1999. Fue condenado a prisión por causar daños por más de 80 millones de dólares.
10. Sven Jaschan. Creador del virus Sasser. A la edad de 17 años fue detenido en mayo de 2004 al ser denunciado por sus vecinos que deseaban obtener la recompensa de Microsoft, pues el virus afectaba directamente la estabilidad de Windows 2000, 2003 Server y Windows XP.⁹¹
11. Richard Stallman. Se convirtió en *hacker*, pero dejó de serlo por la presión del comercio en la industria del software. Creó una alternativa libre al sistema operativo UNIX con el sistema operativo al que denominó GNU y fundó la organización Free Software Foundation e inventó el concepto *copyleft*. En la actualidad Stallman se dedica a crear miles de utilidades gratuitas para entornos UNIX.
12. Dennis Ritchie, Ken Thompson y Brian Kernighan. Llamados *los tres mosqueteros del chip* son buenos programadores y trabajan para Bells Labs. Están especializados en el entorno UNIX y lenguaje C,

⁹¹ Alto Nivel, *Los 10 Hackers más famosos del mundo*, consultado en Abril 18 del 2012 en <http://www.altonivel.com.mx/los-10-hackers-mas-famosos-del-mundo.html>

han tenido que ver con el nacimiento de Internet y su progreso. De no haber estado ellos en este proyecto, Internet quizás no existiría ahora, o de hacerlo, sería muchísimo más lenta.

13. John Draper. (*Capitán Crunch*). Descubrió que con un silbato de los cereales *Crunch* se podía hacer *Phreaking*. El sonido de éste generaba un silbido a 2.600 Hertzios, frecuencia con la que se empleaba para cortar los contadores de los teléfonos de Bell. Este descubrimiento lo llevó a crear la primera “*Blue Box*” una caja electrónica mágica para los teléfonos.
14. Paul Baran. *Anonymous* (otro *Hacker* bastante conocido) lo ha catalogado como el mejor *Hacker* de todos. Baran estuvo enredado con Internet incluso antes de que existiese como tal, por lo que los principios de Internet se deben asignar a Baran, puesto que comenzó a edificar lo que hoy en día conocemos como un *Navegador*, debemos reconocer que el crear esta herramienta fue un gran acierto, pues hasta el día de hoy, es utilizada por millones de internautas en todo el mundo.
15. Eugene Spafford. Creador de COPS “Computer Oracle Password and Security System, un sistema de seguridad para Redes. Es profesor de Informática de la universidad de Purdue, en donde ha descubierto e impulsado a varios estudiantes realmente brillantes, entre los que destaca Dan Farmer.
16. Dan Farmer. Fue alumno destacado del profesor Stafford y participó en la creación de COPS en 1991. Farmer ganó fama al desarrollar SATAN (*System Administrator Tool for Analyzing Networks*), una herramienta muy potente que analiza los defectos y puntos débiles de una red remota.
17. Mark Abene. Alias “Phiber Optik”, es uno de los fundadores del grupo “*Master of deception*”, exclusivamente dedicados al conocimiento y estudio profundo de los teléfonos.
18. Johan Helsingius. Alias *Julf*, el más popular creador de correo anónimo; creó este tipo de correo seguro por medio de una cuenta llamada penet.fi. Julf se inició con un 486 con 200 megas de disco duro.
19. Wietse Venema. Gran programador que ha recibido multitud de reconocimientos. Es coautor con Dan Farmer de la herramienta SATAN, pero lo que lo lanzó a la fama fue el programa *TCP Wrapper*,

una herramienta de seguridad de las más utilizadas en el mundo, que controla y registra los paquetes que entran en una red.

20. Justin Tranner Peterson. (*Agente Steal*). Posee una gran habilidad haciendo *cracking* que le llevó a conocer perfectamente las tarjetas de crédito. Su motivación era ganar dinero de una forma rápida y fácil. Esta falta de ética del *Hacker* verdadero, lo condujo a una sucia jugada con el FBI para trabajar con ellos, en donde denunció a diversos *hackers*, entre ellos a Poulsen, pero al final fue incapaz de protegerse a sí mismo.

21. Vladimir Levin. Matemático ruso de 24 años, famoso por el caso “Como robé 10 millones de dólares”. Penetró vía Internet desde San Petesburgo en los sistemas informáticos centrales del banco Citibank en Wall Street. Una vez dentro, logró transferir a diferentes cuentas de EE.UU, Rusia, Alemania, Israel y Suiza fondos por valor de 10 millones de dólares. Fue detenido en 1995.⁹²

El ser *hacker* en cualquier tipo de los anteriores, es actividad castigada por la ley, pero gracias a las distintas maneras que ofrece el internet para brindar anonimato, estas personas por lo regular suelen pasar desapercibidas.

En el caso particular de México, en Noviembre del 2003 Alejandro Hernández Flores alias “alt3Kx”, un joven ingeniero en sistemas de 26 años de edad, fue detenido por la Agencia Federal de Investigación (AFI), acusado de haber atacado la página de la Presidencia de México en junio del mismo año. El ataque se produjo con el envío de paquetes de datos de hasta 100 megabytes por segundo, lo cual hizo caer el servidor por denegación de servicio (DoS), dejándola inaccesible por largos períodos.⁹³

En Julio del 2005 un mexicano experto en sistemas con 20 años de edad de nombre Ricardo Reyes Orozco, vulneró los sistemas de BancaNet (Portal electrónico de Banamex), transfirió por Internet, los saldos de una cuenta del banco a su propia cuenta, y se presentó más tarde a retirar diferentes cantidades en distintas sucursales. El personal del Banco lo detectó, lograron entretenerlo y fue detenido por el delito de fraude al banco, ya que en México no existe como tal la figura de “Delito Informático”.⁹⁴

En 2007, Mauricio Flores Basurto y Elvia Castrejón Rodríguez, una pareja de expertos en informática, transfirieron ilícitamente fondos de tres empresas por casi un millón de pesos, a cuentas bancarias de personas físicas, sin

⁹² Hernández Claudio, *Hackers. Los piratas del Chip y de Internet*, España, 2001.

⁹³ VSantivirus, *Cae pirata que atacó web de la presidencia de México*, consultado en Abril 12 del 2012 en <http://www.vsantivirus.com/28-11-03.htm>

⁹⁴ El Universal, *Hackers, genios que se desligan del hampa*, consultado en Abril 21 del 2012 en <http://www.eluniversal.com.mx/sociedad/5701.html>

embargo fueron descubiertos por los bancos Banamex, HSBC, y BBVA-Bancomer al detectar desvíos de dinero a través de una clave única interbancaria. Tras ser aprehendidos, confesaron que desde un café internet o laptop, accedían a la información de cuentas empresariales, donde elegían cuál tenía fondos suficientes y cometer los desvíos de dinero, pagando comisión a diversas personas que les pedían abrir cuentas en dichos bancos y poder retirar el efectivo.⁹⁵

Existen casos verídicos como el de Fernando Ernesto Villegas Álvarez, pasante de la carrera de Ingeniero en Sistemas Computacionales, del Instituto Politécnico Nacional, que fue preso por participar obligadamente con narcotraficantes como *La Barbie* y el “Chapo” Guzmán.⁹⁶ Actualmente el narcotráfico aprovecha la inteligencia de los *hackers*, su operación es secuestrarlos y obligarlos a cometer actos ilícitos. México es un albergue para actos de lavado de dinero, clonación de tarjetas bancarias, entre otros.

Sólo hemos hablado de personas, pero cabe destacar que también hay programas dedicados especialmente al *hackeo*, por ejemplo el *mailbombing*, que es el envío masivo de correo electrónico mejor conocido como bombardeo en el entorno del *hacking*.⁹⁷ Son programas que permiten enviar miles de veces un mismo mensaje a una determinada dirección de correo electrónico. A veces el *mailbombing*, también realiza el envío de correo fantasma, esto es, un correo falso sin dejar rastro para quien lo envía (anónimo), pasando inadvertido.

La amenaza persiste, pues México con más de 35 millones de personas como usuarios de Internet⁹⁸, están altamente expuestos, y aún nuestras leyes abarcan diversas *lagunas* sobre el tema.

2.7 PREVENCIÓN FRENTE A LOS DELITOS INFORMÁTICOS

2.7.1 Piratería Informática

Es el acto de copiar para utilizar o comercializar sin autorización cualquier cosa que tenga derechos de autor. Para Aguilera López “se entiende como la distribución o reproducción ilegal de software comercial para su utilización empresarial o particular”⁹⁹. En este caso, específicamente se habla de

⁹⁵ Crónica, “*Hackers*” caen tras defraudar a tres empresas, consultado en Abril 21 del 2012 en <http://www.cronica.com.mx/notas/2007/289573.html>

⁹⁶ Excélsior, *Narcos mexicanos secuestran y esclavizan a hackers*, consultado en Abril 12 del 2012 en <http://www.excelsior.com.mx/2011/07/04/global/749995>

⁹⁷ Hernández Claudio, *Hackers. Los piratas del Chip y de Internet*, España, 2001.

⁹⁸ La Jornada, *En un año creció 14% el número de mexicanos que usan Internet*, consultado en Abril 21 del 2012 en

<http://www.jornada.unam.mx/2011/05/18/index.php?section=sociedad&article=043n1soc>

⁹⁹ Aguilera López Purificación, *Seguridad Informática*, Editex, 2010.

piratería informática. La piratería comienza con la aparición de las computadoras personales, puesto que, hasta ese momento, se trabajaba únicamente en mainframes, en los que se utilizaban programas hechos de tal manera que difícilmente se podían aprovechar de un caso a otro.

Algunas organizaciones disponen de equipos de cómputo que deben contar con licencias de uso de *software*, deberán existir tantas licencias de uso de un producto como la cantidad de usuarios que lo usen. No sólo se trata de la compra múltiple de un mismo producto, sino de acuerdos contractuales entre la firma proveedora del *software* y la organización que lo compra. Esto a veces representa gastos de los que ciertas organizaciones no pueden cubrir, y no solo las empresas, sino también muchos usuarios que con la economía precaria existente, no “alcanza” para lujos como éstos, recurriendo a la compra de piratería, o descarga ilegal de *software*.

El *software* pirata presenta una serie de desventajas, entre ellas:

- Productividad reducida
- Alta exposición a serias represiones legales
- Poca confiabilidad debido a probables infecciones de virus
- Carencia de documentación
- No da derecho a soporte técnico, ni garantía
- Copias por lo general incompletas.

En contraposición el software original, presenta las siguientes ventajas:

- Productividad total
- Completa documentación
- Soporte técnico
- Garantía de todo el paquete
- Posibilidad de actualizaciones a bajo costo
- Acceso a beneficios adicionales (Conferencias, exposiciones, seminarios, etc.)

En aspecto específico a México, la Ley sobre derechos de autor aprobada por el Congreso de México, faculta perseguir el uso ilegal de *software*. La piratería es un “inhibidor” de la competitividad y es un tema que preocupa a largo plazo, el cual tiene que generar cambios en la forma en la que se adquiere tecnología. En México, de acuerdo con datos de la OCDE, el 60% del mercado de las Tecnologías de la Información, está acaparado por la piratería.¹⁰⁰

¹⁰⁰ 24 Horas, *Piratería informática deja pérdidas de mil mdd en México: Microsoft*, consultado en Abril 27 del 2012 en <http://www.24-horas.mx/pirateria-informatica-deja-perdidas-de-mil-mdd-en-mexico-microsoft/>

Como una novedosa solución, ha surgido el cómputo en la nube o “*cloud computing*”, que es un nuevo modelo de prestación de servicio de negocios y tecnología, el cual permite acceder a varios servicios y gestionar servicios de información y aplicaciones. Alberto González, director de la empresa Microsoft en México¹⁰¹, asegura que el cómputo en la nube, servicio del cual son proveedores únicos, sería un factor clave para la reducción de la piratería, ya que ésta nueva modalidad abatiría los costos de adquisición de software para las empresas mexicanas, reduciendo costos de hasta un 67%.

Un tema mundial que en últimos tiempos destacó dentro del mundo tecnológico en contra de la piratería y propiedad intelectual, fue la creación de la Ley SOPA (*Stop Online Piracy Act*), un proyecto de ley introducido en la Cámara de representantes de Estados Unidos el pasado 26 de Octubre de 2011 por Lamar S. Smith, con el objetivo de ampliar las capacidades de los propietarios de derechos intelectuales, para supuestamente combatir el tráfico de contenidos en internet y productos protegidos por derechos de autor o por la propiedad intelectual.¹⁰²

Ésta ley la consideraron un atentado a la libertad de expresión, pues la creación de una “lista negra” de sitios web no accesibles es un peligroso precedente, sobre el cual gobiernos y empresas pueden actuar para censurar y controlar información en base a intereses económicos y políticos. El problema no es la forma en la que la gente accede y comparte información, sino la falta de una reestructuración en las leyes internacionales de propiedad intelectual que deben ajustarse a nuestros tiempos, a la forma en que las personas usan la tecnología que nos acerca a la cultura y la manera en que la compartimos.

2.7.2 Contratos informáticos

Los contratos informáticos tienen por objeto regular la creación y transmisión de derechos y obligaciones respecto de los bienes y servicios informáticos. Es decir, regir conforme a derecho de aquellas relaciones contractuales con motivo de la compra o arrendamiento de un sistema, prestación de un servicio de mantenimiento, programación, capacitación, asesoría, etcétera.¹⁰³

Los contratos informáticos requieren de un tratamiento jurídico especial, que respondan a las características del mercado internacional en materia de tecnología informática, con fines específicos e intereses en juego, así como su trascendencia económica para la empresa y el Estado.

¹⁰¹ *Ídem.*

¹⁰² Los Tiempos, *¿Qué es la Ley SOPA y cómo afecta a Latinoamérica?* Consultado en Abril 27 del 2012 en http://www.lostiempos.com/diario/actualidad/vida-y-futuro/20120119/que-es-la-ley-sopa-y-como-afecta-a-latinoamerica_157237_327978.html

¹⁰³ Téllez Valdés, Julio, *Contratos Informáticos*, 2ª. Edición, McGraw-Hill, México, 1996.

La diferencia que existe entre contratos informáticos y contratación electrónica, radica en que los contratos informáticos se refieren únicamente a bienes y servicios informáticos que se negocian y contratan en forma electrónica o tradicional; mientras que la contratación electrónica se realiza sobre cualquier bien o servicio, sea informático o no, pero utilizando algún medio electrónico.

En los contratos informáticos las partes que participan son:¹⁰⁴

Proveedores. Proporcionan un bien o servicio, y son fundamentalmente los constructores, distribuidores y vendedores de equipos, así como los prestadores de servicios informáticos.

Usuarios. Reciben la prestación de dar o hacer por parte de los proveedores y están constituidos por el sector público y privado en sus diferentes niveles.

2.7.2.1 Tipos de contratos

Existen dos tipos de contratos en cuanto al tipo de prestación a realizar u objeto, que son aquellos referidos a los bienes (equipos, periféricos, dispositivos, etcétera) y aquellos referidos a los servicios (asistencia, formación, mantenimiento, programas, etcétera)

Estos contratos, al igual que muchos otros, deben estar forzados a contener consignas o cláusulas que darán estructura particular. Los contenidos de todo contrato informático se enlistan a continuación:¹⁰⁵

- a) **Objeto.** Derechos y obligaciones respecto a los bienes y servicios informáticos.
- b) **Duración y rescisión.** Término de vigencia del contrato.
- c) **Precio.** Caracterizado por que debe ser justo, verdadero y en dinero.
- d) **Facturación y pago.** Tendrán lugar de acuerdo a las consignas de mutuo acuerdo.
- e) **Control, supervisión y acceso.** Las cuales son responsabilidad de los usuarios, a fin de que las actividades informáticas se den favorablemente.
- f) **Asistencia y formación.** Todo esto con el fin de que las actividades informáticas se den en los términos más atinentes, para evitar actitudes impropias o negligentes.
- g) **Propiedad de los programas.** Es un aspecto controvertido en virtud de la ausencia de un adecuado régimen regulador conforme a los programas de cómputo.

¹⁰⁴ *Ibidem*, p. 97.

¹⁰⁵ *Ibidem* p. 99.

- h) **Protección material de la información.** Esto es en el caso de la información propiedad del usuario que esté bajo resguardo del proveedor a fin de desarrollar un programa.
- i) **Secreto y confidencialidad.** Esto es en cuanto a las informaciones que se provean ambas partes con motivo de celebración del contrato.
- j) **Responsabilidad y garantías.** Se entiende por responsabilidad de aquellas obligaciones inherentes a la firma de un contrato, en este caso informático.
- k) **Disposiciones generales.** Tales como la credibilidad de las obligaciones, incumplimiento del contrato en caso de nulidad, necesidades de anexos.
- l) **Cláusulas diversas.** Se refieren a un concepto en especial y que las partes convienen en insertarlas para una mejor relación contractual.

El problema que generan los contratos informáticos no recibe el tratamiento adecuado en nuestro país actualmente. Los particulares y las Pymes (pequeñas y medianas empresas), son quienes generalmente no disponen de un soporte y apoyo técnico conforme a la elección de un bien o servicio informático, provocando que se encuentren frente a una situación de adversidad ante los proveedores, acentuada aún más por el hecho de que la administración pública no ofrece un apoyo adecuado.

Es importante una reestructuración respecto a la política gubernamental sobre este punto, así como una depuración equitativa, tal como se viene dando en países internacionales en los que, conforme hay un mayor nivel de información, ofrecen por igual una serie de elementos, los cuales debidamente capitalizados permiten disponer un panorama muy prometedor.¹⁰⁶

¹⁰⁶ *Ibidem* p. 102.

APORTACIONES

La evolución tecnológica y la sociedad juegan un papel fundamental en la aplicación del Derecho Informático, pues sin delitos no se aplicaría el Derecho.

La tipificación de estos actos ha sido tema de debate mundial pues los delitos cometidos a través de una computadora o inclusive hacia ella no se pueden comparar en lo absoluto con los delitos tradicionales.

Desafortunadamente la sofisticación entra en estos actos ilícitos, pues no cualquier delincuente es capaz de cometerlos. Es por ello que las autoridades correspondientes rezagan el tratamiento urgente de este problema pues la solución y castigo no es digno.

Para un mayor entendimiento a cómo es que se comete cada delito, porqué surgen y qué tipo de personas son las que generalmente los realizan, este capítulo se desarrolló con el fin de esclarecer esos puntos como una posible prevención a dichos delitos informáticos; con la citación desde su concepto, elementos, cómo es que afecta a la sociedad, su economía y desarrollo en general.

Los delitos informáticos es lo principal que compete a una correcta aplicación del Derecho Informático; sin embargo, en el caso de México, si los delitos tradicionales presentan lentitud en su solución y poca demanda por parte de las víctimas, es incontable el número de casos hablando en términos informáticos.

Es por ello la importancia de fomentar el conocimiento de los delitos que se han venido ocasionando en la actualidad, con sus definiciones, clasificación, características principales y el perfil tanto del delincuente, como de las frecuentes víctimas, presentando también a su vez diversos casos famosos de delitos informáticos cometidos a nivel mundial y en México.

CAPÍTULO 3. LEGISLACIÓN ACTUAL EN MÉXICO EN RELACIÓN AL DERECHO INFORMÁTICO

Dado el creciente uso de la tecnología, Internet y las nuevas formas de comunicación, es importante conocer el panorama jurídico actual que hace frente a las realidades tecnológicas y tendencias a las que se acerca México.

La legislación informática es aquella referida al uso de medios informáticos, en donde el objetivo primordial es regularlos, establecer limitaciones y reglas para que la tecnología informática no se convierta en un medio delictivo, sino que represente un medio tecnológico en beneficio y progreso de la sociedad.

A continuación se citarán diversos artículos de leyes y Códigos existentes en el sistema jurídico mexicano, relacionados con el Derecho Informático.

3.1 LEGISLACIÓN FEDERAL

3.1.1 CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

La Constitución Mexicana padece constantemente diversas reformas acordes a las necesidades de la sociedad, su evolución, sus costumbres, estilo de vida, entre otros aspectos. Dicho lo anterior, el estilo de vida actual del ciudadano mexicano se ha transformado con el uso de la tecnología informática; por ello, este principal documento que rige a la Nación se ha regulado considerando temas relacionados con el Derecho Informático.

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS¹⁰⁷	
Artículo	Análisis
Artículo 6o.- La manifestación de las ideas no será objeto de ninguna adquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercicio en los términos dispuestos por la ley. El derecho a la información será garantizado por el	Libertad de expresión y el derecho a la información son temas del artículo. Para el efectivo ejercicio del derecho de acceso a la información, está el Instituto de Acceso a la Información (IFAI), que fue creado en 2002. El IFAI se encarga de: 1) Garantizar el derecho de acceso a la información pública gubernamental

¹⁰⁷ Cámara de Diputados del H. Congreso de la Unión. *Constitución Política de los Estados Unidos Mexicanos*. Consultado en Mayo 5 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/1.pdf>

<p>Estado.</p>	<p>2) Proteger los datos personales que están en manos del gobierno federal</p> <p>3) Y resolver sobre las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado.¹⁰⁸</p> <p>La información como derecho fundamental, forma parte de una forma de vida actual. Los nuevos medios de información tecnológicos, impactan en la manifestación de ideas, que necesitan regulación en caso de perturbar su integridad.</p>
<p>Artículo 7o.- Es inviolable la libertad de escribir y publicar escritos sobre cualquiera materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.</p>	<p>La libertad de expresión es un derecho ciudadano desde que se nace. Este derecho hoy en día debe tener un especial cuidado en cuanto al periodismo, Internet y las redes sociales, que actualmente son herramientas sumamente poderosas, pero a la vez susceptibles de malversaciones, por lo que es significativo ejercer de manera responsable y adecuada la libertad de expresión.</p>
<p>Artículo 16.- Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como manifestar su oposición (...)</p>	<p>Este artículo tuvo una importante reforma en Junio del 2009 sobre el tema de la protección de datos personales. Este derecho, conocido como "<i>Habeas Data</i>" se refiere al derecho que tiene todo ciudadano a la protección de sus datos personales y a solicitar que sus datos e información sean actualizados, se modifiquen, cancelen o eliminen si la información sobre su persona vulnera su imagen y privacidad o le cause un perjuicio. Las</p>

¹⁰⁸ ¿Qué es el IFAI? Consultado en Mayo 5, 2012 en <http://www.ifai.org.mx/QuienesSomos>

<p>(Párrafo 12)</p> <p>Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas.</p>	<p>comunicaciones están en un nivel cada vez más avanzado, es por eso que ahora con tan sólo el envío de un correo electrónico, el usuario se enfrenta a los riesgos frecuentes de violación a la privacidad.</p> <p>El <i>Habeas Data</i> es una acción constitucional que se ejerce mediante una petición formal del interesado a los tribunales constitucionales para que verifiquen si los datos de un ciudadano tanto en el ámbito público como privado hayan sido obtenidos lícitamente y conforme al marco legislativo aplicable en la materia.¹⁰⁹</p> <p>Existe la Ley Federal de Protección de Datos Personales, que se aprobó el 27 de abril del 2010 y entró en vigor el 6 de Julio del mismo año.</p>
---	--

¹⁰⁹ Protección de datos y privacidad, *Reforma Constitucional para Reconocer el Derecho Habeas Data en México*. Consultado en Mayo 5 del 2012 en <http://www.protecciondedatos.org.mx/2009/06/reforma-constitucional-para-reconocer-el-derecho-habeas-data-en-mexico/>

3.1.2 CÓDIGO PENAL FEDERAL

El 28 de marzo del 2012, la Cámara de Diputados aprobó una iniciativa que reforma y adiciona ciertas disposiciones del Código Penal Federal, en torno al fraude cibernético y demás delitos informáticos, tratando así que las herramientas informáticas y las comunicaciones sean empleadas correctamente y evitar que la tecnología sirva de instrumento delictivo.

Entre las modificaciones que fueron aprobadas en materia de informática y comunicaciones, se encuentra el Título noveno, que es la “Revelación de secretos y acceso ilícito a sistemas y equipos de informática”.

CÓDIGO PENAL FEDERAL¹¹⁰	
Título Noveno Revelación de secretos y acceso ilícito a sistemas y equipos de informática CAPITULO I Revelación de secretos	
Artículo	Análisis
Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.	Hoy en día es difícil imaginar la vida laboral sin equipos de cómputo, en donde se maneja información diversa para el desarrollo de la misma y su resguardo, incluyendo empleados y sus cargos. Por lo que, se sancionará todo aquel empleado que sin consentimiento revele información, en perjuicio de alguien, o en beneficio ilícito inclusive, aprovechándose de su cargo.
Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de	El artículo es claro respecto a la divulgación, utilización o revelación de información e imágenes privadas. Para interceptar mensajes privados existen diversos programas: <i>Sniffer:</i> Monitorea la red y detecta fallos de seguridad en ella o en

¹¹⁰ Cámara de Diputados del H. Congreso de la Unión. *Código Penal Federal*. Consultado en Mayo 8 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf>

<p>trescientos a seiscientos días multa.</p>	<p>nuestro sistema. Intercepta correos electrónicos; filtra los paquetes de la red, los examina y mira las peticiones de algunos puertos, aquí es cuando, en algunos casos, en los primeros 30 segundos se graba algún login y password.</p> <p><i>Spyware o Programas espías:</i> Recopilan información sobre una persona u organización sin su conocimiento, con el fin de distribuirlo a empresas publicitarias u otras organizaciones interesadas por dicha información.</p> <p><i>Adware:</i> Son anuncios emergentes y aparecen durante la navegación web, en algunos casos también pueden recopilar información del usuario.</p>
--	---

CAPITULO II
Acceso ilícito a sistemas y equipos de informática

<p>Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.</p> <p>Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.</p>	<p>Lo establecido en este artículo son sanciones referentes al robo, modificación y destrucción de información que estén protegidos por algún mecanismo de seguridad. Generalmente los ataques son de los <i>crackers</i> y <i>hackers</i>; éstos rompen cualquier tipo de seguridad de algún sistema informático o <i>software</i> y no conformes con eso, también roban información, la cual posteriormente publican sin autorización alguna, en perjuicio de alguien.</p>
---	--

<p>Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.</p> <p>A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.</p>	<p>El delito en cuestión sigue siendo sobre actos ilícitos a la información contenida en medios de almacenamiento, sistemas de información o <i>software</i> debidamente protegido y hacer mal uso de ella, puede traer serias repercusiones.</p> <p>Generalmente el acto ilícito está en el <i>hacking</i> y <i>cracking</i>.</p> <p>No obstante se incluyen también sanciones para servidores públicos que además de las sanciones ya estipuladas, se les impone otras más, como la destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.</p>
<p>Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.</p> <p>Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de</p>	<p>Los últimos 2 artículos si bien contemplan los mismos delitos para sancionar a una persona, aquí la diferencia está en que conlleva al personal del Estado, en donde si tiene la autorización para manejo de información y abusando de su cargo, modifique, destruya o provoque pérdida de dicha información.</p> <p>Por lo tanto todo servidor público que cometa lo anterior eleva su sanción por el hecho de ofrecer sus servicios en una institución pública:</p> <p><i>“Si el responsable es o hubiera sido</i></p>

<p>ciento cincuenta a cuatrocientos cincuenta días multa.</p> <p>A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.</p>	<p><i>servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.”</i></p>
<p>Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.</p> <p>Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.</p>	<p>Se hace referencia a las instituciones que integran el sistema financiero. En este mismo Código Penal Federal en su Título Vigésimo Tercero, Capítulo II párrafo 7, que son las instituciones de crédito, de seguros y de fianzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades financieras de objeto limitado, uniones de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradoras de fondos de retiro y cualquier otro intermediario financiero o cambiario.</p> <p>En dichas instituciones puede ser común la modificación de información, alteración y hasta fraude, debido al frecuente uso de medios electrónicos, como transferencias, consultas en línea etcétera.</p>
<p>Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema</p>	<p>Dicho artículo también se refiere a las instituciones del sistema financiero, pero ahora se encuentra de por medio la autorización al</p>

<p>financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.</p> <p>Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.</p>	<p>acceso a los sistemas o equipos informáticos, donde aprovechándose de ello, pueda cometer actos ilícitos.</p> <p>Aquellos que integran una institución financiera, y sean autorizados para el acceso de información y hagan mal uso de ella, se harán acreedores a la incrementación en una mitad de sanciones además de las penas establecidas en este artículo.</p>
---	--

CAPÍTULO QUINTO
TÍTULO VIGESIMO SEXTO
De los Delitos en Materia de Derechos de Autor

<p>Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:</p> <p>I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.</p> <p>Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a</p>	<p>Este artículo pone en discusión todo lo llamado piratería; este término significa que todo lo que se conoce como copia ilegal de alguna obra, software o música, se le llama piratería. Actualmente existen diversos sitios o programas en internet que distribuyen dichas copias ilegales.</p> <p>En México este es un problema actual, pues el comercio ilegal sobre diversos productos principalmente en materia de tecnología, ha ido en aumento, puesto que apuesta a lo “barato” y a su vez representa grandes pérdidas monetarias a autores, productores o fabricantes de dichas obras. La piratería definitivamente es un tema que presenta debate y ambigüedades en su solución.</p>
---	--

<p>que se refiere el párrafo anterior, o</p> <p>II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.</p>	
<p>Artículo 426.- Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:</p> <p>I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y</p> <p>II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.</p>	<p>Este artículo hace referencia a señales satelitales, las cuales también están propensas a ser robadas por un distribuidor distinto al legítimo u otra persona.</p> <p>Una técnica utilizada para este tipo de hurto es el <i>“Shoulder surfing”</i> que usa técnicas de observación directa, para obtener información, y se utiliza principalmente para obtener contraseñas, números PIN, códigos de seguridad y datos similares. Igualmente existe un dispositivo llamado <i>jammer</i>, un inhibidor de señales satelitales, que bloquea las comunicaciones celulares perdiendo conexión con la torre celular.</p>

3.1.3 CÓDIGO CIVIL FEDERAL

Hasta el día de hoy abunda diversidad de contratos celebrados entre presentes o ausentes, empleando diferentes medios, de los cuales se destacan los de carácter electrónico, ya que promueven la celebración de mayor número de contratos. En Junio 7 de 2000, una reforma al Código Civil Federal, comprendió cambios en diferentes ordenamientos, dirigida básicamente hacia el comercio y la contratación electrónica; se reformaron tres preceptos que actualizan de manera concreta el Derecho de los contratos.

Dicha reforma busca el reconocimiento de la contratación por vía electrónica, para que los actos celebrados sean igualmente válidos que aquellos que se celebran por medio de un papel (contratos).

CÓDIGO CIVIL FEDERAL¹¹¹	
LIBRO CUARTO De las Obligaciones	
PRIMERA PARTE De las Obligaciones en General	
TITULO PRIMERO Fuentes de las Obligaciones	
CAPITULO I Del consentimiento	
Artículo	Análisis
Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente: I. Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y (...)	Para la optimización de tiempo, recursos humanos y materiales entre las instituciones de fianzas, seguros y sus clientes, se ha optado por la emisión de pólizas electrónicas, las cuales eran en formatos pre impresas y seriadas. A partir de esta reforma se opta por emitir pólizas electrónicas, con el seguimiento de su numeración y la impresión digitalizada de la firma del funcionario autorizado.

¹¹¹ Cámara de Diputados del H. Congreso de la Unión. *Código Civil Federal*. Consultado en Mayo 19 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/2.pdf>

	<p>También aplica a contratos que eran por escrito, y era necesaria la firma para una mayor validez, respetando el acuerdo entre los contratantes.</p>
<p>Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente.</p> <p>La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.</p>	<p>Al realizar una oferta por teléfono aunque las partes no estén físicamente presentes, se establece una comunicación directa, lo que permite la posibilidad de hacer la oferta, misma que al ser escuchada por el otro contratante, puede expresar por ese medio, su aceptación.</p> <p>En el caso del contrato electrónico es entre presentes o ausentes, según la oferta-aceptación se produzca o no de forma inmediata.</p> <p>El artículo también refiere a señalar o no un plazo específico para recibir la aceptación, originando ciertas obligaciones en relación al plazo que se concedió al aceptante, tomando en cuenta el medio donde se realiza la oferta.</p>
<p>Artículo 1811.- La propuesta y aceptación hechas por telégrafo producen efectos si los contratantes con anterioridad habían estipulado por escrito esta manera de contratar, y si los originales de los respectivos telegramas contienen las firmas de los contratantes y los signos convencionales establecidos entre ellos. Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos.</p>	<p>Existen contratos que para tener validez requieren de la formalidad. Antes del uso de los medios electrónicos como vías de contratación, el requisito se entendía como aquel contrato soportado en un papel, es decir, en un elemento tangible que le diera permanencia al contrato celebrado.</p> <p>Sin embargo, en el caso del contrato electrónico, no será necesaria alguna condición o cláusula para que el contrato se lleve a cabo.</p>

Forma

Artículo 1834 bis.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesibles para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

El artículo 1834 refiere a la obligación de la firma escrita o huella digital de los obligados (en caso de no saber firmar) en el contrato para su cumplimiento.

Ahora en este artículo, el paso importante es que ya se considera al contrato electrónico para su cumplimiento. En caso de que se requiera constatar de manera mucho más legal dichos contratos, se recurrirá a un fedatario público a quienes el gobierno les otorga la facultad de poder dar fe pública de los actos jurídicos que se celebren ante ellos, y así proporcionar seguridad jurídica a los particulares. Su función es dar forma y legitimar ciertos actos jurídicos, o hacer contar hechos jurídicos que se pretendan oponer ante terceros.¹¹²

Este punto dará fe y legalidad de documentación informática como firmas digitalizadas y la autenticación del contenido de documentos electrónicos en sí, luego procederá a guardar la documentación y especialmente el certificado emitido, en sus registros o protocolos.

¹¹² Servicio de Administración Tributaria, Consultado en Mayo 19 del 2012 en http://www.sat.gob.mx/6_630.html

3.1.4 CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES

CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES ¹¹³	
Artículo	Análisis
<p>Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.</p> <p>Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.</p> <p>Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.</p>	<p>Dicho artículo se modificó el 29 de mayo del 2000, en donde se introdujeron reformas en las que se reconocen efectos jurídicos, validez y fuerza probatoria del documento electrónico, así como los mensajes de datos. Asimismo, también se reconocen los requisitos de autenticidad, integridad y contabilidad de información que se genera a través de la comunicación en mensajes de datos.</p> <p>Es una reforma con una alta importancia debido a que no sólo habrá pruebas en papel escrito, sino también en diversos soportes electrónicos. Para el concepto de valoración de fuerza probatoria se deben considerar peritos especializados en el área de Informática, para determinar su validez, manteniendo íntegra la información a procesar y revisar.</p>

¹¹³ Cámara de Diputados del H. Congreso de la Unión. *Código Federal de Procedimientos Civiles*. Consultado en Mayo 28 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/6.pdf>

3.1.5 CÓDIGO DE COMERCIO

El 29 de agosto de 2003, se publicó en el Diario Oficial de la Federación, el decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de firma electrónica.

CÓDIGO DE COMERCIO ¹¹⁴	
CAPITULO II Del registro de comercio	
Artículo	Análisis
<p>Artículo 20.- El Registro Público de Comercio operará con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas. Las bases de datos contarán con al menos un respaldo electrónico.</p> <p>Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral.</p> <p>Las bases de datos del Registro Público de Comercio en las entidades federativas se integrarán con el conjunto de la información incorporada por medio del programa informático de cada inscripción o anotación de los actos mercantiles inscribibles, y la base de datos central con la información que los responsables del Registro incorporen en las bases de datos ubicadas en las entidades federativas.</p> <p>El programa informático será</p>	<p>La información de cualquier tipo de contrato o en su caso registro de algún comercio, será resguardado por esta base de datos que estará a cargo del Gobierno Federal.</p> <p>En este programa se realizará toda la administración de la información al igual que su difusión y consulta.</p> <p>Igualmente se notifica el uso de programas informáticos y bases de datos, interconectados con una base de datos central. Esto representa un avance tecnológico importante, pues conduce a una mejora en servicios por parte del Registro Público de Comercio, pero también a una correcta regulación jurídica, pues se encuentra de por medio un gran manejo de información.</p>

¹¹⁴ Cámara de Diputados del H. Congreso de la Unión. *Código de Comercio*. Consultado en Junio 11 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/3.pdf>

<p>establecido por la Secretaría. Dicho programa y las bases de datos del Registro Público de Comercio, serán propiedad del Gobierno Federal (...)</p>	
<p>Artículo 20 bis.- Los responsables de las oficinas del Registro Público de Comercio tendrán las atribuciones siguientes:</p> <p>V.- Operar el programa informático del sistema registral automatizado en la oficina a su cargo, conforme a lo previsto en este Capítulo, el reglamento respectivo y en los lineamientos que emita la Secretaría; (...)</p>	<p>Todo personal contratado que sea responsable del manejo de dicho programa informático para oficinas del Registro Público de Comercio, debe contar con conocimientos básicos o al menos una capacitación adecuada para la operación del mismo programa.</p>
<p>Artículo 30 bis.- La Secretaría podrá autorizar el acceso a la base de datos del Registro Público de Comercio a personas que así lo soliciten y cumplan con los requisitos para ello, en los términos de este Capítulo, el reglamento respectivo y los lineamientos que emita la Secretaría, sin que dicha autorización implique en ningún caso inscribir o modificar los asientos registrales.</p> <p>La Secretaría expedirá los certificados digitales que utilicen las personas autorizadas para firmar electrónicamente la información relacionada con el Registro Público de Comercio y demás usuarios; asimismo, podrá reconocer para el mismo fin certificados digitales expedidos por otras autoridades certificadoras siempre y cuando, a su juicio, presenten el mismo grado de confiabilidad y cumplan con las</p>	<p>Se menciona el acceso a la base de datos del Registro Público, donde se deben controlar dichos accesos para su manejo, con la expedición de certificados digitales para su firma electrónico, la Ley de Firma Electrónica avanzada Título segundo Capítulo I, artículo 7 refiere: <i>“La firma electrónica avanzada podrá ser utilizada en documentos electrónicos y, en su caso, en mensajes de datos.”</i></p> <p>Todo documento electrónico que cuente con firma electrónica avanzada tendrá un valor probatorio, dando lugar al comercio electrónico.</p>

medidas de seguridad que al efecto establezca la Secretaría.	
<p>Artículo 30 bis 1.- Cuando la autorización a que se refiere el artículo anterior se otorgue a notarios o corredores públicos, dicha autorización permitirá, además, el envío de información por medios digitales al Registro y la remisión que éste efectúe al fedatario público correspondiente del acuse que contenga el número de control o sello digital de tiempo a que se refiere el artículo 21 bis 1 de este Código.</p> <p>Los notarios y corredores públicos que soliciten dicha autorización deberán otorgar una fianza o garantía a favor de la Tesorería de la Federación y registrarla ante la Secretaría, para garantizar los daños que pudieran ocasionar a los particulares y a la Secretaría con motivo de la operación del programa informático y el uso de la información del registro, incluida la que corresponde a la Sección Única del presente Capítulo, por un monto mínimo equivalente a 10 000 veces el salario mínimo diario vigente en el Distrito Federal (...)</p>	<p>En el caso de que las personas autorizadas al acceso de información del Registro Público de Comercio sean notarios o corredores públicos, se les permitirá el envío y uso de información por medios electrónicos.</p> <p>Esto constata una vez más que también se le da un valor un probatorio al documento electrónico, además del control de información, pues para quienes no sigan los lineamientos de seguridad se les obligará al pago de una fianza, garantizando los daños que se ocasionen mediante un mal uso de la información.</p>
<p>TITULO SEGUNDO De Comercio Electrónico CAPITULO I De los Mensajes de Datos</p>	
<p>Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México</p>	<p>Dicho artículo regirá en toda la República, con una mejor perspectiva de comunicación y comercio (inclusive internacional) con el uso de medios electrónicos, con sus debidos estándares para un</p>

<p>sea parte.</p> <p>Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa.</p> <p>En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología.</p>	<p>mejor manejo de actos de comercio.</p> <p>Nuevamente la Firma electrónica y el documento electrónico toman un valor en la celebración de actos comerciales.</p>
<p>Artículo 89 bis.- No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.</p>	<p>Se rectifica y se reconoce la validez de la información contenida en un Mensaje de Datos, otorgando fiabilidad a la utilización de los mismos en actos comerciales. Un Mensaje de datos puede constituir un pensamiento, idea, imagen, audio, datos o información, ya sea explícito o secreto, dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones</p>
<p>CAPITULO II De las Firmas</p>	
<p>Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos. La Firma Electrónica se considerará Avanzada</p>	<p>La firma electrónica consta de una serie de requisitos que se establecen en este artículo.</p> <p>Es fundamental que para una celebración de contrato exitosa ambas partes acuerden en la confiabilidad de una firma electrónica en cuanto a su validez y significado de compromiso al igual que una</p>

<p>o Fiable si cumple por lo menos los siguientes requisitos:</p> <p>I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;</p> <p>II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;</p> <p>III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y</p> <p>IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.</p>	<p>firma autógrafa, esto beneficia aún más cuando existan casos de comercio electrónico no-personal, es decir, algún acuerdo de forma remota u <i>online</i>, en donde lineamientos como los citados, son de gran ayuda y guía para una correcta implementación de la firma electrónica avanzada.</p>
<p>Artículo 98.- Los Prestadores de Servicios de Certificación determinarán y harán del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97.</p> <p>La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos.</p> <p>Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.</p>	<p>Se puntualiza la obligación de los Prestadores de Servicios a informar a los usuarios si sus Firmas Electrónicas Avanzadas cumplen con los requisitos que se disponen para el uso de las mismas, estos requerimientos se encuentran en el artículo 108 de este mismo código y en el artículo anterior. Los prestadores de servicios que autoriza éste Código son los establecidos en el artículo 100 (notarios y corredores públicos, personas morales de carácter privado e instituciones públicas). En el caso de que los prestadores de servicios no hagan cumplimiento de sus obligaciones, se les sancionará conforme al artículo 110 de éste Código, ya sea inhabilitado, suspendido o en su caso cancelado en su ejercicio.</p>

3.1.6 LEY FEDERAL DEL PROCEDIMIENTO ADMINISTRATIVO

El 15 de diciembre del 2011, se publicó una reforma en el Diario Oficial de la Federación, establecida en la Ley Federal de Procedimiento Administrativo, en donde la contratación electrónica se regula de manera diferente a lo tradicional y requiere a la Firma Digital o Electrónica como elemento para la identificación y vinculación del particular en los trámites ante la Administración Pública Federal.

LEY FEDERAL DEL PROCEDIMIENTO ADMINISTRATIVO¹¹⁵	
TITULO TERCERO A De la mejora regulatoria	
Artículo	Análisis
<p>Artículo 69-B.- Cada dependencia y organismo descentralizado creará un Registro de Personas Acreditadas para realizar trámites ante éstas; asignando al efecto un número de identificación al interesado...</p> <p>Los registros de personas acreditadas deberán estar interconectados informáticamente y el número de identificación asignado por una dependencia u organismo descentralizado será obligatorio para las demás.</p> <p>Para efectos de esta Ley, por trámite se entiende cualquier solicitud o entrega de información que las personas físicas o morales del sector privado hagan ante una dependencia u organismo descentralizado, ya sea para cumplir una obligación, obtener un beneficio o servicio o, en general, a fin de que se emita una resolución, así como cualquier documento que dichas personas estén obligadas a</p>	<p>Una vez entendido lo que es un trámite para esta ley, se creará un Registro de Personas Acreditadas para que puedan realizar trámites ante dependencias y organismos descentralizados.</p> <p>Dichos registros ahora deben estar conectados informáticamente, para una mejor identificación de personas y manejo de información.</p> <p>Se hace énfasis en lo importante del uso de las herramientas informáticas, pues sin duda facilita los procesos administrativos, pero a su vez requiere medidas de seguridad y jurídicas principalmente, por cuestiones de manejo de datos privados e incluso tributarios, pues en cada trámite el número de identificación se asignará con base en la clave del Registro Federal de Contribuyentes.</p>

¹¹⁵ Cámara de Diputados del H. Congreso de la Unión. *Ley Federal de Procedimiento Administrativo*. Consultado en Junio 23 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/112.pdf>

<p>conservar (...)</p>	
<p>Artículo 69-C.</p> <p>(Párrafo segundo)</p> <p>En los procedimientos administrativos, las dependencias y los organismos descentralizados de la Administración Pública Federal recibirán las promociones o solicitudes que, en términos de esta Ley, los particulares presenten por escrito, sin perjuicio de que dichos documentos puedan presentarse a través de medios de comunicación electrónica en las etapas que las propias dependencias y organismos así lo determinen mediante reglas de carácter general publicadas en el Diario Oficial de la Federación. En estos últimos casos se emplearán, en sustitución de la firma autógrafa, medios de identificación electrónica.</p> <p>El uso de dichos medios de comunicación electrónica será optativo para cualquier interesado, incluidos los particulares que se encuentren inscritos en el Registro de Personas Acreditadas a que alude el Artículo 69-B de esta Ley.</p> <p>(...)</p>	<p>Para todo procedimiento administrativo, en sus solicitudes, se podrá hacer uso de medios y documentos electrónicos. Las dependencias podrán realizar citatorios, notificaciones, etcétera, de forma electrónica como lo establece el artículo 35 de esta Ley.</p> <p>Para estos casos, se podrá sustituir la firma autógrafa por la electrónica y hacer uso de certificación de medios de identificación, todo esto de manera responsable por las dependencias u organismos descentralizados.</p> <p>En el artículo se destaca lo siguiente:</p> <p><i>“Los documentos presentados por medios de comunicación electrónica producirán los mismos efectos que las leyes otorgan a los documentos firmados autógrafamente y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos.”</i></p> <p>La responsabilidad en la certificación de medios electrónicos principalmente es de las dependencias, pues son quienes manejan esta información; pero también como usuarios estamos en el deber de prevenir y usar correctamente nuestra información.</p> <p>El valor probatorio de los documentos aquí también toma fuerza.</p>

3.1.7 LEY FEDERAL DEL DERECHO DE AUTOR

En el año de 1991 se produjo una reforma a la Ley Federal de Derechos de Autor, que incluyó entre otros, la incorporación de los programas de computación como un género de obra independiente y autónoma respecto del resto de las demás obras mencionadas por la Ley hasta ese entonces. Por lo anterior, la protección que otorga ésta Ley a los titulares de esos derechos, se hizo extensiva a los creadores y productores de programas de computación.

LEY FEDERAL DEL DERECHO DE AUTOR ¹¹⁶	Artículo 4o.	Protección de obras de acuerdo a su origen y creación. <i>b) Las que han sido puestas a disposición del público mediante su almacenamiento por medios electrónicos que permitan al público obtener ejemplares tangibles de la misma, cualquiera que sea la índole de estos ejemplares;...</i>
	Artículo 6o.	Fijación de elementos en obras protegidas, incluyendo obras digitales: <i>“que en cualquier forma o soporte material, incluyendo los electrónicos, permita su percepción, reproducción u otra forma de comunicación.”</i>
	Artículo 13	Mención de las ramas en que toda obra esté protegida. En el punto XI están los programas de cómputo.
	Artículo 16	Las obras podrán ser de conocimiento público mediante la divulgación, publicación, comunicación pública, ejecución o representación pública, distribución al público y reproducción. En la publicación y reproducción es donde se hace mención al almacenamiento temporal o permanente de la obra por medios electrónicos.
	Artículo 27	Los titulares de los derechos de obras protegidas pueden permitir o autorizar la reproducción incluyendo por medios electrónicos y la forma en que serán transmitidas, mencionando cable, fibra óptica y vía satélite.

¹¹⁶ Cámara de Diputados del H. Congreso de la Unión. *Ley Federal de Derechos de Autor*. Consultado en Mayo 11 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/122.pdf>

Capítulo IV: De los Programas de Computación y las Bases de Datos	
<p>Artículo 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.</p>	<p>El artículo especifica la definición de programa, esto es con el propósito de conocer el elemento al cual se está legislando, elemento que hoy en día es la base de cualquier acción que se realiza un ordenador.</p>
<p>Artículo 102.- Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.</p>	<p>Se determina que los programas de cómputo se protegen tanto al Sistema Operativo (que es el conjunto de programas relacionados entre sí para hacer que el ordenador realice una tarea encomendada), como al código fuente o código objeto; estos se definen como códigos modificables con una serie de instrucciones para que un determinado programa realice una tarea específica.</p>
<p>Artículo 103.- Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.</p> <p>Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.</p>	<p>Si bien el programa corresponde a su creador, un mal acuerdo en la cesión de derechos o contrato del mismo, puede resultar una problemática con fines de lucro.</p> <p>Esta medida jurídica representa una protección importante para el empleado informático u organización tecnológica en su defecto.</p> <p>Se realiza una excepción si existió un pacto de por medio.</p> <p>El plazo en la cesión de los derechos no presenta límite alguno.</p>
<p>Artículo 104.- Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o</p>	<p>Aún después de las ventas en sus obras, el titular de los derechos de la misma todavía podrá decidir si seguirá vendiendo, o distribuyendo sus</p>

<p>sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.</p>	<p>ejemplares.</p> <p>Lo establecido no aplica una vez que el programa tenga su propia licencia de uso, pues sería incongruente prohibir que se siga usando dicho programa, cuando el derecho se obtuvo mediante la compra del <i>software</i>.</p>
<p>Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:</p> <p>I. Sea indispensable para la utilización del programa, o</p> <p>II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.</p>	<p>El usuario tiene un límite de uso de licencia del programa adquirido al igual que un número de copias permitidas, las cuales podrán respaldarse en caso de daño o extravío del programa original.</p> <p>En materia de licencias de cómputo en México, hay una gran proliferación de las mismas en Internet sin control alguno, encontrando cualquier tipo de programa. Internet es una herramienta que facilita una gran difusión de información. Es importante el estudio en precios sobre licencias y compra de <i>software</i>, pues en el caso de países en vías de desarrollo, se considera un “lujo” la compra legal de un programa de cómputo.</p>
<p>Artículo 106.- El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:</p> <p>I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;</p> <p>II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;</p>	<p>Quien cuente con los derechos patrimoniales sobre el programa de cómputo es la única persona facultada para autorizar o prohibir:</p> <p>-El tiempo en que se reproduzca el programa, ya sea de forma provisional o permanente.</p> <p>-Sobre cambios, arreglos, traducción o cualquier acción que implique una modificación al programa original.</p> <p>-La decompilación, que es un proceso</p>

<p>III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y</p> <p>IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.</p>	<p>de conversión de un código leído por una máquina, para después ser leído por el humano; y el desensamblaje que es un programa que se encarga de traducir lenguaje de máquina (instrucciones fuentes a ejecutar en el ordenador) a lenguaje ensamblador (el que interpretan los microprocesadores y ordenador).</p>
<p>Artículo 107.- Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.</p>	<p>Se especifica la protección hacia las bases de datos que formen creaciones intelectuales, es decir, sean originales. Esa información será protegida como compilación sin implicar los datos y materiales, es decir, solamente la información de código como elemento valioso, es la que se protege. La compilación se entiende como una revisión del código fuente de un programa (no tenga errores), para que sea entendido por el ordenador y se ejecute exitosamente.</p>
<p>Artículo 108.- Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.</p>	<p>Las bases de datos aun no siendo originales, se protegerán en su uso para quien(es) exclusivamente las elaboró por un lapso de tiempo de 5 años. Este lapso de tiempo de protección es relativamente corto en comparación a la cantidad de información en la base de datos y al uso que se le dé; por lo que se considera que dicho tiempo debe aumentar conforme al tipo de información que se maneje, además de la frecuencia de uso.</p>
<p>Artículo 109.- El acceso a información de carácter privado relativa a las personas, contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción,</p>	<p>Se protege la información de carácter privado de las bases de datos en su totalidad; se requerirá autorización para tratamiento, consulta y difusión.</p> <p>Se exceptúan las investigaciones</p>

<p>divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.</p> <p>Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.</p>	<p>jurídicas, dejando libre acceso a archivos y a las consultas necesarias, todo esto conforme a los procedimientos que correspondan.</p> <p>Es importante se considere que no sólo la información de carácter privado se debe proteger. El acceso público es un aspecto del que no se debe olvidar, pues no por su carácter público se deja a la intemperie para futuras acciones ilícitas.</p>
<p>Artículo 110.- El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:</p> <p>I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;</p> <p>II. Su traducción, adaptación, reordenación y cualquier otra modificación;</p> <p>III. La distribución del original o copias de la base de datos;</p> <p>IV. La comunicación al público, y</p> <p>V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.</p>	<p>Sólo quien conserva los derechos sobre una base de datos podrá autorizar o prohibir su reproducción, modificación y distribución.</p> <p>Es una primordial medida de seguridad, pues se habla de proteger la estructura que conforma una base de datos, puesto que cualquier modificación a la misma sin autorización alguna, desestabiliza la integridad de la base de datos. A integridad nos referimos a los elementos que la componen, como la colección de información organizada en campos (pieza única de información), registros (sistema completo de campos) y archivos (colección de registros).</p>
<p>Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados</p>	<p>Los programas informáticos lo constituyen elementos visuales, auditivos y gráficos, dependiendo para lo que fue creado. Dichos elementos</p>

<p>quedan protegidos por esta Ley en los elementos primigenios que contengan.</p>	<p>contarán con una protección en el caso exclusivo de que el contenido sea original al programa informático. La mayoría de los casos se resuelven con una inserción de créditos o un permiso para el uso de contenido ya protegido.</p>
<p>Artículo 112.- Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.</p>	<p>Todo aparato que se use para el <i>hackeo</i> técnico de programas de cómputo y las telecomunicaciones en general, se prohibirá importarlo, fabricarlo o distribuirlo.</p> <p>Dicha prohibición no es suficiente, ya que debido a la alta demanda de productos y con precios elevados, el contrabando y distribución de dichos productos seguirá en pie.</p>
<p>Artículo 113.- Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.</p>	<p>Toda obra que se transmita por medios electrónicos, redes de telecomunicaciones y los resultados que se obtengan de dicha obra, serán protegidas por la Ley. Por resultados contrarios, se podría entender como la reproducción indebida o piratería, es decir, acciones ilícitas que afectan directamente la obra.</p> <p>Las obras van referidas al mercado musical, visual, satelital, computacional e inclusive literario.</p>
<p>Artículo 114.- La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.</p>	<p>Se establece protección de transmisión a las obras, mediante cable y satélites; se deben moldear a la legislación mexicana, respetando cualquier disposición sobre el tratamiento de las mismas en su transmisión. Lo esencial está en la adecuación a la ley mexicana, que es la que nos confiere en materia de telecomunicaciones.</p>

3.1.8 LEY FEDERAL DE TELECOMUNICACIONES

La Ley Federal de Telecomunicaciones entró en vigor el 8 de Junio de 1995. Los principales aspectos de ésta Ley, está primeramente, el interés de agrupar en una sola legislación todas las cuestiones y asuntos en materia de telecomunicaciones que anteriormente se encontraban dispersas en distintas leyes relacionadas; otro aspecto es la apertura que se observa en la materia, en relación a la participación privada nacional como extranjera, puesto que, a partir de la entrada en vigor del Tratado de Libre Comercio de América del Norte (TLC) el 1 de enero de 1994, liberaliza las telecomunicaciones en el país.

LEY FEDERAL DE TELECOMUNICACIONES ¹¹⁷	
Artículo	Análisis
Artículo 1. La presente Ley es de orden público y tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, y de la comunicación vía satélite.	La Ley tiene por objetivo regular una parte de las TIC: las comunicaciones que se realizan por medio del espectro radioeléctrico, éste concepto se define como “el medio por el cual se transmiten las frecuencias de ondas de radio electromagnéticas que permiten las telecomunicaciones” ¹¹⁸ por ejemplo: radio, televisión, Internet, telefonía móvil, televisión digital terrestre, etc., en general, las telecomunicaciones en México.

¹¹⁷ Cámara de Diputados del H. Congreso de la Unión. *Ley Federal de Telecomunicaciones*. Consultado en Mayo 23 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/118.pdf>

¹¹⁸ *El espectro radioeléctrico*. Consultado en Mayo 23, 2012 en <http://www.vidadigitalradio.com/el-espectro-radioelectrico/>

3.1.9 LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL

La Ley Federal de Transparencia y Acceso a la información Pública Gubernamental entró en vigor el 12 de junio de 2002. Esta Ley obliga a todas las autoridades del Gobierno Federal a abrir archivos, documentos y toda la información con que cuenten para que la sociedad se entere de la manera en que la gestión pública se lleva a cabo. Es decir, que está obligado el Poder Ejecutivo (incluyendo la Presidencia y la Procuraduría General de la República), los Poderes Legislativo y Judicial, así como a los organismos constitucionales autónomos, por ejemplo el Instituto Federal Electoral (IFE), la Comisión Nacional de Derechos Humanos (CNDH), o el Banco de México.

Mediante esta legislación, toda persona puede solicitar a estas instituciones federales cualquier documento que contenga información pública. Además, una parte importante de la Ley contempla que este acceso a la información se dé de manera sencilla y rápida, y sin necesidad de justificar los propósitos de la solicitud.¹¹⁹

LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL ¹²⁰	
TÍTULO PRIMERO Disposiciones Comunes Para Los Sujetos Obligados	
Capítulo I Disposiciones Generales	
Artículo	Análisis
<p>Artículo 3.- Para los efectos de esta Ley se entenderá por:</p> <p>II. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o</p>	<p>Respecto a los documentos detallados en este Artículo fracción II, se incluyen los documentos digitalizados.</p> <p>Cada dependencia cuenta con la persona responsable para dar a conocer dicha información pública, esto acerca a la ciudadanía para que</p>

¹¹⁹ Funes Grimaldo, María de Lourdes, *Qué es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*. Consultado en Julio 18 del 2012 en <http://fox.presidencia.gob.mx/cambio/transparencia/?contenido=19482&pagina=1>

¹²⁰ Cámara de Diputados del H. Congreso de la Unión. *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*. Consultado en Julio 18 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf>

<p>emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad;</p> <p>III. Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;</p>	<p>conozcan las actividades realizadas por dichas dependencias.</p> <p>Como experiencia laboral, la documentación que se envía al Gobierno Federal en materia de Inventarios es pública, por lo que se obliga a digitalizar y archivar dicha información, y la consulta puede ser en documento físico o de forma electrónica, en donde autoridades superiores nos piden entregar con cortes o plazos de cada uno de ellos. Este archivo tiene Vigencia En Archivo De Concentración de 3 años.¹²¹</p>
<p>Capítulo II Obligaciones de transparencia</p>	
<p>Artículo 7.- Con excepción de la información reservada o confidencial prevista en esta Ley, los sujetos obligados deberán poner a disposición del público y actualizar, en los términos del Reglamento y los lineamientos que expida el Instituto o la instancia equivalente a que se refiere el Artículo 61, entre otra, la información siguiente:</p> <p>I. Su estructura orgánica;</p> <p>II. Las facultades de cada unidad</p>	<p>Aquí se reitera lo que anteriormente se menciona sobre el acceso a la información pero en este caso las dependencias estarán obligadas a dar a conocer su estructura orgánica.</p> <p>Con este artículo se pretende crear un ambiente de confianza con la ciudadanía y que esta esté al tanto de algunos movimientos de los servidores públicos, al igual que las funciones que desempeñan dentro de su institución.</p>

¹²¹ Secretaría de Seguridad Publica Federal.- OADPRS

<p>administrativa;</p> <p>III. El directorio de servidores públicos, desde el nivel de jefe de departamento o sus equivalentes;</p> <p>IV. La remuneración mensual por puesto, incluso el sistema de compensación, según lo establezcan las disposiciones correspondientes;</p> <p>V. El domicilio de la unidad de enlace, además de la dirección electrónica donde podrán recibirse las solicitudes para obtener la información;</p>	<p>Al tener actualizada esta información, también se pone a disposición de la ciudadanía como contacto directo los correos electrónicos de dichos servidores públicos en los cuales se tendrá la libertad de hacer alguna petición de información dentro del gobierno.</p>
<p>Artículo 9.- La información a que se refiere el Artículo 7 deberá estar a disposición del público, a través de medios remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas equipo de cómputo, a fin de que éstas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, éstos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.</p> <p>Las dependencias y entidades deberán preparar la automatización, presentación y contenido de su información, como también su integración en línea, en los términos que disponga el Reglamento y los</p>	<p>Hoy es posible tener la información referida en este artículo al momento que la deseamos. Para esto se encuentra el Instituto Federal de Acceso a la Información y Protección de Datos, el cual cuenta con un sitio web.¹²² Asimismo esta cuenta con el apartado “Portal de Obligaciones de Transparencia”, en el que se podrá consultar la Información del Gobierno Federal.¹²³</p> <p>Para ello es importante que las dependencias y los sujetos obligados a entregar dicha información, lo hagan de forma oportuna, veraz y actualizada.</p> <p>En este portal se da a conocer un directorio de representantes de cada dependencia, el cual se puede descargar.¹²⁴</p> <p>Para proceder a la solicitud de</p>

¹²² Instituto Federal de Acceso a la Información y Protección de Datos, Consultado en Julio 19 del 2012 en <http://www.ifai.org.mx>

¹²³ Portal de Obligaciones de Transparencia. Consultado en Julio 19 del 2012 en <http://portaltransparencia.gob.mx>

¹²⁴ Unidades de Enlace. Consultado en Julio 19 del 2012 en <http://www.ifai.org.mx/Gobierno/#unidadesEnlace>

lineamientos que al respecto expida el Instituto.	acceso a la información, existe una serie de requisitos establecidos en el Capítulo 3, Artículo 40 de esta Ley, en donde el correo electrónico se valida como un medio de contacto oficial también para la atención al ciudadano.
---	---

3.1.10 LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR

En la Ley Federal de Protección al consumidor, el 29 de mayo de 2000, fue necesario reformar en tema de tecnología, en donde se consideran los medios electrónicos en las transacciones efectuadas entre proveedores y consumidores, además de la regulación en el uso de dichos medios electrónicos en actividades publicitarias y de mercadotecnia.

LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR ¹²⁵	
Capítulo I Disposiciones Generales	
Artículo	Análisis
<p>Artículo 1.- Son principios básicos en las relaciones de consumo:</p> <p>VIII. La real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados;</p>	<p>Se habla de transacciones de compra realizadas con el uso de tarjetas de crédito o débito, a su vez este pago se hace por medio de una terminal interconectada a una base de datos de cada una de las instituciones financieras.</p> <p>Otro método de transacción ahora popular es el SPEI “Sistema de Pagos Electrónicos Interbancarios”¹²⁶, desarrollado por el Banco de México, y permite hacer transferencias ya sea de envío o recepción en cuestión de segundos. Para estas transacciones existe un</p>

¹²⁵ PROFECO, *Ley Federal de Protección al Consumidor*. Consultado en Agosto 4 del 2012 en http://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_camDip.pdf

¹²⁶ *Sistema de Pagos Electrónicos Interbancarios*. Consultado en Agosto 4 del 2012 en <http://www.banxico.org.mx/sistemas-de-pago/servicios/sistema-de-pagos-electronicos-interbancarios-spei/sistema-pagos-electronicos-in.html>

	marco normativo que es la Ley de Sistemas de Pago ¹²⁷
<p>Artículo 10 (párrafo segundo)</p> <p>Los proveedores no podrán aplicar métodos o prácticas comerciales coercitivas y desleales, ni cláusulas o condiciones abusivas o impuestas en el abastecimiento de productos o servicios. Asimismo, tampoco podrán prestar servicios adicionales a los originalmente contratados que no hubieren sido solicitados o aceptados expresamente, por escrito o por vía electrónica, por el consumidor.</p>	<p>Los proveedores no deberán actuar con dolo y ventaja, no deben adicionar al contrato algún aspecto del que no se haya tratado, principalmente vía electrónica, donde en su mayoría se anexa una Política de privacidad y uso de términos y condiciones, la cual se deberá leer detalladamente para cualquier aclaración o posibles cargos extras de un servicio contratado.</p>
<p>Artículo 18.- La Procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.</p>	<p>Los consumidores tienen derecho de proteger sus datos ante su utilización con fines publicitarios. A partir de esta problemática se creó el Registro Público de Usuarios (REUS), presentado por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).</p> <p>El problema más común es el famoso <i>spam</i>, el cual sólo contiene publicidad e inclusive propagan virus.</p>
<p>CAPITULO VIII BIS</p> <p>De Los Derechos De Los Consumidores En Las Transacciones Efectuadas a Través Del Uso De Medios Electrónicos, Ópticos o De Cualquier Otra Tecnología</p>	
<p>Artículo 76 BIS.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de</p>	<p>En este artículo el derecho a la privacidad de los datos es muy vital para la relación entre consumidor y proveedor.</p>

¹²⁷ Véase *Ley de Sistemas de Pago* en <http://www.diputados.gob.mx/LeyesBiblio/pdf/255.pdf>

medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;

III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;

IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás

En especial este artículo se dirige a los proveedores, a los cuales el consumidor les otorga sus datos de carácter privado, por lo que al celebrar algún contrato con un proveedor debemos investigarlo, y a su vez éste nos deberá proporcionar los datos respecto a su giro comercial y todo en cuanto al servicio o producto ofrecido, sin estrategias engañosas y respetando la decisión del cliente de su compra.

Sobre este aspecto también existe una Ley, que es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Entre los negocios que pueden ser identificados como sujetos obligados por esta Ley están, desde los grandes bancos, aseguradoras, telefónicas, medios de comunicación, tiendas departamentales y de autoservicio, laboratorios, inmobiliarias, líneas aéreas, hasta escuelas, tintorerías, médicos, dentistas, talleres mecánicos y pizzerías. Es decir, la legislación contempla a todos aquellos giros que recaban datos personales de sus clientes, sin importar su tamaño.¹²⁸

¹²⁸ *Protección de Datos Personales*. Consultado en Agosto 7 del 2012 en <http://www.protecciondedatospersonales.org/sujetos-obligados/>

disposiciones que se deriven de ella;	
V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor; (...)	

3.1.11 LEY DE LA PROPIEDAD INDUSTRIAL

LEY DE LA PROPIEDAD INDUSTRIAL ¹²⁹	
TITULO TERCERO De los Secretos Industriales Capítulo Único	
Artículo	Análisis
Artículo 82.- Se considera secreto industrial a toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.	Este apartado se refiere a toda clase de información que no sea de carácter público y que a su vez mantenga una ventaja competitiva o económica como lo cita el mismo artículo. Debemos tener muy claro que solo la información de aplicación industrial o comercial, puede ser considerada como secreto industrial.
Artículo 83.- La información a que se refiere el artículo anterior, deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfílm, películas u otros instrumentos similares.	Toda información de secreto industrial deberá ser plasmada en alguno de los medios descritos, y así se puedan tener pruebas tangibles e intangibles de dicha información. La persona poseedora del secreto industrial deberá adoptar las medidas necesarias para preservarlo

¹²⁹ Cámara de Diputados del H. Congreso de la Unión. *Ley de la Propiedad Industrial*. Consultado en Agosto 16 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/50.pdf>

	<p>y resguardarlo.</p> <p>El portal del Instituto Mexicano de la Propiedad Industrial explica trámites administrativos para el registro de alguna obra.¹³⁰</p>
--	---

3.1.12 LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

En julio del 2010, se publica la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la ventaja de esta ley en México, es que integran conceptos referentes a la innovación tecnológica de los últimos diez años y hace que el tratamiento de datos sea distinto.

Dentro de los objetivos es proteger y regular que los datos personales sean usados para la finalidad que fueron entregados, con un control de quién y para qué los tiene.

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESION DE LOS PARTICULARES¹³¹	
CAPÍTULO I Disposiciones Generales	
Articulo	Análisis
<p>Artículo 3.- Para los efectos de esta Ley, se entenderá por:</p> <p>I. Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley.</p> <p>II. Bases de datos: El conjunto ordenado de datos personales</p>	<p>En esta primera parte de la ley se desglosa cuáles son las diferentes formas de obtención de los datos o los puntos que se deben cumplir para el tratamiento de los mismos.</p> <p>En la fracción I el aviso de privacidad hace del conocimiento al titular que su información personal será recabada y utilizada para ciertos fines, de igual manera las características del tratamiento al que</p>

¹³⁰ Véase http://www.impi.gob.mx/wb/IMPI/quienes_somos

¹³¹ Cámara de Diputados del H. Congreso de la Unión. *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Consultado en Agosto 26 del 2012 en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

<p>referentes a una persona identificada o identificable.</p> <p>III. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.</p> <p>IV. Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.</p>	<p>serán sometidos los datos personales.</p> <p>A partir de lo anterior a los datos se le dan tratamientos que son explícitos a partir de la fracción II de este artículo.</p>
--	--

CAPÍTULO II

De los Principios de Protección de Datos Personales

<p>Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.</p> <p>La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.</p> <p>En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.</p>	<p>Como bien se describe, la persona confiará en que sus datos personales no se obtuvieron de forma engañosa, sin ningún chantaje o mentira.</p> <p>Todo esto estará plasmado en el documento de Aviso de privacidad</p>
--	--

<p>Artículo 9.- Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.</p> <p>No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.</p>	<p>Para este tipo de datos (Datos personales Sensibles), una firma del usuario es importante para la autenticación y consentimiento de proporcionar sus datos.</p> <p>En el caso de una firma electrónica ayuda también a este tipo de autenticación, haciendo legítimo un trámite muy importante, como lo es la recopilación de datos.</p>
--	---

CAPÍTULO V
De la Transferencia de Datos

<p>Artículo 36.- Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.</p> <p>El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos</p>	<p>Se maneja el aviso de privacidad; en este caso si el responsable pretende transferir datos personales a terceros (nacionales o internacionales) lo debió haber especificado y plasmado en dicho aviso. A esta modalidad se le llama Aviso de privacidad completo y se debe dar a conocer en el momento que se recaban los datos.</p> <p>En el artículo 37, se enlistan algunas excepciones, en las que pueden dar conocer datos sin el consentimiento del titular; por ejemplo:</p> <p style="text-align: center;"><i>“fracción II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;...”</i></p>
--	--

CAPÍTULO X
De las Infracciones y Sanciones

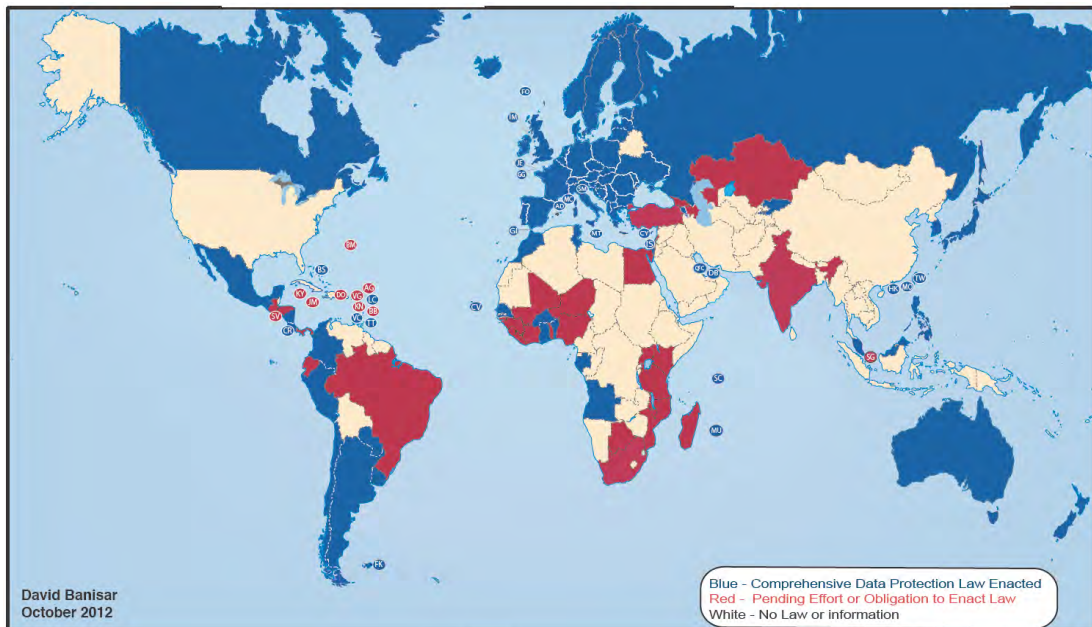
<p>Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:</p> <p>I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;</p> <p>II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;</p> <p>III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;</p> <p>IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;</p> <p>V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;</p> <p>VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;</p> <p>VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;</p> <p>VIII. Incumplir el deber de</p>	<p>En este artículo se detallan las conductas ilícitas que el responsable de los datos personales pueda presentar y serán sancionadas conforme al Artículo 64 de esta ley, el cual está dividido de la siguiente manera:</p> <p>De la fracción I la sanción será de igual manera la fracción I del artículo 64 de esta ley.</p> <p>De la fracción II a la VII, la sanción que corresponde es la fracción II.</p> <p>De la fracción VII a XVIII corresponderá la fracción III.</p> <p>En caso de que sigan las conductas reiteradamente se aplicara la fracción IV.</p>
---	--

<p>confidencialidad establecido en el artículo 21 de esta Ley;</p> <p>IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;</p> <p>X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;</p> <p>XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;</p> <p>XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;</p> <p>XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;</p> <p>XIV. Obstruir los actos de verificación de la autoridad;</p> <p>XV. Recabar datos en forma engañosa y fraudulenta;</p> <p>XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;</p> <p>XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados</p>	
---	--

<p>Unidos Mexicanos;</p> <p>XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y</p> <p>XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.</p>	
--	--

Cabe mencionar que los “Lineamientos del Aviso de privacidad”¹³² son publicados el 17 de enero de 2013 en el Diario Oficial de la Federación. Este es un documento mediante el cual el responsable informa al titular sobre los términos bajo los cuales serán tratados sus datos personales, destacando la identidad de la persona física o moral que decide llevar a cabo el mismo.

En el orden internacional se destacan antecedentes de la protección de la intimidad y el honor de la persona en el tratamiento de sus datos. Algunas de las regulaciones más representativas se muestran en el siguiente mapa:¹³³



¹³² Véase http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

¹³³ Véase http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

3.2 LEGISLACIÓN ESTATAL

Se debe analizar y poner atención en los avances a las reformas de legislación estatal de México, específicamente en el Código Penal, es decir, destacar qué estados han contemplado los delitos informáticos o considerado temas de tecnología e informática, en general sobre Derecho Informático, haciendo su mención a continuación.

Con una adecuada regulación, se tendrá que entre mayores especificaciones de dichos actos en el Derecho e Informática, mayor certeza tendrán las personas al momento de defenderse ante situaciones adversas.

Estado	Artículo	Análisis
Aguascalientes <small>134</small>	Artículo 45, fracción XI	Delito de robo calificado. <i>“XI. Se lleve a cabo el apoderamiento mediante el uso de sistemas de informática, sistema de redes de computadoras, base de datos, soporte lógico o programas de cómputo;...”</i>
	Artículo 49, fracción II, inciso b) Pena de 7 a 13 años de prisión y de 75 a 400 días de multa.	Extorsión. Se especifica que es un delito extorsionar: <i>“b) Utilizando como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica;...”</i>
	Artículo 53, fracción III	Daño a cosas con dolo, realizado a propósito, con fines de perjudicar o por un beneficio propio. <i>“III. Si el daño se causa en forma total o parcial respecto de programas, archivos, bases de datos o cualquier otro elemento intangible contenido en sistemas o redes de computadoras, soportes lógicos o cualquier medio magnético.”</i>

¹³⁴ Legislación Penal para el Estado de Aguascalientes. Consultado en Mayo 29 del 2012 en <http://www.ordenjuridico.gob.mx/Documentos/Estatal/Aguascalientes/wo18762.pdf>

<p>Capítulo décimo segundo Tipos Penales Protectores de la Confidencialidad y la Intimidad de la Información.</p> <p>Artículo 79, fracción I</p>	<p>Revelación de secretos.</p> <p><i>“I. El aprovechamiento o difusión que una persona realice sobre archivos informáticos de uso personal de otra sin que ésta dé su consentimiento;...”</i></p>
<p>Artículo 80 A</p> <p>Se penaliza de 1 a 3 meses de prisión, de 150 a 300 días de multa.</p>	<p>El acceso informático indebido consiste en:</p> <p><i>“I. Acceder a la información contenida en un aparato para el procesamiento de datos o cualquier dispositivo de almacenamiento de información sin autorización de su propietario o poseedor legítimo; o</i></p> <p><i>II. Interferir el buen funcionamiento de un sistema operativo, programa de computadora, base de datos o cualquier archivo informático, sin autorización de su propietario o poseedor legítimo.”</i></p>
<p>Artículo 89, fracción XIII, XIV Y XV</p>	<p>Defraudación fiscal. Se especifica el uso de los medios informáticos.</p> <p><i>“XIII. Llevar dos o más libros similares o sistemas informáticos con distintos asientos o datos para registrar sus operaciones contables, fiscales o sociales;</i></p> <p><i>XIV. Destruir, ordenar o permitir la destrucción total o parcial de los libros de contabilidad o sistemas informáticos previstos en la fracción anterior;</i></p> <p><i>XV. Utilizar pastas o encuadernaciones de los libros a que se refiere la fracción XIII, para sustituir o cambiar las páginas foliadas, o alterar los sistemas informáticos de contabilidad que correspondan; ...”</i></p>

Baja California ¹³⁵	<p>Título tercero Delitos contra la inviolabilidad del secreto y de los sistemas y equipos de informática.</p> <p>Capítulo primero Revelación del secreto.</p> <p>Artículo 175</p> <p>Se castiga con 1 a 3 años de prisión y hasta 100 días de multa.</p>	<p>Tipo y punibilidad. Revelación del secreto.</p> <p><i>“Al que sin consentimiento de quien tenga derecho a otorgarlo revele un secreto, de carácter científico, industrial o comercial, o lo obtenga a través de medios electrónicos o computacionales, se le haya confiado, conoce o ha recibido con motivo de su empleo o profesión y obtenga provecho propio o ajeno...”</i></p>
	<p>Capítulo segundo Acceso ilícito a sistemas y equipos de informática</p> <p>Artículo 175 BIS</p> <p>Se impone de 6 meses a 2 años de prisión y multa de 100 a 300 días. La pena se duplica en casos contra sistemas o equipos de informática del Estado o Municipios.</p>	<p>Se penaliza el uso indebido a los sistemas informáticos.</p> <p><i>“A quien sin autorización o indebidamente, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad...”</i></p>

¹³⁵ Congreso del Estado de B.C., *Código Penal para el Estado de Baja California*. Consultado en Junio 4 del 2012 en <http://www.ordenjuridico.gob.mx/Estatal/BAJA%20CALIFORNIA/Codigos/BCOD05.pdf>

	<p>Artículo 175 TER</p> <p>Pena de 3 meses a 1 año de prisión y multa de 50 a 150 días de salario mínimo.</p>	<p>Acceso ilícito a sistemas y equipos de informática.</p> <p><i>“A quien sin autorización o indebidamente, copie o accese a información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad...”</i></p>
	<p>Artículo 224</p> <p>Se penaliza con 4 a 8 años de prisión y hasta 500 días de multa.</p>	<p>Tipo y punibilidad, actuar con fines de lucro en perjuicio del patrimonio a una persona o terceros.</p> <p><i>“Cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica...”</i></p>
	<p>Capítulo II Pornografía y turismo sexual de personas menores de dieciocho años de edad o de quienes no tienen la capacidad para comprender el significado del hecho o de personas que no tiene capacidad para resistirlo.</p> <p>Artículo 262</p> <p>Pena de 7 a 12 años de prisión y de mil a 2 mil días de multa.</p>	<p>Delito de pornografía infantil. Haciendo uso de los medios informáticos.</p> <p><i>“...o exhibirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, medios electrónicos o de cualquier otra naturaleza...”</i></p>

Baja California Sur ¹³⁶	Artículo 182 Pena de 2 a 12 años de prisión y multa hasta de 200 días de salario.	Robo o destrucción dolosa de expedientes, constancias o documentos. <i>“... quien destruya, altere o copie indebidamente constancias, resoluciones o informes contenidos en memorias o archivos electrónicos pertenecientes a los órganos de procuración y administración de justicia o a las autoridades encargadas de la ejecución de penas.”</i>
	Artículo 195 Pena de 1 a 9 años de prisión y multa de hasta 5 mil días de salario.	Sanción para quien(es): <i>“III.- Acceda ilegalmente a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo; IV.- Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo...”</i>
	Artículo 217 Se impone de 3 a 10 años de prisión.	Pornografía infantil. <i>“Cuando los actos lascivos se realicen para videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos...”</i>
	Artículo 335 Pena de 5 años de prisión y multa de 150 a 200 días de salario.	El <i>hackeo</i> es sanción en el caso de: <i>“intercepción de cualquier comunicación verbal, gestual, electrónica o de cualquier otro tipo, sin consentimiento de quien la emite o sin</i>

¹³⁶ H. Congreso del Estado de Baja California Sur, *Código Penal para el Estado de Baja California Sur*. Consultado en Junio 9 del 2012 en <http://www.ordenjuridico.gob.mx/Estatal/BAJA%20CALIFORNIA%20SUR/Codigos/BCSCOD05.pdf>

		<i>autorización del Juez federal,”</i>
Chiapas ¹³⁷	Artículo 200, fracción XXVII	Castigo para quien(es): <i>“XXVII.- Al que para obtener algún beneficio, para sí o para un tercero, por cualquier medio acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimiento de dinero o de valores, independientemente de que los recursos no salgan de la institución.”</i>
	Artículo 208 BIS. Penalización de 5 a 10 años, de prisión y de mil a dos mil días multa.	Pornografía infantil. <i>“...realizar actos de exhibicionismo corporal lascivos o sexuales, con el objeto y fin de video grabarlo, fotografiarlo o exhibirlo mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro,...”</i>
Chihuahua ¹³⁸	Artículo 162 Pena de hasta 6 meses de prisión y multa hasta 50 veces de salario.	Intercepción de datos. <i>“La misma sanción se impondrá en los casos en que la comunicación se encuentre registrada o archivada en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.”</i>
	Artículo 168 BIS Pena de 6 meses a 3 años de prisión y multa de 30 a 80 veces el salario mínimo.	Falsificación de documentos, en donde se sanciona a quien(es): <i>“...indebidamente modifique, altere o imite de los originales, cualquier dato que se encuentre registrado o archivado en sistemas o equipos de informática protegidos por algún</i>

¹³⁷ Código Penal para el Estado Libre y Soberano de Chiapas. Consultado en Junio 15 del 2012 en http://www.amdh.com.mx/ocpi/pj/mj/docs/chi_cp.pdf

¹³⁸ Código Penal del Estado de Chihuahua. Consultado en Junio 19 del 2012 en http://www.cjf.gob.mx/documentos/2011/HTML/DGDHEGyAI/Tortura/Tortura/DOCUMENTOS/Punto_II/II.8.pdf

		<i>mecanismo de seguridad.”</i>
	<p>Capítulo IV Revelación de Secretos</p> <p>Artículo 234</p> <p>Pena 3 meses a 2 años de prisión o multa de 30 a 50 veces el salario.</p>	<p>Revelación de secretos.</p> <p><i>“...posesión de un documento, grabación o de cualquier dato que se encuentre registrado o archivado en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, que se le hubiera confiado, los revele o entregue sin consentimiento de quien tiene derecho a otorgarlo, y ello pueda causar daño para cualquier persona...”</i></p>
	<p>Artículo 265, fracción VII</p> <p>Pena de 3 meses a 3 años de prisión.</p>	<p>Robo, el cual se sanciona cuando:</p> <p><i>“VII.- Recaiga un expediente, documento o en cualquier información que se encuentre registrada o archivada en sistema o equipo de informática protegidos por algún mecanismo de seguridad, con afectación de alguna función pública.”</i></p>
	<p>Artículo 286</p> <p>Pena de 6 meses a 6 años de prisión.</p>	<p>Destrucción o alteración grave a archivos públicos.</p> <p><i>“Las mismas penas se aplicarán al que destruya, altere o provoque pérdida de información contenida en sistema o equipo de informática de oficina o archivos públicos, protegidos por algún mecanismo de seguridad.”</i></p>
Coahuila ¹³⁹	<p>Artículo 301</p> <p>Pena de 7 a 11 años de prisión y multa.</p>	<p>Pornografía infantil.</p> <p><i>“...para realizar actos de exhibicionismo corporal, o sexuales, lascivos o pornográficos, con el propósito de videograbarlos, filmarlos, fotografiarlos o exhibirlos, por cualquier medio, con o sin fin de obtener un lucro. La misma sanción se impondrá a quien financie,</i></p>

¹³⁹ Código Penal de Coahuila. Consultado en Junio 25 del 2012 en <http://docs.mexico.justia.com.s3.amazonaws.com/estatales/coahuila/codigo-penal-de-coahuila.pdf>

		<i>elabore, reproduzca, comercialice, distribuya, arriende, exponga o publicite el material a que se refieren las conductas descritas.”</i>
Colima ¹⁴⁰	Artículo 157 BIS Pena de 2 años 6 meses a 8 años de prisión y multa hasta por 500 unidades.	Pornografía infantil. Reforma aplicada en el 2002, indica: <i>“... se tipifica como explotación de menor o de quien no tenga capacidad para comprender el significado del hecho, el permitir, inducir u obligar al sujeto pasivo, a la práctica de la mendicidad, o a realizar acto de exhibicionismo corporal, libidinoso o de naturaleza sexual, con el objeto de videograbararlo o fotografiarlo o exhibirlo mediante cualquier tipo de impreso o medio electrónico.”</i>
	Artículo 234 Pena de 3 a 9 años de prisión y multa hasta por 100 unidades.	Fraude, valiéndose de medios electrónicos. <i>“V.- Acceso indebido a los equipos y sistemas de cómputo o electromagnéticos. Al que con el ánimo de lucro y en perjuicio del titular de una tarjeta, documento o instrumentos para el pago de bienes y servicios o para disposición en efectivo, acceda independientemente a los equipos y servicios de computo o electromagnéticos de las instituciones emisoras de los mismos, y...”</i>
Durango ¹⁴¹	Artículo 235, fracción V y VI Pena de 3 a 9 años de prisión y de 100 a 5 mil	Acceso indebido para la sustracción de información de tarjetas, documentos para realizar pagos de servicios. <i>”V.- Acceda a los equipos electromagnéticos de las instituciones</i>

¹⁴⁰ *Nuevo Código Penal para el Estado de Colima.* Consultado en Junio 28 del 2012 en <http://docs.mexico.justia.com.s3.amazonaws.com/estatales/colima/codigo-penal-para-el-estado-de-colima.pdf>

¹⁴¹ H. Congreso del Estado de Durango, *Código Penal para el Estado Libre y Soberano del Estado de Durango.* Consultado en Julio 1 del 2012 en <http://congresodurango.gob.mx/Leyes/7.PDF>

	días de multa.	<i>emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo; VI.- Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos,...</i>
	Artículo 426, fracción XXIII	El delito que se establece es el de fraude. <i>“XXIII.- Quien para obtener algún lucro para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores en perjuicio de persona alguna, independientemente de que los recursos no salgan de la Institución;”</i>
Estado de México ¹⁴²	Artículo 174, fracción V Pena de 4 a 10 años de prisión y de 150 a 500 días de salario mínimo de multa.	Falsificación de documentos. <i>“V. Acceda indebidamente a los equipos de electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.”</i>
	Artículo 204 Pena de 6 meses a 2 años de prisión y multa de 50 a 300 días de multa.	Pornografía infantil. <i>“A quien permita directa o indirectamente el acceso a personas menores de edad a escenas, espectáculos, obras gráficas o audiovisuales de carácter pornográfico, incluyendo la información generada o comunicada por medios electrónicos o cualquier otra tecnología...”</i>

¹⁴² H. LIII Legislatura del Estado de México, *Código Penal del Estado de México*. Consultado en Julio 5 del 2012 en <http://www.edomex.gob.mx/legistelfon/doc/pdf/cod/vig/codvig006.pdf>

Jalisco ¹⁴³	Artículo 136 BIS, fracción I Pena de 3 a 15 años de prisión y multa de 500 a 10 mil días de salario mínimo.	Delito de Pornografía infantil. Pena a quien(es): <i>“I. Induzca, obligue o entregue a un menor de dieciocho años o incapaz, con o sin su consentimiento, para que realice actos de exhibicionismo corporal, de naturaleza sexual o lasciva, con el fin de producir imágenes de dichos actos a través de fotografías, filmes, videos, revistas o cualquier otro medio impreso, electrónico o tecnológico, con o sin ánimo de lucro; “</i>
	Capítulo VIII Falsificación de Medios Electrónicos o Magnéticos. Artículo 170 BIS, fracción III Pena de 3 a 9 años de prisión y multa de 200 a 400 días de salario mínimo.	Piratería de documentos e información que un usuario común no pueda poseer. <i>“III. Acceda, obtenga, posea o detente indebidamente información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo, y los destine a alguno de los supuestos que contempla el presente artículo; y”</i>
	Artículo 194, fracción I, inciso k) Pena de 18 a 35 años de prisión y multa de mil a 2 mil días de salario mínimo.	Delito de secuestro, en donde se valga del uso de medios electrónicos. <i>“k) Para lograr sus propósitos, se valga de redes o sistemas informáticos internacionales o de otros medios de alta tecnología, que impliquen marcada ventaja en el logro de su fin;”</i>

¹⁴³ Secretaría del H. Congreso del Estado, *Código Penal para el Estado Libre y Soberano de Jalisco*. Consultado en Julio 9 del 2012 en http://www.amdh.com.mx/ocpi/pj/mj/docs/jal_cp.pdf

<p>Michoacán¹⁴⁴</p>	<p>Artículo 133 BIS, fracción I y II</p> <p>Pena de 2 a 8 años de prisión y de 500 a mil días de salario mínimo.</p>	<p>Acceso indebido a sistemas informáticos de la Seguridad Pública del Estado. Pena para quien:</p> <p><i>“I. Ingrese a los bancos de datos del Sistema previstos en la Ley del Sistema de Seguridad Pública del Estado de Michoacán de Ocampo, información errónea, que dañe o que pretenda dañar en cualquier forma los registros, los bancos de datos o los equipos o sistemas que las contengan;</i></p> <p><i>II. Divulgue información clasificada de los bancos de datos o sistemas informáticos a que se refiere la Ley mencionada en la fracción anterior;...”</i></p>
	<p>Artículo 164, fracción I</p> <p>Pena de 6 a 10 años de prisión y multa de mil a 4 mil días de salario mínimo.</p>	<p>Pornografía infantil.</p> <p><i>“I. Quien induzca, procure, facilite o permita por cualquier medio a persona menor de edad o a persona que no tiene capacidad para comprender el significado del hecho, a realizar actos sexuales o de exhibicionismo corporal, reales o simulados, de índole sexual, con el fin de grabarlos, videograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, medios electrónicos o de cualquier otra naturaleza, independientemente de que se logre la finalidad;...”</i></p>
<p>Morelos¹⁴⁵</p>	<p>Artículo 123, fracción II</p> <p>Pena de 6 meses a 3 años de prisión y 300 a 500 días de</p>	<p>Sanción a toda difusión y exhibición ilegal de situaciones obscenas para la sociedad.</p> <p><i>“II.- Al que realice exhibiciones públicas obscenas por cualquier medio electrónico, incluyendo Internet, así como las ejecute o haga ejecutar por</i></p>

¹⁴⁴ H. Congreso del Estado, *Código Penal del Estado de Michoacán*. Consultado en Julio 13 del 2012 en

http://www.cjf.gob.mx/documentos/2011/html/dgdhegyai/tortura/tortura/documentos/punto_ii/ii.19.pdf

¹⁴⁵ Gobierno del Estado de Morelos, *Código Penal para el Estado de Morelos*. Consultado en Julio 19 del 2012 en <http://www.morelos.gob.mx/10consejeria/files/Codigos/CodigoPenal.pdf>

	multa.	otro;”
	Artículo 213 Quater.	<p>Pornografía infantil.</p> <p><i>“Al que procure, facilite o induzca por cualquier medio a un menor, o a un incapaz, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbar, fotografiarlo o exhibirlo mediante anuncios impresos o electrónicos, incluyendo la Internet, se le impondrá de seis a quince años de prisión y de cien a quinientos días-multa.”</i></p>
Oaxaca ¹⁴⁶	Artículo 195, fracción III Pena de 7 a 12 años de prisión y multa de 700 a 900 días de salario mínimo.	Delito de pornografía infantil. <i>“III. Quien reproduzca, publique, ofrezca, publicite, almacene, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales, explícitas o no, reales o simuladas, o toda la representación de los órganos sexuales de la víctima con fines primordialmente sexuales; y ...”</i>
	Artículo 348 BIS. Pena de 10 a 15 años de prisión y multa de 500 a 730 días de salario mínimo.	Delito de secuestro. <i>“...el que prive de la libertad a otra persona, con el objeto de obtener un lucro mediante el uso de cualesquiera de los siguientes medios: Tarjetas de crédito, tarjetas de débito, título de crédito, medios electrónicos,</i>

¹⁴⁶ H. Congreso del Estado Libre y Soberano de Oaxaca, *Código Penal para el Estado Libre y Soberano de Oaxaca*. Consultado en Julio 24 del 2012 en <http://www.congresoaxaca.gob.mx/lxi/info/legislacion/008.pdf>

		<i>informáticos, mecánicos, en especie o efectivo. “</i>
	Artículo 383 BIS, fracción IV	Delito de extorsión. <i>“IV).- Al que cometa una extorsión por vía telefónica o por cualquier medio electrónico se le impondrá de ocho a catorce años de prisión y multa de quinientos a mil salarios mínimos.”</i>
Puebla ¹⁴⁷	Artículo 219, fracción I	Pornografía infantil. Pena para quien(es): <i>“I.- Produzca imágenes o representaciones de exhibicionismo sexual, mediante fotografías, filmes, videos, o cualquier otro medio impreso, electrónico o producido por el avance tecnológico;”</i>
	Artículo 221	A las personas que favorezcan a que el delito no se detenga, serán sancionadas también: <i>“...posesión de una o más fotografías, filmes, videos o cualquier otro medio impreso o electrónico, que contenga imágenes de las que se refiere el artículo 219, se sancionará con prisión de uno a cinco años y multa de cien a quinientos días de salario...”</i>
	Artículo 245 BIS, fracción V Pena de 3 a 9 años de prisión y multa de 150 a 400 días de salario.	Falsificación de documentos. <i>“V.- Al que acceda indebidamente a los equipos y sistemas de cómputo o electromagnéticos de las Instituciones emisoras de tarjetas, títulos, documentos o instrumentos, para el pago de bienes y servicios o para disposición de efectivo.”</i>

¹⁴⁷ Código de Defensa Social del Estado Libre y Soberano de Puebla. Consultado en Agosto 2 del 2012 en <http://www.inegi.org.mx/est/contenidos/espanol/sistemas/pryCMD/codigos/cp21.pdf>

Querétaro ¹⁴⁸	<p>Artículo 149 BIS.</p> <p>Pena de 6 a 15 años de prisión y de 100 a 250 días de multa. La pena aumenta en una mitad si hay violencia, vejación o tortura a la víctima.</p>	<p>Delito de secuestro, en donde se haga uso de medios informáticos.</p> <p><i>“...la privación de la libertad se realice con la finalidad de obtener un lucro mediante el uso de cualquier medio bancario, electrónico o informático...”</i></p>
	<p>Título séptimo. Delitos contra la inviolabilidad del secreto y el acceso ilícito a sistemas de informática</p> <p>Capítulo I. Revelación del secreto.</p> <p>Artículo 159</p> <p>Pena de 3 meses a 1 año de prisión y hasta 20 días de multa o trabajo en favor de la comunidad hasta por 3 meses.</p>	<p>Violación de la confianza, revelación de secretos.</p> <p><i>“A quien teniendo conocimiento de un secreto, o estando en posesión de un documento, grabación, filmación o cualquier otro objeto que se le hubiese confiado, lo revele o entregue, sin consentimiento de quien tenga derecho a otorgarlo y que pueda causar daño para cualquier persona...”</i></p>
	<p>Título séptimo. Delitos contra la inviolabilidad del secreto y el acceso ilícito a sistemas de informática</p>	<p>Se especifican los casos en que se protege a la víctima por algún otro usuario que tenga en poder documentos, archivos de importancia, para la víctima y estén en peligro de divulgación sin su consentimiento:</p> <p><i>“...se apodere de sus papeles, cartas, mensajes de correo electrónico o</i></p>

¹⁴⁸ Código Penal para el Estado de Querétaro. Consultado en Agosto 8 del 2012 en http://www.cjf.gob.mx/documentos/2011/HTML/DGDHEGyAI/Tortura/Tortura/DOCUMENTOS/Punto_II/II.25.pdf

	<p>Capítulo I. Revelación del secreto.</p> <p>Artículo 159 BIS</p> <p>Pena de 6 meses a 3 años de prisión y de 100 a 300 días de multa.</p>	<p><i>cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones...”</i></p>
	<p>Capítulo II Acceso ilícito a sistemas de informática.</p> <p>Artículo 159 Ter.</p>	<p>Uso indebido a sistemas informáticos.</p> <p><i>“Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos protegidos o no por algún sistema de seguridad se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.”</i></p>
	<p>Capítulo II Acceso ilícito a sistemas de informática.</p> <p>Artículo 159 Quater.</p>	<p>Acceso indebido sistemas informáticos del Estado.</p> <p><i>“Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos del Estado, protegidos o no por algún sistema de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.”</i></p>
	<p>Artículo 198, fracción V</p> <p>Pena de 4 a 10 años de prisión y</p>	<p>El delito de extorsión por medios informáticos.</p> <p><i>“V. Se utilice como medio comisivo la vía telefónica, el correo electrónico o</i></p>

	de 100 a 300 días de multa.	<i>cualquier otro medio de comunicación electrónica;...</i>
	Artículo 232 BIS, fracción III y IV Pena de 3 a 9 años de prisión y multa de 200 a 400 días de salario mínimo.	Falsificación de documentos. <i>“III. Acceda, obtenga, posea, utilice o detente indebidamente información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones</i> <i>IV. Adquiera, utilice o detente equipos electromagnéticos, electrónicos o de comunicación remota para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas, tarjetas de crédito, tarjetas de débito u otros documentos;”</i>
	Artículo 239 BIS	Delito de pornografía infantil. <i>“Al que por cualquier medio filme, grabe o imprima actos de exhibicionismo corporal, lascivos o sexuales de menores de dieciocho años de edad o de incapaces, con el fin de exhibirlos, difundirlos, o transmitirlos por cualquier medio impreso o electrónico, se le impondrá prisión de 2 a 10 años, de 20 a 600 días multa y se le inhabilitará para ser tutor o curador.”</i>
Quintana Roo ¹⁴⁹	Artículo 189 BIS, fracción III y IV	Falsificación y alteración de documentos. <i>“III. Copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios para disposición en efectivo.</i> <i>IV. Accese indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones</i>

¹⁴⁹ Código Penal para el Estado Libre y Soberano del Estado de Quintana Roo. Consultado en Agosto 17 del 2012 en http://www.amdh.com.mx/ocpi/pj/mj/docs/quin_cp.pdf

		<i>emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo. “</i>
San Luis Potosí ¹⁵⁰	Artículo 136, fracción XII Pena de 30 a 50 años de prisión y sanción pecuniaria de 2 mil a 6 mil días de salario.	Delito de secuestro, valiéndose del uso de medios electrónicos: <i>“XIII. Se utilicen instalaciones dependientes de cualquier autoridad o instrumentos de trabajo oficiales, tales como frecuencias electrónicas, sistemas de cómputo, claves o códigos oficiales, o cualquier sistema de comunicación de uso exclusivo de la autoridad;”</i>
	Artículo 182 Pena 10 a 14 años de prisión y de 500 a 5 mil días de multa.	Delito de pornografía infantil. <i>“...procure, obligue facilite, o induzca a una persona menor de dieciocho años de edad... ...a realizar actos de exhibicionismo corporal o sexuales, con el objeto de video grabarla, fotografiarla, exhibirla o describirla mediante cualquier tipo de material visual, de audio, electrónico, sistemas de cómputo, transmisión de archivos de datos de red pública o privada de telecomunicaciones, o cualquier medio,...”</i>

¹⁵⁰ H. Congreso del Estado de San Luis Potosí, *Código Penal del Estado de San Luis Potosí*. Consultado en Agosto 22 del 2012 en http://www.cjf.gob.mx/documentos/2011/html/dgdhegyai/tortura/tortura/documentos/punto_ii/ii.27.pdf

	<p>Artículo 212 BIS</p> <p>Se impondrá además de las penas previstas, aumentadas en una mitad más, la destitución definitiva e inhabilitación desde uno hasta veinte años para desempeñar cualquier empleo, cargo o comisión pública.</p>	<p>Extorsión por un miembro de corporación policiaca o servidor público.</p> <p><i>“...manejen información de clientes o tengan acceso a la misma, y que la utilicen de cualquier forma o la sustraigan para sí o para terceros con el objeto de obtener un lucro o beneficio por medio de la extorsión...”</i></p>
<p>Sinaloa¹⁵¹</p>	<p>Capítulo V</p> <p>Delito Informático.</p> <p>Artículo 217</p> <p>Pena de 6 meses a 2 años de prisión y de 90 a 300 días multa.</p>	<p>Engloba y especifica a la vez, lo que es delito informático:</p> <p>Comete delito informático, la persona que dolosamente y sin derecho:</p> <p><i>“I.- Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o</i></p> <p><i>II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.”</i></p>

¹⁵¹ Código Penal para el Estado de Sinaloa. Consultado en Agosto 28 del 2012 en <http://www.laipsinaloa.gob.mx/images/stories/ARCHIVOS%20PUBLICOS/Leyes%20Estatales%20Actuales/codigo%20penal.pdf>

	<p>Artículo 271 BIS, fracción IV y V</p> <p>Pena de 3 a 9 años de prisión y de 100 a 500 días de multa.</p>	<p>Delito de falsificación de documentos.</p> <p><i>“IV. Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.</i></p> <p><i>V. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma; ...”</i></p>
<p>Sonora¹⁵²</p>	<p>Artículo 144 BIS 2, fracción I</p> <p>Pena de 1 a 8 años de prisión y de 100 a mil días de multa.</p>	<p>Acceso indebido a sistemas informáticos de la Seguridad Pública del Estado.</p> <p><i>“I.- Acceda sin autorización o sin tener derecho para hacerlo, a la información contenida en las bases de datos del Sistema Estatal de Seguridad Pública para el Estado de Sonora;</i></p> <p><i>II.- Ingrese dolosamente o permita dolosamente el acceso de información errónea o indebida, o que dañe o pueda dañar en cualquier forma la información, las bases de datos o los equipos o sistemas que contengan la información del Sistema Estatal de Seguridad Pública;</i></p> <p><i>III.- Divulgue de manera ilícita información proveniente de las bases de datos o del Sistema Estatal de Seguridad Pública a que se refiere la Ley de Seguridad Pública para el Estado de Sonora; y”</i></p>

¹⁵² Código Penal del Estado de Sonora. Consultado en Septiembre 5 del 2012 en http://www.congresoson.gob.mx/Leyes_Archivos/doc_6.pdf

	<p>Artículo 169 BIS 1, fracción II</p> <p>Pena de 4 a 7 años de prisión y de mil a 2 mil días de multa.</p>	<p>Pornografía infantil.</p> <p><i>“II. Quien reproduzca, publique, ofrezca, publicite, almacene, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades de exhibicionismo corporal, sexuales o eróticas, explícitas o no, reales o simuladas.”</i></p>
Tabasco ¹⁵³	<p>Artículo 316</p> <p>Pena de 1 a 5 años.</p>	<p>Interceptación de comunicaciones privadas, considerado un delito.</p> <p><i>“Al que intervenga la comunicación privada de terceras personas, a través de medios eléctricos o electrónicos, se le aplicará prisión de uno a cinco años.”</i></p>
Tamaulipas ¹⁵⁴	<p>Artículo 194 BIS, fracción I</p>	<p>Pornografía infantil.</p> <p><i>“I.- El que obligue o induzca a uno o más menores de dieciséis años a realizar actos de exhibicionismo corporal, lascivos, sexuales o pornográficos con la finalidad de videograbarlos, filmarlos, fotografiarlos o exhibirlos mediante anuncios impresos, electromagnéticos, electrónicos, o por vía internet, de telefonía o cualquiera otra similar; ...”</i></p>

¹⁵³ Código Penal para el Estado de Tabasco. Consultado en Septiembre 11 del 2012 en http://www.congresotabasco.gob.mx/60legislatura/trabajo_legislativo/pdfs/codigos/Codigo_Penal_Tabasco.pdf

¹⁵⁴ Código Penal de Tamaulipas. Consultado en Septiembre 14 del 2012 en <http://www.pjetam.gob.mx/legislacion/leyes/pdf/codpen.PDF>

	<p>Título Séptimo Delitos de revelación de secretos y de acceso ilícito a sistemas y equipos de informática.</p> <p>Capítulo I Revelación de secretos</p> <p>Artículo 205</p> <p>En éste y el artículo 206, la pena es de 1 año a 3 años 6 meses de prisión y multa de 20 a 60 días de salario.</p>	<p>Revelación de secretos.</p> <p><i>“Comete el delito de revelación de secretos el que sin causa justa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, puesto o cargo.”</i></p>
	<p>Artículo 207</p>	<p><i>“Cuando la revelación punible sea hecha por personas que presten servicios profesionales o técnicos, o cuando el secreto revelado o publicado sea de carácter industrial, la sanción será de dos a cinco años de prisión y multa de treinta a ochenta días salario.”</i></p>
<p>Tlaxcala¹⁵⁵</p>	<p>Artículo 166, fracción I</p> <p>Pena de 6 meses a 2 años de prisión y multa hasta de 20 días de salario.</p>	<p>Delito de pornografía infantil.</p> <p><i>“I.- Quien induzca, procure, facilite o permita por cualquier medio, la realización de actos eróticos o de exhibicionismo corporal, reales o simulados con el fin de grabarlos, videograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, medios electrónicos o de</i></p>

¹⁵⁵ H. Congreso del Estado Libre y Soberano de Tlaxcala, *Código de Procedimientos Penales para el Estado Libre y Soberano de Tlaxcala*. Consultado en Septiembre 21 del 2012 en <http://docs.mexico.justia.com.s3.amazonaws.com/estatales/tlaxcala/codigo-de-procedimientos-penales-para-el-estado-libre-y-soberano-de-tlaxcala.pdf>

		<i>cualquier otra naturaleza;”</i>
Veracruz ¹⁵⁶	<p align="center">Capítulo III Delitos Informáticos</p> <p>Artículo 181</p> <p>Pena de 6 meses a 2 años de prisión y multa hasta de 300 días de salario, si se comete con fines de lucro, la pena aumenta una mitad.</p>	<p>El estado especifica y engloba los actos que se consideran como delitos informáticos.</p> <p><i>“Comete delito informático quien, sin derecho y con perjuicio de tercero:</i></p> <p><i>I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o</i></p> <p><i>II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.”</i></p>
	<p>Artículo 217, fracción X</p>	<p>Delito de fraude, mediante el uso de medios informáticos.</p> <p><i>“X. Por cualquier medio, ingrese a sistemas o programas de informática de naturaleza financiera e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, con el propósito de obtener algún beneficio para sí o de un tercero.”</i></p>
	<p>Artículo 290</p> <p>Pena de 5 a 15 años de prisión y multa hasta de 500 días de salario.</p>	<p>Delito de pornografía infantil.</p> <p><i>“... quien induzca, facilite u obligue por cualquier medio, a un menor de dieciséis años o a un incapaz a realizar actos sexuales o de exhibicionismo corporal, para fotografiarlos, filmarlos o</i></p>

¹⁵⁶ Código Penal para el Estado Libre y Soberano del Estado de Veracruz de Ignacio de la Llave. Consultado en Septiembre 24 del 2012 en <http://www.veracruz.gob.mx/comunicaciones/files/2011/08/15.-CODIGO-PENAL-PARA-EL-ESTADO-LIBRE-Y-SOBERANO-DE-VERACRUZ-DE-IGNACIO-DE-LA-LLAVE.pdf>

		<i>exhibirlos mediante anuncios impresos, electrónicos o cualquier otro medio.”</i>
Yucatán ¹⁵⁷	Artículo 211 Pena de 5 a 10 años de prisión y de 400 a 500 días de multa.	Pornografía infantil. <i>“... obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro,...”</i>

Se puede observar que el delito más penado dentro de la legislación estatal, es la pornografía infantil. Cabe destacar que México ocupa el segundo lugar en producción de pornografía infantil a nivel mundial¹⁵⁸, una razón de ello es debido a que con el auge de la tecnología e Internet, se ha cometido con mayor frecuencia dicho delito gracias a los ingresos monetarios que genera para el crimen organizado, incluso más que la venta de armas. Se debe evitar que la tecnología informática sea una poderosa herramienta en el cometido del delito, puesto que ésta se convierte en arma fácil para la captura de víctimas, que también abarca la población infantil.

Como segundo aspecto más importante en la legislación estatal, se encuentra el acceso ilícito a sistemas, seguido por revelación de secretos o violación a la confidencialidad. Estados como Sinaloa y Veracruz ya han integrado a su respectivo Código Penal los capítulos de Delitos Informáticos, es decir que éstos ya reconocen como tal los delitos que se cometan por medio de las herramientas informáticas. Por su parte, Jalisco integró el capítulo “Falsificación de medios electrónicos y magnéticos” en donde por medio de la tecnología informática se recurre a la falsificación de documentos de uso público, privado y personal.

El avance ya está presente y se debe continuar, pues aún se requieren esfuerzos para un mayor progreso y alcanzar un máximo nivel posible en materia de Derecho Informático en México.

¹⁵⁷ H. Congreso del Estado Libre y Soberano de Yucatán, Código Penal del Estado de Yucatán. Consultado en Septiembre 30 del 2012 en http://www.yucatan.gob.mx/gobierno/orden_juridico/Yucatan/Codigos/nr249rf2.pdf

¹⁵⁸ Grupo Fórmula México, *segundo lugar en pornografía infantil a nivel mundial*. Consultado en Noviembre 3, 2012 en <http://www.radioformula.com.mx/notas.asp?Idn=221857>

CAPÍTULO 4. LA IMPORTANCIA DEL DERECHO INFORMÁTICO EN MÉXICO Y SU EVOLUCIÓN

4.1 PROBLEMÁTICA A NIVEL INTERNACIONAL

Las computadoras y su alcance internacional permiten la difusión de programas, datos, y en definitiva, sistemas que sobrepasan las fronteras de los países. Esta es la razón por la que resulta de gran utilidad atenerse a los resultados de derecho comparado en el ámbito internacional, en concreto al que hace referencia a los aspectos informáticos.¹⁵⁹ Se han enlistado los problemas existentes que ha presentado la tecnología; pero a la vez se han ido generando otros más; en un inicio lo más importante era crear infraestructura tecnológica para proporcionar el servicio de internet a los usuarios; después, era necesario crear los diversos espacios en la red para ofrecer las alternativas de servicios, ahora, por ejemplo, está regular la normatividad o reglamentación jurídica por los diferentes usos que se tienen de Internet.

En esta sociedad de la información, en donde el conocimiento está basado en la ciencia y la tecnología aplicadas, el capitalismo y globalización económica en que nos encontramos, el Derecho Informático como una rama reciente acorde a las nuevas tecnologías, se ha ido ajustando al paso del tiempo, pero a la vez con cierto descontrol, pues no se puede aplicar de la misma manera en todos los países, pues estos se rigen por diferentes leyes, costumbres y estilo de vida en su población, convirtiendo que dicha regulación jurídica se convierta en una problemática a nivel internacional que requiere de atención urgente, para así evitar un mayor impacto negativo en el uso de la tecnología informática.

En el primer capítulo se citan diversas definiciones de Derecho Informático que en los últimos años se han simplificado, pero en un inicio, cuando ésta rama surgió, existían diversas razones que complicaban una definición precisa y razón de ser independientes, o mejor llamados, criterios de inclusión.

Se ha señalado que la “estructura temática del Derecho Informático afecta a las ramas del Derecho tradicionales. Así, se inscriben en el ámbito del Derecho público: el problema de la regulación del flujo internacional de datos informatizados, que interesa al Derecho Internacional público; la libertad informática o defensa de las libertades frente a eventuales agresiones

¹⁵⁹Albizuri Begaña, *El Fraude y la Delincuencia Informática: Un Problema Jurídico y Ético*, Revista Digital Universitaria, Vol. 3 No. 2, México, 2002, consultado en Noviembre 20 del 2012 en: <http://www.revista.unam.mx/vol.3/num2/art3/>

perpetradas por las tecnologías de la información y la comunicación, objeto de especial atención por el Derecho Constitucional o administrativo; o los delitos informáticos, que tienden a configurar un ámbito propio en el Derecho penal actual. Mientras que inciden directamente en el Derecho privado cuestiones tales como: los contratos informáticos, que pueden afectar lo mismo al hardware que al software, dando lugar a una rica tipología negocial en la que pueden distinguirse contratos de compraventa, alquiler, *leasing*, copropiedad, multipropiedad, mantenimiento y servicios; así como los distintos sistemas para la protección jurídica de los programas de ordenador, temas que innovan los objetos tradicionales de los Derechos civil y mercantil”.¹⁶⁰

En primera instancia, cuando el Derecho Informático surge, se trata de un Derecho nuevo, por la novedad y rápida evolución informática, además de un nuevo ciclo cultural¹⁶¹, que bastaron para evidenciar la juventud de la rama en relación a la gran mayoría de las otras ramas jurídicas.

En relación a la novedad, es un Derecho influido por la tecnología informática, dada la innegable incidencia del hecho técnico sobre su origen y su desarrollo. De modo similar a la influencia que el avión ha tenido respecto al Derecho Aeronáutico.¹⁶², en este caso, estando ahora en una nueva sociedad de la información tiene como consecuencias diversas problemáticas jurídicas.

Como siguiente término, es un Derecho en formación ya que, no obstante su significativo crecimiento, es aún incompleto y está en proceso de extensión permanente. En consecuencia, en cuarto lugar, se puede decir que es un Derecho dinámico por encontrarse en constante transformación, principalmente por las variaciones tecnológicas que someten a nuevas exigencias.¹⁶³ Por lo que también se califica como un Derecho de adaptación.¹⁶⁴

En quinto lugar, es un Derecho con tendencia a la internacionalización, por el hecho de la convergencia de tecnologías que rebasan las fronteras nacionales, por ello se ha calificado como “un Derecho común a todos los países”.¹⁶⁵

¹⁶⁰ Pérez Luño, Antonio Enrique, *Manual de Informática y Derecho*, Ed. Ariel, Barcelona, 1996.

¹⁶¹ Pérez Luño, Antonio Enrique, *Cibernética, Informática y Derecho*, Publicaciones del Real Colegio de España, Bolonia, 1976, p. 19 y ss.

¹⁶² Delpiazzo Carlos E. et al. *Introducción a la informática jurídica y al derecho informático*, cit., p. 129.

¹⁶³ Correa Carlos et al., *Derecho Informático*, cit. p. 286 y ss.

¹⁶⁴ Hajna Eduardo, *El derecho informático*, en Rev. Derecho de la Alta Tecnología, Buenos Aires, 1991, Año I, N°10, p. 8.

¹⁶⁵ Losano Mario G. *Corso di informatica giuridica*, Einaudi, Torino, 1986, vol. II, p. 16.

Por esto, el Derecho Informático finalmente se califica como un Derecho transversal¹⁶⁶, a partir de la interdisciplinariedad¹⁶⁷ que presenta como característica de rebasar las disciplinas tradicionales del Derecho tocándolas prácticamente a todas.

El Derecho se ha conjugado fuertemente con la Informática y su relación alcanzado un gran nivel internacional. Sin embargo, problemas como los tratados en **este trabajo de investigación**, propios de ésta época, no se encuentran regulados adecuadamente o se ignora el alcance negativo de tales problemas.

4.1.1 Tecnología y trabajo

La expansión de las TIC (Tecnologías de Información y Comunicación), son un factor de una transformación social, y también, de una diferente realidad laboral. Gracias al surgimiento de la revolución tecnológica, se ha impulsado el sector de los servicios, donde se demandan nuevos tipos de empleos para la producción y una mejor administración de los mismos.

En el mundo laboral ha surgido un nuevo concepto y modo de empleo, con diversos términos, pero que conllevan a un mismo objetivo: el trabajo a distancia o también llamado teletrabajo; esto se refiere como aquel que se realiza en el domicilio del trabajador o en un lugar seleccionado por él, fuera del centro del trabajo.¹⁶⁸ Esto permite una variación en el modo de emplear personas, en donde tanto la empresa como el empleado obtienen mutuos beneficios, como una mayor flexibilidad de organización, se deja de convivir con el cotidiano tráfico urbano, etcétera, pero también ciertas desventajas implican este nuevo modo laboral como una compleja sincronización, además del peligro de desarraigo del trabajador respecto a su medio laboral, es decir, que se genere un gran aislamiento del empleado para el cumplimiento de sus deberes. Por ello en conjunto con las ventajas mencionadas, es preciso que se evite la precarización de prestaciones laborales y se incentive al capital humano para una mejor adaptación a la evolución y cambios tecnológicos, de igual forma fomentar la participación del empleado en donde no se conviertan en simples esclavos de las máquinas.

Es por todo esto que surge una problemática en este tipo de empleo en el que se procura en menor medida, puesto que hay empresas que consideran el trabajo a distancia menos relevante y contrariamente a lo que se piensa,

¹⁶⁶ Álvarez Rico Manuel, *Informática y derecho en España*, en Rev. Iberoamericana de Derecho Informático, Mérida, 1998, núm. 23-26, p. 1036 y ss.

¹⁶⁷ Falcón Enrique M., *¿Qué es la informática jurídica?* Abeledo Perrot, Buenos Aires, 1992, p. 128 y

ss.

¹⁶⁸ Salgado Flores Lucerito, *Derecho Informático*, Grupo Editorial Patria, 2009, p. 144.

implica también un esfuerzo laboral por el empleado que la mayoría de las veces, las empresas y patrones no valoran lo suficiente.

4.1.2 Ética en la Informática

Primeramente definimos a la ética, que es una disciplina filosófica con “principios directivos que orientan a las personas en cuanto a la concepción de la vida, el hombre, los juicios, los hechos, y la moral.”¹⁶⁹

Cuando hablamos de ética como un concepto global, en general nos referimos a una serie de principios y valores con los que se forja el hombre en cuanto a la concepción de la vida, sus criterios, ideas y juicios hacia la misma, de los hechos determinados por la sociedad que consideran “buenos o malos”, debidos o moralmente correctos. Se determina que la ética en las TIC surge como una disciplina en la que se trata de identificar y analizar el impacto de las tecnologías de información y comunicaciones en la percepción de los valores tanto personales como sociales, y en donde determinamos en qué medida se agravan los problemas éticos a partir del surgimiento y uso de las TIC (Tecnologías de Información y Comunicaciones) como un fenómeno global.

La Ética de la Informática es considerada como la disciplina que analiza los problemas éticos que son creados por la tecnología de las computadoras, o también que son agravados o transformados por la misma, es decir, por las personas que hacen uso de los avances de las tecnologías de la información.¹⁷⁰

Es necesario y fundamental aplicar la ética a la informática, puesto que nos indica cómo actuar ante ciertos conflictos en la vida profesional, mediante principios que determinan términos, teorías y métodos de disciplina. Estos principios están basados en cuatro conceptos éticos claves que son: intimidad, exactitud, propiedad intelectual y accesibilidad.¹⁷¹

Principios:

- Secreto profesional del informático, confidencialidad.
- Responsabilidad profesional del informático.
- Lealtad a su empresa y a su público.
- Dignidad, honestidad, honradez del informático.
- Primacía del servicio al bien común y al bien público.
- Preparación académica y formación continuada del informático.
- Solidaridad profesional.

¹⁶⁹ Garza de Flores, María, *Ética*, Ed. Alhambra Mexicana, México, 1993.

¹⁷⁰ Guibert JM. *¿Qué es la ética de la informática?*, España, Universidad de Deusto, 1997.

¹⁷¹ Barroso Asenjo Porfirio, *Ética e Informática*, Computación aplicada a Contabilidad, Administración y Economía, consultado en Noviembre 25 del 2012 en:
<http://www.ccee.edu.uy/ensenian/catcomp/material/etica.pdf>

- Integridad profesional.
- El informático debe apoyar y practicar el derecho a proveer y recibir información.
- Debe transmitir datos con exactitud.
- Debe evitar invasiones de la intimidad.
- Utilizar solamente justos y honestos medios en el ejercicio de su actividad profesional.
- Colaborar en el desarrollo y promoción de la informática.
- Debe demostrar su competencia.
- Respetar y proteger la propiedad intelectual observando los derechos de autor, mencionando las fuentes, haciendo citas y referencias apropiadas.¹⁷²

Son diversos principios que difícilmente una persona cumple en su totalidad, pues el comportamiento y valores son diversos en cada persona. Esto representa una problemática social, y sus principales consecuencias convergen en comportamientos ilícitos que van desde actos accidentales, vandálicos, hasta delitos con dolo y ventaja. Es fundamental crear conciencia de la ética en nuestra vida personal y profesional.

Es necesario también un mayor estudio e inducción por parte de instituciones educativas, empresariales y gubernamentales, que impulsen el conocimiento y uso de la ética profesional, incluyendo el área Informática, en donde fácilmente el hombre puede cometer actos ilícitos que atenten contra la integridad de los sistemas informáticos y personas.

La ética tiene el fin de ayudarnos a entender nuestras responsabilidades y encaminarnos hacia la toma de decisiones correctas, se exige así misma responder a las inquietudes de los individuos, y desempeñar nuestra labor acorde a nuestros valores y en conformidad con las leyes pertinentes.¹⁷³

En este trabajo se incluye como **Anexo**, el Código de Ética Profesional del Licenciado en Informática, el cual servirá para tener en cuenta las responsabilidades que tenemos como Licenciados en Informática al ejercer nuestra carrera profesional.

¹⁷² *Ídem.*

¹⁷³ Sosa Carabeo Marcel, *Problemas éticos y de seguridad asociados al uso de las tecnologías*, consultado en Noviembre 26 del 2012 en <http://bvs.sld.cu/revistas/inf/n909/inf130910.htm>

4.2 TENDENCIAS INTERNACIONALES DE LA INFORMÁTICA Y EL DERECHO¹⁷⁴

En la evolución del Derecho Informático a nivel internacional, se establecen las tendencias respecto al desarrollo de la materia: inicial o básica, progresiva o creciente, avanzada o próspera y culminante o innovadora.

4.2.1 Tendencia Inicial o Básica:

- Poco avance y desarrollo en informática jurídica y Derecho Informático, debido a la escasa importancia por parte de los profesores de derecho de Universidades para impartir como materia, y poca importancia también por parte de los funcionarios de gobierno.
- Se comienza a promover que se incluya la materia de Derecho Informático en los planes de estudio de las universidades.

4.2.2 Tendencia Creciente o Progresiva:

- Hay una distinción clara entre informática jurídica y Derecho Informático, como ramas independientes una de la otra, pero que están relacionadas entre sí.
- Consideración del Derecho Informático como rama autónoma del derecho; incluyéndose en los planes de estudio de las principales universidades especialmente, en las de derecho.

4.2.3 Tendencia Avanzada o Próspera

- Destaca la necesidad e importancia de desarrollar la labor legislativa respecto al Derecho Informático, normas específicas que aporten para su regulación y aplicación; auge importante en la doctrina y jurisprudencia al respecto.
- Desarrollo y consolidación importante de la legislación, doctrina y jurisprudencia nacional del Derecho Informático; controversia de casos prácticos nacionales o internacionales en la Corte Suprema del país.

4.2.4 Tendencia Culminante o Innovadora

- Avances importantes respecto a la informática jurídica metadocumental, auge de centros de investigación para la utilización de sistemas de inteligencia artificial aplicados al derecho y desarrollo de tesis doctorales relativas a ello.
- Desarrollo de proyectos prácticos y específicos de utilización de la inteligencia artificial aplicados al derecho.

¹⁷⁴ UNINET DERIN, *Tendencias actuales de la Informática y el Derecho a Nivel Internacional*. Consultado en Diciembre 12 del 2012 en <http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=36>

4.3 TENDENCIAS DE LA INFORMÁTICA Y EL DERECHO EN EL DERECHO COMPARADO¹⁷⁵

Se han determinado tendencias que presentan algunos países de Europa y América Latina, respecto al Derecho Informático, agrupándolos por el tipo de tendencia que reflejan actualmente, siendo un comparativo que puede cambiar día con día.

4.3.1 Países con Tendencia Inicial-Creciente:

Colombia.- La Universidad Externado de Colombia cuenta con un departamento de informática jurídica. Se dio valor legal al documento electrónico al expedirse la Ley número 527 del 18 de agosto de 1999, donde se define y reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firma digital. Y la nueva Ley 1437 de 2011, que implementa el uso de los medios electrónicos como medio para llevar a cabo la actividad administrativa.

Brasil.- Cuenta con el Centro de Procesamiento de Datos de la República de Brasil. Una de sus propuestas recientes, es el “Marco Civil”, el cual busca establecer los derechos y responsabilidad de los usuarios, basados en principios de la defensa a la neutralidad de la red. Sin embargo, sigue sin su aprobación.

Perú.- Se imparte la materia de informática jurídica en la Facultad de Derecho y Ciencias Políticas de la Universidad de Lima. Estableció el “Cibertribunal Peruano”, en donde se resuelven controversias sobre comercio o contratación electrónica, contratos informáticos, derechos de autor y propiedad intelectual. En el 2011, integró en su legislación la Ley 29733 de Protección de Datos Personales de Perú.

Chile.- Cuenta con el Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile (CCIJ), que se encarga del procesamiento y recuperación de información de las principales leyes del país. Es pionero en América Latina en crear una ley que regula los delitos informáticos (LEY-19223).

Costa Rica.- Interesados en proteger la intimidad de los usuarios respecto al procesamiento automatizado de datos personales, se publicó la Ley 8968 de Protección de las Personas Frente al Tratamiento de sus Datos Personales en Noviembre del 2011. En Julio del 2012, se creó una Nueva Ley de Delitos Informáticos.

¹⁷⁵ *Ídem.*

4.3.2 Países con Tendencia Avanzada o Próspera:

Argentina.- Cuenta con el Sistema Argentino de Informática Jurídica (SAIJ), uno de los mejores bancos de datos legislativos de América Latina. Imparten un “Posgrado de Derecho de la Alta Tecnología” y un “Curso de Actualización en Informática Jurídica” en la Facultad de Derecho. Emitieron una ley que penaliza la piratería del software, al igual que una ley sobre delitos informáticos.

Uruguay.- Cuenta con el CINADE (Comisión de Investigaciones en Informática Aplicada al Derecho), creada en 2001, donde se desarrollan proyectos de la materia. Además del Instituto de Derecho Informático de la Facultad de Derecho, Universidad de la República Oriental de Uruguay.

4.3.3 Países con Tendencias Culminante o Innovadora:

Estados Unidos.- Cuenta con la mejor base de datos jurídica a nivel mundial (Lexis-Nexis). Incontables son los casos legislativos que se han tratado en este país en cuanto a Derecho Informático. En tema de legislación informática, es de los países más avanzados en la materia, con una extensa legislación.

España.- Desde hace varios años se imparten conferencias, simposiums importantes en las Facultades de Derecho, sobre el uso de la informática aplicada al derecho. En aportes legislativos, se desarrolló el proyecto de ley sobre firma electrónica que fue aprobado por la Unión Europea.

Francia.- En este país la informática jurídica data de hace más de 20 años, su jurisprudencia se encuentra avanzada y clasificada por áreas de especialización: derecho de autor, nombres de dominio, protección de datos personales, reglamentación de Internet, comercio electrónico, contenidos ilícitos, derechos de imagen, etcétera. Cuenta con el DEA de Informática Jurídica y Derecho de la Informática, de la Facultad de Derecho de la Universidad de Montpellier I.

Italia.- País sumamente desarrollado en relación a legislación sobre Derecho Informático. Dio una solución integral al problema relativo a la autoridad de certificación, sobre la firma digital asimétrica, problema en el que grupos y categorías, disputa tener el monopolio de esa autoridad.

Japón.- Se encuentra dentro de la quinta generación del desarrollo de la informática en el mundo, la cual considera la comunicación con la computadora en lenguaje natural y la utilización de sistemas expertos.

4.4 CASOS INTERNACIONALES

Entre los diversos problemas que se enfrentan a nivel internacional e inclusive nacional en temas de Derecho Informático, actualmente la propiedad intelectual y la piratería informática han sido tema de interés internacional, en los que diversos países han participado a favor de que se regulen jurídicamente, situación que ha desatado protestas en las que se argumenta que con el “pretexto” de penalizar todo tipo de delitos relacionados con la propiedad intelectual y piratería informática, se viola el derecho de intimidad y la libertad de expresión, puesto que los acuerdos que han surgido últimamente proponen dar un total control a los proveedores de Internet para monitorear a cada usuario y prácticamente denunciarlo si se viola el régimen de esos acuerdos.

Dichos acuerdos con los que ha surgido protestas y debates a nivel internacional son: SOPA, ACTA y PIPA.

4.4.1 SOPA¹⁷⁶

La ley Stop Online Piracy Act (SOPA), pretende frenar la piratería en internet, fue propuesta por el legislador Lamar Smith del partido republicano estadounidense y fue discutida en la Cámara de representantes. Entre los más interesados en que ésta ley se aplicara se encontraban la Motion Picture Association of America, el Screen Actors Guild, NBC Universal, EMI Music y Time Warner, empresa matriz de CNN y CNNMéxico. Y por el contrario, los principales opositores fueron Google, Wikipedia, AOL, Yahoo y Twitter, inclusive mostraron su total rechazo mediante pequeños “paros” en sus contenidos web.

Sus repercusiones habrían sido globales, pues esta ley permitía cerrar páginas web de sitios que violaran el derecho de autor de los contenidos creados en Estados Unidos y alojados en servidores de otros países. Su discusión en el Congreso fue pospuesta indefinidamente, tras las diversas protestas electrónicas de varios sitios como Wikipedia, Wordpress y Reddit, que anteriormente se mencionan. Por su parte la administración del presidente Barack Obama ha rechazado la iniciativa por “poner en riesgo la libertad de expresión de internet”.

4.4.2 ACTA¹⁷⁷

El Acuerdo Comercial Antifalsificación (ACTA por sus siglas en inglés) fue firmado por los gobiernos de distintas naciones para evitar la piratería y violación de derechos de autor en internet. Australia, Canadá, Corea del Sur,

¹⁷⁶ CNN México, *Cuatro leyes polémicas que buscan regular internet*, consultado en Diciembre 14 del 2012 en <http://mexico.cnn.com/tecnologia/2012/01/24/sopa>

¹⁷⁷ *Ídem*.

Marruecos, Nueva Zelanda, Singapur y Estados Unidos firmaron el acuerdo en Octubre del 2011. En cuanto compete a nuestro país, México firmó el documento el pasado 11 de Julio del 2012.

El acuerdo permite que los proveedores de internet revelen a las autoridades información de aquellos usuarios que violen los derechos de autor. Las autoridades podrán establecer multas y suspender el servicio a los infractores. Este acuerdo fue polémico puesto que gran parte de las negociaciones se realizaron de manera privada entre los gobiernos. México firmó el documento en Japón, a través del embajador Claude Heller, aunque cabe destacar, que se necesita su aprobación en el Congreso mexicano para que dicho acuerdo pueda aplicarse en el país.

4.4.3 PIPA¹⁷⁸

Es una Propuesta para prevenir las amenazas reales en línea contra la creatividad económica y el robo de propiedad intelectual (*Protect IP Act*, o PIPA) es el complemento de la ley SOPA y se discutió en el senado de Estados Unidos. Compañías de la industria del entretenimiento como la Motion Picture Association of America (MPAA), el Screen Actors Guild (SAG), NBC Universal, EMI Music, TimeWarner, matriz de CNN y CNNMéxico, y senadores tanto del partido republicano como demócrata se encontraban a favor dicha propuesta. Después de las protestas realizadas en internet, 18 legisladores estadounidenses retiraron su apoyo. La diferencia de SOPA con PIPA, era que esta última sólo suspendería sitios de internet, cuyo acto principal fuera el de “violación de los derechos de autor”, es decir atacaría sitios de transferencia de contenidos. PIPA estaba programada para ser discutida el 24 de enero, pero fue pospuesta luego de las protestas en internet.

4.5 EVOLUCIÓN DEL DERECHO INFORMÁTICO EN MÉXICO

El impacto de las TIC (Tecnologías de Información y la Comunicación) reconocidas como un fenómeno global, debe pasar por las decisiones de los gobiernos, en impulsar la aplicación de nuevas tecnologías, lo que conlleva a que estos procesos de decisión se transformen en un mecanismo lento y difícil, sobre todo en México, donde a pesar de los esfuerzos, faltan los recursos necesarios para realizar éstos cambios. De hecho la primera vez que se realizó una mención a la Informática en la legislación mexicana, fue en el año de 1984 en el acuerdo 114 de la Secretaría de Educación Pública,

¹⁷⁸ CNN México, *Cuatro leyes polémicas que buscan regular internet*, consultado en Diciembre 14 del 2012 en <http://mexico.cnn.com/tecnologia/2012/01/24/pipa>

mediante el cual se permitió la inclusión de los programas de cómputo en el Registro de Derecho de Autor.¹⁷⁹

No obstante, a nivel internacional, en la década de los 90 se inició un mayor énfasis e importancia a la informática, tanto por parte de la sociedad, como de los gobiernos. Muchas de las reformas a nivel nacional han tratado de referirse a normativas de otros países, cuyas labores legislativas son más avanzadas.

La Informática y el Derecho han evolucionado a nivel internacional con las tendencias anteriormente mencionadas: inicial o básica, progresiva o creciente, avanzada o próspera y culminante o innovadora. Se puede decir que México se encuentra en una tendencia inicial-creciente, puesto que ya hay una distinción para el Derecho Informático en general, tanto para nivel legislativo como en educación, además de que en dicho nivel legislativo se ha considerado en impulsar la labor legislativa nacional en relación al Derecho Informático.

México está constituido como una República Federal, en donde los Estados que la integran son libres y soberanos en cuanto a su régimen interno, si bien unidos por el pacto federal, por ello, los asuntos en cuanto a informática se refiere, inciden en el ámbito del Derecho Civil o Penal, pueden ser regulados por cada una de las Entidades Federativas a su libre y mejor parecer,¹⁸⁰

4.5.1 Delitos informáticos en el ámbito Federal:¹⁸¹

- Pornografía infantil
- Conocer o copiar información contenida en sistemas informáticos o equipos.
- Modificación, destrucción o pérdida de información contenida en sistemas informáticos o equipos (virus, troyanos, gusanos, etc.)
- Uso y/o reproducción no autorizada de programas informáticos, todo esto con fines de lucro, lo que viene siendo en resumen, la piratería.
- Ataque a las vías de comunicación y obtención de información que pasa por el medio.
- Asociación delictuosa y vandalismo.
- Violación a la intimidad en términos cibernéticos.

¹⁷⁹ Gleason Santana Arturo, *El Marco Jurídico de la Informática y la Piratería*, consultado en Diciembre 15 del 2012 en http://www.debate.iteso.mx/numero09/Articulos_9/MARCOJURIDICO.htm

¹⁸⁰ Geraldine Da Cunha Lopes, Teresa M., *El estado del arte del Derecho de Protección de Datos Personales en México*, Centro de Investigaciones Jurídicas y Sociales/Universidad Michoacana de San Nicolás de Hidalgo, consultado en Diciembre 15 del 2012 en http://www.egov.ufsc.br/portal/sites/default/files/el_estado_del_arte_del_derecho_de_proteccion_de_datos_personales_en_mexico.pdf

¹⁸¹ Bátiz-Álvarez V y Farías-Elinos M. *Panorama General del Marco Jurídico en materia Informática en México*. Consultado en Diciembre 15 del 2012 en http://seguridad.cudi.edu.mx/congresos/2003/cldi/marco_juridico_info_mx.pdf

4.5.2 Delitos informáticos en el ámbito Local:

- Pornografía infantil.
- Fraude (sistemas financieros y administradores de negocios).

4.5.3 Policía cibernética en México

Para la regulación de los diversos delitos informáticos en el país, surgió en el año 2000 la primera Unidad de Policía Cibernética y Delitos Contra Menores en México¹⁸², dedicada a:

- Delitos en y a través de computadoras
- Seguridad y protección en Internet
- Patrullajes en la supercarretera de la información
- Investigación del crimen computacional
- Computación forense

Además, comprende las siguientes áreas:

Delitos cibernéticos

- Atención a delitos cibernéticos
- Atención a delitos usando computadoras
- Análisis de cómputo forense
- Delitos contra menores
- Análisis de explotación de menores
- Atención a menores desaparecidos

Coordinación interinstitucional

- DC México
 - Centro de Análisis e Intercambio de Información para la Identificación de alerta temprana y riesgos
- Mecanismos de Coordinación Interinstitucional
- Información y Prevención

Esta Unidad ha realizado avances en la prevención de delitos informáticos, principalmente en el tema de pornografía infantil. Estados como Jalisco, Querétaro, Tamaulipas, Chihuahua, Yucatán, Distrito Federal y próximamente Quintana Roo, ya cuentan con su respectiva Unidad de Policía Cibernética.

¹⁸² DISC P.F.P., Unidad de Policía Cibernética y Delitos Contra Menores. Consultado en Diciembre 16 del 2012 en http://www.disc.unam.mx/2005/presentaciones/delitos_menores.pdf

4.5.4 Gobierno Electrónico

Seguramente hoy en día una parte de usuarios conocen cómo transferir electrónicamente dinero, pagar diversos servicios y realizar trámites de forma electrónica, y hasta tener la facilidad de usar dispositivos móviles para pagos monetarios. El sector de los servicios en México se ha esforzado en la innovación, con el uso de la tecnología conjugado con las actividades cotidianas en las que una persona consideraba tardía y con diversos procesos.

Es importante analizar que la transición a un esquema de Gobierno Electrónico no es un proceso sencillo y mucho menos inmediato, sino que se vino dando en diversas etapas con características particulares:¹⁸³

1. **Diseminación y publicación de información.** Es la etapa básica, en la que se da prioridad a la creación de una nueva forma de comunicación con los ciudadanos, a través de un sitio web, en donde se puedan enterar de los servicios, contactos y asistencia que puedan recibir de una entidad gubernamental. Por mencionar ejemplos, los diversos sitios web de cada gobierno estatal en México, o de entidades gubernamentales que muestren como tramitar diversos servicios.
2. **Transacciones bidireccionales “oficiales” de una sola entidad gubernamental.** En esta etapa se desarrollan sistemas tecnológicos en los que se identifica de manera única a los ciudadanos, para realizar transacciones monetarias con alguna entidad gubernamental. En este aspecto, México se encuentra al tanto de dichos procesos, por ejemplo, los actuales trámites de la Firma Electrónica Avanzada y pago de impuestos a través del portal de la Secretaría de Hacienda.
3. **Portales multipropósito.** Consiste en el desarrollo de un sitio web en el que se realicen múltiples servicios gubernamentales a través de una sola forma de acceso. Es decir, que en un solo sitio el ciudadano pueda realizar transacciones con distintas entidades gubernamentales, así como también obtengan información para algún tipo de trámite.
4. **Personalización de un portal.** El objetivo es realizar un portal multipropósito otorgando mayor poder de decisión para que el ciudadano defina qué le interesa ver y hacer.

¹⁸³ Aceves Gutiérrez Luis Carlos, *Gobierno Electrónico en México: ¿Dónde estamos?* Consultado en Diciembre 16 del 2012 en <http://www.luiscarlosoceves.com/articuloconocimiento1.html>

5. **Conjunción de servicios comunes.** El ciudadano lleva a cabo una transacción única, dejando de notar entidades gubernamentales que se encuentren aisladas; la transacción se realiza a pesar de que parte del proceso recae en una entidad, y parte en otra.
6. **Integración total y transformación de la organización.** En este último proceso, cualquier servicio gubernamental se puede llevar a cabo de forma electrónica, y el ciudadano puede personalizar los servicios importantes que él decida. Muchas veces esta situación implica crear entidades gubernamentales para sustituir a otras.

Como se observa, por servicios electrónicos se ha avanzado satisfactoriamente; sin embargo hay aspectos que no permiten que dichos procesos se lleven a cabo en su totalidad.

En primer lugar se tiene la abismal diferencia en el uso de Internet, puesto que a nivel geográfico no todas las personas cuentan con dicho servicio, puesto la infraestructura representa un costo y resulta complicado llegar a ciertos puntos del país.

En segundo, la falta de cultura en el uso de la tecnología, pues aunque por increíble parezca, hay personas que no saben encender una computadora y mucho menos usarla, además de que otras, tienen miedo de realizar trámites por Internet por la falta de comprobantes físicos, además de no acostumbrarse o no saber resguardar archivos electrónicos.

Y por último el tema más crítico: el de la seguridad y privacidad. Se ha avanzado en la relación ciudadano-gobierno en términos tecnológicos, pero aún existen aspectos sobre seguridad en las que se viola por medios y personas externas, a pesar de ya ser delitos tipificados. Es por ello que aún en México resulta complicado un rápido avance, cuando a trabajos forzados se ha iniciado. Se deberán concretar esfuerzos para consolidar el uso de la tecnología que permita mayores beneficios para los ciudadanos y al gobierno de nuestro país.

4.5.5 Evolución del valor probatorio del documento electrónico

El concepto de prueba documental ha tomado fuerza en tema de tecnología e Informática, ahora no sólo la legislación se ha visto en la necesidad de adaptarse en cuanto al valor probatorio del documento electrónico, sino también jueces y abogados. Como se afirma en el Capítulo 1, este concepto se ha considerado con el mismo valor jurídico que tiene una prueba escrita.

A través del tiempo la prueba ha sido de gran importancia para la solución de conflictos en litigios; cada prueba tiene por objetivo acreditar los hechos y

los motivos con que se cuenta para decidir el conflicto a favor de una de las partes.¹⁸⁴

Como señala el Dr. Julio Téllez:

“Si bien es cierto que la mayoría de los medios de prueba pueden interrelacionarse con las computadoras, es la prueba documental la que, en última instancia, guarda un vínculo más estrecho debido a que los soportes magnéticos pueden ‘constar’ al igual que un documento.”¹⁸⁵

Al documento se le concibe como “una cosa, en sentido físico corporal, que *Docet*, que enseña, que hace conocer”.¹⁸⁶ La doctrina del Derecho distingue a dos elementos constitutivos del documento: el *corpus* y el *docet*. El *corpus* es la cosa corporal, en donde se consta una representación gráfica de un hecho; el *docet* es la enseñanza, lo que intenta expresar el autor al destinatario del documento.¹⁸⁷

Ante tales descripciones se analiza que los medios informáticos como los correos electrónicos, mensajes de datos, certificados digitales, etcétera, al contener dichos elementos, tienen materia, pues aun cuando estos medios se podrían borrar de manera sencilla y copiarse en otros formatos de forma indefinida, los archivos electrónicos están soportados en medios físicos. Así entonces los medios informáticos cumplen con la función del *docere*. Por esto se concluye que son documentos aptos y verídicos para mostrar algún grado de evidencia ante un Juez y se constituyen como medios de prueba dentro del proceso. Incluso, se ha establecido en los códigos penales estatales, que todo acto que atente contra los documentos electrónicos, archivos y equipo físico se considere un delito, otorgando una valoración a los medios informáticos dentro del Derecho.

4.5.6 La Firma electrónica¹⁸⁸

Para llevar a cabo en México un mejor desarrollo en esta sociedad de la información, se ha implementado el uso de instrumentos tecnológicos como la firma electrónica, en la que los ciudadanos realizan diversos trámites administrativos y gubernamentales a través de Internet. Esto se aprobó en el Senado de la República en Marzo del 2011, con la publicación de la Ley de Firma Electrónica Avanzada.

¹⁸⁴ Olmos Jasso, María Teresa, *Valor Probatorio de los Documentos Electrónicos*, 2009, consultado en Diciembre 17 del 2012 en

<http://www.tfjfa.gob.mx/investigaciones/pdf/valorprobatoriodelosmedioselectronicos.pdf>

¹⁸⁵ Téllez Valdés Julio, *Derecho Informático*, 3ª. Ed., México, 2007, p.243.

¹⁸⁶ Riofrio Martínez Villalva, Juan Carlos, *La Prueba Electrónica*, Bogotá, Colombia, Temis, 2004.

¹⁸⁷ Olmos Jasso, María Teresa, *Valor Probatorio de los Documentos Electrónicos*, 2009, consultado en Diciembre 17 del 2012 en

<http://www.tfjfa.gob.mx/investigaciones/pdf/valorprobatoriodelosmedioselectronicos.pdf>

¹⁸⁸ Izquierdo Enciso León, *La implementación de la Firma Electrónica en México*. Consultado en Diciembre 17 del 2012 en

<http://www.economia.unam.mx/publicaciones/econinforma/369/08leonizquierdo.pdf>

Los primeros indicios por implementar un mecanismo que permitiera identificar al emisor de un mensaje electrónico como autor legítimo al igual que una firma autógrafa, fue el proyecto llamado “Tu firma” que el Sistema de Administración Tributaria (SAT) implementó en el 2004 como un mecanismo alternativo en su inicio y obligatorio para el 2005. El SAT presentaba el primer intento y esfuerzo de sustituir la firma autógrafa del firmante con los mismos efectos y alcances, además, también permitían la expedición de facturación electrónica trayendo como beneficios:¹⁸⁹

- Consulta de situación fiscal del contribuyente por internet.
- Los documentos firmados electrónicamente tienen las mismas funcionalidades y garantías que un documento físico.
- Posibilidad de presentar avisos a través de internet.
- Envío de información fiscal de relevancia mediante boletines vía correo o buzón electrónico.
- Gracias a sus características de autenticidad, se dará más certeza jurídica al contribuyente en sus transacciones.
- Ahorro en insumos y demás gastos administrativos, al reducir el uso de papel.

La segunda etapa de la firma electrónica se inicia con el cambio de la Clave de Identificación Electrónica Confidencial (CIEC) por la denominada Firma Electrónica Avanzada, la cual inicialmente tenía las mismas funciones que la CIEC, pero fue creciendo en funcionalidad.

El Gobierno Federal define a La Firma Electrónica Avanzada como “un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa”.¹⁹⁰

La Firma Electrónica Avanzada (FIEL) ofrece seguridad a toda transacción electrónica de los contribuyentes, con su uso se identifica al autor del mensaje y se verifica que no haya sido modificado. Su diseño está basado en estándares internacionales de infraestructura de claves públicas (o PKI por sus siglas en inglés *Public Key Infrastructure*) en donde se utilizan dos claves o llaves para el envío de mensajes:

- La “llave o clave privada” que únicamente es conocida por el titular de la Fiel, que sirve para cifrar datos; y
- La “llave o clave pública”, disponible en Internet para consulta de todos los usuarios de servicios electrónicos, con la que se descifran

¹⁸⁹ *Ídem.*

¹⁹⁰ Secretaría de la Función Pública, *¿Qué es y para qué sirve la Firma Electrónica Avanzada?*, consultado en Diciembre 17 del 2012 en <http://www.funcionpublica.gob.mx/index.php/temas/declaracion-de-modificacion-patrimonial.html>

datos. En términos computacionales es imposible descifrar un mensaje utilizando una llave que no corresponda.¹⁹¹

El éxito de la firma electrónica obedece a la confianza de los agentes económicos, ya que esta firma es tan segura como la firma autógrafa. Pero de igual manera, no debe ser presentada como un mecanismo que adopte valores superiores a los tradicionales, aunque en términos tecnológicos tenga sustento estadístico y de seguridad informática. Para ello debe tener un reconocimiento, iniciando en el sector público, pues la validez de este instrumento ahorra tiempo, movilidad, emisión de documentos en papel, y fortalece los mecanismos jurídicos.

4.5.7 El voto electrónico

La democracia en México ha adquirido nuevas perspectivas. En los procesos electorales se ha tenido que mejorar la calidad en su formación y toma de decisiones con el llamado “voto electrónico”; esto rompe con una tradición en los procesos electorales de un país, apoyándose de la tecnología informática para convertir un proceso de votación en una jornada que beneficie su ejecución, con el propósito de brindar la confianza al ciudadano de que su participación sea democrática y participe de este avance tecnológico.

Votar electrónicamente significa que el ciudadano emita su voto a través de medios electrónicos, como una computadora, urna electrónica con teclado y/o pantalla, o el recuento automatizado del voto al momento de ser emitido;¹⁹² todos estos procesos implican que cambie la materialización del voto hasta su registro, a nuevos procedimientos tecnológicos. El acto de votar electrónicamente consiste en la tecnología que se aplica en las etapas que se desarrollan el día de un proceso electoral como lo son: el registro y la verificación de la identidad del elector, la emisión del voto, el recuento de votos y la transmisión de los resultados.

El voto electrónico ha sido bien aceptado porque lo consideran un gran elemento opcional para la realización de un proceso electoral. Por lo general este novedoso proceso se ha introducido en los programas de modernización y reforma del Estado, siendo una gran herramienta de los procesos de reforma política y gobierno electrónico.

Su uso ha determinado ciertas necesidades para el conteo y recuento de votos, el establecimiento para una infraestructura de voto electrónico como son:¹⁹³

¹⁹¹ *Ídem.*

¹⁹² Flores Salgado, Lucerito, Derecho Informático, Grupo Editorial Patria, 2009, p. 141.

¹⁹³ *Ibidem*, p. 142.

- La verificación y transparencia, preservando el principio de que la tecnología está al servicio del hombre.
- Vigilar e imposibilitar que se impida el ejercicio de un derecho político de forma maliciosa o intencional.
- Manipulación de votos o adueñarse de la identidad electrónica de un ciudadano para fines electorales u otros.
- Mantener en total secreto el valor del voto e impedir la unión de la identidad del elector y el valor de su voto.
- Establecer una restringida vigilancia de la base de datos que contenga los votos.
- Las autoridades electorales deben de anteponer los derechos políticos de los electores ante la administración electoral e instituciones públicas o privadas.

Las elecciones representan una pieza clave en el funcionamiento de la democracia, y el sistema del voto electrónico rompe con las barreras tradicionales de ejercerla, teniendo claro el objetivo de un resultado con validez, garantizando el carácter secreto del voto.

Actualmente, el derecho electoral de cualquier Estado democrático contempla la celebración de elecciones competitivas mediante el sufragio universal, libre, igual, secreto y directo.¹⁹⁴

4.5.8 Comercio electrónico

El comercio es uno de los principales motores de la economía, pero debido a la creciente tecnología en el país, tanto sectores públicos como privados, han tenido que modernizar sus formas de ventas para adquirir mayores ganancias. Internet es un medio que con un gran número de usuarios genera una nueva forma de beneficiar a la economía tanto para quien compra, como para quien vende; esto es lo que hoy llamamos comercio electrónico.

El comercio electrónico es definido por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) como el proceso de compra, venta o intercambio de bienes o servicios e información a través de las redes de comunicación.¹⁹⁵

Según la Asociación Mexicana de Internet (AMPICI), el comercio electrónico sumó 3 mil 600 millones de dólares el 2011, lo que representó un aumento de 28% en comparación con el año 2010.¹⁹⁶

¹⁹⁴ *Ibidem*, p. 144.

¹⁹⁵ Comercio Electrónico, Consultado en Diciembre 22 del 2012, en http://www.profeco.gob.mx/internacionales/com_elec.asp.

¹⁹⁶ Alto Nivel, Comercio electrónico en México crecerá 30% en 2012. Consultado en Diciembre 22 del 2012 en <http://www.altonivel.com.mx/19629-comercio-electronico-en-mexico-crecera-30-en-2012.html>.

El comercio electrónico representa una extensa variedad de posibilidades y oportunidades para la adquisición de bienes o servicios que ofrecen proveedores en diversas partes del mundo. Todas las compras de artículos y servicios por Internet o de forma on-line resultan atractivas por la facilidad para realizarlas; sin embargo, es igualmente atractivo cometer prácticas comerciales fraudulentas.

En relación al marco jurídico del comercio electrónico, el usuario o *ciberconsumidor* mexicano está protegido cuando realiza compras por internet. La Ley Federal de Protección al Consumidor (LFPC) contiene disposiciones generales sobre comercio electrónico en su capítulo VIII bis, “Derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología”.¹⁹⁷

Para que las transacciones comerciales en línea resulten exitosas, están una serie de recomendaciones que la PROFECO¹⁹⁸ enlistó dirigida a los usuarios:

- El proveedor debe informar de manera muy clara su identidad, denominación legal y datos de su ubicación, todo esto para que el usuario pueda realizar algún reclamo en caso de que surja un problema.
- El proveedor por Internet tiene la obligación de proporcionar una descripción veraz de las características de los productos, para que el consumidor tenga una decisión de compra bien informada.
- Los proveedores deben expresar sus precios en moneda nacional, y en caso de haber cargos adicionales por envío de productos, se deben señalar junto con las condiciones y formas de pago.
- El portal debe declarar sus políticas de privacidad. Esto es de suma importancia pues es probable que se requiera que el usuario tenga que revelar datos privados o números de tarjetas de crédito. Además de que deben estipular claramente las políticas de devolución de mercancía, así como garantías y condiciones de transacción en la devolución.

4.6 DERECHO INFORMÁTICO COMO MATERIA DE EDUCACIÓN EN MÉXICO

Existen Facultades de Derecho en México que incluyen la materia de Derecho Informático o legislación informática en su plan de estudios, las cuales son:

¹⁹⁷ Portal del Consumidor, *Decálogo de los derechos mínimos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos*, consultado en Diciembre 22 del 2012 en <http://www.consumidor.gob.mx/wordpress/?p=11743>

¹⁹⁸ *Comercio Electrónico*, Consultado en Diciembre 22 del 2012, en http://www.profeco.gob.mx/internacionales/com_elec.asp.

- Estudios de Posgrado de la Facultad de Derecho de la Universidad Nacional Autónoma de México (UNAM).
- Facultad de Contaduría y Administración, UNAM.
- Facultad de Derecho de la Universidad La Salle de la Ciudad de México.
- Facultad de Derecho y Ciencias Sociales de la UANL.
- Facultad de Derecho de Culiacán de la Universidad Autónoma de Sinaloa.
- Facultad de Derecho de Mazatlán de la Universidad Autónoma de Sinaloa.
- Universidad Panamericana, Campus Guadalajara, México.
- Maestría en Derecho con Especialidad en Amparo, Universidad Iberoamericana León (Guanajuato).¹⁹⁹

Como se observa, en su mayoría se encuentran Universidades en Derecho, esto puede crear una expectativa errónea de que solamente los profesionales en Derecho conozcan sobre Derecho Informático. Es importante contemplar que no sólo en éstas Facultades se impartan materias sobre Derecho Informático, sino también en Facultades que impartan carreras tecnológicas, como la Informática, Ciencias de la Computación, Ingeniería en sistemas y computación; para que así entonces, se fomente el interés de estudio de la materia tanto para los estudiantes de Derecho, como para los estudiantes de carreras tecnológicas.

4.6.1 Primeros avances de Informática Jurídica en México

En México existen los llamados bancos de datos jurídicos que fueron desarrollados por Infosel-legal²⁰⁰, que es un sistema nacional de información en línea que contiene la colección jurídica y legal disponible más completa de México. El UNAM-JURE es un departamento del Instituto de Investigaciones Jurídicas de la UNAM cuyo objetivo es la compilación, análisis y sistematización de documentación legislativa y jurisprudencial, tanto nacional como extranjera. El instituto se inició desde hace dos décadas. El primero de ellos fue el sistema UNAM-JURE, diseñado para almacenar, identificar y dar seguimiento a todas las disposiciones legislativas emitidas en la República Mexicana publicadas en el Diario Oficial de la Federación y en todos los periódicos, gacetas y boletines oficiales de los Estados.²⁰¹

Desde inicios de los 90's el Instituto a través de su Centro de Documentación y su Departamento de Informática, ha desarrollado diversos

¹⁹⁹ UNINET DERIN, *Tendencias actuales de la Informática y el Derecho a Nivel Internacional*.

Consultado en Diciembre 23 del 2012 en <http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=36>

²⁰⁰ Véase <http://legal.terra.com.mx/>

²⁰¹ Instituto de Investigaciones Jurídicas, *Presentación*, consultado en Diciembre 23 del 2012 en <http://www.juridicas.unam.mx/infjur/leg/presenta.htm>

sistemas capaces de brindar información jurisprudencial en materia penal, civil, laboral, constitucional, así como información legislativa federal y estatal, en texto completo. Algunos de éstos sistemas son CFE-JURE, DF-JURE, Sistema de Información Jurídica en materia de Seguridad Pública, UNIJUS, ADPROJUS, Sistema de Información Jurídico Laboral, Sistema de Información Jurídico Constitucional, JUS-TUR, Sistema de Información Jurídico Electoral e ISSSTE-JURE.²⁰²

4.7 SITUACIÓN ACTUAL Y POSIBLES DIRECCIONES

En México, el sistema jurídico se ha adecuado a las diversas inclinaciones y tendencias en el ámbito de la economía, y la ciencia y tecnología.

En la economía, se tiene una Secretaría de Economía, la cual tiene por objeto la creación de las condiciones necesarias para fortalecer la competitividad, en el mercado nacional e internacional, promoviendo la creación y consolidación de proyectos productivos.²⁰³ Se basa en una serie de normas, leyes y tratados que permiten realizar estas actividades mercantiles y comerciales, garantizando la seguridad y promoviendo la vanguardia, por ejemplo, el Código de Comercio, en donde ya se incluyen aspectos informáticos.

Respecto a la ciencia y tecnología, existe el Programa especial de Ciencia y Tecnología 2008-2012²⁰⁴, que es el instrumento fundamental de planeación del Gobierno de la República en ésta área. Su objetivo es integrar y coordinar el esfuerzo nacional para dar un mayor impulso a las actividades científicas y tecnológicas del país, contribuye a que las dependencias y entidades de la Administración Pública Federal inviertan en ciencia y tecnología de forma eficiente.

Las tendencias o posibles direcciones que deben surgir en ésta área, es que la inversión nacional en investigación y desarrollo experimental, alcance por lo menos el 1.0% del PIB. El Programa plantea estrategias para la ciencia y tecnología, en donde se permita que se alcance la meta con eficiencia en cuanto a gasto y una alta calidad en investigación científica y tecnológica, además como también en la formación de posgrados.

²⁰² *Ídem.*

²⁰³ Estrategia programática, Secretaría de Economía, consultado en Diciembre 26 del 2012 en http://www.apartados.hacienda.gob.mx/contabilidad/documentos/informe_avances/2002/temas/banco/g10t01.pdf

²⁰⁴ Véase <http://132.247.1.49/pronaledh/pdfs/Peciti%202008-2012.pdf>

La clave del éxito para avanzar a ésta tendencia será:

- La transformación de los equipos tradicionales de voz a comunicación vía Internet, traspasando las fronteras.
- Migración de computadoras personales al cómputo móvil e inalámbrico.
- Servicios de redes privadas virtuales y banda ancha.
- Y principalmente, el desarrollo de una mayor cultura informática.

En las TIC (Tecnologías de Información y la Comunicación), existe el mito de la calidad del trabajo y los productos mexicanos respecto a los extranjeros, es decir, las desafortunadas comparaciones. Por ejemplo, al usuario, ya no le da lo mismo cualquier tecnología, puesto que ha aprendido a cuestionar más sobre las características de los productos, dando pie a que se deja llevar por el “*glamour*” de ciertas marcas y no tomar en cuenta los productos nacionales, o inclusive, discriminarlos. Este es uno de los principales retos de los fabricantes y desarrolladores nacionales, apostar a una mayor calidad nacional ante la mercadotecnia y capitalismo.

Internet se está convirtiendo en un medio indispensable para la sociedad, y constituye un parte-aguas jurídico, ya que ha venido a romper con las formas tradicionales en las que se manifiesta el Derecho. Como se mencionó anteriormente, en nuestro país ya existen consideraciones respecto al marco jurídico que representa el uso de Internet, sus dispositivos y herramientas.

El total de usuarios de Internet en México ha ascendido rápidamente, para finales del 2004 la cifra era de 14, 901, 687 personas, sin contar menores de 13 y mayores de 65 años, ciudades con población menor a 100,000 habitantes, usuarios de internet que accedían menos de 3 veces al mes. Luego, a finales del 2005, el número de usuarios de Internet ascendió a 16, 995, 400. Para Mayo del 2007 ya existían 22.7 millones de usuarios de Internet.²⁰⁵

Actualmente la cifra en lo que va hasta Mayo del 2012, presenta un crecimiento del 14%, resultando un total de 40.6 millones, a comparación del 2010 con 32.8 millones de usuarios, pasando al 2011 con 37.6 millones, con cifras del Instituto Nacional de Estadística y Geografía (INEGI).²⁰⁶ Según un estudio de la Asociación Mexicana de Internet, el mayor número de usuarios se encuentra en el Estado de México (6.04 millones), y le siguen el Distrito Federal (4.4 millones) y Jalisco (3 millones). Los hábitos que en la actualidad presentan los mexicanos respecto al uso de Internet está: para buscar

²⁰⁵ Razón y Palabra, *Las cifras de la industria de Internet en México, 2004*, consultado en Diciembre 26 del 2012 en <http://www.razonypalabra.org.mx/antecedentes/n43/oislas.html>.

²⁰⁶ Animal político, *Aumentan 14% usuarios mexicanos de internet en un año: Inegi*, consultado en Diciembre 26 del 2012 en <http://www.animalpolitico.com/2012/08/aumentan-14-usuarios-mexicanos-de-internet-en-un-ano-inegi/>.

información (29%), para enviar correos electrónicos (28%) y para juegos y acceder a redes sociales (17%),²⁰⁷ además de que existe un tiempo promedio de conexión diaria de 4 horas y 9 minutos en los que los usuarios pasan en Internet.²⁰⁸

Con relación a la protección que se ofrece a los usuarios por daño o perjuicio en el uso de la tecnología informática, entre los aspectos que se tienen contemplados en la legislación Mexicana se encuentran los siguientes:²⁰⁹

- Piratería de software y su documentación cuyos derechos de autor estén reconocidos.
- Marcas, nombres comerciales, patentes y secretos industriales.
- Regulación de las comunicaciones.

Sin embargo, es importante señalar aquellos aspectos que aún no se han contemplado en su totalidad en la legislación nacional y que por la naturaleza de la actividad informática es imperiosa la necesidad de regulaciones específicas, y un mejor análisis para su integración.

Dichos aspectos son:

- Delitos informáticos con una mayor cobertura en cuanto su tipificación y sanciones.
- Regulación total y específica de la privacidad, es decir, derecho a la confidencialidad de información personal almacenada en bases de datos públicas, o privadas.
- Mayor regulación en la web con el objetivo de evitar actividades negativas en la misma, sin la violación a la manifestación de ideas, libertad de expresión y derecho a la información.
- Protección total de datos.
- Mayor regulación en el comercio electrónico, con el fin de minimizar fraudes, publicidad engañosa, teniendo un mejor cuidado y atención a los contratos electrónicos.
- Valor de prueba de documentos electromagnéticos para procesos administrativos y jurídicos.²¹⁰

Estos aspectos continúan rezagados y requieren una mayor atención. Esto representa una gran responsabilidad y mayor compromiso, por parte de la sociedad, sus autoridades y gobierno.

²⁰⁷ CNN México, *Los usuarios de internet aumentan un 14% en México, según un estudio*, consultado en Diciembre 26 del 2012 en <http://mexico.cnn.com/tecnologia/2012/05/17/los-usuarios-de-internet-aumentan-un-14-en-mexico-segun-un-estudio>.

²⁰⁸ AMIPCI & TELEVISA, *Hábitos de los Usuarios de Internet en México*, consultado en Diciembre 26 del 2012 en <http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=115&Type=1>.

²⁰⁹ Arroyo Cortez L. y Farías Elinos M., *Importancia del marco jurídico en la función de auditoría Informática*, consultado en Diciembre 28 del 2012 en

<http://seguridad.cudi.edu.mx/grponly/congresos/marcolegal.pdf>

²¹⁰ Salgado Flores Lucerito, *Derecho Informático*, Grupo Editorial Patria, México, 2009, p. 85.

APORTACIONES

Este capítulo aportó información sobre la problemática a la que el Derecho Informático se enfrenta para su aplicación y evolución en México en comparación a nivel internacional. Todo ello definiendo desde la relación que presenta el Derecho Informático junto con las demás ramas del Derecho, como el Penal, Internacional, Civil y Mercantil, pues todos los diversos delitos y aspectos tratados en todo este trabajo de investigación de forma alguna se relacionan con demás ramas del Derecho en general.

Se enlistan diversos aspectos que competen tanto en el país como a nivel internacional, definiendo primeramente las tendencias en los que cada país, inclusive México, puede encontrarse. Asimismo también se aportó temas de los cuales se destacan como parte de la evolución del Derecho Informático, tal como la ética informática, el teletrabajo, el voto electrónico, los avances en el valor probatorio de los documentos electrónicos con la participación de la firma electrónica en diversos trámites gubernamentales, el comercio electrónico, y la aportación en materia de educación sobre la enseñanza del Derecho Informático.

En sus posibles direcciones sobre el Derecho Informático se aportó cómo es que se puede avanzar con paso firme y preciso para la correcta implementación de esta importante rama, con la investigación de estadísticas, definiciones y aspectos enlistados de los que puede derivar el rezago actual.

CONCLUSIONES Y RECOMENDACIONES

El Derecho Informático siendo una rama reciente, nos deja muy claro su participación fundamental para la ejecución penal en México en relación a la tecnología informática y su impacto en la sociedad.

En este trabajo de investigación se cumple la hipótesis planteada al principio del mismo, ya que entre las principales deficiencias está la deficiente regulación del Derecho Informático en México en la legislación existente. De las vertientes de esta rama que son la Informática Jurídica y el Derecho de la Informática, principalmente en este último se derivan diversos problemas que dan lugar al tratamiento necesario a profundidad como son la protección de la información, el flujo de datos transfrontera, los convenios y contratos informáticos, el valor probatorio de los documentos electromagnéticos, y el más notorio: los delitos informáticos.

Como aportación en tema de legislación nacional actual, se destacan algunas leyes como la Ley de Protección de Datos, Ley Federal del Derecho de Autor, Código Penal, Código Civil, entre otras, así como reformas a la legislación estatal en relación al Derecho Informático, dichas reformas se aplican a delitos generales, pero que fueron modificados refiriéndose a delitos relacionados con la tecnología informática. Sin embargo estas reformas legislativas no cuentan con una penalización acorde, por lo que en consecuencia puede resultar que una vez cometido el delito, su seguimiento no tenga la firmeza y aplicación suficiente, por lo que el deber en algunas autoridades está en evitar dicha problemática en estos delitos cibernéticos.

Con base en el Derecho Comparado Internacional, la cual está en constante evolución en países desarrollados, evidencia un rezago en Derecho Informático tanto a nivel nacional, como en América Latina. A pesar de los esfuerzos en creación de Tratados y Acuerdos de los cuales también se aportó información en este trabajo de investigación, puede no ser suficiente para una legislación a la altura de lo que este país y su población necesita. Dichos avances internacionales constituyen un ejemplo a seguir para alcanzar el nivel deseado en tratamiento del Derecho Informático en México.

Entre los problemas que el país enfrenta en Derecho Informático están los delitos informáticos, los cuales de acuerdo a su clasificación como método o instrumento, se desglosan en variadas actividades ilícitas, provocadas por la irresponsabilidad del usuario ya sea intencional o por accidente y de vulnerabilidades en seguridad informática, son delitos que presentan fallas de un control legislativo preciso y eficiente, en donde incluso afectan al sector económico del país. Dichas actividades ilícitas a las que nos referimos, se encuentran ampliamente explicadas en el Capítulo 2 y que

están presentes en la delincuencia de cuello blanco, y son: los fraudes informáticos, la pornografía infantil, *hackeos* intencionales y la alteración a la privacidad de datos o mejor llamado, revelación de secretos.

Es preocupante que este tipo de delitos presentan altos porcentajes con un perfil del delincuente más sofisticado al común, lo que dificulta su persecución y aprehensión. Desafortunadamente, la mayoría de las veces se teme a la denuncia por ignorancia, no perder prestigio en el caso de las empresas o por creer una pérdida de tiempo una denuncia cibernética. Todos esos factores hacen que los delitos informáticos se conviertan en una problemática nacional.

Aunado a esto, el no crear la suficiente cultura en prevención a la población que recurre a los medios informáticos como parte de su vida cotidiana y que no dan la debida importancia en su impacto negativo, aumenta la deficiencia de una mejor regulación de los delitos informáticos.

Un problema que se enfrentó al realizar este trabajo de investigación, fue el no contar con la suficiente información en relación a la aplicación e importancia del Derecho Informático en México, debido a que éste es un tema reciente al que no se le ha dado la suficiente importancia e impulso en este país; sin embargo, actualmente en diversas Universidades del país se ha tenido la intención de colocar al Derecho Informático como materia opcional u obligatoria en los planes de estudio, tal es el caso del Plan de Estudios de la Licenciatura en Informática de la Universidad Nacional Autónoma de México, esta asignatura es obligatoria. Se deduce que en educación de nivel superior en México ya se realiza un esfuerzo en especializar a abogados e informáticos sobre la materia, intentando cultivar el interés y estudio de esta importante rama.

La evolución del Derecho Informático en el país se ha realizado a paso lento, pues aunque los esfuerzos en implementar e-gobierno, firma electrónica, comercio electrónico y el voto electrónico que forman parte de ésa evolución, en ciertos aspectos esta implementación es limitada:

- Es una ciencia jurídica poco difundida y conocida.
- No despierta gran interés dado que no se establece como materia obligatoria y de importancia en el estudio de nivel superior.
- Las fuentes de información son servicios o herramientas costosas.

Queda mucho por resolver, por el simple hecho de que México como un país en vías de desarrollo, el gobierno decide enfocar soluciones hacia otros problemas y sectores, reduciendo el interés a los asuntos informáticos tratados en este trabajo de investigación.

Pese a ello es inevitable percibir que, con el rápido crecimiento tecnológico, tarde o temprano el gobierno decida darle la importancia que requiere la correcta aplicación del Derecho Informático y éste sea atendido como un problema más por resolver, pasando de una tendencia en inicial-creciente, para evolucionar a una tendencia avanzada, con el objetivo de disminuir y evitar su impacto negativo.

Sin embargo, se puede concluir que la solución no está en cada gobierno, cada presidente, cada autoridad, sino también en cada individuo que ayude a contribuir que como sociedad en un futuro no muy lejano estaremos obligados a tener cultura, prevención, respeto, y principalmente responsabilidad y ética al hacer uso de los medios informáticos. Con esa contribución en conjunto con las debidas acciones del gobierno y sus autoridades, la evolución y aplicación del Derecho Informático se reforzará y tomará un rumbo apropiado.

La Informática nació como apoyo a la humanidad, no como un riesgo para la misma; pero se debe reforzar en que la solución está en cada uno de nosotros para evitar el mal uso de sus herramientas y elementos. Por lo anterior se debe prestar mayor atención para una correcta regulación jurídica sin afectar los derechos y garantías individuales; y por lo tanto, tener una mejor aplicación del Derecho Informático en México.

ANEXO²¹¹

CÓDIGO DE ÉTICA PROFESIONAL DEL LICENCIADO EN INFORMÁTICA

- I. INTRODUCCION
- II. ALCANCE DEL CÓDIGO
- III. RESPONSABILIDAD HACIA LA SOCIEDAD
- IV. RESPONSABILIDAD HACIA LA PROFESIÓN
- V. RESPONSABILIDAD HACIA LOS USUARIOS
- VI. RESPONSABILIDAD HACIA EL PROVEEDOR DE RECURSOS
PARA EL EJERCICIO PROFESIONAL
- VII. EL PROFESIONAL COMO VENDEDOR Y/O COMPRADOR DE
PRODUCTOS INFORMÁTICOS
- VIII. EL PROFESIONAL EN INFORMÁTICA EN LA DOCENCIA
- IX. SANCIONES

²¹¹ Código realizado por la Academia de Informática de la Facultad de Contaduría y Administración.

I. Introducción

Al elaborar el presente código, se ha reconocido la existencia de varios principios de ética aplicables directamente al profesional en informática, principios a los que en este código nos referimos como postulados. Se estima que estos postulados representan la esencia de las intenciones de la profesión para vivir y actuar dentro de la ética. Se han agrupado en el ALCANCE DEL CÓDIGO y seis rubros fundamentales.

- Responsabilidad hacia la sociedad
- Responsabilidad hacia la profesión
- Responsabilidad hacia los usuarios
- Responsabilidad hacia el proveedor de recursos
- Responsabilidades del profesional como vendedor y/o comprador de productos informáticos
- Responsabilidad en la docencia

II. Alcance del código

Postulado A.

Aplicación universal del código: Este código de ética profesional es aplicable a todo profesional en informática por el hecho de serlo, sin importar la índole de su actividad o especialidad que cultive tanto en el ejercicio independiente o cuando actúe como funcionario de una organización.

Abarca también a los profesionales en informática que, además de ésta, ejerzan otra profesión u oficio.

Artículo 1.

El conocimiento de este código es obligatorio para todo profesional en informática, miembro activo del Colegio de Profesionales en Informática y Computación, para ejercer la profesión y por ninguna circunstancia, se podrá alegar su desconocimiento.

Artículo 2

Los profesionales en informática tiene la obligación de regir su conducta de acuerdo a las reglas contenidas en este código, las cuales deberán considerarse mínimas ya que se conoce la existencia de otras normas de carácter legal y moral, cuyo espíritu amplía el de las presentes.

Artículo 3

Este código rige la conducta del profesional en informática en sus relaciones con el público en general, con quien patrocina sus servicios (cliente o patrón) y sus compañeros de profesión, y le será aplicable a cualquiera que sea la forma que revista su actividad, especialidad que cultive o naturaleza de la retribución que perciba por sus servicios.

Artículo 4

Los profesionales en informática que además ejerzan otra profesión, deberán acatar estas reglas de conducta independientemente de las que señale la otra profesión para sus miembros.

Artículo 5

Toda falta planteada ante el Tribunal de Ética será juzgada por el Tribunal de Ética del Colegio de Profesionales en Informática y Computación, el cual calificara su gravedad y transcribirá su dictamen a la Junta Directiva del Colegio de Profesionales en Informática y Computación, al que corresponde imponer la sanción del caso.

Artículo 6

El Colegio de Profesionales en Informática y Computación directamente o a través de sus asociaciones afiliadas promoverá entre sus afiliados y empresas del ramo, el conocimiento y acatamiento de las normas de conducta estipuladas en este Código.

III. Responsabilidad hacia la sociedad

Postulado B.

Calidad profesional de los trabajos: En la presentación de cualquier servicio se espera del profesional en informática un verdadero trabajo de profesional, por lo que deberá tener presentes las disposiciones normativas de la profesión que sean aplicables al trabajo específico que esté desempeñando.

Responsabilidad de los trabajos: El profesional en informática actuara con la intención, el cuidado y la diligencia propias de un profesional íntegro y respetuoso de las leyes que rigen su vida ciudadana y profesional.

Independencia de criterio: Al expresar cualquier juicio, el profesional en informática aceptara la obligación de mantener un criterio libre e imparcial

Preparación y calidad del profesional: Como requisito para que el profesional en informática acepte prestar sus servicios, deberá tener el entrenamiento

técnico y la capacidad necesaria para realizar las actividades profesionales satisfactoriamente y de conformidad con las reglamentaciones y estipulaciones de contratación.

Artículo 7

El profesional en informática no deberá utilizar sus conocimientos profesionales en tareas reñidas con la moral o contrarias a las leyes nacionales vigentes. Se espera tenga un comportamiento digno en su vida personal, a fin de que esté acorde con su ejercicio profesional.

IV. Responsabilidad hacia la profesión

Postulado C.

Respecto a los colegas y a la profesión: Todo profesional en informática cuidará sus relaciones con sus colaboradores, con sus colegas y con las instituciones que los agrupan, buscando que nunca se menoscabe la dignidad de la profesión, sino que se enaltezca, actuando con espíritu de grupo.

Dignificación de la imagen profesional con base en la calidad: Para hacer llegar a quien patrocina sus servicios y a la sociedad en general una imagen positiva y de prestigio del profesional en informática, se valdrá únicamente de su calidad profesional y personal.

Artículo 8

Por respeto a su profesión y a sus colegas, el profesional en informática no deberá aceptar tareas para las que no esté capacitado.

Artículo 9

El profesional en informática se abstendrá de emitir juicio sobre otro profesional en informática, cuando dicho comentario perjudique su reputación o el prestigio de la profesión en general, a menos que se le solicite por parte de quien tenga un interés legítimo en ello o porque así lo establezcan las leyes nacionales vigentes.

Artículo 10

El profesional en informática deberá dar a sus colaboradores el trato que les corresponde como profesionales y vigilará y promoverá su adecuado entrenamiento superación y justa retribución.

Artículo 11

El profesional en informática deberá cimentar su reputación en la honradez, laboriosidad y capacidad profesional, observando las reglas de ética más elevadas en sus actos. No deberá anunciarse o solicitar trabajo por conducto de medios masivos de comunicación o de otros cuando menoscaben la dignidad del profesional en informática.

Artículo 12

El profesional establecerá conclusiones sobre un tema cuando puede ser demostrado que se basa en un adecuado conocimiento. Emitirá una opinión calificada cuando exprese un punto de vista en un área de su competencia.

Artículo 13

Ningún profesional en informática deberá interponer influencias indebidas u ofrecer comisiones u otras prebendas para obtener trabajo profesional, directa o indirectamente.

V. Responsabilidad hacia los usuarios

Postulado D

La relación que mantendrá el profesional en informática con los usuarios, sean estos directos o indirectos, deberá estar inspirada en:

- Respeto mutuo
- Sinceridad
- Justicia
- Leyes vigentes

Artículo 14

Entre otras cosas deberá:

Éticamente:

- No hacer afirmaciones falsas o exageradas, acerca de lo esperado de las herramientas informáticas.
- Respetar siempre los intereses legítimos de los usuarios y su poder de decisión.

Técnicamente:

- Considerar en todo momento las necesidades computacionales y ambientales de los usuarios que atiende.
- Deberá abstenerse de usar términos o expresiones técnicas en idioma extranjero, a menos que no existan términos equivalentes en

español, o que su empleo favorezca el mejor entendimiento de lo expresado.

- Facilitar y brindar toda la información conducente al entendimiento total de los procedimientos y cambios
- Prevenir y dar atención pronta a los problemas de su competencia.

VI. Responsabilidad hacia el proveedor de recursos para el ejercicio profesional

Postulado E

Secreto profesional: El profesional en informática tiene la obligación de guardar el secreto profesional y de no revelar por ningún motivo los hechos, datos o circunstancias de que tenga conocimiento en el ejercicio de su profesión, a menos que lo autoricen los interesados.

Obligación de rechazar tareas que no cumplan con la moral: Faltarán al honor y la dignidad profesional todo profesional en informática y computación que directa o indirectamente intervenga en arreglos o asuntos que no cumplan con la moral o riñan con la legislación nacional vigente.

Lealtad hacia el proveedor de recursos: El profesional en informática se abstendrá de aprovecharse de situaciones que puedan perjudicar a quien haya contratado sus servicios.

Retribución económica: Al establecer una relación laboral, el profesional en informática, además de la justa retribución económica, debe considerar la dimensión social de su labor profesional.

Artículo 15

El profesional en informática deberá analizar cuidadosamente las verdaderas necesidades que pueda tenerse de sus servicios, para proponer aquellos que más convengan dentro de las circunstancias. Este consejo deberá darse en forma desinteresada y estará basado en los conocimientos y experiencia profesional.

Artículo 16

Ningún profesional en informática podrá obtener ventajas económicas directas o indirectas por la venta al patrocinador de su trabajo, de productos o servicios que el haya sugerido en el ejercicio de su profesión, excepto de aquellas que le sean propias a su actividad, como profesional en informática.

Artículo 17

El monto de la retribución económica que reciba el profesional en informática debe considerar la importancia de las labores a desarrollar, el tiempo que a esa labor se destine y el grado requerido de especialización y responsabilidad.

VII. El profesional como vendedor o comprador de productos informáticos

Postulado F

Dado el enorme impacto que puede tener las decisiones y acciones sobre inversiones en productos informáticos, en instituciones y empresas de prestigio, que sirven a un amplio público, se hace aún más necesario el proceder con total integridad moral.

Artículo 18

En el intercambio que se genera en la contratación no puede pasarse por alto el interés social. El objetivo del trato será encontrar la opción que mejor favorezca a quien este adquiriendo el producto informático.

Artículo 19

El proveedor de bienes y servicios, profesional en informática, debe manifestar, en forma clara, consideraciones éticas sobre aspectos tales como: cumplimiento del ordenamiento jurídico; condiciones de calidad y económicas justas; garantías sobre las mercancías y servicios; cumplimientos de plazos y lugares de entrega; respeto a los márgenes de utilidad fijados oficialmente; entregar las cantidades ofrecidas; cumplir con las especificaciones técnicas solicitadas en la compra; no ofrecer regalos, dadas o comisiones a los compradores en sus decisiones y acciones; no hacer uso de compadrazgos para concretar las ventas; y en general, decir siempre la verdad.

VIII. El profesional en informática en la docencia

Postulado G

Difusión y enseñanza de conocimientos técnicos y teóricos: Todo profesional en informática que de alguna manera transmita sus conocimientos, tendrá como objetivo mantener las más altas normas profesionales y de conducta y contribuir al desarrollo y difusión de los conocimientos propios de su profesión.

Artículo 20

El profesional en informática que imparta cátedra debe orientar a sus alumnos para que en su futuro ejercicio profesional actúen con estricto apego a las normas de ética profesional.

Artículo 21

Es obligación del profesional en informática dedicado a la docencia, el mantenerse actualizado en las áreas de su ejercicio, a fin de transmitir al alumno los conocimientos más avanzados de la materia existentes en la teoría y la práctica profesional.

Artículo 22

El profesional en informática dedicado a la docencia debe dar a sus alumnos un trato digno y respetuoso, instándolos permanentemente a su constante superación.

IX. Sanciones

Las denuncias por escrito y firmadas se tramitarán, según lo establece la Ley Constitutiva del Colegio, ante el Tribunal de Ética Profesional que será nombrado por la Asamblea del Colegio

Artículo 23

El profesional en informática que viole este código se hará acreedor de las sanciones que le imponga el Colegio.

Artículo 24

Para la imposición de sanciones se tomara en cuenta la gravedad de la violación cometida, valuando dicha gravedad de acuerdo con la trascendencia que la falta tenga para el prestigio y estabilidad de la profesión.

Artículo 25

Según la gravedad de la falta y de conformidad con la ley, la sanción puede consistir en:

- a. Amonestación confidencial
- b. Amonestación por escrito
- c. Suspensión hasta por dos años de los derechos y prerrogativas inherentes a los miembros del Colegio

BIBLIOGRAFIA GENERAL

AGUILAR CASTILLO, Gildardo, *Ética y Legislación Informática*, Universidad Veracruzana, p 1.

AGUILERA LÓPEZ Purificación, *Seguridad Informática*, Editex, 2010.

APIPILHUASCO RAMÍREZ José Antonio, *Derecho Internacional Privado*, Instituto de Investigaciones Jurídicas, UNAM, México, 2007.

CARRILO SALCEDO, Juan Antonio, *Curso de Derecho Internacional Público: Introducción a su estructura, Dinámica y Funciones*. Peruvian Book Central S.R.L. 1992. p. 103.

CORREA Carlos et al., *Derecho Informático*, cit. p. 286 y ss.

DEL PESO NAVARRO Emilio, *Peritajes Informáticos*, 2ª ed., Ediciones Díaz de Santos, España, 2001, p. 161.

DELPIAZZO Carlos E. et al. *Introducción a la informática jurídica y al Derecho Informático*, cit., p. 129.

FALCÓN Enrique M., *¿Qué es la informática jurídica?* Abeledo Perrot, Buenos Aires, 1992, p. 128 y ss.

FIX FIERRO, Héctor, *Informática y documentación jurídica*. p. 57 y 58.

FLORES SALGADO, Lucerito, *Derecho Informático*, Grupo Editorial Patria, 2009.

FROSINI, Vittorio, *Informática y derecho*, Colombia, Temis, 1998. p. 135.

GAMBA Jacopo, *Panorama del Derecho Informático en América Latina y el Caribe*, CEPAL, Chile, 2010, p.6.

GARZA DE FLORES María, *Ética*, Ed. Alhambra Mexicana, México, 1993.

GHERSI, Carlos Alberto, *Contratos civiles y comerciales*, 2ª, edición, Buenos Aires, Depalma, 1992, t II, p 306.

GÓMEZ ROBLEDO VERDUZO, Alonso, citado por CASTRILLÓN y LUNA, Víctor Manuel. *“La protección Constitucional de los Derechos Humanos”*, Ed. Porrúa, México, 2006. p. 100.

GUIBERT JM. *¿Qué es la ética de la informática?*, España, Universidad de Deusto, 1997.

HERNÁNDEZ CLAUDIO, *Hackers. Los piratas del Chip y de Internet*, España, 2001.

Instituto Nacional de Estadística e Informática (INEI), *Delitos Informáticos*. Colección Seguridad de la Información, Lima, 2001.

LANDA DURÁN, Graciela M., *Los delitos informáticos en el Derecho penal de México y España*, España, 2007.

LIMA DE LA LUZ, María, *Criminalia N° 1-6 año L. Delitos Electrónicos*. Ediciones Porrúa, México, 1984.

LÓPEZ MUÑIZ GOÑI, Miguel, *Informática jurídica documental*, Madrid, Díaz de Santos, 1984, pp.10 y ss.

LOSANO Mario G. *Corso di informatica giuridica*, Einaudi, Torino, 1986, vol. II, p. 16.

OMPI, *Reseñas de los Convenios, Tratados y Acuerdos administrados por la OMPI*, México, 2011.

MARTÍNEZ ALARCÓN, Benjamín, *La filosofía Hacking & Cracking*, Universidad Autónoma del Estado de Hidalgo, México, 2006.

NACIONALES UNIDAS. *Octavo Congreso de Las Naciones Unidas sobre prevención del delito y tratamiento del delincuente*. La Habana. 27 de agosto, 7 de septiembre de 1990 (a/conf 144/28/Rev.1) Nueva York, Naciones Unidas, 1991.

NÚÑEZ PONCE, Julio, *Derecho Informático*, Marsol, Perú, 1996. p. 22.

PÉREZ LUÑO, Antonio Enrique, *Manual de Informática y Derecho*, Ed. Ariel, Barcelona, 1996.

PEREZNIETO y CASTRO, Leonel, LEDESMA MONDRAGÓN, Abel, *Introducción al estudio del Derecho*, 2ª edición, Harla, p. 9.

RIOFRIO MARTÍNEZ VILLALVA, Juan Carlos, *La Prueba Electrónica*, Bogotá, Colombia, Temis, 2004.

RIOS ESTAVILLO, Juan José, *Derecho e Informática en México, Informática jurídica y derecho de la informática*, UNAM, México, 1997.

SALGADO FLORES, Lucerito. *Derecho Informático*. Grupo Editorial Patria, 2009.

TÉLLEZ, Julio, *Contratos Informáticos*, México, UNAM, 1989, p. 17.

TÉLLEZ, Julio, *Derecho Informático*, 2ª edición, México, McGraw-Hill, 1996.

TÉLLEZ VALDÉS, Julio, *Derecho Informático*, 3ª edición, México, McGraw-Hill, 2004.

UNICEF. *Protocolo Facultativo Convención sobre los Derechos de los Niños relativo a la Venta de Niños, Prostitución infantil y la utilización de Niños en Pornografía* Resolución A/RES/54/263 del 25 de Mayo de 2000.

VELÁZQUEZ ELIZARRARÁS Juan Carlos, *El estudio de caso en las relaciones jurídicas internacionales: modalidades de aplicación del derecho internacional*, UNAM, México, 2007, p. 301.

VILLORO TORANZO, Miguel, *Introducción al Estudio del Derecho*, México, Porrúa, 2000, p.4.

Revistas

ÁLVAREZ RICO, Manuel, *Informática y Derecho en España*, Revista Iberoamericana de Derecho Informático, No. 23-26, 1998.

CASSOU RUIZ, JORGE ESTEBAN, *Delitos informáticos en México*, Revista del Instituto de la Judicatura Federal Núm. 28, 2009, p.210.

GÓMEZ-ROBLEDO VERDUZCO, Alonso, *El derecho a la intimidad y el derecho a la libertad de expresión: derechos humanos fundamentales*, Ars Iuris, Revista del Instituto de Documentación e Investigación Jurídica de la Facultad de Derecho de la Universidad Panamericana, vol. 14, 1995, p 81.

GUERRERO M. MARÍA FERNANDA, *La inteligencia artificial aplicada al derecho*, Revista uno y cero, Milán, pp.10 y ss.

HAJNA Eduardo, *El Derecho Informático*, en Rev. Derecho de la Alta Tecnología, Buenos Aires, 1991, Año I, N°10, p. 8.

SUÑÉ, Emilio, "Introducción a la informática jurídica y al derecho de la Informática", Revista de la Facultad de Derecho de la Universidad Complutense, Informática y Derecho, Monográfico 12, Madrid, septiembre de 1986.

VIEGA RODRÍGUEZ, María José, *Delitos Informáticos*, REDI Revista Electrónica de Derecho Informático, Núm. 9, 1999.

Legislación

Código Civil Federal. Diario Oficial de la Federación, México, 26 de Mayo de 1928.

Código de Comercio. Diario Oficial de la Federación, México, 7 de Octubre de 1889.

Código de Defensa Social del Estado Libre y Soberano de Puebla, México, 24 de Septiembre de 1986.

Código Federal de Procedimientos Civiles. Diario Oficial de la Federación, México, 24 de Febrero de 1943.

Código Penal Federal. Diario Oficial de la Federación, México, 14 de Agosto de 1931.

Código Penal para el Estado de Baja California. Periódico Oficial No 23, México, 20 de Agosto de 1989.

Código Penal para el Estado de Baja California Sur. Boletín Oficial del Estado de Baja California Sur, México, 20 de Marzo de 2005.

Código Penal del Estado de Chihuahua. Congreso del Estado LX Legislatura, México, 4 de Marzo de 1987.

Código Penal para el Estado de Chiapas. Periódico Oficial del Estado número 97, México, 11 de Octubre de 1990.

Código Penal de Coahuila. Periódico Oficial, México, 28 de Mayo de 1999.

Código Penal para el Estado de Colima. Periódico Oficial "El Estado de Colima", México, 27 de Julio de 1985.

Código Penal para el Estado Libre y Soberano del Estado de Durango. Periódico Oficial del Gobierno del Estado, México, 1 de Abril de 2004.

Código Penal del Estado de México. Gaceta del Gobierno, México, 20 de Marzo de 2000.

Código Penal para el Estado de Michoacán. Periódico Oficial del Estado, México, 7 de Julio de 1980.

Código Penal para el Estado Libre y Soberano de Jalisco. Periódico Oficial del Estado de Jalisco, México, 2 de Septiembre de 1982.

Código Penal para el Estado Libre y Soberano de Oaxaca. Periódico Oficial del Estado de Oaxaca, México, 9 de Agosto de 1980.

Código Penal para el Estado Libre y Soberano de Puebla. Periódico Oficial, México, 22 de Diciembre de 1986.

Código Penal para el Estado Libre y Soberano del Estado de Quintana Roo. Periódico Oficial, México, 11 de Julio de 1979.

Código Penal para el Estado de Querétaro. Periódico Oficial de Gobierno del Estado, México, 10 de Julio de 1987.

Código Penal del Estado de San Luis Potosí. Edición Extraordinario del Periódico Oficial, México, 30 de Septiembre de 2000.

Código Penal para el Estado de Sinaloa. Periódico Oficial, México, 9 de Octubre de 1992.

Código Penal del Estado de Sonora. Boletín Oficial del Gobierno del Estado, México, 1 de Mayo de 1994.

Código de Procedimientos Penales para el Estado Libre y Soberano de Tlaxcala. Periódico Oficial del Gobierno del Estado, México, 21 de Diciembre de 1979.

Código Penal para el Estado de Tabasco. Periódico Oficial del Estado, México, 24 de Abril del 2003.

Código Penal de Tamaulipas. Periódico Oficial, México, 24 de Octubre de 1986.

Código Penal para el Estado Libre y Soberano del Estado de Veracruz de Ignacio de la Llave. Gaceta Oficial, México, 7 de Noviembre de 2003.

Código Penal del Estado de Yucatán. Diario Oficial del Gobierno del Estado, México, 30 de Marzo de 2000.

Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación, México, 5 de Febrero de 1917.

Ley Federal de Derechos de Autor. Diario Oficial de la Federación, México, 24 de Diciembre de 1996.

Ley Federal de Procedimiento Administrativo. Diario Oficial de la Federación, México, 4 de Agosto de 1994.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación, México, 5 de Julio de 2010.

Ley Federal de Protección al Consumidor. Diario Oficial de la Federación, México, 24 de Diciembre de 1992.

Ley Federal de Telecomunicaciones. Diario Oficial de la Federación, México, 7 de Junio de 1995.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Diario Oficial de la Federación, México, 11 de Junio de 2002.

Ley de la Propiedad Industrial. Diario Oficial de la Federación, México, 27 de Junio de 1991.

Ley de Sistemas de Pagos. Diario Oficial de la Federación, México, 12 de Diciembre de 2002.

Legislación Penal para el Estado de Aguascalientes. Periódico Oficial del Estado, México, 21 de Julio de 2003.

Páginas Web

24 HORAS, Piratería informática deja pérdidas de mil mdd en México: Microsoft. Consultado en Abril 27 de 2012 en:
<http://www.24-horas.mx/pirateria-informatica-deja-perdidas-de-mil-mdd-en-mexico-microsoft/>

Aceves Gutiérrez Luis Carlos, *Gobierno Electrónico en México: ¿Dónde estamos?* Consultado en Diciembre 16 del 2012 en:
<http://www.luiscarlosaceves.com/articuloconocimiento1.html>

Acurio del Pino Santiago, *Delitos Informáticos: Generalidades*, consultado en Marzo 18 del 2012 en:
http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Albizuri Begoña, *El Fraude y la Delincuencia Informática: Un Problema Jurídico y Ético*, Revista Digital Universitaria, Vol. 3 No. 2, México, 2002, consultado en Noviembre 20 del 2012 en:
<http://www.revista.unam.mx/vol.3/num2/art3/>

Alto Nivel, *Comercio electrónico en México crecerá 30% en 2012*. Consultado en Noviembre 23 del 2012 en:
<http://www.altonivel.com.mx/19629-comercio-electronico-en-mexico-crecera-30-en-2012.html>.

Alto Nivel, *Los 10 Hackers más famosos del mundo*, consultado en Abril 18 del 2012 en:
<http://www.altonivel.com.mx/los-10-hackers-mas-famosos-del-mundo.html>

AMIPCI & Televisa, *Hábitos de los Usuarios de Internet en México*, consultado en Diciembre 15 del 2012 en:
<http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=115&Type=1>.

Animal político, *Aumentan 14% usuarios mexicanos de internet en un año: INEGI*, consultado en Diciembre 13 del 2012 en:
<http://www.animalpolitico.com/2012/08/aumentan-14-usuarios-mexicanos-de-internet-en-un-ano-inegi/>.

Aprende en línea, *¿Qué es copyright?*, Programa Integración de Tecnologías a la Docencia, Universidad de Antioquia, consultado en Marzo 16 del 2012 en:
<http://aprendeonline.udea.edu.co/lms/moodle/mod/resource/view.php?inpopup=true&id=55823>

Arroyo Cortez L. y Farías Elinos M., *Importancia del marco jurídico en la función de auditoría Informática*, consultado en Diciembre 28 del 2012 en:
<http://seguridad.cudi.edu.mx/grponly/congresos/marcolegal.pdf>

Barroso Asenjo Porfirio, *Ética e Informática*, Computación aplicada a Contabilidad, Administración y Economía, consultado en Noviembre 25 del 2012 en:
<http://www.ccee.edu.uy/ensenian/catcomp/material/etica.pdf>

Bátiz-Álvarez V. y Farías-Elinos M. *Panorama General del Marco Jurídico en materia Informática en México*. Consultado en Noviembre 14 del 2012 en:
http://seguridad.cudi.edu.mx/congresos/2003/cldi/marco_juridico_info_mx.pdf

Bramont-Arias Torres Luis Alberto, *Delitos Informáticos*, Revista Peruana de Derecho de la Empresa No. 51, consultado en Marzo 5 del 2013 en
http://perso.unifr.ch/derechopenal/assets/files/obrasportales/op_20130408_02.pdf

Comercio Electrónico, Consultado en Noviembre 22 del 2012, en:
http://www.profeco.gob.mx/internacionales/com_elec.asp.

Comisión Especial de Acceso digital, *Informe de labores 2010-2012*, Cámara de Diputados, consultado en Abril 2, 2012 en:
http://archivos.diputados.gob.mx/Programas_anuales/informes/LXI/informe_final_acceso_digital_2012.pdf

CNN México, *Cuatro leyes polémicas que buscan regular internet*, consultado en Diciembre 14 del 2012 en:
<http://mexico.cnn.com/tecnologia/2012/01/24/cuatro-leyes-polemicas-que-buscan-regular-internet>

CNN México, *'Cyberbulling': la amenaza constante de la generación 'hiperconectada'*, consultado en Abril 25 del 2012 en:
<http://mexico.cnn.com/salud/2011/08/05/cyberbullying-la-amenaza-constante-de-la-generacion-hiperconectada>

CNN México, *Legisladores definen cuáles son los delitos informáticos y su castigo*. Consultado en Abril 18 del 2012 en:

<http://mexico.cnn.com/tecnologia/2012/03/29/legisladores-definen-cuales-son-los-delitos-informaticos-y-su-castigo>

CNN México, *Los usuarios de internet aumentan un 14% en México, según un estudio*, consultado en Diciembre 16 del 2012 en:

<http://mexico.cnn.com/tecnologia/2012/05/17/los-usuarios-de-internet-aumentan-un-14-en-mexico-segun-un-estudio>.

Crónica, *"Hackers" caen tras defraudar a tres empresas*, consultado en Abril 21 del 2012 en:

<http://www.cronica.com.mx/notas/2007/289573.html>

De Sola Quintero René, *Delitos Informáticos*, consultado en abril 5 del 2012 en:

http://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

DISC P.F.P., *Unidad de Policía Cibernética y Delitos Contra Menores*. Consultado en Noviembre 15 del 2012 en:

http://www.disc.unam.mx/2005/presentaciones/delitos_menores.pdf

DIARIO TI, *Delitos Informáticos causan pérdidas millonarias en bancos y empresas*. Consultado en Abril, 2, 2012 en:

http://www.diarioti.com/noticia/Delitos_informaticos_causan_perdidas_millonarias_en_bancos_y_empresas/31409

El espectro radioeléctrico. Consultado en Mayo 23, 2012 en:

<http://www.vidadigitalradio.com/el-espectro-radioelectrico/>

El Universal, *Hackers, genios que se desligan del hampa*, consultado en Abril 21 del 2012 en:

<http://www.eluniversal.com.mx/sociedad/5701.html>

El Universal, *Rezagos en la tipificación y persecución de delitos informáticos*, Consultado en Marzo 20 del 2013 en:

<http://www.eluniversal.com.mx/cultura/69843.html>

Estrategia programática, Secretaría de Economía, consultado en Diciembre 26 del 2012 en:

http://www.apartados.hacienda.gob.mx/contabilidad/documentos/informe_avances/2002/temas/banco/g10t01.pdf

Excelsior, *Narcos mexicanos secuestran y esclavizan a hackers*, consultado en:

Abril 12 del 2012 en <http://www.excelsior.com.mx/2011/07/04/global/749995>

Funes Grimaldo, María de Lourdes, *Qué es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*. Consultado en Julio 18 del 2012 en:

<http://fox.presidencia.gob.mx/cambio/transparencia/?contenido=19482&pagina=1>

Geraldes Da Cunha Lopes, Teresa M., *El estado del arte del Derecho de Protección de Datos Personales en México*, Centro de Investigaciones Jurídicas y Sociales/Universidad Michoacana de San Nicolás de Hidalgo, consultado en Diciembre 15 del 2012 en:
http://www.egov.ufsc.br/portal/sites/default/files/el_estado_del_arte_del_derecho_de_proteccion_de_datos_personales_en_mexico.pdf

Gleason Santana Arturo, *El Marco Jurídico de la Informática y la Piratería*, consultado en Diciembre 15 del 2012 en:
http://www.debate.iteso.mx/numero09/Articulos_9/MARCOJURIDICO.htm

Grupo Fórmula México, *segundo lugar en pornografía infantil a nivel mundial*. Consultado en Noviembre 3, 2012 en:
<http://www.radioformula.com.mx/notas.asp?Idn=221857>

Hernández Claudio, *Hackers: Los Clanes de la RED 2000*, consultado en Abril 19 del 2012 en:
<http://ucapanama.org/wp-content/uploads/2011/12/Hackers-1-Claudio-Hernandez.pdf>

Informática jurídica.com, *Legislación de Derecho Informático*, consultado en Marzo 20 del 2013, en:
<http://www.informatica-juridica.com/legislacion/mexico.asp>

INEGI, *Usuarios de Internet en México*, consultado en Marzo 20 del 2013 en:
<http://www.inegi.gob.mx/est/contenidos/espanol/temas/Sociodem/notatinf212.asp>

Instituto de Investigaciones Jurídicas, *Presentación*, consultado en Diciembre 23 del 2012 en:
<http://www.juridicas.unam.mx/infjur/leg/presenta.htm>

Instituto Federal de Acceso a la Información y Protección de Datos, Consultado en Julio 19 del 2012 en:
<http://www.ifai.org.mx>

Instituto Mexicano de la Propiedad Industrial. Consultado en Agosto 17 del 2012 en:
http://www.impi.gob.mx/wb/IMPI/quienes_somos

Izquierdo Enciso León, *La implementación de la Firma Electrónica en México*. Consultado en Noviembre 17 del 2012 en:
<http://www.economia.unam.mx/publicaciones/econinforma/369/08leonizquierdo.pdf>

La Jornada, *En un año creció 14% el número de mexicanos que usan Internet*, consultado en Abril 21 del 2012 en:

<http://www.jornada.unam.mx/2011/05/18/index.php?section=sociedad&article=043n1soc>

Los Tiempos, *¿Qué es la Ley SOPA y cómo afecta a Latinoamérica?* Consultado en Abril 27 del 2012 en:

http://www.lostiempos.com/diario/actualidad/vida-y-futuro/20120119/que-es-la-ley-sopa-y-como-afecta-a-latinoamerica_157237_327978.html

Montalvo Romero, María Teresa, *El marco jurídico de la propiedad intelectual en México*, consultado en Marzo 21 del 2012 en:

<http://www.letrasjuridicas.com/Volumenes/15/tmontalvo15.pdf>

Olmos Jasso, María Teresa, *Valor Probatorio de los Documentos Electrónicos*, 2009, consultado en Diciembre 17 del 2012 en:

<http://www.tfjfa.gob.mx/investigaciones/pdf/valorprobatoriodelosmedios electronicos.pdf>

OMPI, *Cómo proteger sus invenciones en otros países: preguntas frecuentes sobre el tratado de cooperación en materia de patentes (PCT)*, consultado en Marzo 21 del 2012 en:

http://www.wipo.int/export/sites/www/freepublications/es/patents/433/wipo_public_433.pdf

OMPI, *Convenio que establece la Organización Mundial de la Propiedad Intelectual*, consultado en Marzo 20 del 2012 en:

http://www.wipo.int/treaties/es/convention/trtdocs_wo029.html#P38_1300

Organización Mundial del Comercio, *¿Qué se entiende por ADPIC?*, consultado en Marzo 15 del 2012 en:

http://www.wto.org/spanish/tratop_s/trips_s/intel1_s.htm

Portal del Consumidor, *Decálogo de los derechos mínimos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos*, consultado en Diciembre 22 del 2012 en:

<http://www.consumidor.gob.mx/wordpress/?p=11743>

Portal de Obligaciones de Transparencia. Consultado en Julio 19 del 2012 en: <http://portaltransparencia.gob.mx>

PROFECO, *Ley Federal de Protección al Consumidor*. Consultado en Agosto 4 del 2012 en:

http://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_camDip.pdf

Proceso, *Diputados tipifican delitos cibernéticos como el “ciberfraude”* consultado en Abril 2 del 2012 en:

<http://www.proceso.com.mx/?p=302516>

Protección de Datos Personales. Consultado en Agosto 7 del 2012 en: <http://www.protecciondedatospersonales.org/sujetos-obligados/>

Protección de datos y privacidad, *Reforma Constitucional para Reconocer el Derecho Habeas Data en México*. Consultado en Mayo 5 del 2012 en: <http://www.protecciondedatos.org.mx/2009/06/reforma-constitucional-para-reconocer-el-derecho-habeas-data-en-mexico/>

¿Qué es el IFAI? Consultado en Mayo 5, 2012 en: <http://www.ifai.org.mx/QuienesSomos>

Razón y Palabra, *Las cifras de la industria de Internet en México, 2004*, consultado en Diciembre 6 del 2012 en: <http://www.razonypalabra.org.mx/anteriores/n43/oislas.html>.

Secretaría de la Función Pública, *¿Qué es y para qué sirve la Firma Electrónica Avanzada?*, consultado en Diciembre 17 del 2012 en: <http://www.funcionpublica.gob.mx/index.php/temas/declaracion-de-modificacion-patrimonial.html>

Servicio de Administración Tributaria, Consultado en Mayo 19 del 2012 en: http://www.sat.gob.mx/6_630.html

Sistema de Pagos Electrónicos Interbancarios. Consultado en Agosto 4 del 2012 en: <http://www.banxico.org.mx/sistemas-de-pago/servicios/sistema-de-pagos-electronicos-interbancarios-spei/sistema-pagos-electronicos-in.html>

Sosa Carabeo Marcel, *Problemas éticos y de seguridad asociados al uso de las tecnologías*, consultado en Noviembre 26 del 2012 en: <http://bvs.sld.cu/revistas/infid/n909/infid130910.htm>

Standler, Ronald B., *Computer Crime*, 2002, Consultado en Abril 19 del 2012 en: <http://www.rbs2.com/ccrime.htm>

Unidades de Enlace. Consultado en Julio 19 del 2012 en: <http://www.ifai.org.mx/Gobierno/#unidadesEnlace>

UNINET DERIN, *Tendencias actuales de la Informática y el Derecho a Nivel Internacional*. Consultado en Noviembre 30 del 2012 en: <http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=36>

VSantivirus, *Cae pirata que atacó web de la presidencia de México*, consultado en Abril 12 del 2012 en: <http://www.vsantivirus.com/28-11-03.htm>