UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

FACULTAD DE DERECHO Y CIENCIAS SOCIALES
DIVISIÓN DE ESTUDIOS SUPERIORES DE POSGRADO

MAESTRÍA EN DERECHO
CON ACREDITACIÓN PNPC (002478)

PENALIZACIÓN DE LOS DELITOS INFORMATICOS

T E S I S

PARA OBTENER EL GRADO DE
MAESTRO EN DERECHO

PRESENTA

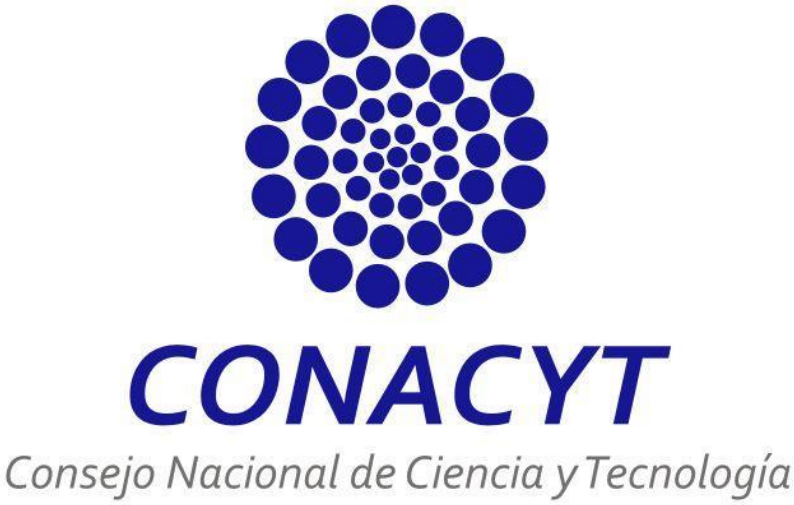
LIC. OSCAR MANUEL VENCES SANCHEZ

DIRECTOR DE TESIS

DR. DANIEL MONTERO ZENDEJAS

CUERNAVACA, MORELOS DICIEMBRE 2019

RECONOCIMIENTO



ESTA TESIS FUE REALIZADA POR BECARIO NACIONAL CONACYT EN EL PROGRAMA EDUCATIVO DE MAESTRÍA EN DERECHO PNPC (002478)

GRACIAS A MIS PADRES QUE ME DIERON TODO

GRACIAS A MI FAMILIA QUE ME IMPULSA A SER MEJOR CADA DIA

“PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS”

INDICE

CAPÍTULO PRIMERO

MARCO TEÓRICO DE LOS DELITOS INFORMÁTICOS

1 Introducción 7

1.1. Elementos Metodológicos 10

1.2. Concepto de Informática 11

1.2.1. Concepto de Cibernética 12

1.2.2. Diferencia Entre Informática y Cibernética 13

1.3. Informática Jurídica 15

1.3.1. Derecho Informático 16

1.3.2. Naturaleza Jurídica 18

1.4. Teoría del Delito 19

1.4.1. Nociones Generales del Delito 23

1.4.2. Delitos Informáticos en General 24

1.4.3. Características de los Delitos Informáticos 27

1.4.4. Clasificación de los Delitos Informáticos 29

1.4.5. Sujetos de los Delitos Informáticos 35

A) Sujeto Activo 36

B) Sujeto Pasivo 38

1.5. Tipos de Delitos Informáticos 38

1.6. Daños o Modificaciones de Programas o Datos Computarizados 43

1.7. Características Especiales que Dificultan

la Tipificación de los Delitos Informáticos. 48

CAPÍTULO SEGUNDO

EVOLUCIÓN HISTORICA DEL INTERNET EN RELACION CON LOS DELITOS INFORMATICOS

Internet
Sociedad de la información

2.1. Antecedentes de la Informática 52
2.1.1. Evolución de la Computadora 59
2.2. Antecedentes de la Cibernética 66
2.3. Internet 69
2.3.1. Antecedentes Del Internet 71
2.3.2. Antecedentes Del Internet En México 73
2.3.3. Antecedentes del Derecho a la Información 77
2.4.1. Sociedad de la Información 78
2.4.2. Seguridad, Derecho a la Intimidad y Propiedad Intelectual 81
2.5.1. Antecedentes De Los Delitos Informáticos 82
2.6.1. Los Diez Grandes Hackers de la Historia 83
2.6.1. Estados Unidos 87
2.6.2. Alemania 87
2.6.3. Francia 88
2.6.4. España 89
2.6.5. Austria 89
2.6.6. Gran Bretaña 90
2.6.7. Holanda 90

CAPÍTULO TERCERO

ANALISIS DE LA LEGISLACION EN MATERIA DE DELITOS INFORMATICOS

3.1 Tratamiento del Problema en el Ámbito Internacional 93
3.2 En la Organización de las Naciones Unidas 94
3.3 En la Comisión de las Comunidades Europeas 95
3.4 Convenio Sobre la Ciber-Criminalidad 96
3.4.1. Marco Normativo de España 107
3.5 La Criminalística Informática 114
3.5.1. La Criminalística 115
3.5.2. Principios de la Criminalística. 117
3.6. La Unidad de Policía Cibernética 119
3.6. 1. De la Policía Federal Preventiva en México 120
3.6. 2. Policías Internacionales 123
3.6. 3.Oficina Europea de Policía 125
3.6. 4.El Buró Federal de Investigaciones (FBI) 129
3.7.procuración de justicia en México en relación a los Delitos Informáticos 130

CAPÍTULO CUARTO

ESTUDIO Y ANALISIS DE LA LEGISLACION EN MATERIA DE DELITOS INFORMATICOS EN MEXICO

4.1. Delitos Informáticos en el derecho positivo Mexicano 135
4.2. Constitución Política de los Estados Unidos Mexicanos 136
4.3. Código Penal Federal 137
4.4. Ley Federal de Telecomunicaciones 140
4.5. Código de Comercio 141
4.6. Ley Federal de Derechos de Autor 143
4.7. Ley de Propiedad Industrial 147
4.8. Ley de Instituciones de Crédito 148
4.9. Ley Federal de Juegos y Sorteos 155
4.10. Ley de seguridad Nacional 155
4.11. Ley Federal Contra Delincuencia Organizada 157
4.12. Legislaciones Locales 159
4.12.1. Código Penal Para el Estado de Morelos 159
4.12.2. Código Penal Para el Estado de Sinaloa 159
4.12.3. Código Penal Para el Distrito Federal 160
4.12.4. Código Penal Para el Estado de Veracruz 161

PROPUESTAS 162
BIBLIOGRAFIA **163**

INTRODUCCIÓN

Como hemos podido apreciar en nuestro acontecer diario, las nuevas tecnologías nos han facilitado la vida y nos han ayudado de manera eficaz en diversas áreas como lo son la economía, la política, la organización del trabajo, en la rama industrial, entre otros. Facilitándonos desde el aprendizaje hasta el funcionamiento de los mecanismos más complejos, pero de igual forma la aparición de las nuevas tecnologías trae consigo nuevos retos, para la regulación de las conductas que se realizan por medio de un ordenador, las cuales pueden afectar a terceros, los cuales deben ser protegidos a través de organismos que regulen dichas conductas antijurídicas.

Si bien es cierto que algunas conductas realizadas a través de un ordenador ya han sido exteriorizadas sin necesidad de él, y dichas conductas se encontraban tipificadas como delitos en la norma penal, es de igual forma importante regular dichas conductas en el ciber espacio, las cuales no se encuentran tipificadas en ningún ordenamiento legal, y ante la falta de regulación, existe la impunidad para aquellas personas que se conducen en ese sentido tanto a nivel nacional como internacional.

En la actualidad existen diversas actividades ilícitas que se realizan por medio de la informática dentro de las cuales podemos señalar: fraudes, intrusiones, actividades delictivas dedicadas al robo, fraude electrónico, robo de tarjetas e información personal, lenocinio, tráfico y corrupción de menores, prostitución infantil, narcotráfico, elaboración, distribución y promoción de pornografía infantil, ciber terrorismo, extorsión e infinidad de delitos que tienen su origen en cualquier instrumento de comunicaciones y actividades informáticas.

En relación a esto, los sistemas informáticos logran potencializar las posibilidades de las distintas modalidades delictivas, ya que con la ayuda de dichas herramientas tecnológicas, la posibilidad de determinar y castigar a aquella persona que transgreda las normas jurídicas establecidas, es cada vez más difícil, esto a consecuencias de la extraterritorialidad.

Es por ello que debemos tomar en cuenta que el internet y las nuevas tecnologías se han vuelto el medio a través del cual las diversas células criminales realizan sus operaciones, las cuales se encuentran tipificadas en diversas legislaciones, como lo son: el fraude, violación a la intimidad, violación a los derechos de autor, pornografía, terrorismo, y de manera secundaria: inducción al suicidio, robo, entre otras figuras, que nuestro derecho positivo parece no saber cómo resolver.

Por consecuencia en la actualidad existen diversas actividades ilícitas que se realizan por medio de la informática y es por ello la necesidad de regular dichas conductas delictivas a través de los mecanismos coercitivos con los que cuenta el estado. A lo cual es importante tomar en cuenta y no pasar por alto distintos marcos referenciales como los son: la libertad, los medios de comunicación el internet y los avances tecnológicos.

Una de las finalidades del derecho penal y en consecuencia del mismo estado de derecho, es la protección de todos los bienes jurídicos tutelados por la ley, preservando además el orden y la paz pública. Bajo estas condiciones, en los delitos informáticos existe una gran cantidad de bienes jurídicos que no se tutelan por la legislación punitiva de nuestra entidad, razón por la cual se justifica la necesidad de integrar los tipos penales bajo los parámetros de raciocinio, ponderación y argumentación que tiendan a definir aquellas conductas típicas que se generan por los usuarios de la red.

Es por ello que en la presente investigación existe la necesidad de profundizar tanto en las teorías del delito como de la pena para determinar si estas pueden influir en Código punitiva Nacional, con la finalidad de que los tipos penales relacionados con los delitos informáticos puedan ser incorporados a dicha codificación local, bajo los parámetro que anteriormente se han mencionado, como son el de la razonabilidad, la ponderación, la argumentación y todos aquellos principios reguladores del derecho penal contenidos tanto en tratados internacionales como en la constitución y en la misma doctrina jurídica contemporánea.

CAPÍTULO PRIMERO

MARCO TEÓRICO DE LOS DELITOS INFORMÁTICOS

ELEMENTOS METODÓLOGICOS

En el presente proyecto de investigación es importante tomar en cuenta los diversos tipos de estudio en donde predominara el estudio histórico, confirmatorio, ya que posee una aproximación basada en el marco teórico y en los resultados. Los elementos de aplicación son: el deductivo, histórico, comparativo, didáctico y el estadístico entre otros.

La metodología consiste en la recopilación de datos en este caso internet, libros, revistas, la aplicación de entrevistas, publicaciones, la concentración y análisis de los datos, se elaboraran resultados de la investigación, conclusiones y sugerencias alternativas a la problemática presentada utilizando como base distintos tipos de métodos, mismos que a continuación analizaremos brevemente:

1) Método empírico-analítico.- Conocimiento autocorrectivo y progresivo aplicable a la solución de planteamientos en las ciencias naturales y/o sociales.
2) Método histórico.- Vinculado al conocimiento de las distintas etapas de los objetos en su sucesión cronológica, para conocer la evolución y desarrollo del objeto o fenómeno de investigación se hace necesario revelar su historia, las etapas principales de su desenvolvimiento y las conexiones intrínsecas fundamentales.

3) Método sistemático.- Dirigido a modelar el objeto mediante la determinación de sus componentes asi como la relación entre ellos.

4) Método sintético.- Relaciona hechos aparentemente aislados y formula una teoría que unifica los diversos elementos, (este se presenta mas en el planteamiento de la hipótesis).

5) Método lógico.- es una gran rama del método científico, aun que es más clásica y de menor fiabilidad.

6) Método lógico deductivo.- se aplican los principios descubiertos a casos particulares a partir de un enlace de juicios.

7) Método lógico inductivo.- Es el razonamiento que partiendo de casos particulares se eleva a conocimientos generales.[1]

Una vez analizado lo anterior es importante señalar que en la presente investigación se tomara en consideración las diversas disciplinas, gobiernos, actores económicos y sociales, para conceptualizar de una manera atinada las diversas conductas atípicas en las que nos encontramos inmersos, la cual es de un crecimiento masivo de los medios de informática, a nivel mundial, por lo que dichas conductas delictivas han retomado mayor fuerza, para lo cual es necesaria un regulación de las mismas de manera urgente.

CONCEPTO DE INFORMÁTICA.

Es una ciencia que trata y automática o automatizada a la información. Estudia los procesos que se ejercen sobre datos e información como: generación, obtención, registro, depuración, concentración, filtrado, ordenamiento, integración, calculo, acceso, recuperación, visualización,

[1] Lira Arteaga, Oscar Manuel *Cibercriminalidad*, Instituto Nacional de Ciencias Penales, 1ª edición México, 2010. p.54.

interpretación, análisis, difusión y como fin de la informática encontramos la elaboración de métodos y medios óptimos para representación, recopilación, elaboración analítica-sintética, memorización, búsqueda y difusión de informaciones científicas.[2]

Ahora bien, es importante analizar de donde surge dicho concepto y la manera en que se encuentra inmersa en las diversas áreas del conocimiento.

La informática, surge como uno de los fenómenos más significativos de los últimos tiempos, ha influido prácticamente en todas las áreas del conocimiento humano dentro de las cuales el derecho no puede ser la excepción, dando lugar, en términos instrumentales a la informática jurídica.

La relación de la informática y el derecho es percibida desde los primeros tiempos de la computación, es por ello que los diversos avances tecnológicos traen consigo modificaciones jurídicas, lo que da lugar a la transformación de las organizaciones sociales y políticas de un país. Por lo tanto, el aspecto informático no puede quedar sin un control legal, por lo que la informática debe tener un marco legal que la regule y el derecho debe tener un respaldo en el procesamiento de datos que proporciona.

CONCEPTO DE CIBERNÉTICA

Es la ciencia de la comunicación y el control entre el hombre y la maquina, los aspectos aplicados de esta disciplina están relacionados con cualquier campo de estudio y sus aspectos formales estudian una teoría general de control, la cual tiene aplicación en diversos campos.[3]Estudiando y aprovechando todos sus aspectos y mecanismos comunes, la cibernética

[2] Flores Salgado, Lucerito, *Derecho Informático,* ed. Patria, 2009 p. 53.
[3] Téllez Valdés, Julio, *Derecho Informático,* Ed. Mc Graw Hill, 1996, p. 3.

puede derivar en la robotica,[4] la cual se encarga de crear mecanismos de control, los cuales funcionen en forma automática, que buscan simular la actividad humana.

Robert Wiener la define como el estudio analítico del isomorfismo de la estructura de las comunicaciones en los mecanismos organismos y sociedades; entendiéndose como isomorfismo una identidad entre dos sistemas, que para que exista se requiere de determinadas relaciones entre los objetos del otro.[5]

El sentido moderno del vocablo cibernética radica en el énfasis especial que pone sobre el estudio de las comunicaciones mensajes y la forma como se encuentran regulados internamente todos los sistemas de comunicación ya sean biológicos, sociales o, sino sobre las maquinas que imitan procesos de regulación u ordenación o búsqueda de objetivos.

DIFERENCIA ENTRE INFORMÁTICA Y CIBERNÉTICA

Es indispensable destacar la diferencia entre cibernética e informática; aunque ambas tratan la información en matemática, lógica y analítica existen diversas diferencias:

La cibernética, en sus aspectos más generales, trata del empleo de métodos científicos para explicar fenómenos en la naturaleza o en la

[4] La robótica es la técnica que aplica la información al diseño y empleo de aparatos que, en sustitución de personas, realizan operaciones o trabajos, por lo general en instalaciones industriales. Se emplean en tareas peligrosas o para labores que requieren una manipulación rápida y exacta. En los últimos años con los avances de la inteligencia artificial se han desarrollado sistemas que desarrollan tareas que requieren decisiones y auto programación y se han incorporado sensores de visión y tacto artificial.

[5] Livas, Javier, *Cibernética, Estado y Derecho*, Mexico, Gernika, 1988. p. 48.

sociedad y la forma de representación del comportamiento humano de forma matemática en una máquina.

- La informática parte del estudio de las computadoras, de sus principios básicos y de su utilización. Comprende materias tales como programación; estructura de la información; ingeniería del software; lenguajes de programación; hardware; arquitectura de las computadoras, entre otras.
- La cibernética, entre otros aspectos, trata de la creación de instrumentos informáticos que simulen actividades del hombre, por ejemplo, robots; desarrollo de la inteligencia artificial; utilización de métodos heurísticos; entre otros.
- La informática es un instrumento de apoyo para el desarrollo de la propia cibernética.
- La cibernética implica en esencia un sistema en el cual puede o no existir la relación entre las partes (isomorfismo).
- La informática, por su parte, implica también un sistema en el que siempre habrá relación entre las partes que lo integran.[6]

Sobre este particular y respecto a la diferenciación entre cibernética e informática, Fix Fierro ha señalado que:

La informática, como tal, ha sido comúnmente considerada como una ciencia particular integrada a la cibernética. Aunque esta opinión parece en sí misma lógica y evidente, existen sin embargo diferencias de objeto y finalidad entre ambas disciplinas. En efecto, la cibernética se ocupa de los fenómenos de control y comunicación, lo cual puede traducirse en el diseño y construcción de máquinas, y más recientemente, desemboca en los problemas de la llamada. “Inteligencia artificial”. La informática, por su parte, si bien hace uso

[6] Ríos Estavillo, Juan José, *Derecho e informática en México,* Instituto de Investigaciones Jurídicas, Serie E: varios, numero 83, Universidad Nacional Autónoma de México, México, 1997, p. 38.

de las tecnologías desarrolladas con auxilio de la cibernética, se centra en cuestiones de tratamiento, representación y manejo automático de la información.[7]

Ante esto se ha considerado que el término. “informática”, concepto acuñado por Philipe Dreyfus mediante la contracción de información y automática, es la ciencia del tratamiento automático o automatizado de la información, primordialmente mediante las computadoras.

INFORMÁTICA JURÍDICA

A pesar de que la informática jurídica tuvo su origen desde hace muchos años, el pretender dar una definición de esta disciplina como otras de reciente surgimiento no resulta nada fácil, sin embargo, en términos generales podríamos decir que la informática jurídica “se refiere a la utilización de las computadoras en el ámbito jurídico, o bien a la aplicación de la informática (entendiendo a esta como la ciencia del tratamiento lógico y automático de la información) en el ámbito del derecho”.[8]

La informática jurídica tiene por objeto la aplicación de la tecnología de la información al derecho. Para Julio Téllez la informática jurídica es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática en general, aplicables a la recuperación jurídica así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesaria para lograr dicha recuperación.[9]

---

[7] Fix Fierro, Héctor, *Informática y documentación jurídica*, México, UNAM, Facultad de Derecho, 1990, pp. 44 y 45.

[8]

[9] Op. cit. Téllez Valdés, Julio, p. 19.

Enrique Cáseres establece que es la disciplina que estriba en reconocer las propiedades necesarias y suficientes, así determinar los tipos de coordinación en conocimiento que se da entre la informática y el derecho.

Antonio Rivero señala que no es sino la informática considerada como sujeto del derecho, es decir, como instrumento puesto al servicio de la ciencia jurídica.

Emilio Suñé establece que es la aplicación de los ordenadores electrónicos orientada a la resolución de los problemas jurídicos.[10]

DERECHO INFORMÁTICO

Si bien es cierto que los precursores informáticos nunca imaginaron los alcances que llegarían a tener las computadoras en general o aun en campos tan aparentemente fuera de influencia como el jurídico, todavía más difícil hubiera sido concebir que el derecho llegara a regular a la informática.

Pese a lo anterior la informática ha planteado al derecho problemas nuevos, que los juristas y legisladores se esfuerzan para resolver jurídicamente. Así la respuesta del derecho a esos planteamientos suele recibir el nombre de derecho de la informática (también denominado derecho informático).

Diversos autores consideran que el derecho de la informática es una categoría propia que obedece sus reglas, y que surge como una inevitable respuesta social al fenómeno informático, y que por lo tanto, es un derecho en el que su existencia prevalece dentro de su esencia.

[10] Op. cit. Flores Salgado, Lucerito, p. 64

Derivado de lo anterior el derecho de la informática se define como el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.[11]

Por lo que es importante mencionar que el derecho de la informática no es lo mismo que informática jurídica, ya que la informática jurídica constituye una ciencia que forma parte del ámbito informático, demostrando de esta manera que la informática ha penetrado en infinidad de sistemas y ámbitos, prueba de ello es que ha penetrado en el campo jurídico para servirle de ayuda y como fuente.

Es por ello que la informática jurídica puede ser considerada como fuente del derecho ya que es una ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el derecho.

A lo cual diversos autores han señalado que la informática como objeto de regulación jurídica ha dado origen al llamado derecho de la informática.

El derecho informático o derecho de la informática es el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática.[12]

Juan José Estavillo lo define al Derecho Informático como el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la

[11]Op. cit. Téllez Valdés, Julio, p. 21.
[12] Pérez Luño, Antonio Enrique, *Ensayos de Informática Juridica*, ed. Coyoacan, 2009, p. 12

informática o de los problemas que se derivan de la misma, con las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas.[13]

El derecho informático se integra con el conjunto de normas jurídicas que regulan la creación y las diversas aplicaciones de la informática y sus derivados así como teorías, doctrinas y jurisprudencias aplicables.

NATURALEZA JURÍDICA

El derecho informático, surge como una nueva rama del Derecho, como consecuencia de las siguientes consideraciones de que se requiere una regularización de los bienes informacionales, porque la información como producto informático requiere de un tratamiento jurídico en función de su innegable carácter económico; es necesaria la protección de datos personales. Debido al atentado sufrido a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas; el flujo de datos transfronterizos. Sobre el favorecimiento de restricción en la circulación de datos a través de fronteras nacionales; la protección de programas. Como solución a los problemas mas provocados por la llama piratería o pillaje de programas de cómputo; los delitos informáticos en sentido amplio. Así como la comisión de verdaderos actos ilícitos en los que se tenga en la computadora un instrumento o fin.[14]

Ante el avance tecnológico y los usos tan diversos en el manejo de la información, tanto entes públicos como privados se han visto en la necesidad de modificar sus medios de archivar la información recopilada, para lo cual han recurrido a las computadoras. Por lo tanto resulta necesario vislumbrar este fenómeno, como una posible inmiscusión en la esfera privada o intima

[13] Op. cit. Rios Estavillo, Juan José, p. 6
[14] López Betancourt, Eduardo, *Delitos en particular*, México, Porrúa, 2004, p. 271.

de las personas y del propio estado, siendo necesario establecer si el derecho, particularmente el penal debe determinar estos alcances.

LA TEORÍA DEL DELITO

Para abordar la teoría del delito es importante es importante abordar la definición del mismo, del cual la palabra delito deriva del verbo latino *delinquiere,* que significa abandonar apartarse del buen camino, alejarse del sendero señalado por la ley.[15]

A lo cual Daniel Montero[16] Señala que: Determinar la existencia de un delito, es decir, establecer que un determinado hecho constituye una infracción punible es un proceso axiológico, basado en un estudio normativo que metodológicamente se realiza a través de un análisis y síntesis.

Dicho estudio se realiza mediante la teoría del delito, un sistema por niveles, conformado por el estudio de los presupuestos jurídico- penales de carácter general que deben concurrir para establecer la existencia de un delito.

Esta teoría no se ocupa de los elementos o requisitos específicos de un delito en particular (homicidio, robo, violación, etc.), si no de los elementos y condiciones básicas y comunes a todos los delitos.

En consecuencia se puede afirmar que los elementos esenciales del delito son: la conducta, tipicidad, antijuricidad, culpabilidad y por último la imputabilidad. Los cuales son necesarios la clasificación de los delitos,

---

[15] Fernando Castellanos, Lineamientos Elementales del Derecho penal 39ª Ed. México, Ed. Porrúa,1998, p.125.

[16] Montero Zendejas, Daniel, *Derecho Penal y Crimen Organizado*: Crisis de la Seguridad, 1ª Ed. México, Ed. Porrúa,2008, p.13.

mismos que pueden ser realizados a través de un ordenador y producir sus efectos a kilómetros de distancia, gracias a la ayuda de la tecnología.

De igual forma es necesario atender al presupuesto del delito, es decir las circunstancias previas al delito que deben existir, los cuales son: generales y especiales, el primero de ellos son los que deben existir para la configuración de un delito, de lo contrario no se podría clasificar como delito, los cuales son: sujeto activo, sujeto pasivo y el bien jurídico tutelado y los específicos son las condicionantes de un delito en específico que ante la falta de él no se da dicha figura.

La creación de tipos delictivos no puede considerarse como una actividad sometida al capricho temporal de la sociedad. Por lo que es necesario realizar un minucioso estudio en cuanto a la creación e interpretación de la ley Penal para arribar a la conclusión de que la ley penal no debe ser y menos en casos como éste, tan relativa para fragmentarse. Sin pretender una ley perfecta creo necesario que se debe aspirar a la creación de leyes eficaces en todo el territorio mexicano.

El derecho penal es una rama del Derecho Público, no por emanar del Estado las normas en donde se establecen los delitos y las penas, ni tampoco por corresponder su imposición a los órganos estatales, pues, como se ha expresado, todo derecho positivo emerge del Estado y por éste se impone, sino porque al cometerse un delito, la relación se forma entre el delincuente y el estado como soberano y no entre aquel y el particular ofendido.

Es por ello que al ser un órgano regulador de la sociedad, recae en él, la obligación de garantizar a la sociedad misma, la seguridad jurídica a través de las leyes e instituciones a su cargo encargadas mantener esa estabilidad para alcanzar los fines establecidos en las mismas.

La ciencia del derecho penal es esencialmente normativa; su objeto lo constituye, de modo esencial, el estudio del Derecho Penal en forma ordenada, sistemática y racional; pero al lado de ella existen otras ciencias diversas en sus objetos y métodos; se trata de disciplinas causales explicativas conocidas con el nombre genérico de *Ciencias Penales;* no intentan guiar la conducta humana, sino explicar causas estudiar el nexo entre el delito y los factores que influyen en su producción.[17]

Es por esto que en la presente investigación se tomara en cuenta la corriente de la "Escuela positiva", ya que como bien se pretende demostrar, la sociedad necesita de normas establecidas mediante las cuales el estado provea de seguridad a una determinada población en específico a través de normas específicas.

Ignacio Villalobos en su libro "Derecho Penal Mexicano" señala que la Antropología, la Sociología, y la criminología son ciencias naturales cuyo fin es desentrañar la naturaleza de la conducta humana, escudriñar sus orígenes y fijar su mecanismo de producción; son ciencias naturales y deben de tener como método preponderante la inducción. El Derecho Penal, en cambio que trata de fijar un cauce a esa conducta y de imponerle una forma y limites determinados, se refiere al mismo objeto, pero se diferencia precisamente por su carácter eminentemente práctico, por su fin normativo.[18]

Atendiendo a lo anterior y como bien lo señalan diversos autores se puede considerar a la "escuela positiva" como una de las bases para la presente investigación ya que lo que se pretende en la misma es la creación de un cuerpo normativo en el cual se regule la conducta de los individuos a

[17] Op. cit. Fernando Castellanos, p.18.

[18] Ibidem, p.64.

través del positivismo especificando las sanciones a las cuales de harán acreedores aquellos que no cumplan la misma.

Respecto a lo anterior, no podemos dejar de mencionar a los a los principales exponente de dicha corriente, entre los que destacan: Cesar Lombroso, Enrique Ferri y Rafael Garofalo, a los cuales el profesor Ignacion Villalobos estudio y afirmo que "el delito es la violación de los sentimientos de piedad y probidad poseídos por una población en la medida que es indispensable para la adaptación de un individuo en sociedad.

La naturaleza de la norma penal se crea y se interpreta, por lo que un tipo penal es creado con el fin de servir a la sociedad. La creación de nuevos tipos delictivos nos obliga a estudiar el problema criminal que deberá enfrentarse con los nuevos tipos penales y el estudio e interpretación de los ya existentes.

Una situación preocupante para la sociedad consiste en enfrentarse a una conducta
Antisocial, y más cuando esta conducta no ha sido tipificada como delito ya sea por política criminal o bien porque la conducta rebasa la imaginación del legislador, fenómenos y hechos que producen inseguridad jurídica.

El conocido tratadista Eugenio Zaffaroni, en su libro denominado "Manual de Derecho Penal", señala la gran importancia de la Teoría del Delito, estableciendo que la teoría del delito, es la parte de la ciencia del Derecho Penal que se ocupa de explicar qué es el delito en general, es decir, cuáles son las características que debe tener cualquier delito.

Para Fernando Castellanos la Teoría del Delito comprenderá fundamentalmente generalidades sobre la definición; concepto; elementos; factores negativos; la vida del delito; la participación; y el concurso.[19]

NOCIONES GENERALES DEL DELITO

Antes de entrar al análisis de los delitos informáticos hay que entender que es un delito. Etimológicamente La palabra delito proviene del latín delito o delictum, del verbo delinquí, delinquiere que significa desviarse, resbalar, abandonar, que significa abandonar el camino prescrito por la ley.

Sociológicamente se entiende como una conducta desplegada, por un ser humano, calificada como nociva para la sociedad en la que convive. Dicha calificación es realizada de acuerdo con el momento histórico; de aquí que existan conductas que sean consideradas como delitos en determinadas circunstancias de modo, tiempo y lugar, y al variar las mismas dicha conducta deja de considerarse como delito.[20]

Pablo Juan Anselmo Von Feurbach, señala que: “la imposición de la pena precisa de una ley anterior (*nulla poenasine lege).* La aplicación de una pena supone la existencia de la acción prevista por la amenaza legal (*nulla poenasine sine crime).* Es la ley la creadora del vínculo entre la lesión del derecho y el mal de la pena. (*nullum crimen sine poena legalis).*El crimen es una acción contraria al derecho de los demás reprimidos por una pena”.

---

[19] Ibidem, p.18.

[20] Azaola Calderón, Luis, *Delitos informáticos y derecho Penal*, 1ª Ed. México, Ed. Ubijus, 2010, p. 49.

LOS DELITOS INFORMÁTICOS EN GENERAL.

Los Delitos Informáticos, son todos aquéllos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por la utilización indebida de medios informáticos. A nivel internacional se considera que no existe una definición propia del delito informático, pero han sido muchos los esfuerzos de expertos que se han ocupado del tema, y aun cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas

En un principio, doctrinalmente los delitos informáticos se distinguían entre aquellos de carácter económico y los que atentaban contra la privacidad, posteriormente con el valor económico que adquirió la información se fueron valorando de la misma manera o más que cualquier otro bien. En esa evolución del valor que la sociedad ha dado a la información, ha repercutido directamente en el desarrollo del derecho informático y principalmente en la protección penal que se pretende dar a las violaciones informáticas.[21]

Actualmente la información es un bien con valor económico y cuando se produce una violación directa es sancionada por las normas penales. Los delitos informáticos se clasifican y tipifican hoy en día en muchas legislaciones según el grado de afectación que provocan en el ámbito privado de la persona, cuando se comete un ingreso ilegitimo al sistema de información, vulnerando los mecanismos de seguridad, o si se comercializa con esa información o se produce una afectación mayor mediante la alteración o destrucción de los datos con el fin de cometer un fraude informático.

[21] Simón Hocsman, Heriberto, *Negocios en Internet*, Editorial Astrea, Cd. Buenos Aires, Argentina. 2005, pp. 246-247.

Primeramente para el desarrollo medular de esta tesina, es necesario definir el concepto de “Delito Informático”, a efecto de delimitar el ámbito de aplicación de las leyes, doctrina y jurisprudencia sobre la materia. Así entonces se define a esta conducta ilícita como “aquellas acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro social (abarcativo de otros intereses, v.gr., propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas”[22].

Asimismo Julio Téllez Valdés los define mediante dos conceptos, el atípico y el típico.

En el concepto atípico, los delitos informáticos son “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”.

En el concepto típico, los delitos informáticos son “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin”. [23]

El propio Julio Téllez Valdés cita el concepto del tratadista penal italiano Carlos Sarzana, quien define a los delitos informáticos como “cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo”[24].

---

[22] Ibidem, p. 249.
[23] Op. cit. Téllez Valdés, Julio, p. 167.
[24] Sarzana, Carlos. Criminalita e Tecnologia Computer Crimes, Resegna Penitenziaria e Criminologia Nos. 1-2. Anno 1, Gennaio-Geugno, 1979, Roma, Italia, p. 59.

Cada concepto nos aporta distintas características particulares de los delitos informáticos, sin embargo, todas ellas se refieren a conductas o comportamientos ilícitos que encuadran en las legislaciones penales como delitos.

Por último, el Código Penal Federal contempla como delito informático el acceso ilícito a sistemas y equipos de informática.[25]

Para la especialista en tecnologías de Información y comunicación Ivonne Muñoz Torres nos señala que:

"En el argot jurídico se conocen distintas acepciones con respecto al derecho penal y las tecnologías de la información y comunicación, enunciando para ello conceptos como: Delitos cibernéticos, delitos computacionales, delitos telemáticos y el más común delitos informáticos.

DELITO CIBERNETICO.- Es aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar a las comunicaciones que se llevan a cabo a través de las tecnologías de información y comunicación.

DELITO ELECTRONICO.- Es aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar el flujo electrónico de datos, y que consecuencia afecte el funcionamiento de internet así como de los sistemas de información que dependen de la electrónica para desarrollarse.

DELITO COMPUTACIONAL.- Se define como aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar las operaciones de una computadora y cuya consecuencia sea la interrupción de cualquiera de las fases de procesamiento de datos.

[25] Titulo Noveno del Código Penal Federal.

*DELITO TELEMATICO.- S*e define como aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar las telecomunicaciones y/o las tecnologías de información, cuya consecuencia sea la interrupción de la transmisión de información que este depositado en un sistema de información.

*DELITO INFORMATICO.- S*e define como aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar datos, información o sistemas de información cuya consecuencia sea el daño directo o indirecto en ellos así como el mal uso de estos."[26]

CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS.

Nuevamente el Doctor en Derecho Informático Julio Téllez Valdés, nos establece algunas características que diferencian a los delitos informáticos de los delitos normales, y son las siguientes:

1. Son conductas criminales de cuello blanco, *White collar crimes*, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

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

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

[26] Muñoz Torres, Ivonne. *Delitos Informáticos. Diez Años Después* Editorial Ubijus, Mexico 2009 p. 14.

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

5. Ofrecen posibilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.

6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.

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

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

9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.

10. Ofrecen a los menores de edad facilidades para su comisión.

11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional.

Estas características especiales de los delitos informáticos nos permiten dar cuenta de que quienes cometen estas conductas malintencionadas, son personas con ciertos conocimientos técnicos sobre sistemas informáticos, sin que sea necesaria su presencia en el lugar en que se cometen, lo que dificulta su persecución y penalización.

CLASIFICACIÓN DE LOS DELITOS INFORMATICOS.

Para realizar una clasificación adecuada de los delitos informáticos, tenemos que tomar en cuenta la clase de actividades, contenidos y derechos relacionados con los sistemas informáticos y/o internet pueden regularse, y que actos específicamente pueden constituir un delito o ilícito.

En primer término encontramos que en la tecnología informática todas las actividades, contenidos y derechos relacionados con ella son susceptibles de regulación, es decir, pueden regularse las actividades de los usuarios y proveedores de los sistemas desde que se enciende una computadora hasta que se accede a ella, o en su caso, se apaga o se sale del sistema.

Por otra parte, toda clase de datos e información y su manejo, reproducción, modificación y eliminación puede ser regulada, ya que son derechos del usuario para comercializar, prestar servicios, consumir o recibir información de otros medios informáticos. Sin embargo, a pesar de todas las actividades en las que se emplean sistemas informáticos, no se puede realizar por el momento una clasificación legal objetiva en virtud de que en la legislación actual no se han establecido delitos de tipo informático, por lo que en base a la doctrina existente es posible encontrar una clasificación de delitos informáticos.[27]

En primer lugar tenemos que para María de la Luz Lima Malvido, los "delitos electrónicos" se clasifican en tres categorías:

1. Los que utilizan la tecnología electrónica como método,
2. Los que utilizan la tecnología electrónica como medio y,

[27] Molina Salgado, Jesús Antonio, *Breviarios Jurídicos*, 1ª ed., Editorial Porrúa, S.A. de C.V., México, D, F, 2003, pp. 20 y 21.

3. Los que utilizan la tecnología electrónica como fin.

Como método.- Conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como medio.- Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

Como fin.- Conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla"[28].

Por otra parte, tenemos nuevamente la clasificación que el Doctor Julio Téllez Valdés considera apropiada para los delitos informáticos como sigue:

Como instrumento o medio. En esta categoría se encuentran las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
b) Variación de los activos y pasivos en la situación contable de la empresa.
c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
d) Robo de tiempo de computadora.
e) Lectura, sustracción o copiado de información confidencial.
f) Modificación de datos tanto en la entrada como en la salida.

[28] Lima Malvado, María de la Luz. Delitos Electrónicos, *Criminalia*. México, Ed. Porrúa No. 1-6. Año L, Enero-Junio, 1984. p. 100.

g) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del “caballo de Troya”).
h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la “técnica de salami”.
i) Uso no autorizado de programas de cómputo.
j) Introducción de instrucciones que provocan “interrupciones” en la lógica interna de los programas, a fin de obtener beneficios.
k) Alteración en el funcionamiento de los sistemas.
l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.
m) Acceso a áreas informatizadas en forma no automatizada.
n) Intervención en las líneas de comunicación de datos o teleproceso.[29]

Como fin u objetivo. En esta categoría encuadramos a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

a) Programación de programas por cualquier método.
b) Daño a la memoria.
c) Atentado físico contra la maquina o sus accesorios (discos, cintas, terminales, etcétera).
d) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurológicos computarizados.
e) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etc.)[30]

[29] Op. cit. Téllez Valdés, Julio, p. 190.
[30] Ibidem, p. 191.

En cuanto a la clasificación de los delitos informáticos bajo la presente acepción, cabe destacar la multitud de criterios y tipologías expuestas al efecto. Sin embargo, si hubiera que reseñar una por encima de la demás esa es, sin lugar a dudas, la de Ulrich Sieber, reconocida a nivel internacional, a tal efecto Sieber estructura su tipología en las siguientes áreas de afectación criminológica:

a) Infracciones a la intimidad. Orientados a proteger la privacidad de los datos personales hallados principalmente en las bases de datos públicas o privadas.

b) Delitos económicos. Este tipo de delincuencia surge en los años ochenta como consecuencia del desarrollo de bienes intangibles, nuevos soportes informáticos y el nacimiento del dinero electrónico. entre sus principales manifestaciones delictivas cabe citar el hacking, el espionaje informático, la piratería, el sabotaje y el fraude informático.
c) Contenidos ilegales y nocivos. Son los ya reseñados delitos de contenido. Menciona de forma expresa la información ubicada en el internet y en especial aquella de contenido discriminatorio para las minorías o el caso de la pornografía infantil.
d) Otros delitos. Con semejante terminología pretende agrupar cualquier otra manifestación delictiva derivada del uso de la informática. De forma expresa destaca los delitos contra la vida. piénsese, por ejemplo la manipulación del sistema de control de vuelo o la base de datos de un hospital; el crimen organizado como forma de comunicación o actuación; o las guerras electrónicas, principalmente en referencia a las manipulaciones militares. [31]

[31] http://books.google.com.mx/books?id=mWk1VSOpmA8C&pg=PA112&lpg=PA112&dq=clasificaci%C3%B3n+de+Uhlrich+Sieber&source=bl&ots=pigTqHh4jC&sig=8Z4gX6Ie0H7crDySy5AbKgb80AQ&hl=es-419&sa=X&ei=IP6jUM3CNaHJyAGP9oHABQ&sqi=2&ved=0CBwQ6AEwAA#v=onepage&q=clasificaci%C3%B3n%20de%20Uhlrich%20Sieber&f=false Sieber U, legal cit. pp. 39-59 consultada el 2 de Agosto del 2012.

Asimismo, Carlos Correa basado en la clasificación de Ulrich Sieber, clasifica a los delitos informáticos en las siguientes categorías:

> a) Fraude por manipulaciones de un contador contra un sistema de procesamiento de datos;
> b) Espionaje informático y robo de software;
> c) Sabotaje informático;
> d) Robo de servicios;
> e) Acceso no autorizado a sistemas de procesamiento de datos; y ofensas tradicionales en los negocios asistidos por computador"[32].

En esta clasificación más particular, determina las características de los delitos en particular, en virtud de que se refiere a conductas particularmente ya definidas.

Por otro lado, Gabriel Cámpoli va más allá de una clasificación genérica de los delitos informáticos, señalando que primero se debe recordar que los códigos penales mantienen un orden y una clasificación basada específicamente en los bienes jurídicos protegidos. En este sentido los clasifica en tres tipos de violaciones: *a) al patrimonio, b) a la intimidad,* y; c) *a la integridad física y lógica de los equipos de internet y o páginas web,* cuando ello no implique a los dos anteriores.

a. Faltas al patrimonio; En estas se puede incluir a los delitos que no se encuentren tipificados en otros grupos. Cuando se utilicen armas para su ejecución, en cuyo caso se encuentran agravados por la indefensión que la utilización de la misma produce en el sujeto pasivo.

[32] Correa, Carlos, y otros. *Derecho Informático*, Buenos aires, Argentina, Ed. Depalma., 1987, p. 296.

b. Faltas a la intimidad; Encontramos en este apartado los conceptos y figuras del hacking, el craking[33] y el robo de información. Así mismo, podemos hablar de la lesión al bien jurídico.

c. Faltas a la integridad física y/o lógica de los equipos de cómputo y/o páginas *web* cuando ello no implique los dos anteriores.son aquellos que sin afectar expresamente a un equipo informático en particular disminuyen o anulan su capacidad de transmisión o procesamiento de datos a distancia, ya sea actuando en forma indirecta sobre el equipo, sobre su capacidad de recepción o envío de datos, sobre sus parámetros lógicos o sobre las vías de comunicación necesarias para las funciones normales del mismo a distancia[34].

En esta clasificación tenemos la que hace Palazzi, acercándose más a la dogmática penal, casi de la misma manera que Cámpoli, pero con algunas características más:

a) Delitos contra el patrimonio.
b) Delitos contra la intimidad.
c) Delitos contra la seguridad pública y las comunicaciones.
d) Falsificaciones informáticas.
e) Contenidos ilegales en internet.[35]

Por último, la Organización de las Naciones Unidas, reconoce como delitos informáticos las siguientes conductas:

[33] El cracking es la modificación del software con la intención de eliminar los métodos de protección de los cuales este disponga: protección de copias, versiones de prueba, números de serie, claves de hardware, verificación de fechas, verificación de CD o publicidad y ad-aware.
[34] Cámpoli, Gabriel. *Delitos Informáticos en la Legislación Mexicana*. INACIPE. México 2005. pp. 61-65.
[35] Palazzi, Pablo A. *Delitos Informáticos*, 1ª ed. Ad Hoc, Buenos Aires, 2000, p. 33.

1. Fraudes cometidos mediante manipulación de computadoras:
a) Manipulación de los datos de entrada.
b) Manipulación de programas.
c) Manipulación de datos de salida.
d) Fraude efectuado por manipulación informática.

2. Falsificaciones informáticas
a) Utilizando sistemas informáticos como objetos.
b) Utilizando sistemas informáticos como instrumentos.
3. Daños o modificaciones de programas o datos computarizados.
a) Sabotaje informático.
b) Virus.
c) Gusanos.
d) Bomba lógica o cronológica.
e) Acceso no autorizado a sistemas o servicios.
f) Piratas informáticos o hackers.
g) Reproducción no autorizada de programas informáticos con protección legal.[36]

Las anteriores clasificaciones varían según el autor y el país en el que han realizado, debido a que en cada Estado se presentan conductas distintas en razón de la sociedad, sus costumbres, capacitación en nuevas tecnologías de información y comunicación, etcétera, por lo que no ha sido posible unificar criterios internacionales para regular todas las conductas en particular.

SUJETOS DE LOS DELITOS INFORMÁTICOS.

La tratadista argentina Bibiana Luz Clara señala: Encontramos entonces distintas figuras y modalidades que a diario se mencionan.

[36] Op. cit. López Betancourt, Eduardo, p. 271.

A) SUJETO ACTIVO:

las opiniones en cuanto a tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional o nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

Estos delitos se han calificado de "cuello blanco" porque generalmente el sujeto que comete el delito es una persona de cierto status socioeconómico.[37]

Son las personas que tienen habilidades para el manejo de los sistemas informáticos y puede ocurrir que por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible. *(Hacker, Cracker, Phreaker, Spammer, Piratas, spoofers, etc.)*

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

2. ***Cracker:*** aquí se inutilizan los sistemas de protección de

[37]Op. cit. Azaola Calderón, Luis, p. 28.

aplicaciones informáticas mediante programas elaborados a tal fin. A diferencia del *hacker* el *cracker* tiene la intención precisa de provocar un daño. [38]

Tipos de cracker:

1. ***Pirata***. Su actividad consiste en la copia ilegal de programas, rompiendo sus sistemas de protección y licencias. Luego distribuye los productos por Internet, A través de CD`s, etc.

2. ***Lammer***. Son personas con poco conocimiento de informática que consiguen e intercambian herramientas no creadas por ellos para atacar ordenadores. Ejecutan aplicaciones sin saber mucho de ellas causando grandes daños.

3. ***Phreakers***. Son los crackers de las líneas telefónicas. Se dedican a atacar y "romper" los sistemas telefónicos ya sea para dañarlos o realizar llamadas de forma gratuita.

4. ***Trasher***. Su traducción al español es la de 'basurero'. Se trata de personas que buscan en la basura y en papeleras de los cajeros automáticos para conseguir claves de tarjetas, números de cuentas bancarias o información secreta para cometer estafas y actividades fraudulentas a través de Internet.

[38] Franco Guzmán, Ricardo. *Análisis de los delitos informáticos*. Ed. Porrúa. México 2005. p. 28.

B) SUJETO PASIVO:

Es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones, gobiernos, etc.

La mayoría de los delitos informáticos no son descubiertos, como ya dijimos, pero es importante destacar que se debe en gran parte a que los mismos no son denunciados, las empresas o bancos tienen miedo al desprestigio y a su consecuente pérdida económica.

TIPOS DE DELITOS INFORMÁTICOS:

la Organización de las Naciones Unidas, reconoce como delitos informáticos las siguientes conductas:

Manipulación de los datos de entrada. Insiders*.* Conocido también como sustracción de datos y estamos ante el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Son los *crackers* 'corporativos', empleados de las empresas que las atacan desde dentro, movidos usualmente por la venganza[39].

La manipulación de programas. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática.

[39] Consulta Virtual en: http://www.ecured.cu/index.php/Cracker, consultada el 08 de junio de 2012.

Manipulación de los datos de salida – outsiders. El caso de manipulación más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, hoy en día se usan equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Para establecer los delitos que se cometen en base al bien jurídico que se tutela por la legislación, se presenta la siguiente tipología de delitos:

> **Fraude informático:** Es cometido a través de la manipulación de datos o programas (caballo de "Troya") para la obtención de un lucro ilícito.[40] Se puede cometer en distintas modalidades; *uso de datos falsos o engañosos (data diddling), técnica del "salami", falsificaciones informáticas, manipulación de datos de salida o pishing*[41]*.* (Artículo 248 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Español). En nuestra legislación se regula por el Código Penal Federal en los artículos 230 y 231 Fracc. XIV y el Código Penal para el Estado de Sinaloa en su artículo 217.
>
> ***Caballo de Toya.*** Otro caso muy difícil de descubrir y a menudo pasa inadvertido debido a que el sujeto activo en este caso debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de

[40]Op. cit. Franco Guzmán, Ricardo. p. 92.
[41] Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática.

El cual consiste en insertar instrucciones de computadora en forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Técnica del salami. Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salami" en la que cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se transfieren a otra. Esta modalidad de fraude informático se realiza sin grandes dificultades y es muy difícil de detectar. Uno de los casos más ingeniosos en el "redondeo hacia abajo", 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.

Infracciones a la Ley de Propiedad Industrial: Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas[42]. (artículo 270 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Español). En nuestra legislación se regula por la Ley de la Propiedad Industrial en sus artículos 82 al 86-Bis-1, 223, fracciones IV, V y VI y 224.

[42]Ibidem p. 90

Daño o Sabotaje Informático: Consiste en borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Las técnicas que permiten cometer sabotajes informáticos son:

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, se reproduce y causa daño. La gravedad de los virus es variable, puede ser simplemente una molestia en la pantalla, como el caso del "ping-pong" y también existen aquellos que pueden llegar a eliminar el contenido de una base de datos.

En función de las consecuencias del virus. Habría que diferenciar entre:

Virus inocuos*:* aquellos que solo expanden información, sin dañar ni ralentizar sistemas informáticos.

Virus como herramienta de hacking*:* su diseño como virus está destinado a introducirse en los sistemas, no para dañarlos, sino para obtener información como contraseñas, topología de redes, o para crear cuentas de usuario.

Virus como herramienta de estafa*:* son aquellos destinados al fraude electrónico, que consiguen transferencias de activos, defraudando a empresas y bancas online, así como mediante operaciones fraudulentas en bolsa.

***Virus destructivos**:* serian aquellos cuya finalidad es la destrucción y alteración de la información contenida en sistemas informáticos.[43]

Entre los virus más conocidos tenemos, a modo de ejemplo:

ping-pong: consiste en un punto que se mueve por toda la pantalla y parece rebotar en los bordes.

Datacrime o virus del viernes 13: el virus Jerusalem estaba destinado para destruir todas las memorias militares y científicas de Israel el 13 de mayo de 1988.

MIchelangelo. Actualmente existe una gran carrera entre aquellos que crean los virus y los que desarrollan los antivirus. Hasta ha llegado a decirse que los virus son desarrollados por los mismos productores de antivirus, ya que hoy en día es fundamental adquirir antivirus y los mismos deben ser renovados constantemente, por supuesto que no existe ninguna prueba concreta.

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 graves, por ejemplo un programa gusano puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego se destruirá.

[43] Op. cit. Azaola Calderón, Luis, p. 84.

Rutinas cáncer. Se define como aquellas que "*distorsionan el funcionamiento del programa y se auto reproducen al estilo de las células orgánicas alcanzadas por un tumor maligno*".

Bomba lógica o cronológica. Consiste en la introducción en un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha o circunstancia, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo. Las bombas lógicas son difíciles de detectar antes de que exploten, son las que pueden resultar más dañinas y prever que exploten cuando el delincuente ya se encuentre lejos. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla.

DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS.

Puede darse por motivos diferentes: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático. Estos ingresos no autorizados comprometen la integridad y la confidencialidad de los datos. Podríamos llegar hasta actos de atentados terroristas, por ejemplo en el caso de intervenir sistemas de tráfico aéreo.

El acceso puede darse en forma directa, por ejemplo cuando un empleado accede en forma no autorizada, estamos frente a un riesgo interno.

Pero se puede acceder en forma indirecta, o sea a través de una terminal remota.

El delincuente puede aprovechar la falta de medidas de seguridad para obtener acceso o puede descubrirle las deficiencias a las medidas existentes de seguridad. A menudo, los hackers se hacen pasar por usuarios legítimos del sistema, esto suele suceder debido a la frecuencia en que los usuarios utilizan contraseñas comunes.

La fuga de datos consiste en la versión informática de las tradicionales prácticas de "espionaje industrial"

El acceso no autorizado a sistemas informáticos reviste diversas modalidades, que son:

Puertas falsas. Se trata de intromisión indebida a los sistemas informáticos aprovechando los accesos o "puertas" de entrada, que no están previstas en las instrucciones de la aplicación, pero que facilitan la revisión o permiten recuperar información en casos de errores de sistemas. También llamadas "puertas trampa" porque permiten a los programadores producir rupturas en el código y posibilitar accesos futuros.

Llave maestra (Superzapping). Consiste en el uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático. El nombre proviene de un programa de utilidad que se llama superzap, que permite abrir cualquier archivo de una computadora aunque se halle protegido por medidas de seguridad.

Pinchado de líneas. Se realiza a través de la interferencia de las líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas.[44]

Heriberto Simón Hocsman cita en su libro a Jijena Leiva quien define a este delito informático como "toda acción típica antijurídica y culpable para cuya consumación se usa la tecnología de las computadoras, o se afecta la información contenida en un sistema de tratamiento automatizado de datos, y/o la transmisión de datos". **[45]** Este delito también puede cometerse empleando Virus[46] y Gusanos informáticos[47].(Artículo 263 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Español y en el artículo 264 se tipifica el delito de destrucción de datos). En nuestra legislación ambos delitos no son más que una variante o modalidad del daño en propiedad ajena.

---

[44] http://comunidad.derecho.org/mjviega/deli_inf.htm, consultada 08 de Septiembre del 2012.

[45] Op. cit. Simón Hocsman, Heriberto. Pág. 254.

[46] ***Virus Informático***, son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del *Caballo de Troya*. Han sido definidos como *"pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autorreporducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar."*

[47] ***Gusano Informático,*** se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Ciberterrorismo o Terrorismo Informático. [48] Es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista, por lo que los nuevos medios que nos ofrece la informática y el internet, aptos para sembrar el terror son:

1. ***Sniffing****:* es por medio de programas de monitoreo de redes y captura de paquetes durante su transmisión.

2. ***Trapping****:* es por medio del envío de mails falsos o bien la creación de páginas web clonadas que hacen de trampas para la captura de datos de manera ilegítima.

El espionaje informático y el robo o hurto de software: fuga de datos (*data leakage*), también conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, "*la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al*

[48] Consulta Virtual: Acurio Del Pino, Santiago. *La delincuencia Informática transnacional y la UDIMP* en http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/acurio.pdf

alcance de cualquiera". Actualmente este delito no se contempla en nuestra legislación.

Ataques que se producen contra el derecho a la intimidad: Delito de descubrimiento y revelación de secretos reservados registrados en ficheros o soportes informáticos.[49] (Artículo 197 al 201 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Español).

Espionaje: Es definido como el acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos. [50] Ejemplo el caso *WikiLeaks* en el que se cometió el delito de espionaje en contra de varias naciones y empresas del mundo.[51]

Falsificación de documentos informáticos: lo comete quien de cualquier modo falsifique documentos informáticos con intención de causar un perjuicio a otro.[52] (Artículo 462-5 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Español). En nuestra legislación solo en un concepto genérico del delito de falsificación de documentos.

Uso de documentos informáticos falsos: es cometido por quien conscientemente haga uso de documentos falsos. (Artículo 462-6

[49] Op. cit. Franco Guzmán, Ricardo, Pág. 90.
[50] Op. cit. Téllez Valdés, Julio, p. 204.
[51] Sobre el particular se puede consultar la página electrónica ubicada en: http://www.oem.com.mx/oem/notas/n1875272.htm
[52] Op. cit. Franco Guzmán, Ricardo. Pág. 95.

de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Español). En nuestra legislación solo en un concepto genérico del delito de uso de documentos falsos.

Pornografía infantil: uno de los delitos más importantes dentro del marco de regulación jurídica de los delitos informáticos en el contexto internacional es el relativo a la prostitución de menores o incapaces con fines exhibicionistas o pornográficos. La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art. 187). La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (Art. 189). La posesión de dicho material para la realización de dichas conductas.

CARACTERÍSTICAS ESPECIALES QUE DIFICULTAN LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

A) El problema de la extraterritorialidad en los tipos informáticos.

Como se ha dejado claro a lo largo de toda esta investigación, los delitos informáticos tienen características muy particulares que los diferencian de aquellos que no son cometidos mediante el uso de herramientas informáticas, por lo que no es posible aplicar al cien por ciento las teorías clásicas del tipo penal, ya que aunque existan similitudes en su comisión, constitucionalmente es violatorio de garantías aplicar una pena o medida de seguridad por simple analogía. Aunado a lo anterior, existe el problema de la extraterritorialidad de los delitos informáticos, ya que una de sus características es que el sujeto activo comete la conducta típica y antijurídica en un país A, y con ayuda de software especializado o no, los

efectos de esa conducta son programados para iniciarse en un país que pude ser A o B. es entonces cuando se rebasa la jurisdicción de un estado y se queda a expensas de que en el otro la conducta pueda ser perseguida y castigada por ser delito. Ahí surge otro problema aun mayor, ya que una vez que se ha perseguido y detenido al ciberdelincuente en el país B, se debe determinar cuál de los dos países aplicara su legislación. Una tarea muy difícil de realizar, porque seguramente ninguno de los dos países querrá ceder jurisdicción sobre el caso. En este sentido es necesario hablar de la cooperación internacional que debe existir para la resolución de los conflictos que generan los delitos informáticos.[53]

B) La disociación temporal

Se refiere a la posibilidad que se tiene de programar la ejecución del delito en una determinada fecha, lo que ocasiona que algún virus o gusano informático se activen y causen el efecto deseado el día y la hora en que el sujeto activo ha premeditado hacerlo. Circunstancia que entre otras dificultades tendría la de obstruir la investigación de la conducta por parte de las autoridades correspondientes.[54]

CONCLUSIONES DEL PRIMER CAPITULO

En el transcurso de la historia los seres humanos se han visto en la necesidad de compartir información de manera constante, para lo cual se han creado múltiples métodos para el procesamiento y transmisión de esa información, que hasta el día de hoy, ha beneficiado a la sociedad con las diversas innovaciones; Razón por la cual nace la informática como una ciencia que se

[53] Op. cit. Téllez Valdez Julio, pp. 37 y 38.

[54]

encarga del estudio y desarrollo de estos métodos de trasmisión de información.

Posteriormente surge lo que hoy en día conocemos como Internet, una herramienta tecnológica que nos ayuda a transmitir información y a ponerla al alcance de millones de personas en cualquier parte del mundo, pero de igual manera le da el acceso a los delincuentes para poder hacer mal uso de esta tecnología y lo que es peor, la mayoría de las ocasiones impunemente. Situación que se presenta en razón de que este tipo de tecnología se encuentra al alcance de todos y que ha facilitado las conductas anti sociales y delictivas, que en la actualidad cada vez son más frecuentes, y cualquier usuarios de esta tecnología se encuentra expuesto a ser blanco de los delitos en la red.

El desarrollo que se ha venido presentando en la tecnología hoy en día puede tener dos vertientes muy importantes la primera de ellas es manejarla que ayuda a los individuos que hacen uso de ella al facilitarles sus tareas cotidianas y el otro es realizar conductas delictivas con una mayor impunidad ante la imposibilidad de acreditar dichos delitos.

Gran parte de las personas que utilizan la tecnología desconocen los diversos tipo de delitos informáticos, de igual manera los delincuentes informáticos desconocen los alcances que puede llegar tener dichas conductas, ya que si bien es cierto que físicamente no lastiman a las personas o a los usuarios del internet sus conocimientos en el rubro de la informática, si realizan afectaciones de tipo económico personal y colectivo, y los riesgos al ser víctima de alguna conducta ilícita cometida a través de la tecnología puede ser desde mínimas hasta graves; afectando tanto estructura públicas o privadas.

Es de suma importancia que la sociedad en general las formas y métodos actuales que se utilizan como ataques a la información y la violación de la privacidad de las personas y que como resultado de ello nos de un sentido de responsabilidad y prevención para no ser víctima de este tipo de conductas delictivas que se dan a través de la tecnología.

Derivado de lo anterior se da lo que es la informática jurídica que si bien es cierto tuvo su origen hace muchos años, hasta el día de hoy no es fácil hablar de una conceptualización de la misma, pero lo que sí es de suma importancia para la sociedad de hoy en día, ya que aun cuando es inimaginable los alcances que se pueden llegar a tener a través de la tecnología, todavía era más difícil pensar que el ámbito jurídico se relacionaría con la informática.

En virtud de lo anterior y en consecuencia de todas las conductas ilícitas que se realizan a través de la informática surge la imperiosa necesidad de regular a través de los medios con que cuenta el estado dichas conductas, con lo que podemos apreciar que una de las finalidades mas importantes del derecho de la informática es la protección de bienes jurídicos tutelados por la ley.

Naturalmente el derecho, como un ordenamiento regulador de conductas ilícitas, no está exento del impacto de nuevas tecnologías con la que hoy en día cuenta nuestra sociedad, mismas que han abierto nuevos horizontes a los delincuentes cibernéticos favoreciendo la impunidad de sus delitos.

Por lo que en conclusión podemos observar que la informática hoy en día es de suma importancia para los seres humanos pero de igual manera es importante saber cuál es el alcance que puede llegar a tener y las afectaciones que nos puede llegar a causar ser víctima de los delitos cibernéticos.

CAPÍTULO SEGUNDO

EVOLUCIÓN HISTORICA DEL INTERNET EN RELACION CON LOS DELITOS INFORMATICOS

ANTECEDENTES DE LA INFORMÁTICA.

Recordemos que la PRIMERA REVOLUCIÓN técnico científica fue la escritura, y esta fue tan importante que dividió la historia de la prehistoria, su historia, es la del proceso de perfeccionamiento de los signos convencionales de su evolución, hacia formas más precisas y objetivas que permitieron una fácil comunicación escrita, la formación de los grupos sociales, la trasformaciones de sus relaciones por medio de la comunicación dieron lugar a la creación del llamado estado moderno, posteriormente la lucha por la conquista de la tierra que desemboco en el descubrimiento geográfico de nuevos territorios.

Por lo que desde tiempos remotos el hombre al verse en la necesidad de cuantificar sus pertenecías, animales, objetos de casa, pieles, etc. ha tenido que procesar datos. En un principio este procedimiento fue muy rudimentario; utilizaba sus manos y almacenaba toda la información posible en su memoria. Esto impedía un flujo fácil de la información, porque la no existir representaciones fijas de los elementos que se tenían en un proceso determinado, las conclusiones a las que llegaba resultaban ser meras especulaciones. El hombre para contar se encontraba limitado al número de sus dedos y a su memoria, siendo esto superado cuando empezó a utilizar como cuentas, granos y objetos similares.

Poco después el hombre invento sistemas numéricos que le permitieron realizar sus operaciones con mayor confiablidad y rapidez, sin

embargo, pese a ello dichas operaciones con su respectivo resultados no tenían la exactitud deseada, y con el afán de lograr dicha exactitud invento algunas herramientas que le ayudaron en su afán de cuantificar y transmitir la información.

Entre las primeras creaciones del hombre dirigidas a facilitar las operaciones de cálculo se encuentran:

a) El ábaco.

Este fue el primer dispositivo mecánico para realizar cálculos. Dicho invento aparece en forma independiente en varias culturas de la antigüedad, aunque se han atribuido el crédito de su realización al pueblo babilónico.

La palabra ábaco encuentra su raíz etimológica en la voz fenicia abak, que significa "tabla lista cubierta de arena". Estas tabletas de arcilla tienen una antigüedad de cuatro mil años y con ellas se llevaban registros de bancos y empresas de préstamos que funcionaban en aquella época. "Elías Awad manifiesta que el código Hammurabi incluye referencias de transacciones de negocios tales como contratos, escrituras, bonos, recibos, inventarios, ventas y otros tipos de operaciones semejantes. Usaban comúnmente giros y cheques, asimismo se cobraban derechos aduanales y peajes en los transbordadores y carreteras". [55]

El ábaco que actualmente conocemos apareció a fines del imperio romano y con él se puede realizar rápidamente operaciones de suma y resta así como de multiplicación y división. El ábaco ha resistido la prueba del tiempo, y la velocidad con la que realiza las operaciones resulta aún hoy en día extraordinario, teniendo en cuenta de que se trata de un proceso

[55] Cfr. Awad M. Elías, *Procesamiento Automático de Datos*, 18ª ed. Ed. Mc Graw Hill, México, 1982, p. 51.

manual. Asombrosamente hay cultura que todavía lo utiliza, principalmente aquellas en donde realizan operaciones basándose en el sistema arábigo.

La SEGUNDA REVOLUCIÓN tecnológica que cambio al mundo fue la creación de la imprenta en el año de 1440, lo que permitió que la información se difundiera y fuera conocida por la mayoría de las personas, lo que causo una gran movilización social, con el que se abrió un nuevo mundo de información gracias a la difusión que permitió y construyo un nuevo punto de partida de una nueva época que culmino con los medios masivos de comunicación.

Resultando de esta revolución científico tecnológica el surgimiento de nuevos procesos y métodos de contabilidad a través de los cuales se dio origen a una época de innovación.

b) Tablas de logaritmos.

"La dificultad para realizar operaciones motivo a John Napier para que en 1614 creara un nuevo método que redujera de manera notable ese trabajo.[56]

Fue así como surgieron las tablas de logaritmos, a través de las cuales era posible realizar multiplicaciones en forma sencilla y rápida: las multiplicaciones se traducían en sumas y las divisiones en restas. Sin embargo, había que crear las tablas con sus respectivos antilogaritmos e imprimirlas, lo cual representaba un enorme trabajo que fue realizado por H. Briggs. "No obstante la magnitud del esfuerzo que realizaron, de manera inmediata salieron a flote los errores en que se incurría con el uso de dichas tablas". [57]

[56] Op. cit. Correa, Carlos, p.28.
[57] Ibidem p.9.

c) Regla de Cálculo.

Poco tiempo después en el año de 1630, surgió otro invento menos exacto pero más fácil de utilizar: la regla de cálculo. “Esta funciona con base en la medición de longitudes entre dos reglitas que guardan relación, utilizando la escala logarítmica. Esta herramienta a sido muy utilizada inclusive en la actualidad sigue utilizándose y los resultados de las operaciones que se realizan con ella se aproximan con suficiente exactitud. No es sino hasta estos últimos años que ha sido desplazada por las calculadoras electrónicas de bolsillo”. [58]

d) La máquina de Pascal.

En 1642, un hombre llamado Pascal construyo una sumadora mecánica, misma que tomo el nombre de máquina de calcular. “esta máquina, llamada Pascaline, contaba con un conjunto de ruedas dentadas, cada una de ellas numeradas del 0 al 9. Cuando una rueda, después de una vuelta completa, pasaba del 9 al, hacia mover un décimo de vuelta la rueda situada a su izquierda con esto se incrementaba el número de lectura de esta última en una unidad. Dicho artefacto contaba con un dispositivo de memoria que acumulaba los resultados. Sin embargo, pese a la confiabilidad que esta máquina llego a generar entre muchas personas, los empleados en trabajos de cálculo vieron en la Pascaline una amenaza de desempleo y finalmente el desarrollo de la idea se interrumpió”.[59]

Posteriormente Leibniz[60], introdujo dos avances muy importantes. Construyo una máquina que no solo sumaba y restaba sino que también

[58] Ibidem p.52.
[59] Ibidem p. 10.
[60]Gottfried Wilhelm Leibniz (1646-1716), Filosofo, Lógico y Matemático Alemán, fue uno de los últimos representantes del saber universal clásico. Su obra abarca la metafísica y la teología, aparte de la historia y el derecho. pero sus aportaciones a

multiplicaba y dividía. También procuro la simplificación de la aritmética mediante el sistema binario. En efecto, estamos habituados a contar de diez en diez, mil son diez centenas, una centena consta de diez decenas y una decena está integrada por diez unidades, de modo que cada digito de un numero de varias cifras representa diez veces más unidades que el digito situado a la derecha. Sin embargo Leibniz se preguntaba ¿Por qué no imaginar un numero distinto con base del sistema numérico?, si la base fuese dos en lugar de diez la sucesión que ahora se lee 0,1,2,3,4,5,6,7,8,9 se representaría así: 0,1,10,11,100,101,110,111,1000,1001. Este sistema es llamado binario ya que consta de dos dígitos y tiene la ventaja de que sus símbolos pueden representarse por dos estados de un circuito eléctrico que pasa por el pase o no pase una corriente.

Este es el principio fundamental del funcionamiento de las computadoras actuales.

Así tenemos que a partir de las ideas que fueran desarrolladas por Pascal y Leibniz desarrollo la tecnología de las máquinas de calcular, primero mecánicas y luego eléctricas. Esas calculadoras ahorraban al hombre un muy significativo esfuerzo mental, pero solo hacían una operación por vez: esto es, no eran capaces de obtener resultados de operaciones repetitivas o seriadas.

e) La tarjeta perforadora.

En 1804, Joseph Marie Jacquard, mecánico francés ideo un telar automático capaz de crear copias perfectas de un original mediante una memoria compuesta de tarjetas de cartón perforadas. “Así Jacquard quedo vinculado a un tipo de tejido que lleva su nombre y al mismo tiempo a las

---

la lógica constituyen una base importante para el proceso de mecanización del pensamiento de acuerdo a un modelo matemático.

famosas tarjetas de computación que hasta hace algunos años eran la base principal de los archivos informatizados".[61]

f) La máquina Babbage.

"Babbage invento en 1823 lo que denomino máquina de diferencias. Trabajo en ella cerca de veinte años, obteniendo para ello un subsidio gubernamental, pero finalmente la abandono. Esto se debió a otro proyecto más ambicioso: el de la maquina analítica, concebida en 1834 y destinada a ejecutar cualquier operación matemática sin intervención del ser humano en el proceso de cálculo". [62]

La máquina analítica se componía de cuatro unidades: una memoria para almacenar los datos inmediatos, una unidad aritmética para efectuar los cálculos; un sistema de engranajes y palancas para transferir datos entre la memoria y la unidad aritmética y por último, un dispositivo para introducir datos y extraer resultados.

Babbage, aprovecho el invento de Jacquard (las tarjetas perforadas) para suministrar datos de entrada y para controlar su máquina analítica.

En el proyecto de Babbage las tarjetas se agrupan en dos clases: las tarjetas de operación, cada una de las cuales seleccionaba una de las cuatro operaciones aritméticas y las tarjetas variables destinadas a elegir las posiciones de memoria que se usaban en una operación en particular. La máquina también contaba con un mecanismo que permitía alterar automáticamente la secuencia de las operaciones siguiendo un curso de acción distinto según el signo de un numero fuese positivo o negativo.

[61] Op. cit. Téllez Valdez Julio, p.10.
[62] Idem. p.10 y 11.

Pese al avance de Babbage en el campo del cálculo, la información a elaborar seguía siendo estrictamente numérica: se trataba siempre de tomar números, almacenarlos, combinarlos según distintas operaciones y ofrecer a los resultados de esas operaciones.

g) El código de Herman Hollerith.

En 1880 Hollerith comprendió que las tarjetas de Jacquard permitían codificar cualquier tipo de información incluyendo la alfabética. De esta manera, surgió en la mente de Hollerith la primera aplicación práctica, la que consistía en el procesamiento de datos para el censo de población de los estados de América en 1890. Cada característica de habitante que fuese relevante para el censo se indicaba mediante perforaciones en lugares específicos de la tarjeta correspondiente. Luego las tarjetas se leían con un dispositivo eléctrico y se contaban mecánicamente. La población había aumentado considerablemente y los cómputos del censo se terminaron rápidamente.

Como podemos ver, a lo largo del tiempo hubo grandes avances en cuanto a máquinas de cálculo se refiere, pero la historia no termina ahí, tal y como lo menciona el maestro Julio Téllez Valdez “después del código de Herman Hollerith le siguieron otros que inventaron maquinas con el fin de realizar operaciones lo más rápido y sencillo posible. Tal es el caso de Konrad Zuse, que en 1938 ideo una calculadora mecánica conocida como la Z1 y más tarde la Z2 con una unidad aritmética basada en relés electromagnéticos (un relé (del inglés relay y del francés relais) es un dispositivo que utiliza una variación de intensidad en un circuito para controlar las condiciones existentes en otro. Todos ellos se componen básicamente de tres partes: un elemento operador, un elemento móvil y un juego de contactos. Los electromagnéticos abren o cierran los contactos mediante la acción de piezas móviles. Los electromagnéticos lo hacen por la acción de electroimanes o de

campos magnéticos giratorios como los que sirven de base a los motores de corriente alterna) puede considerarse la primera calculadora de aplicación general con programa controlado.[63]

Evolución de la Computadora

Sería difícil encontrar en la historia otro ejemplo de transformación tan rápido y amplio como el provocado por la aparición de las computadoras y sus respectivas implicaciones en el mundo moderno.

A nivel operacional la computadora puede definirse como "la maquina automatizada de propósito general integrada por elementos de entrada, procesador central, dispositivo de almacenamiento y elementos de salida".[64]

Otros la definen como "un dispositivo que bajo el control de un programa o plan preestablecido, acepta datos del exterior, los procesa y produce información como resultado de un proceso".[65]

Después de haber definido a la computadora resulta necesario analizar las diferentes etapas de evolución por las que ha atravesado la misma hasta llegar a la actualidad.

Podríamos mencionar a las máquinas de cálculos más destacados:

1. LA MARK (1937-1944)

Donald Sanders menciona que esta máquina fue la realización del sueño de Babbage a la que se le llamo LA MARK I o ASCC (Automatic

[63] Idem. p. 11
[64] Ibidem, p.15
[65] Ulbarri Millan J. Manuel y otro, *Computación 6ª* ed. Sep México, 1988, p.18

Sequence Controlled Calculator) misma que fue construida a finales de los treinta y principios de los cuarenta. En la universidad de Harvard recibiendo el apoyo de la IBM. “Fue considerada como la primera computadora electromagnética automática. Tenía la capacidad de realizar largas secuencias de operaciones codificadas previamente, misma que registraba en una cinta de papel perforada y calculaba los resultados con la ayuda de las unidades de almacenamiento (memoria)”.[66]

La MARK I demostró la utilidad de los sistemas automáticos de tratamientos de la información y estuvo en servicio hasta 1959. La capacidad de las computadoras de esta clase (que muchos consideraban como cerebros artificiales) asombraba a los grandes de esta época. Sin embargo, hoy las podríamos recordar con ternura ya que su memoria era muy reducida si se les compara con los equipos actuales, incluso hasta con los más pequeños. “Otra limitación de su velocidad dependía del tiempo necesario para introducir las instrucciones mediante tarjetas o cintas perforadas y hasta su funcionamiento no era eternamente confiable”.[67] Esta computadora fue utilizada durante quince años para realizar cálculos astronómicos, ello en relación a la lentitud con que realizaba las operaciones y la limitada confiabilidad de los resultados obtenidos.

2. LA ENIAC (1943-1945)

“La primera calculadora electrónica de aplicación general fue construida en la Universidad de Pensilvania entre 1943 1945, bajo la dirección de John William Maunchly y John Presper Eckert, compuesta de miles de válvulas electrónicas e interruptores, aparte de bobinas resistencias

[66] Sanders Donald, Informática Presente y Futuro, 4ª ed. Ed. Mc Graw Hill, México, 1985, p.45.
[67] Idem., p.20

y condensadores. Necesitaba una central eléctrica propia y operaba sobre la base del sistema eléctrico decimal. Esta computadora recibió el nombre de ENIAC (Electronic Numerical Integrator and Computer). [68]

Para tener una imagen visual de la ENIAC es necesario recordar las computadoras que aparecen en los antiguos filmes de ficción científica: un armatoste muy costosa y de gran tamaño, a cuyo alrededor se juntaban de manera respetuosa, sabios y técnicos para vigilar su continuo funcionamiento.

Para hacer funcionar a la ENIAC era preciso enchufar cientos de clavijas y activar algunos interruptores, haciendo esto largo y tedioso el trabajo. Pese a esto esta computadora era capaz de realizar cinco mil operaciones por segundo, utilizándose principalmente para resolver problemas e balística y aeronáutica. Su mayor mérito, fue contar con una gran cantidad de componentes y trabajar de manera simultánea con ellos. “La desventaja era su tamaño (demasiado grande) y que su calentamiento era bastante rápido y alcanzaba una temperatura radicalmente elevada”.[69]

3. LA EDVAC (1945-1952)

A partir de 1945, Mauchly y Eckert desarrollaron una nueva máquina a la que llamaron EDVAC (Electronical Discrete Variable Automatic Computer), la cual era capaz de realizar operaciones aritméticas con números binarios y almacenar instrucciones internamente. La carrera de las computadoras iba cada vez más en ascenso por lo que no se podía detener y se tenía que lograr el gran avance de nuestros días.

[68] Rodríguez Gilberto. Revista e Computación. 17° ed. SEP. México, 1987. p.3
[69] Ibidem. p.4

4. LA UNIVAC (1951)

La compañía Renigton Red fundada por los mismos Ecker y Mauchly desarrollo la UNIVAC (Universal Automatic Computer) que fue la primera computadora de uso comercial, apareció en 1951.

“Entre su principales características se encuentran el uso de cinta magnética para la entrada y salida de datos, la capacidad de aceptar y procesar datos alfabéticos y numéricos, si como el uso de un programa especial capaz de traducir programas en un lenguaje particular a lenguaje de maquina”.[70]

Estas máquinas constituyeron la primera generación de computadoras. Eran demasiado voluminosas, utilizaban bulbos de vació, consumían mucha energía y producían mucho calor; no fueron tan confiables como se había esperado, eran rápidas pero no lo suficiente y tenían capacidad de almacenamiento interno pero limitado.

El siguiente avance tecnológico en la industria de las computadoras fue la sustitución de los bulbos por transistores que redujeron las deficiencias y mejoraron las ventajas ya existentes, introduciendo las memorias de ferrita que permitían reducir el tamaño dela computadora. Es así como surge la llamada segunda generación de computadoras.

En 1963 aparece en el mercado las computadoras de la tercera generación, cuya principal característica la constituía el uso de circuitos integrados monolíticos, que aumentaron considerablemente la velocidad de operación, incrementando de esta manera la confiabilidad de las mismas y disminuyeron su costo y tamaño.

[70] Levine Gutiérrez Guillermo, Ulibarri Milan. J. Manuel y otros. *Computación* P.18

A partir de la tercera generación, lo avances de la industria de la computación han sido tan numerosos y frecuentes que han hecho que el propio hombre deje de asombrarse y le parezcan “normales” dichos avances. Las computadoras han invadido todas las esferas de actividades en que pueda desarrollarse el hombre, tal es el caso de la industria, el comercio, la administración, la educación, el hogar, y llegando a adquirir tanta importancia que “actualmente se le considera la segunda industria más importante del mundo después de la automotriz, y no dudamos que llegue en un futuro no muy lejano a ser la primera en el mundo, inclusive por encima de la automotriz”. [71]

“Después aparece la cuarta generación, con integración a larga escala (LSI) y la aparición de microcircuitos integrados en plaquetas de silicio (chips) se tuvieron mejoras, en especial a nivel de la microprogramación”.[72]

Lo anterior, es solo una parte de la evolución de las computadoras, si embargo, el desarrollo computacional no se detiene aun, avanza cada vez más y no sabemos hasta dónde puede llegar.

Los actuales avances tecnológicos han logrado que las computadoras se conviertan en una de las fuerzas más poderosas dela sociedad actual, haciendo su uso posible tanto en organizaciones de todos tamaños como en los mismos hogares. Actualmente dichas maquinas constituyen la fuerza motriz dela revolución informática, la cual esta provocando serios cambios en los individuos, tanto de índole positivo como negativo, como lo son nuevas oportunidades de trabajo, mayor satisfacción en el trabajo y un aumento en la productividad, así como también la continua amenaza de desempleo, problemas físicos, psicológicos y problemas jurídicos.

[71] Op. cit. Téllez Valdez, Julio, P.19
[72] Idem.

De esta manera, las computadoras han adquirido tal importancia, que su uso forma parte de todo tipo de actividad. Tal es el caso e aquellas actividades que realizan las instituciones que forman parte de nuestro sistema financiero (como lo son instituciones de Crédito, Organizaciones Auxiliares de Crédito, Casas de Bolsas, etc.).

"Los orígenes de la informática se remontan a la cibernética, misma que tiene sus inicios en 1948, donde un notable personaje matemático originario de Estados Unidos de nombre Norbert Wiener, escribe un libro titulado "cibernética", en donde empleó este término con la finalidad de designar a la nueva ciencia de la comunicación y control entre el hombre y la maquina".[73]

Posteriormente, en el año de 1963, Hans Baade edita la obra Jurimetrics: the Methodology of Legal Inquiry, en la que especifica que para el desarrollo de esta materia se debían aplicar tres tipos distintos de investigación:
En primer lugar, aplicar modelos lógicos a normas jurídicas establecidas según los criterios tradicionales;
En segundo, aplicar el ordenador o computadora a la actividad Jurídica.
En tercero, llegar a prever futuras sentencias de los jueces.

La insatisfacción por los resultados concretos ofrecidos por la jurimetría y la presencia de instrumentos teóricos atractivos, como los ofrecidos por la cibernética teórica, hicieron que en Europa los estudios puramente empíricos se unieran con estudios de tipo puramente teórico, con el resultado de que, entre 1966 y 1969, con la denominación de cibernética y derecho. Se designaron, por ejemplo, tanto las encuestas de estadística judicial que recurrieran al ordenador, como los estudios de lógica formal aplicada al derecho; tanto los trabajos puramente computacionales que de

[73] Ibidem, p. 3.

alguna manera tuvieran que ver con normas jurídicas, como las investigaciones de filosofía del derecho que recurrieran a esquemas teóricos provenientes de la cibernética o de la teoría de la información.[74]

En el año de 1968 y después de estudiar un poco los fenómenos científicos que representaba la utilización de la computadora en el campo del derecho, Mario Losano propuso sustituir el término de "jurimetría" por el de "iuscibernética", y ante tal cambio, abandonar el esquema de la jurimetría y subdividir a la iusciber-nética en cuatro sectores correspondientes a cuatro modos distintos de acercarse a las relaciones entre derecho y cibernética.

La aparición de la cibernética obedeció principalmente a tres tipos de factores:

1. "Un factor social, ello porque los tiempos que se vivían entonces, requerían de una aumento a nivel de producción y consecuentemente de capital. Eran tiempos difíciles y por ello era necesario la aparición de una nueva ciencia que fuera más allá de una simple emergencia racional.
2. Un factor técnico científico, en virtud de que varias líneas de pensamiento, originadas en las distintas esferas de actividad, como lo eran la ciencia y la técnica, se empezaran a reunir, y así lograr avances y facilitar la interrelación que pudiera surgir entre ambas, con lo que se requeriría del surgimiento de una ciencia que regulara dicha interrelación.
3. Un factor histórico, por que surge de la necesidad del nacimiento de una ciencia de unión que controlara y vinculara a todas las demás."[75]

[74] Losano, Mario G., *Introducción a la Informática Jurídica*, España, Universidad de Palma de Mallorca, Facultad de Derecho, 1982, p.25.
[75] Ibidem, p. 4

De esta manera surge la TERCERA REVOLUCIÓN técnico científica que tuvo lugar a partir de los años setenta, siendo la micro eléctrica una ciencia primordial y que tenía como ramas dinámicas a la electrónica de información y redes de telecomunicaciones, dando lugar a que surgieran otras tecnologías emergentes; donde encontramos las nuevas fuentes de energía, como la biotecnología, biochips, optoelectrónica, mecatrónica, informática y biología molecular, las cuales son las nuevas ciencias que conformaran la cultura global.

Gracias a la TERCERA REVOLUCIÓN nos encontramos dentro de la llamada “sociedad de información”, donde se da en relación con la informática y las telecomunicaciones, mismas que erosionan nuestra sociedad advirtiendo que esta nueva sociedad traería transformaciones culturales, económicas y sociales, derivadas de las nuevas tecnologías, y que por tanto traerían el establecimiento de nuevos derechos y nuevos paradigmas tecno productivos.

ANTECEDENTES DE LA CIBERNÉTICA

La palabra cibernética fue utilizada por los griegos como arte de guiar o dirigir ciertos fenómenos.

El concepto de “cibernética” ha sido utilizado en diversas disciplinas que parten desde un estudio de carácter propiamente derivado de la ciencia política, hasta estudios con enfoques matemáticos.

Fue utilizado por primera vez en 1848 por el francés ampere en una clasificación de las ciencias políticas, ya que había creado un sistema para coordinar todo el conocimiento humano y había introducido el término “cibernética” para indicar el arte del gobierno entendiendo en sentido político.

Cibernética es el vocablo griego que indica el arte de gobierno, arte de guiar.[76]

Los estudios de Wiener fueron dirigidos en forma matemática al estudio del comportamiento humano visto y representado en una máquina; esto es, por un lado, la identidad de los mecanismos de control y regulación tanto en los hombres y en los animales como en las máquinas, y por el otro, la conexión entre estos mecanismos y la transmisión de informaciones.

En 1940 Robert Wiener realizo trabajos matemáticos de carácter estadístico aplicados durante la segunda guerra mundial.

La cibernética se considera como aquella ciencia que pretende abarcar la comunicación y el control en cualquier campo de estudio.

Ahora bien, entendiendo a la cibernética como la ciencia de la comunicación y el control, surge la informática, de una inquietud racional del hombre, el cual, ante la cada vez más creciente necesidad de la información para una adecuada toma de decisiones, es impulsado a formular nuevos postulados y a desarrollar nuevas técnicas que satisfagan dichos propósitos.

A lo largo de la historia, el mundo ha sufrido distintas revoluciones tecnológicas relacionadas con la información, mismas que han repercutido y modificado tanto la economía como la sociedad misma.

Sin embargo, pese a las múltiples revoluciones tecnológicas que se han presentado, estas no se han detenido, por lo que actualmente estamos ante una nueva revolución tecnológica. “la informática, junto con sus micros, minis y macro computadoras ,los bancos de datos, las unidades de

[76] Ibidem, p.35.

tratamiento y almacenamiento, la telemática, etc. están transformando de manera indudable nuestro mundo".[77]

Con el avance y perfeccionamiento de la ciencia y la tecnología se ha visto el rápido crecimiento de los medios masivos de comunicación, que a la fecha se han desarrollado múltiples medios que facilitan la comunicación y difusión de información, esto se presentó desde la imprenta, la radio, la televisión y ahora contamos con equipos con mayor poder de difusión de la información, como lo son las computadoras, los medios satelitales y la telemática, con lo cual se da lugar a la proliferación de mensajes, mismos que hoy en día ya son un problema de sobrecarga de información.

El avance tecnológico desarrolla una nueva forma de integrar a la sociedad con el aspecto político y laboral pues en los últimos años el escenario mundial se ha visto impactado por un cambio tecnológico profundo que se desarrolla en una nueva forma de concebir y practicar la producción la cual es conocida como la revolución de la microelectrónica.

La tecnología electro informática se ha desarrollado mediante un proceso de confrontación en el que las innovaciones se concentran en la transformación de la maquinaria de bases electromecánicas hacia las de base electrónica, primero analógica y luego digital. En este periodo hubo despidos de personal porque la maquinaria incorporo sistemas de control automático de muchas funciones incluyendo la auto supervisión.

[77] Op. cit. Téllez Valdés, Julio, p.5

INTERNET

La Internet es una red de computadoras conectadas entre sí. Esta red permite el intercambio de información. A fin de poder intercambiar información entre diferentes computadoras ubicadas en distintas partes del mundo se utiliza un lenguaje común a todas las máquinas. Este lenguaje se conoce como protocolo.[78]

Es el instrumento idóneo que proporciona la información a un bajo costo y de acceso masivo, al cual lo podemos definir como:

"El conjunto de servidores de archivos distribuidos en todo el mundo interconectados mediante un sistema maestro de redes de computo".[79]

Hoy lo más impactante en cuanto a este tema, es como la información ha permitido que desaparezcan las fronteras; basta analizar como el flujo de datos transfronterizos permite derribar las fronteras internacionales.

A su vez, este intercambio de información crea un universo virtual, diferente del universo físico conocido. Este espacio universal o ciberespacio no tiene la localización fija, esto es, no se puede ubicar el lugar en donde se asienta.

Una de las características de este ciberespacio es que está formado por información contenida en medios electrónicos de almacenamiento y que estos medios de almacenamiento son de orden físico, por lo que en última instancia esa información esa ubicada en cierto lugar físico territorial, pero puede ser accedida desde cualquier parte del mundo.

---

[78] Barriuso Ruiz, Carlos, *La contratación electrónica*, Madrid, Dykison, S.L., 2002, p. 37.
[79] Rojas Amandi, Víctor Manuel, *El uso de internet en el derecho* ed. Oxford p.1

Dentro del ciberespacio o del espacio virtual, es decir dentro de la red, existen diferentes métodos de comunicación, cada uno de ellos acorde con una finalidad. Así tenemos el mail que funciona como un correo tradicional, el ftp que funciona como el sistema de intercambio de libros de la biblioteca. Existe uno de estos servicios que ha cobrado más fuerza que los demás y es el servicio web, consiste en una "página" en la que se coloca cierto tipo de información sobre algún tema en particular. El servicio funciona como un tabloide de anuncios o como un sistema de reparto de propaganda.[80]

El Internet como vehículo no tan sólo de la información, sino de medios para llevar a cabo actos de comercio como compras, rentas, arrendamientos, etcétera, ha propiciado una revolución en el mundo entero, de ahí que haya sido comparado al tercer movimiento de cambio de la humanidad, los dos primeros fueron el manejo de la agricultura y el segundo la revolución industrial; por ello se le ha considerado un prodigio para el desarrollo de un gran número de actividades del ser humano, visto de este modo se podría estimar que nada de malo tiene un bien accesible a la humanidad a través de corriente eléctrica y un equipo pc de bajo costo, aunque actualmente hay tantas innovaciones tecnológicas que el Internet corre incluso a través del teléfono celular; sin embargo.

El Internet también representa un gran reto y problema, nos referimos a que ha sido utilizado cono vehículo para llevar a cabo conductas que han propiciado en el menor de los daños intromisión a la privacidad de las comunicaciones, y en otras situaciones han causado graves daños al patrimonio de las personas e incluso también ha dado pauta, a que individuos conformen bandas de delincuencia organizada que por su nivel de tecnificación han llevado a cabo conductas graves.

---

[80] Zabale, Ezequiel, *La competencia en materia de acciones civiles o penales derivadas del uso de la red Internet*, Derechos Informáticos, Argentina, 2002, pp. 121-131.

Este fenómeno que tomó por sorpresa a muchos gobiernos, y que a pesar de los intentos por lograr un consenso entre los diversos países a fin de tipificar los delitos informáticos ha sido lento en comparación con las actividades delictivas, lo que ha propiciado que a los esfuerzos de los diversos Estados, se sumen incluso acciones de instituciones particulares para tratar de agilizar y controlar mejor el flujo de la información, así como restringir en la medida de lo posible las conductas delictivas a través de mecanismos tecnológicos.

ANTECEDENTES DEL INTERNET.

Es preciso abordar lo relativo los antecedentes del internet, el cual se desarrolló como medio de comunicación durante de la Guerra Fría, ya que nace como un proyecto militar de los Estados Unidos de Norteamérica financiado por la Agencia de Proyectos de Investigación Avanzada (*Advanced Research Projets Agency, ARPA*), creada en 1957 por el Departamento de dicho país.

Con este proyecto se buscaba la transmisión de información por medios alternativos a los existentes en ese momento, de manera tal que no existiese un único centro neurálgico que causara un colapso en la organización defensiva en el supuesto de que el enemigo lo destruyese. La descentralización y la inexistencia de jerarquía servían para que no hubiera centros que hipotecasen el funcionamiento de todo el conjunto, incluso ante una agresión nuclear. Así las cosas, se creó una red interconectada entre equipos informáticos que se mantendría operativa aunque grandes partes de la misma resultaran dañadas por un ataque.

De esta manera fue como se creó el “internet”, primeramente para satisfacer las necesidades del ministro de defensa de los Estados Unidos De América, ya que se necesitaba una red que no fuera dependiente de una

sola computadora central, ya que un ataque a la misma significaría la caída de toda la red.

Por lo que a partir de 1960 empezó a desarrollarse un sistema de red que no dependiera de un servidor, sino que cada computadora funcionara de manera independiente de las otras, al cual lo denominaron *ARPANET.*

Para el funcionamiento del sistema *ARPANET* fue necesario construir procesadores especiales, los cuales fueron puestos en funcionamiento en el año de 1969 por la universidad de *(UCLA)* en los Ángeles California, la cual comenzó a intercambiar paquetes de datos a larga distancia con la universidad de Utah en Salt Lake City, por lo cual científicos y profesores de Estados Unidos de América comenzaron a considerar la posibilidad de transmitir mensajes electrónicas mediante la red para participar en el desarrollo de proyectos científicos.

En 1971 Ray Tomlinson realizó el programa de correo electrónico para Arpanet, que se prueba con éxito ese mismo año.

Tomlinson primero diseñó un sistema de mensajería para depositar notas en una misma máquina. Después realizó transmisiones de una máquina a otra. En 1973 se iniciaron las primeras conexiones internacionales entre equipos informáticos.

La investigación universitaria cobra importancia a finales de los setenta del siglo XX, poniéndose de manifiesto la utilidad de la Red para fines civiles. Con la intención de resolver los problemas de saturación y lentitud que nacían del incremento de los usuarios, se crea el protocolo IP y, más adelante, el protocolo TCP, que se siguen utilizando en la actualidad.

En el año de 1980 Internet se separó de *ARPANET* de tal forma que se desligó de los objetivos militares y se expandió de una manera más rápida, lo cual permitió que instituciones científicas tanto estadounidenses como extranjeras se enlazaran a internet.

La aparición del PC de IBM, en 1981, y del Macintosh de Apple, en 1984, es un importante paso para abrir la Red a los hogares y sentar las bases de la generalización de su uso. El fenómeno informático se expande y llega a las masas. También en 1984 se introduce el aludido "sistema de nombres de dominio" o DNS.

En 1986, se fundó la NSFNET, financiada por el gobierno federal estadounidense, la cual creo diferentes líneas de enlace para internet, a las que se denominó backbones, con las que se facilitaba la trasferencia de datos. A partir de entonces, internet inicio su expansión hacia el exterior de Estados Unidos de América, sobre todo hacia Europa.[81]

ANTECEDENTES DEL INTERNET EN MÉXICO

En 1991, tras la colaboración inicial entre las dos principales instituciones académicas que trabajaron para difundir y establecer más enlaces de Internet en México, la Universidad Nacional Autónoma de México, el Instituto Tecnológico y de Estudios Superiores de Monterrey, el Consejo Nacional de Ciencia y Tecnología, a instancias de la National Science Foundation, se propuso establecer un comité llamado Red Académica Mexicana (RAM) a fin de que las tareas de mantenimiento y expansión se dividieran entre el Centro de Investigación Científica y de Educación Superior de Ensenada, la UNAM y el Tecnológico de Monterrey. A la par, la compañía telefónica Telmex, que ya había comenzado a instalar redes de fibra óptica

[81] Op. cit. Rojas Amandi, Victor Manuel, p.3

en poblaciones urbanas, obtuvo los primeros grandes logros en velocidad de redes

En ese momento el ITESM, a través de uno de sus directivos, había sido nombrado grupo técnico de la RAM. Con ese grupo técnico se acordaron las reuniones para formalizar la constitución de la RAM: la primera se hizo en la ciudad de México, la segunda en Ensenada, la tercera en Saltillo y la cuarta en Monterrey; en esta última se decidió fundar una asociación de universidades cuyo nombre sería Red Académica Mexicana.

Sin embargo, al mismo tiempo se estaba formando un organismo con el nombre de RedMEX, asociación civil constituida por la academia donde se discutirían por vez primera las políticas, estatutos y procedimientos que habrían de guiar la organización de la red de comunicación de datos en México.

Dado que por desacuerdos interinstitucionales no pudo establecerse bajo el nombre de RedMEX, el 20 de enero de 1992 en la Universidad de Guadalajara se obtuvo la formación de MEXNET, luego de meses de correspondencia y acuerdos postergados; esta asociación civil tendría los mismos objetivos que los del proyecto previo. MEXNET fue integrada por los siguientes institutos: Instituto Tecnológico de Estudios Superiores de Monterrey, Universidad de Guadalajara, Universidad de las Américas, Instituto Tecnológico de Estudios Superiores de Occidente, Colegio de Posgraduados, Laboratorio Nacional de Informática Avanzada (en Jalapa, Veracruz), Centro de Investigación en Química Aplicada (en Saltillo, Coahuila), Universidad de Guanajuato, Universidad Veracruzana, Instituto de Ecología, Universidad Iberoamericana y el Instituto Tecnológico de Mexicali.

La UNAM no se integró a MEXNET, lo que evidenció la existencia de tres diferentes proyectos de trabajo, pero también la percepción de que Internet

crecería en México bajo tres proyectos distintos y, en ocasiones, irreconciliables: por un lado la Red de la UNAM, que para 1992 representaba el segmento mayor por la extensión que cubrían sus campus; por otro MEXNET, representado por las universidades con conexiones independientes y por el Tecnológico de Monterrey y las universidades que se conectaban a través suyo; y por último RUTYC (Red de Universidades Técnicas y Centros), donde se encontraban congregadas las universidades públicas de la SEP, la Universidad de Guanajuato y el Instituto Politécnico Nacional, en total 35 universidades públicas del país. RUTYC se desintegraría al año siguiente, en 1993.

En 1992 se inauguró la Red Integral de Telecomunicaciones de la UNAM, la cual interconectó a 90% de la población universitaria en 96 centros, a través de 31 nodos unidos por 500km de fibra óptica, 12 enlaces satelitales y 8 estaciones terrestres de microondas.

En 1993 la Universidad de las Américas creó la primera página web; (Gutiérrez y López, 1998) a partir del mismo año la información sobre Internet cobró mayor presencia en los medios de comunicación colectiva, incrustada específicamente en las secciones financieras de algunos diarios y en revistas especializadas. Sin embargo, todavía más importante fue este año por la conexión del CONACyT y del ITAM a Internet a través de un enlace satelital directo al Centro Nacional de Investigación Atmosférica (National Centre of Atmospheric Research, NCAR) en Boulder, Colorado; Con ese enlace CONACyT estableció su propia red, a la cual denominó Red Total CONACyT.

Al año siguiente, 1994, el uso de la red comenzó a diversificarse, pues hasta ese momento las universidades fungieron como únicos proveedores de acceso a Internet. En primer lugar, el Consejo Nacional de Ciencia y Tecnología, que un año antes se había conectado directamente a la red

mediante satélite, se unió a la asociación MEXNET y formaron juntos la Red Tecnológica Nacional (RTN).

En 1994 la reunión de la Asociación Nacional de Universidades e Institutos de Educación Superior (ANUIES) dio pie a la formación de una “red dorsal de cómputo”, cuya función sería integrar a todas las universidades del país, así como formar una asociación civil encargada de consolidar, operar y administrar esa red.

En 1995 la red de la UNAM tenía dos salidas a Estados Unidos, específicamente a Houston, una de las cuales se dirigía hacia la Rice University. Por las características de la infraestructura que ofrecía la red de la universidad, fortalecida con los enlaces directos a Internet, y dada la reunión de las redes académicas más importantes en la RTN, a partir de ese año y durante el siguiente fue posible crear un *backbone* o salida principal a Internet de carácter nacional.

En la misma tesitura comercial, ese año se observó un mayor interés en el registro de dominios comerciales bajo los sufijos “.com.mx”, incremento fomentado, entre otros factores, por la consolidación mundial de uno de los servicios o herramientas de Internet, la World Wide Web o WWW. El 10 de octubre de 1995, el número de dominios mexicanos comerciales alcanzó la cifra de 100, superando en 15 los dominios de instituciones educativas. Para entonces el total de dominios registrados bajo “.mx” era de 211, de acuerdo con el Centro de Información de la Red en México o NIC-México. El hecho definió el inicio de una etapa distinta del desarrollo de la red en México y en el mundo: la incursión de los proveedores comerciales de acceso y de las empresas nacionales y transnacionales en el control de los mercados emergentes de Internet.

En 1996, surgió también la representación mexicana de la Internet organización internacional no gubernamental y no lucrativa creada en 1992, con los propósitos de establecer relaciones de cooperación y coordinación con la instancia responsable de los estándares y direcciones de Internet en el mundo; incorporarse al estudio y divulgación del desarrollo de la red en diferentes regiones; y conocer las regulaciones sobre el aspecto técnico del crecimiento de la red.[82]

ANTECEDENTES DEL DERECHO A LA INFORMACIÓN

El derecho a la información nace de la necesidad que tenemos los seres humanos dentro de una sociedad de estar informados de lo que sucede en nuestro entorno no solo municipal, local, o internacional, también en los aspectos económicos, políticos y sociales. Este derecho se concibe como una garantía constitucional consagrada en el artículo sexto y como derecho social establecido en el artículo 41 fracción I, segundo párrafo que a la letra dice: "por tanto tendrán derecho al uso en forma permanente de los medios de comunicación social, de acuerdo con las formas y procedimientos que establezca la misma"[83]

Como bien se señala el derecho a la información se ha adquirido con el transcurso del tiempo desde los inicios de nuestra época, el hombre había luchados por adquirir ese derecho el cual hasta nuestros días se considera un derecho universal, el cual trae aparejado diversos factores positivos y negativos para la sociedad.

El artículo 13 de la Convención Americana sobre Derechos Humanos conocido como pacto de San José de Costa Rica suscrita el 22 de noviembre de 1969 y ratificada por la ley Nº 15.737 de 8 de marzo de 1985, dice: "Toda

82 http://www.revista.unam.mx/vol.4/num4/art7/ago_art7.pdf (última consulta 3 de diciembre 2012)

83 Op. cit. Flores Salgado, Lucerito, p. 16

persona tiene derecho a libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir información e ideas de toda índole sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".[84]

SOCIEDAD DE LA INFORMACIÓN

Así como la tecnología avanza cada día más, nos enfrentamos a una verdadera revolución tecnológica, distinta a la revolución industrial, pues esta fue liberadora de trabajos y rutinas de orden físico, mientras que la tecnología es liberadora del intelecto, pues hoy el manejo de la información por medios automatizados marca a las sociedades como sociedades de la información, mismas que implican el uso masivo de tecnologías de la información y comunicación para difundir el conocimiento e intercambio en una sociedad.

Se advierte sobre un nuevo tipo de sociedad que surge por las transformaciones sociales a las que da lugar la tecnología, pues la sociedad ha cambiado al generalizarse el uso de la información a bajo costo, el almacenamiento de datos, y nuevas tecnologías de transmisión, donde la materia prima es la información.

Se cree que la llamada sociedad de información también es una sociedad de aprendizaje, pues el avanzar conforme lo hace la tecnología implica no conformarse con la educación tradicional o el poco conocimiento que se pueda adquirir, sino que comprende la adquisición de conocimientos actuales para poder enfrentar la cambiante tecnología que es un fenómeno mundial y constantemente inestable.

[84] Castrillón y Luna, Víctor Manuel, *La Protección Constitucional de los Derechos Humanos*. Ed. Porrua Mexico 2006, p. 77 y 130

La digitalización y la automatización han provocado una profunda revolución, caracterizada especialmente por la aparición de dispositivos multimedia y por una expansión espectacular de las redes telemáticas. Los sistemas expertos y la inteligencia artificial aumentan vertiginosamente la interactividad. La velocidad de procesamiento de la información crece constantemente, así como la capacidad casi ilimitada de almacenamiento.

En cualquier caso, no es posible entender la configuración de esta sociedad sin la influencia de la información. "Esta revolución tecnológica constituye a todas luces un elemento esencial para entender nuestra sociedad, en la medida que crea nuevas formas de socialización, e incluso nuevas definiciones de identidad individual y colectiva"[85]

Una sociedad de la información es aquella en la cual la tecnología nos facilita la creación, manipulación y distribución de la información, y que hoy en día juegan un papel muy importante a nivel social, cultural y económico. La existencia de lo que llamamos sociedad de información ha sido inspirada por los programar de desarrollo de países industrializados, que trae consigo una serie de disposiciones de acontecimientos desde años atrás hasta la modernidad.

En realidad, la sociedad de la información no existe más que en la imaginación de los utópicos tecnológicos, sin embargo Julio Téllez Valdez define a la sociedad de la información como: "el usos masivo de tecnologías de la información y comunicación para difundir el conocimiento e intercambio de la sociedad".[86]

[85] UNESCO Organización de las Naciones Unidas para la educación, la Ciencia y la Cultura http://www.unesco.org/new/es/
[86] Op. Cit. Téllez Valdés, Julio. Pág. 6.

Los beneficios que ha traído la informática y la Internet en el mundo han cambiado la vida alrededor del mundo en todas sus ciencias, aun como en la sociedad, en los gobiernos y en la forma de como ver la vida, por lo que la ONU junto con la Unión Internacional de Telecomunicaciones convocaron en Túnez la Cumbre Mundial de la Sociedad de la Información, siendo los participantes los miembros de las Naciones Unidas, empresas privadas y la sociedad civil, siendo el principal punto a discutir la eliminación de la brecha digital existente en el acceso a las nuevas tecnologías en el mundo con el fin de alcanzar beneficios a cada persona en cualquier parte del mundo.

Además de este importante hecho la Unión Europea, preocupada por hacer accesible las nuevas tecnologías informáticas a cada uno de sus países miembros se emitieron las Directivas 98/34/CE de 22 de junio y 98/48/CE de 20 de julio de 1998 del Parlamento Europeo y del Consejo[87].

las cuales tenían el objeto de eliminar en lo posible o de reducir los obstáculos en el intercambio comercial de productos industriales, agrícolas y pesqueros, así como la libre prestación de servicios de la sociedad de la información dentro de la Unión con la implementación de cada país miembro de reglamentos o leyes tendientes a crear mecanismos de comunicación y transparencia entre Estados, o el público.

Tiempo después se emitió la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de Junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información en particular el comercio electrónico en el mercado interior, la cual surge para regular determinados aspectos del comercio electrónico llevado entre los países

[87] Eur-LEx, Directiva 93/34CE. http: //eur-lex.europa.eu/ LexUriServ/ site/ es/ oj/ 1998/l_204/ l_20419980721es00370048. Consultada el 28 de mayo de 2013.

miembros de la Unión Europea, desprendida de las anteriores directivas sobre la Sociedad de la Información.[88]

Entre los Estados miembros de la Unión Europea que han adoptado seguir esta Directiva se presenta España, emitiendo la Ley de Servicios de la Sociedad de la Informática y del Comercio Electrónico o Ley 34/2002 de 11 de julio de 2002, la cual en su Artículo 1º, de esta Ley determina el objeto de la regulación del régimen jurídico de los servidores de la sociedad de la información y de la contratación por vía electrónica, y a las obligaciones de los prestadores de servicios intermediarios en la prestación de contenido de la información en las redes de telecomunicaciones.[89]

SEGURIDAD, DERECHO A LA INTIMIDAD Y PROPIEDAD INTELECTUAL

Las implicaciones políticas, sociales, y legislativas de la seguridad son abrumadoras. Las reacciones de los gobiernos ante las necesidades de seguridad por parte de sus ciudadanos en las comunicaciones de datos varían desde la postura del ejecutivo francés que prohíbe cualquier transmisión codificada a no ser que el gobierno tenga todas las claves empleadas, a las mostradas por la administración estadounidense, la cual permite esquemas criptográficos siempre y cuando se asegure la posibilidad tecnológica de romperlos por orden judicial.[90]

[88] Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de Junio de 2000, www.mityc.es/NR/rdonlyres/ 62C8DF55-516E-4294-90A2-69F754C8AAE0/0/3Directiva_2000_31_CE.pdf. Consultada el 28 de mayo de 2013.

[89] Área del Derecho civil de la Universidad de Girona, España. http://civil.udg.es/normacivil/estatal/contract/LSSI.htm

[90] Op. Cit. Flores Salgado, Lucerito, p. 88

ANTECEDENTES DE LOS DELITOS INFORMÁTICOS

La primera propuesta de legislar con este respecto, se presentó en los Estados Unidos de Norteamérica en 1977 por el senador Ribicoff en el Congreso Federal.[91]

Durante la década de los setenta, la difusión de los ordenadores en el mundo empresarial supuso que la mayoría de las manifestaciones de la delincuencia informática tuviesen relación con la delincuencia económica, siendo las más comunes el fraude informático, la manipulación de datos, sabotajes informáticos, espionajes empresariales, etc. Hasta el punto de que en este periodo eran estas nuevas modalidades de delincuencia económica las que integraban el concepto de delito informático; o, al menos, éstas eran las principales manifestaciones del mismo.

En los años ochenta, la generalización de los ordenadores personales entre la población trajo consigo, al mismo tiempo, el surgimiento de la piratería del *software* de los mismos, dando comienzo así a las primeras infracciones contra la propiedad intelectual que se generalizarían a finales de los años noventa, extendiéndose además de a dicho *software*, a productos como música o películas.

La expansión de Internet en la década de los noventa llevó aparejado el surgimiento de un nuevo método para difundir contenidos ilegales o dañosos, tales como pornografía infantil o discursos racistas o xenófobos. Serán justamente las conductas vinculadas a la difusión de contenidos ilícitos las que más pueden aprovecharse de la enorme implantación que tiene la Red a nivel mundial, así como de sus características técnicas que dificultan su descubrimiento, persecución y prueba.

[91] Op. Cit. López Betancourt, Eduardo, p. 274.

En este período también se consolida la dependencia que los gobiernos y organismos internacionales tienen de los sistemas informáticos, tanto para su buen funcionamiento como para el almacenamiento de datos importantes y/o secretos y ello pondrá en el punto de mira para la comisión de delitos que atenten contra la seguridad del Estado, como la comisión de ataques terroristas a través de la Red, a los sistemas informáticos de estos Entes.

LOS DIEZ GRANDES HACKERS DE LA HISTORIA

10- David L. Smith

David L. Smith es el autor del famoso “Gusano Melissa” responsable del cierre y sobrecarga de los servidores de los correos electrónicos en el 1999, este hacker fue arrestado y condenado a 10 años de prisión en el 2002 fue el responsable de la pérdida de 80 millones de dólares.

La pena se le redujo a 20 meses $50000 y un acuerdo de trabajar 40 horas a la semana para el FBI para delatar a nuevos autores de virus nuevos y vulnerabilidad de softwares.

9- Robert Morris

Es hijo del científico jefe de la Seguridad Nacional de Informática de los EEUU y fue el responsable de crear un virus que llego afectar a unos 6,000 equipos.

Cuando lo descubrieron, Morris fue la primera persona acusada de hackear la red, fue declarado culpable en el 1990 por la Ley de Fraude y Abuso de los EEUU, aunque no cumplió la sentencia, y actualmente es considerado el maestro de los creadores de malware y trabaja como profesor titular en el Artificial Intelligence Laboratory del MIT.

8-Kevin Poulsen

Pirata informático llamado Dark Dante, su principal logro fue en 1990, cuando Poulsen intercepto todas las líneas de teléfono de la estación de radio KIIS-FM, y de esta forma poder ganar un concurso celebrado por esta emisora de radio en California. El premio era un Porche 944 S2 para el oyente que hiciera la llamada numero 102. Poulsen aseguró su coche, pero pasó 51 meses en prisión. En la actualidad es director del sitio web de Security Focus y el editor de Wired.

No todo los trabajos de este hacker han sido para su beneficios, con su ayuda en el 2006 en las redes sociales como MySpace se identificaron y detuvieron pedófilos que solicitaban sexo a menores de edad.

7-Onel de Guzmán

Creador del Virus “I love You” este filipino que envió este virus por correo por puro despecho ya que su obra fue rechazada en la facultad.

El virus I Love You fue enviado a más 84 millones de personas con pérdida de unos 8.7 millones, este virus entraba a los ordenadores como un archivo adjunto y al ejecutarse se reenvía a todos los contactos de la victima de manera automática infectando también a los archivos del computador.

6- Vladimir Levin

Bioquímico y matemático ruso quien dejo la ciencia para dedicarse al asalto de sistemas Informáticos de entidades como Citibank, accediendo a las redes bancarias hacia transferencias de cuentas a los clientes y llego a desviar unos 3.7 millones de dólares a diferentes cuentas y países, fue detenido en 1995 por la Interpol.

5-Jon Lech Johansen

Jon Lech Johansen también conocido como DVD Jon, a este lo ponemos aquí porque a sus solo 15 años se las arregló para eludir la protección

incorporada en los DVD comerciales, sus padres fueron demandados por el ya que era menor de edad, no fue hallado culpable de ningún comportamiento ilegal, después en el 2003 libero un programa usado para cifrar contenido de la música distribuidos por iTunes el libero QT Fair Use, 2004 libero otro programa DeDRMS también para la prohibición de copias y FairKey, también este año libero un programa que permite a los usuarios de Linux utilizar archivos de microsoft.

Hackeo la protección del Blu-ray y el iPhone, el sigue trabajando para romper los sistemas de anti-copia.

4-Jonathan James

Fue el primer adolescente arrestado por delitos informáticos en los EEUU en 1999.

Jonathan James o “comrade” como era conocido fue un cracker (Black Hat), entro ilegalmente a la NASA y robos unos software y a las computadoras del Departamento de Defensa (agencia encargada para reducir amenazas de armas nucleares, biológicas y convencionales) de los EEUU.

Es para muchos su suicido un misterio, después de haberse quitado la vida su padre publico una carta de 5 páginas que dejo donde el acusaba al gobierno federal de estarlo acusando falsamente de encabezar un grupo que robaba identidades vía Internet de sitios como Office Max. Dice en su carta que no esperaba recibir ningún trato justo por parte de las autoridades ya que estas necesitaban un “chivo expiatorio”.

3-Raphael Gray

Raphael Gray alias Curador a sus 19 años hackeo los sistemas informáticos de todo el mundo robo 23 000 números de tarjetas de créditos, entre ellas la de Bill Gates (a quien le envió viagra a domicilio). Con los datos de las tarjetas

de créditos robadas creo las páginas web “creafreecreditcards.com” y “ecrackers.com” donde publico toda la información. EL FBI lo visito en marzo del 1999 su sentencia fueron dos años con libertad condicional y 36 meses de tratamiento psiquiátrico.

2-Adrian Lamo

El estadounidense de 30 años se convirtió en el más famoso “hacker de sombrero gris” de la última década. En 2003, invadió el sistema de The New York Times acaba de salir en la lista de contribuyentes. También es conocido por romper una serie de sistemas de alta seguridad para la red informática, como Microsoft, Yahoo, MCI WorldCom, Excite @ Home, y las empresas de telefonía SBC Ameritech y Cingular.

1-Mitnick

El hacker crackers y phreakers más famoso de la historia. En 1990, Mitnick o Condor como se hacía llamar rompió varios ordenadores, operadores de telecomunicaciones y proveedores de servicios de Internet, y de engañar al FBI y convertirse en uno de los delincuentes cibernéticos más buscados en Internet (esa historia incluso ha convertido en una película). En 1995 fue arrestado cinco años después de ser puesto en libertad bajo fianza, pero los primeros tres años de libertad no puede conectarse a Internet. En la actualidad, Mitnick es consultor en seguridad digital mitnicksecurity.com.[92]

Una vez que se presentaron estos acontecimientos diversos países comenzaron a crear leyes específicas en materia de delitos informáticos, de los cuales podemos señalar:

[92] www.taringa.net/posts/info/9270756/Los-10-hackers-mas-famosos.html, consultada, el 03 de abril de 2013.

ESTADOS UNIDOS

Estados Unidos, ha sido el ejemplo a seguir cuando se trata de diversificación de leyes. Cada estado cuenta con su propia legislación en diversas áreas, sin embargo, podremos observar que, a pesar de este aspecto tan característico del sistema federal, cuando sucedió un evento como el de los atentados a las torres gemelas en Nueva York, se optó por federalizar el tratamiento a las conductas realizadas a través de medios informáticos.[93]

Este país adopto en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modifico el acta de fraude y abuso computacional de 1986.

La ley de 1994 diferencia al tratamiento de los que de manera temeraria lanzan ataques de virus a aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles para el tratamiento de quienes crean virus:

α) Para los que intencionalmente causan daño por la transmisión de un virus, el castigo de hasta diez años de prisión más una multa.

β) Para los que transmiten solo de manera imprudencial, la sanción fluctúa entre una multa y un año de prisión.

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma que se realicen. Al diferenciar los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

ALEMANIA

En Alemania la denominada segunda ley para la lucha contra la ciber criminalidad económica de 15 de Mayo de 1986, relaciona una variada gama de hechos punibles cometidos con medios electromagnéticos o informáticos o de la información como bien jurídico u objeto material de los mismos,

[93] Nava Garcés, Alberto, *Delitos Informáticos*, México, Porrúa, 2007, p. 130.

acorde con la realidad tecnológica. En esta relación punitiva observamos los delitos contra los datos o las informaciones, a diferencia de la legislación canadiense donde se destacan los delitos de los datos contra otro bien jurídico como la intimidad. La legislación española como veremos prevé una y otra clasificación.

Las formas típicas del derecho alemán son:

- Espionaje de datos (arts. 202 a);
- Estafa informática (263 a)
- Utilización abusiva de cheques o tarjetas de crédito (266);
- Falsificación de datos con valor probatorio (269);
- Engaño en el trafico jurídico mediante elaboración de datos (270);
- Falsedad ideológica (271);
- Uso de documentos falsos (273);
- Destrucción de datos (303);
- Sabotaje informático (303);[94]

FRANCIA

En enero de 1988 esta país dicto la ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por intromisión fraudulenta que suprima o modifique datos:
Así mimo esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de los terceros que haya impedido o alterado el funcionamiento de un sistema automatizado de datos. Por su parte, el artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de vulnerar los derechos de terceros, en forma directa o indirecta, haya introducido datos a un sistema de procesamiento automatizado o haya suprimido o modificado los datos que este contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena al mero acceso agravando la pena cuando resultare la supresión o modificación de

[94] Ibidem, p. 109.

datos contenidos en el sistema, o bien en la alteración del funcionamiento de éste (sabotaje). [95]

ESPANA

El artículo 264-2, del *Nuevo Código Penal Español,* establece que se aplicara la pena de prisión de uno a tres años multa…. A quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Este código sanciona en forma detallada esta categoría delictiva (violación de secretos/espionaje/divulgación), aplicando pena de prisión y multa, agravándolas cuando existe intensión dolosa y cuando el hecho es cometido por parte de funcionarios públicos se castiga con la inhabilitación.[96]

AUSTRIA

La ley de reforma del código penal, promulgada el 22 de diciembre de 1987, en el artículo 148, sanciona aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de la elaboración automática de datos, a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además completa sanciones para quienes cometen este hecho utilizando su profesión de especialista en sistemas.

[95] Op. Cit. Téllez Valdés, Julio, p.178
[96] Idem.

GRAN BRETAÑA

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no de alterar datos informáticos es penado hasta con cinco años de prisión o multa.
Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esta categoría.

El liberar tiene penas desde un mes a cinco años, dependiendo del daño que causen.

HOLANDA

En marzo de 1993 entro en vigencia la ley de los delitos informáticos, en la cual se penaliza el hacking, el phreaking (uso de servicios de telecomunicaciones para evitar el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superara el mes de prisión; pero si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.[97]

[97] Idem.

CONCLUSIONES SEGUNDO CAPITULO

La informática es una de las ciencias que mayor desarrollo y evolución ha tenido en los últimos tiempos, la vida moderna que tenemos hoy en día sería muy difícil de imaginar al no tener a nuestro alcance la tecnología con la que hoy contamos.

Dentro de este capítulo pudimos observar y analizar cómo es que ha ido evolucionando la informática a través del paso del tiempo, desde máquinas de cálculo hasta llegar a las computadoras que hoy en día conocemos; Sería sumamente difícil encontrar en nuestra historia otro evolución más rápida e importante que la de la tecnología, de esta manera las computadoras han sido de vital importancia para los seres humanos, ya que el uso de las mismas forma parte fundamental de nuestras vidas y actividades diarias.

Derivado de la evolución de la tecnología se da a lo que hoy conocemos como informática, la cual tiene sus inicios desde el año de 1948, y cuya finalidad primordial fue designar un nombre a una nueva ciencia entre el ser humano, la tecnología y la máquina.

Posterior a esto se da entrada a nuevas tecnologías lo que nos lleva a “una sociedad de información” donde se da la relación entre la informática y las telecomunicaciones lo cual traería consigo una importante transformación en el mundo de la informática y la cibernética.

El internet es uno de los más importantes avances en el mundo de la cibernética ya que es la red de redes que hoy en día todos conocemos y sobre todo que se traduce en un avance a nivel mundial como un sistema gigante cuyo fin es globalizar la información y que la misma se encuentre al alcance de cualquiera que la quiera obtener.

Siendo el internet uno de los medios de comunicación más utilizados en todo el mundo, nuestro país no ha sido la excepción en el uso del internet y de las nuevas tecnologías que hoy en día tenemos a nuestro alcance y pese a que todavía no ha llegado a todos los rincones de nuestro país y que en nuestro país todavía falta mucho por avanzar en el ámbito de la tecnología es de suma importancia que vayamos conociendo y difundiendo el uso adecuado del internet y vayamos educándonos a hacer uso de las tecnologías que tenemos a nuestro alcance con responsabilidad y sacar el mejor provecho de ella.

Ya que la sociedad en la que vivimos es una sociedad necesitada de estar informados de lo que sucede día con día, por lo que a consecuencia de ello nace lo que conocemos como derecho a la información que no es más que una garantía consagrada en nuestra Carta Magna, tal y como ya lo hemos mencionado dentro de este capítulo.

Tal derecho se ha podido adquirir a través del paso del tiempo y hoy lo conocemos como un derecho universal con el que contamos todos los seres humanos pero que también es importante mencionar que tal derecho trae consigo aspectos positivos pero también aspectos negativos, los cuales se llegan a presentar por el mal uso de la tecnología.

Los beneficios que se han obtenido de este mundo de tecnologías y su evolución han cambiado la forma de ver la vida a nivel mundial pero también es importante saber que esta expansión de internet lleva consigo aparejado un fácil método de distribución y difusión de contenido ilegal, además de que a través de ella también se abre una amplia puerta para la realización de conductas de carácter ilícito e ilegal como lo es cualquier delito cibernético de los que se han mencionado y que puede llegar a afectar a cualquier persona del mundo que sea usuarios de las tecnologías con las que hoy en día contamos o simplemente por ser usuario del internet.

CAPÍTULO TERCERO

ANALISIS DE LA LEGISLACION EN MATERIA INFORMATICA

TRATAMIENTO DEL PROBLEMA EN EL AMBITO INTERNACIONAL

Como lo hemos venido observando la tecnología ha avanzado en grandes pasos en los últimos años, basta con comparar un equipo de cómputo de hacer varios años con una actual y ver que sus alcances son mucho más avanzados, y es el ejemplo de que día a día existe un manifiesto de avance tecnológico.

Pero no ocurre del mismo modo con la producción legislativa, lo que significa que algunos países se hayan quedado sin enfrentar los problemas de delincuencia por este medio. Algunos realizaron actos en contra de la delincuencia sin que para tal efecto hubiera una ley de por medio.

Otros países, en cambio, fueron permisivos hasta el día en que descubrieron con asombro lo que esta tecnología podía ocasionarles, como lo que ocurrió el 11 de septiembre de 2001, como se le denomina de manera general el día en que fueron derribados los edificios del World Trade Center en Nueva York, Estados Unidos por un comando terrorista, pues debe recordarse que ese comando tenia diversas sedes y se comunicaba por medio de correos electrónicos, que instruía y recibía a su vez instrucciones por internet y que además realizo la compra de boletos de avión, también a través de la llamada red de redes.[98]

[98] Op. Cit. Nava, Garcés Alberto E., p.108

En la Organización de las Naciones Unidas

Hace sesenta años, en 1948, la Asamblea General de Naciones Unidas adoptó la Declaración Universal de los Derechos Humanos, documento que constituye uno de los logros más importantes de la humanidad, ya que establece los principios universales que garantizan la igualdad y la libertad de todos los seres humanos.

Los descubrimientos tecnológicos y la industrialización que se registraron a partir de la segunda mitad del siglo XVIII y durante todo el siglo XIX propiciaron un crecimiento sin precedentes del capitalismo y del comercio alrededor del mundo. Como consecuencia, el siglo xx vería surgir las dos guerras más grandes en la historia de la humanidad, en las que la tecnología y las invenciones que habían ayudado al Influencia para destruir a la especie humana.[99]

La Organización de las Naciones Unidas, reconoce como delitos informáticos las siguientes conductas:

1. Fraudes cometidos mediante manipulación de computadoras:
a) Manipulación de los datos de entrada.
b) Manipulación de programas.
c) Manipulación de datos de salida.
d) Fraude efectuado por manipulación informática.

2. Falsificaciones informáticas
a) Utilizando sistemas informáticos como objetos.
b) Utilizando sistemas informáticos como instrumentos.

[99] Manual de los Derechos Humanos en México, Emilio Álvarez Icaza Longoria, Primera edición: Nostra Ediciones, 2009.

3. Daños o modificaciones de programas o datos computarizados.

a) Sabotaje informático.

b) Virus.

c) Gusanos.

d) Bomba lógica o cronológica.

e) Acceso no autorizado a sistemas o servicios.

f) Piratas informáticos o hackers.

g) Reproducción no autorizada de programas informáticos con protección legal.

EN LA COMISIÓN DE LAS COMUNIDADES EUROPEAS

La transición de Europa a la sociedad de la información se ha caracterizado por enormes cambios en la vida de los seres humanos, como lo es en su trabajo, educación, entretenimiento, industria y comercio. En el año de 1999, la Comisión puso en marcha la iniciativa en Europa con el fin de garantizar que Europa se beneficie de las tecnologías digitales, y que la nueva sociedad de la información sea socialmente inclusiva.

En junio de 2000, el Consejo Europeo de Feira adoptó el Plan de acción Europa, y solicitó que se aplicase antes de finales de 2002. El plan de acción resalta la importancia de la seguridad de las redes y de la lucha contra la delincuencia informática.

Las estructuras de información y comunicación se han convertido en algo de suma importancia en nuestras vida y también para la economía, pero desafortunadamente son muy vulnerables y amplias para la delincuencia, por lo que estas actividades delictivas se pueden dar de diferentes maneras y formas por consecuencia, pueden cruzar casi todas las fronteras y no cabe duda que este tipo de delitos que se comenten a través de la tecnología que

existe hoy en día, es una amenaza creciente para la seguridad y confianza en la sociedad de la información.

Puede actuarse en términos de prevención de la actividad delictiva, aumentando la seguridad de la infraestructura de la información. Otro aspecto a considerar es garantizar que las autoridades responsables de la aplicación de la ley cuenten con los medios adecuados para intervenir, respetando plenamente los derechos fundamentales de los individuos.

La Unión Europea ha tomado medidas para contrarrestar la delincuencia cibernética ya que existe una obvia necesidad que garantice a los Estados miembros de la Unión Europea la erradicación de la delincuencia informática, y la seguridad de todos aquellos que hoy en día la utilizan tanto como un medio de trabajo, comunicación o simplemente como entretenimiento.

En virtud de seguir generando dicha seguridad jurídica, la Unión Europea ha realizado diversos tratados referentes a la problemática que hoy en día se están viviendo, de los cuales se destacan: El Convenio para la Protección de las Personas Referente al Tratamiento Automático de Datos de Carácter Personal en 1991 y el Convenio sobre Ciber-criminalidad del año 2001.

CONVENIO SOBRE LA CIBER-CRIMINALIDAD

El Convenio sobre cibercriminalidad, también conocido como el Convenio de Budapest sobre el Cibercrimen o simplemente como Convenio Budapest, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China.

El Convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001 y el 23 de noviembre de 2001 se abrió a la firma en Budapest por lo que entró en vigor el 1 de julio de 2004. A partir del 28 de octubre de 2010, 30 estados firmaron, ratificaron y se adhirieron a la Convención, mientras que otros 16 estados firmaron la Convención, pero no la ratificaron sino hasta el 1 de marzo de 2006, el Protocolo Adicional a la Convención sobre Cibercrimen entró en vigor. Los estados que han ratificado el Protocolo Adicional son necesarios para penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como de las amenazas racistas y xenófobas e insultos.[100]

Este Convenio es el primer tratado internacional sobre delitos cibernéticos cometidos a través del internet y otras redes. Este Convenio es el único que se encarga de la seguridad de la información y trata los delitos contra la Confidencialidad, Integridad y Disponibilidad de Datos y los sistemas informáticos. Dentro de este documento destaca la descripción de las conductas delictivas, de aplicación para los Estados miembros de los que cabe resaltar los siguientes artículos:

Capítulo I – Terminología

Artículo 1.- Definiciones
A los efectos del presente Convenio, la expresión:

a)."Sistema informático" designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;

[100] http://es.wikipedia.org/wiki/Convenio_sobre_cibercriminalidad consultada el 24 de abril de 2013.

b). "Datos informáticos" designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;

c). "Prestador de servicio" designa:

I. Toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;
II. Cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;

d). "Datos de tráfico" designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II – Medidas que deben ser adoptadas a nivel nacional

Sección 1 – Derecho penal material

Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2.- Acceso ilícito

Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las partes podrán exigir que la infracción sea cometida con vulneración de

medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 3.- Interceptación ilícita

Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos en transmisiones no públicas en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 4.- Atentados contra la integridad de los datos

1. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

Artículo 5.- Atentados contra la integridad del sistema

Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6.- Abuso de equipos e instrumentos técnicos

1. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

Artículo 6 – Abuso de equipos e instrumentos técnicos

1. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a).La producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición:

I. De un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;

II. De una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5 ; y

b). La posesión de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal.

2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el parágrafo 1 (a)(2).

Título 2 – Infracciones informáticas

Artículo 7 – Falsedad informática.

Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que

sean percibidos o utilizados a efectos legales como auténticos , con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

Artículo 8 – Estafa informática.

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

a). La introducción, alteración, borrado o supresión de datos informáticos,

b). Cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

Título 3 – Infracciones relativas al contenido.

Artículo 9 – Infracciones relativas a la pornografía infantil.

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a). La producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

b). El ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;
c). La difusión o la transmisión de pornografía infantil a través de un sistema informático;
d). El hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;
e). La posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la “pornografía infantil” comprende cualquier material pornográfico que represente de manera visual:

a). Un menor adoptando un comportamiento sexualmente explícito;

b). Una persona que aparece como un menor adoptando un comportamiento sexualmente explícito;

c). Unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Las Partes podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Título 4 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Artículo 10.- Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

1. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor , a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Las partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Cabe señalar que esta convención hace referencia a otros temas de gran relevancia para los Delitos informáticos, de los cuales destacan:

Artículo 11 – Tentativa y complicidad.
Artículo 12 – Responsabilidad de las personas jurídicas.
Artículo 13 – Sanciones y medidas.
Sección 2 – Derecho procesal.
Artículo 14 – Ámbito de aplicación de las medidas de derecho procesal.
Artículo 15 – Condiciones y garantías.
Artículo 16 – Conservación inmediata de datos informáticos almacenados.
Artículo 17 – Conservación y divulgación inmediata de los datos de tráfico.
Artículo 18 – Mandato de comunicación.
Artículo 19 – Registro y decomiso de datos informáticos almacenados.
Artículo 20 – Recogida en tiempo real de datos informáticos.
Artículo 21 – Interceptación de datos relativos al contenido.
Artículo 22 – Competencia.
Artículo 23 – Principios generales relativos a la cooperación internacional.
Artículo 24 – Extradición.
Artículo 25 – Principios generales relativos a la colaboración.
Artículo 26 – Información espontánea.

Artículo 27 – Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable.
Artículo 28 – Confidencialidad y restricciones de uso.
Artículo 29 – Conservación inmediata datos informáticos almacenados.
Artículo 30 – Comunicación inmediata de los datos informáticos conservados.
Artículo 31 – Asistencia concerniente al acceso a datos informáticos almacenados.
Artículo 32 – Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso.
Artículo 33 – Asistencia para la recogida en tiempo real de datos de tráfico.
Artículo 34 – Asistencia en materia de interceptación de datos relativos al contenido.
Artículo 35 – Red 24/7 (Punto de contacto localizable las 24 horas del día, y los siete días de la semana, para asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal).
Artículo 36 – Firma y entrada en vigor.
Artículo 37 – Adhesión al Convenio.
Artículo 38 – Aplicación territorial.
Artículo 39 – Efectos del Convenio.
Artículo 40 – Declaraciones.
Artículo 41 – Cláusula federal.
Artículo 42 – Reserva.
Artículo 43 – Mantenimiento y retirada de las reservas.
Artículo 44 – Enmiendas.
Artículo 45 – Reglamento de controversia.
Artículo 46 – Reuniones de los Estados.
Artículo 47 – Denuncia, y

Artículo 48 – Notificación.[101]

El Convenio Europeo sobre Ciber-criminalidad está abierto a la adhesión de los Estados no europeos que sean invitados a suscribirlo. Hasta ahora, fuera del Viejo Continente, lo han suscrito Canadá, Japón, África del Sur y Estados Unidos, aunque solo este último lo ha ratificado.

Para ser parte del Convenio, el Comité de Ministros del Consejo de Europa, luego de realizar las consultas del caso y de haber obtenido el asentimiento unánime de los Estados parte, puede invitar a un país solicitante a adherirse. Como lo indica el proyecto de ley publicado, el Comité de Ministros, en el curso de la reunión de delegados del 31 de enero de 2007, invitó a Costa Rica a adherirse, lo cual también se hizo con Argentina, México, Chile y República Dominicana. Sin embargo, puesto que ninguno de éstos ha concluido aún el proceso de adhesión, nuestro país sería el primero de la región en hacerlo.[102]

MARCO NORMATIVO DE ESPAÑA

En España, los delitos informáticos son una acción sancionable por el código penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estos delitos y sus sanciones se concentran dentro del Código Penal español de 1995, así tenemos:

a) ATAQUES QUE SE PRODUCEN CONTRA EL DERECHO A LA INTIMIDAD. Delitos de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados

101 http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf consultada el 5 de mayo de 2013.

102 http://www.nacion.com/2012-09-10/Opinion/adhesion-al-convenio-europeo-sobre-ciberdelincuencia.aspx consultada el 7 de mayo de 2013.

en ficheros o soportes informáticos. (Los que se contemplan dentro de los artículos 197 al 201 del Código Penal).

b) INFRACCIONES A LA PROPIEDAD INTELECTUAL A TRAVÉS DE LA PROTECCION DE LOS DERECHOS DE AUTOR. Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Mismos que se contemplan dentro del artículo 270 del Código Penal).

c) FALSEDADES. Concepto de documentos como todo soporte material que exprese o incorpore datos. Extensión de falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Estos se contemplan dentro del artículo 386 del Código Penal español).

d) SABOTAJES INFORMATICOS. Delito de daños mediante la destrucción o alteración de datos o documentos electrónicos contenidos en redes o sistemas informáticos. (Se señalan dentro del artículo 263 del Código Penal).

e) FRAUDES INFORMATICOS. Delitos de estafa a través de la manipulación de datos o programas para la obtención de un grupo ilícito. (Dentro de los artículos 248 y ss. Del Código Penal).

f) AMENAZAS. Realizadas por cualquier medio de comunicación.

g) CALUMNIAS E INJURIAS. Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o a la radiodifusión, (Se contemplan dentro de los artículos 205 y ss. Del Código Penal).

h) PORNOGRAFIA INFANTIL. Delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos. La introducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (Se contempla dentro del artículo 187).[103]

A continuación se transcribe algunos de los artículos del **Código Penal Español** que contemplan estas conductas:

Artículo 197

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3.- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de

[103] Op. Cit. Nava, Garcés Alberto E., p.113-119.

prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

Artículo 201

1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Artículo 270

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte

comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Artículo 278

1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2.- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3.- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 400

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados

a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.[104]

Enrique Orts Berenguer, realiza un análisis detallado sobre los delitos informáticos en España:

Es de notar que el análisis de estos tipos penales tan solo entraña una visión sesgada de la amplia problemática que hoy plantea la utilización fraudulenta de la tecnología de la informática, cuyo tratamiento no ha de ser solo interdisciplinar si no también global, al menos en algunos aspectos.

Téngase en cuenta que la eclosión de Internet ha dado lugar a numerosos delitos de carácter transfronterizo, y a una criminalidad de alta tecnología, de carácter organizado, que actúa a través de la red, cuya persecución no encuentra tan solo trabas procesales, derivadas de las propias limitaciones a la aplicación ultra territorial de la leyes nacionales, si no también escollos sustantivos, que conducen a veces a la impunidad, de ciertas personas que

[104] http://delitosinformaticos.com/legislacion/espana.shtml, consultada el 26 de mayo del 2013

contribuyen a la información de la información delictiva. En el orden procedimental, no resulta difícil a los delincuentes informáticos orillar la competencia de los Tribunales cuando actúan desde lo que suele denominarse paraísos informáticos, toda vez que en principio, la Ley de cada Estado alcanza hasta donde llegan los confines de su soberanía. En concreto se puede hablar de determinados delitos, como los relativos a la propiedad intelectual, que en el ámbito virtual, presentan una particular importancia. Es cierto, también, que para sortear esta laguna legal bastaría mantener un criterio flexible en materia competencial, entendiendo realizado el delito, tanto en el lugar en el que se ejecute la acción, como en aquel en que se produzca el resultado delictivo. Sin embargo, tal solución no solo estaría sembrada de dificultades prácticas, si no que podría conducir a soluciones palmariamente injustas, dadas las diferencias de trato que respecto a una misma infracción suelen existir entre los diferentes ordenamientos.[105]

LA CRIMINALÍSTICA INFORMÁTICA

Independientemente de la problemática que presenta la ley por cuanto a la legislación, es importante hacer referencia a otros de los grandes problemas a que se ha enfrentado el Derecho Penal, que es la detención del delincuente, para lo cual son necesarias las ciencia auxiliares como lo son la Criminología y la Criminalística.

La Criminología es el conjunto ordenado de saberes empíricos sobre el delito, el delincuente, el comportamiento socia/mente negativo y sobre los controles de esta conducta. Su ámbito científico puede caracterizarse de modo preciso con los tres conceptos básicos de delito, delincuente y control del delito. A

[105] Orts Berenguer, Enrique y Margarita Roig Torres, Delitos informáticos y delitos comunes cometidos a través de la informática, Tirant lo Blanch, "colección de delitos", Valencia España, 2001, pp. 162-163.

ellos hay que agregar también lo que concierne a la víctima y a la prevención del delito.[106]

Encuentra su principal objetivo en explicar las causas por las que surge el delito, es decir encontrar factores criminológicos que se presentan en la comisión de un delito.

Por su parte la Criminalística como "una disciplina científica que estudia los indicios dejados en lugar del delito, con el propósito de descubrir la identidad del criminal y las circunstancia que concurrieron en el hecho delictuoso."[107]

Desde un punto de vista amplio es el conjunto de procedimientos aplicables a la investigación y al estudio del crimen. En otro sentido podemos definir a la criminalística como una disciplina que tiene como objeto el reconocimiento, identificación e individualización de las evidencias físicas o materiales con el fin de determinar un hecho ilícito.

LA CRIMINALÍSTICA

Como ciencia auxiliar del Derecho Penal encontramos a la Criminalística que se asiste de las diversas ciencias naturales, disciplinas y técnicas a efecto de encontrar el *modus vivendi* y *operandi* del delincuente, es decir, para lograr

---

106 http://criminologiausco.blogspot.mx/2005/08/concepto-de-criminologa.html consultada el 24 de junio de 2013.

107 http://justiciaforense.com/material/ARCHIVOS%20FORENSES/CRIMINALISTICA%20GENERAL%20Y%20DE%20CAMPO/ARCHIVOS%20PDF/NOCIONES%20DE%20CRIMINALISTICA.pdf consultada el 26 de junio de 2013.

principalmente su localización a través de los diversos vestigios que pueden ser dejados en la comisión de un delito.

La Criminalística se encuentra constituida por un conjunto de conocimientos heterogéneos encaminados al hallazgo de los delincuentes, al conocimiento del *modus operandi* del delito y al descubrimiento de las pruebas y de los procedimientos para utilizarlas.[108]

Los objetivos de la criminalística son:

a) Investigar técnicamente y demostrar científicamente la existencia de un hecho en particular probablemente delictuoso.

b) Determinar los fenómenos y reconstruir el mecanismo del hecho, señalando los instrumentos y objetos de ejecución, sus manifestaciones y las maniobras que se pusieron en juego para realizarlo.

c) Aportar evidencias o coordinar técnicas o sistemas para la identificación de la víctima si existiere.

d) Aportar evidencias para la identificación de los presuntos autores y coautores.

e) Aportar las pruebas materiales con estudios técnicos científicos para probar el grado de participación del o de los presuntos autores y demás involucrados.[109]

---

[108] Op. Cit. Castellanos Tena, Fernando. Pág. 29.
[109] Montiel Sosa, Juventino: *Criminalística*. Editorial Limusa. Segunda edición México 2007. Pág. 86

La criminalística cumple con las siguientes finalidades:

a) Auxiliar al órgano investigador en sus funciones para que realice adecuadas conclusiones en su labor en la procuración de justicia.

b) Apoyo a través de dictámenes periciales a los órganos de procuración y de impartición de justicia.

c) Participar en las diligencias ministeriales y judiciales para tratar de llegar a la verdad histórica.

Existen siete principios que hacen valido el método de la criminalística, que se basan principalmente en dos teorías:

a. Criminalística técnico-científica o especulativa. Es el conjunto de conocimientos establecidos.
b. Criminalística aplicada. Es la solución de casos concretos.

PRINCIPIOS DE LA CRIMINALISTICA.

1) Principio de uso: en los hechos que se comenten o realizan siempre se utiliza agentes mecánicos, químicos, físicos o biológicos.

2) Principio de producción: en la utilización de agentes mecánicos, químicos, físicos o biológicos para la comisión presuntamente delictuosa siempre se producen indicios o evidencias materiales en gran variedad.

3) Principio de intercambio: al consumarse el hecho y de acuerdo con las característica de su mecanismo se origina un intercambio de indicios

entre el autor, víctima y el lugar de los hechos o en su caso entre el autor y el lugar de los hechos.

4) Principio de correspondencia de características: basados en un principio universal establecido criminalistamente como “la acción dinámica de los agentes mecánicos venerantes sobre determinados cuerpos dejan impresas sus características reproduciendo la figura de su cara que impacta”. Fenómeno que da la base científica para realizar estudios micro y macro comparativos de elemento problema y elemento testigo, con el objeto de identificar al agente de producción.

5) Principio de reconstrucción de hechos o fenómenos: el estudio de todas las evidencias materiales asociadas al hecho darán las bases y los elementos para conocer el desarrollo de los fenómenos de un caso concreto y reconstruir el mecanismo del hecho o fenómeno para acercarse a conocer la verdad del hecho investigado.

6) Principio de probabilidad: la reconstrucción de los fenómenos y de ciertos hechos que los acerquen al conocimiento de la verdad puede ser con un bajo, mediano o alta grado de probabilidad o simplemente sin ninguna probabilidad, pero nunca se podrá decir “el hecho sucedió exactamente así.

7) Principio de certeza: las identificaciones cualitativas, cuantitativas y comparativas de la mayoría de los agentes venerantes que se utilizan e indicios que se producen en la comisión de los hechos logran por medio de metodología, tecnología y procedimientos adecuados que dan certeza de su existencia y procedencia.

LA UNIDAD DE POLICÍA CIBERNÉTICA

Ya hemos dejado en claro la importancia de la información en el mundo altamente tecnificado de hoy. También se ha dejado en claro cada uno de los riesgos "naturales" con los que se enfrenta nuestro conocimiento y la forma de enfrentarlos por el mal uso de la tecnología que hoy en día existe y la gran cantidad de delitos que se cometen a través de ella.

El desarrollo de la tecnología informática y el mal uso de ella por el hombre ha abierto las puertas a nuevas posibilidades de delincuencia nunca antes pensadas. Por lo que es necesario contar con un órgano que se dedique a la prevención de estas conductas delictivas, la cual es llamada “policía cibernética”, que es la encargada de investigar los actos delictivos que permiten la comisión de daños en contra de las personas que son ejecutados por medio del uso de las computadoras o con la tecnología con que actualmente contamos los seres humanos a través del mundo virtual que nos proporciona el internet, y que es una actividad ilegal como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad.

Como ya lo mencionamos el mal uso que hace el hombre del internet, ha hecho que nos encontremos en la imperiosa necesidad de generar un cuerpo llamado Policía Cibernética, que se encargara de proteger y dar seguridad a los usuarios de la red.

La policía cibernética está adscrita a la Dirección General de Tráficos y Contrabandos, que además de prevenir delitos cometidos por medio del internet usando los mismos medios informáticos, cuenta con un área específica de prevención y atención de las denuncia de los usuarios de la red.

Dicho organismo se basa en cuatro objetivos primordiales que son:

• Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración y distribución y promoción de pornografía infantil.

• Localización y puestas a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.

• Realización de operaciones de patrullaje antihacker, utilizando Internet como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.

• Análisis y desarrollo de investigaciones en el campo sobre las actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.[110]

Estos cuerpos policiacos son los encargados de acudir al lugar donde se realizaron los hechos y la función de esto es recabar todos aquellos indicios que servirán para que en su momento se integrar la averiguación previa correspondiente, por la comisión de los delitos que se hayan cometido, y definitivamente deben contar con un grado de especialización en delitos cibernéticos.

DE LA POLICÍA FEDERAL PREVENTIVA EN MÉXICO

Ante el alarmante número de delitos que se comenten en México a través del internet o de la tecnología, nuestro país se vio en la gran necesidad de contar con una policía cibernética, la cual es un cuerpo policiaco, el primero en su

[110] http://delitosinformaticos.weebly.com/policia-cibernetica.html consultada el 2 de junio de 2013.

tipo de América Latina y que depende de la Secretaria de Seguridad Pública (SSP).

Este órgano fue creado en Diciembre de 2002, y como ya lo mencionamos depende de la Policía Federal Preventiva, y las principales funciones de esta institución son:

1. Detectar fraudes.
2. Falsificaciones
3. Intrusión en sistema de cómputo.
4. Pornografía infantil
5. Amenazas, entre otros.
6. Identificación.
7. Monitoreo.
8. Rastreo y localización de todas aquellas manifestaciones delictivas tanto en territorio nacional como fuera de él.[111]

Es importante señalar que esta policía está encargada además de combatir la pornografía infantil, ya que es uno de los delitos con mayor número de incidencia, también se encarga de combatir otros delitos cometidos vía internet o a través de una computadora, principalmente aquellos que atentan contra la integridad de las personas.

De acuerdo con la Dirección de inteligencia de la Policía Federal Preventiva (PFP) se trabaja en la integración de un banco de datos, la cual sirve para identificar patrones y el modus operandi de todos los casos y denuncias

[111] http://www.ssp.gob.mx/application?pageid=pcibernetica consultada el 6 de junio de 2013.

reportadas, además de intercambiar datos con organizaciones internacionales.

Como ya se mencionó anteriormente la policía cibernética opera por medio de "patrullajes antihacker por el ciberespacio, a través de computadoras, con lo que han comprobado el "alarmante crecimiento de organizaciones de pedófilos que transmiten pornografía infantil y promueven la corrupción de menores vía Internet".

La Policía Cibernética está adscrita a la Coordinación General de Inteligencia para la Prevención de la SSP y patrulla Internet mediante software convencional para rastreo de hackers y sitios de Internet, comunidades y chat rooms en los que promueven la pornografía y el turismo sexual infantil. Con ello se busca hacer de Internet en México "un lugar seguro para el intercambio de información, además de analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su modus operandi. Sin embargo, la PFP aclaró que "la supervisión de los padres no sustituye ningún precedente de seguridad que podamos ofrecerle", por lo que emitió algunos consejos para evitar que sus hijos sean víctimas de toda clase de delincuentes a través de Internet.[112]

La policía cibernética en México comprende las siguientes áreas:

- DELITOS CIBERNETICOS.
  - ✓ Atención de delitos cibernéticos.
  - ✓ Atención a delitos usando computadoras.
  - ✓ Análisis de cómputo forense.

[112] http://www.elsiglodetorreon.com.mx/noticia/18839.las-funciones-de-la-policia-cibernetica-de-me.html consultada el 8 de junio de 2013.

- DELITOS CONTRA MENORES.
  - ✓ Análisis de explotación de menores.
  - ✓ Atención a menores desaparecidos.

- COORDINACION 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.[113]

POLICIAS INTERNACIONALES

Organización Internacional de Policía (INTERPOL)

La ciberdelincuencia es uno de los ámbitos delictivos de mayor crecimiento, cada vez las tecnologías modernas constituyen una amplia puerta para la comisión de conductas ilícitas, pero el enlace mundial que tiene el internet a permitido a los ciberdelincuentes cometer delitos en cualquier parte del mundo a través de un sistema de cómputo o tecnología que le permita realizar estas actividades, por lo que todos los países se han visto en la necesidad de crear y poner en marcha un método de control para poder combatir estos delitos cometidos a través del ciberespacio ya que el terrorismo cibernético que hoy en día estamos viviendo representa una grave amenaza tanto a nivel nacional como internacional.

[113] http://www.disc.unam.mx/2005/presentaciones/delitos_menores.pdf consultada el 9 de junio de 2013.

Este problema obliga a las autoridades a preocuparse pero principalmente a ocuparse en tratar de erradicar esta situación tan alarmante y proporcionar a todos los usuarios de las redes informáticas la seguridad que necesitan.

Por lo que actualmente se cuenta con la "Comisión Criminal internacional de Policía" denominada INTERPOL, cuya historia comienza en el año de 1914 en el marco del primer Congreso Internacional de Policía Criminal, celebrado en Mónaco, es la organización más grandes del mundo pues tiene afiliados a más de 190 países miembros de esta organización, fue creada como tal en el año de 1923 y su función principal es la de permitir que todas las policías colaboren para hacer del mundo un lugar más seguro, es decir facilitar la cooperación policial internacional aun cuando no existan relaciones diplomáticas entre determinados países y actúa dentro de los límites impuestos por las legislaciones vigentes en los diferentes Estados y de conformidad con la Declaración Universal de Derechos Humanos.[114]

El programa de INTERPOL sobre ciberdelincuencia se basa en la información y las operaciones; así como en diversas actuaciones para hacer frente a los peligros incipientes. Sus principales objetivos son:

- Promover el intercambio de información entre los países miembros a través de grupos de trabajo y conferencias de alcance regional.
- Impartir cursos con miras a establecer y mantener normas válidas para los profesionales del sector.
- Coordinar operaciones internacionales y contribuir a su realización.
- Confeccionar una lista de funcionarios de contacto disponible las 24 horas del día en relación con las investigaciones sobre ciberdelincuencia.

[114] http://www.interpol.int/es/Acerca-de-INTERPOL/Estructura-y-gobernanza consultada el 10 de junio de 2013.

- Ayudar a los países miembros en el caso de que sufran ataques informáticos o en sus pesquisas sobre ciberdelincuencia poniendo a su disposición servicios de investigación y de base de datos.
- Establecer colaboraciones estratégicas con otras organizaciones internacionales y entidades del sector privado.
- Poner de manifiesto peligros incipientes y compartir esta información con los países miembros; abrir un portal de internet protegido que ofrezca datos y documentos operativos.[115]

OFICINA EUROPEA DE POLICÍA

(EUROPOL)

El establecimiento de la Europol fue convenido en el tratado de *Maastricht* en la Unión Europea del 7 de febrero de 1992 en La Haya, Países Bajos, En la Europol comenzaron operaciones limitadas el 3 de enero de 1994 bajo la forma de unidad de las drogas de Europol (EDU). La Europol comenzó sus actividades el 1º de julio de 1999, y el día 1o. de enero de 2002, el mandato de Europol fue extendido al reparto con todas las formas serias de crimen internacional según lo enumerado en el anexo a la convención de Europol.
El anexo se refiere a lo previsto en el artículo 2 de la convención en donde se incluye la persecución de las siguientes conductas criminales: *"murder, grievous bodily injury - illicit trade in human organs and tissue -kidnapping, illegal restraint and hostage-taking - racism and xenophobia.*

Esta Oficina Europea de Policía es un órgano encargado de facilitar las operaciones de la lucha contra la criminalidad en la Unión Europea, con esta

[115] http://www.interpol.int/es/Criminalidad/Delincuenciainform%C3%A1tica/Ciberdelincuencia consultada 10 de junio de 2013.

organización se da la Cooperación Judicial por parte de estos países ya que como ya se mencionó la criminalidad informática no respeta fronteras.

La Oficina europea de policía denominada "Europol", (se rige por el Convenio Europol) está establecida en los Países Bajos, La Haya. La misión de dicha oficina es mejorar la eficacia de los servicios competentes de los Estados miembros y su cooperación en ámbitos cada vez más numerosos:

- la prevención y la lucha contra el terrorismo,
- el tráfico ilícito de estupefacientes,
- el tráfico de seres humanos,
- las redes de inmigración clandestina,
- el tráfico ilícito de materias radioactivas y nucleares,
- el tráfico ilícito de vehículos,
- la lucha contra la falsificación del euro,
- el blanqueo de dinero vinculado a las actividades delictivas internacionales.

Europol colabora con los Estados miembros del siguiente modo:

- Facilitando el intercambio de información, de conformidad con la legislación nacional, entre funcionarios de enlace de Europol (ELO). Dichos funcionarios están acreditados por los Estados miembros como representantes de sus organismos nacionales encargados de velar por el cumplimiento de la ley.
- Llevando a cabo análisis operativos que apoyen las actuaciones de los Estados miembros.
- Elaborando informes estratégicos (por ej. evaluaciones de amenazas) y análisis de los delitos sobre la base de la información suministrada por los Estados miembros, generada por Europol o reunida a partir de otras fuentes.
- Aportando su experiencia y colaboración técnica en las investigaciones y actuaciones efectuadas en la Unión Europea, bajo

la supervisión y la responsabilidad jurídica de los Estados miembros interesados.[116]

El nuevo Centro Europeo de Ciberdelincuencia (EC3) para contribuir a proteger a las empresas y a los ciudadanos europeos frente a la ciberdelincuencia. Tiene su sede en la Oficina Europea de Policía, Europol, en La Haya.

El Centro Europeo de Ciberdelincuencia dará un fuerte impulso a la capacidad de la Unión Europea para luchar contra la ciberdelincuencia y defender la existencia de una Internet libre, abierta y segura. Los ciberdelincuentes son inteligentes y rápidos en la utilización de nuevas tecnologías con fines delictivos; el EC3 nos ayudará a ser aún más inteligentes y rápidos que ellos para poder contribuir a prevenir y combatir sus delitos.

Para luchar contra la ciberdelincuencia, que por naturaleza no respeta fronteras, y la gran habilidad de los delincuentes para ocultarse, tenemos que responder de manera flexible y adecuada. El Centro Europeo de Ciberdelincuencia está diseñado para aportar sus conocimientos como centro de fusión de la información y de apoyo operativo forense y de investigación, pero también, por su capacidad para movilizar todos los recursos pertinentes en los Estados miembros de la Unión Europea, para aliviar y reducir la amenaza que representan los ciberdelincuentes con independencia del lugar desde el que actúen.

Las investigaciones sobre los fraudes en línea y sobre los abusos de menores en línea y otros delitos informáticos afectan con frecuencia a cientos de víctimas simultáneamente e implican a sospechosos en diversas partes del

[116] http://www.intelpage.info/web/europol.htm consultada el 11 de junio de 2013.

mundo. Las operaciones de esta magnitud no pueden llevarse a buen término con la única participación de los efectivos de las policías nacionales.

La apertura del Centro Europeo de Ciberdelincuencia (EC3) constituye un cambio importante en la forma en que la Unión Europea ha abordado la ciberdelincuencia hasta la fecha. Por encima de todo, el planteamiento del EC3 tendrá más visión de futuro y será más integrador. Se pondrán en común los conocimientos técnicos y la información, se prestará apoyo a las investigaciones criminales y se fomentarán las soluciones a escala de la Unión Europea.

La actividad del EC3 se centrará en las actividades ilegales en línea de las bandas de delincuencia organizada, especialmente en los ataques dirigidos contra las operaciones bancarias y otras actividades financieras en línea, la explotación sexual infantil en línea y los delitos que afecten a las infraestructuras críticas y a los sistemas de información en la Unión Europea.

El Centro también facilitará la investigación y el desarrollo y garantizará el refuerzo de las capacidades de las autoridades responsables de la aplicación de la ley, los jueces y los fiscales; asimismo, llevará a cabo evaluaciones de las posibles amenazas, que incluirán análisis, previsiones de tendencias y alertas tempranas. Con el fin de desmantelar un mayor número de redes de delitos informáticos y de perseguir a un mayor número de sospechosos, el EC3 recopilará y tratará los datos relacionados con la ciberdelincuencia y ofrecerá un servicio de asistencia en materia de ciberdelincuencia a las fuerzas de seguridad de los países de la Unión Europea. Además, prestará apoyo operativo a los países de la Unión Europea (por ejemplo, contra la intrusión, el fraude, el abuso sexual de menores en Internet, etc.) y aportará

conocimientos técnicos, analíticos y de peritaje forense de alto nivel en el marco de investigaciones conjuntas.[117]

EL BURÓ FEDERAL DE INVESTIGACIONES (FBI)

El FBI (Federal Bureau of Investigation) es una especie de Policía Federal perteneciente al territorio estadounidense, una agencia gubernamental que tiene la función de apoyo a la ley a través de la investigación de las violaciones de la ley penal. Sin embargo, contrariamente a lo que algunos piensan, el FBI no es un departamento de policía nacional ya que posee jurisdicción diferente para ciertos tipos de crímenes, administrada por el Fiscal General de los Estados Unidos. Fundada el 26 de julio de 1908 por el fiscal de distrito Charles Joseph Bonaparte, el FBI se considera la mayor agencia de policía en el mundo, con treinta mil empleados y operando en sesenta países.

Las oficinas centrales del FBI están ubicadas en Washington, DC, y también hay 56 oficinas locales ubicadas en las principales ciudades de los Estados Unidos, así como más de 400 organismos residentes en pequeñas ciudades y pueblos en toda la nación, y más de 50 oficinas internacionales, llamadas " Diplomacias Legales", en embajadas de Estados Unidos varios países.

La misión del FBI puede resumirse en diez aspectos:

1. Proteger a los Estados Unidos de ataques terroristas.
2. Proteger a los Estados Unidos de operaciones extranjeras de espionaje e inteligencia.
3. Proteger a los Estados Unidos de *ciberataques* y crímenes de alta tecnología.

[117] http://europa.eu/rapid/press-release_IP-13-13_es.htm consultada el 11 de junio de 2013.

4. Combatir la corrupción de los servicios públicos en todos los niveles.
5. Proteger los derechos civiles.
6. Combatir organizaciones y empresas de carácter criminal nacionales y transnacionales.
7. Combatir el *crimen de cuello blanco*, estafas corporativas, fraudes financieros, robo de identidad, etc.
8. Combatir crímenes violentos de conmoción pública.
9. Apoyar al gobierno federal, estatal, local y organizaciones internacionales asociadas.
10. Mejorar su tecnología para asegurar el éxito de sus actos.[118]

LA PROCURACIÓN DE JUSTICIA EN MÉXICO EN RELACIÓN A LOS DELITOS INFORMÁTICOS

No obstante, de que en nuestro país contamos con una Policía Cibernética la cual se encuentra adscrita a la Policía Federal Preventiva, también en México ya existe una unidad especializada en delitos informáticos de la Procuraduría General de la República, por lo que sería más conveniente aprovechar los recursos y cobertura tecnológica que se le han asignado para tratar de contrarrestar los ilícitos informáticos que se cometen a través de Internet.

En México se requiere una regularización de los bienes informacionales, porque la información como producto informático requiere de un tratamiento jurídico en función de su innegable carácter económico; es necesaria la protección de datos personales.

118

http://translate.google.com.mx/translate?hl=es&sl=en&u=http://www.fbi.gov/&prev=/search%3Fq%3Dfbi%26biw%3D1366%26bih%3D667 consultada el 11 de junio de 2013.

Debido al atentado sufrido a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas; el flujo de datos transfronterizos. Sobre el favorecimiento de restricción en la circulación de datos a través de fronteras nacionales; la protección de programas. Como solución a los problemas más provocados por la llama piratería o pillaje de programas de cómputo; los delitos informáticos en sentido amplio.

Así como la comisión de verdaderos actos ilícitos en los que se tenga en la computadora un instrumento o fin.[119]

Evidentemente, el desarrollo de nuevos ordenamientos destinados a regular el flujo de información a través de los sistemas computacionales, tendrá incidencia en el ámbito penal.

Muy importante sería que existiera con claridad una definición de competencia de las áreas que investigue los delitos cibernéticos tanto en el ámbito federal como en el local, toda vez que como lo hemos venido analizando los delitos cibernéticos no se frenan para traspasar cualquier tipo de fronteras.

[119] op. cit. López Betancourt, Eduardo, p. 271

CONCLUSIONES TERCER CAPITULO

Como hemos podido observar la tecnología ha avanzado a pasos agigantados y cada vez más rápido, y el proceso es cada día más importante por lo que hoy se nos permite procesar y poner a disposición de cualquiera una cantidad creciente e importante de información, al alcance de millones de usuarios de esta tecnología, y dada esta situación se ha logrado tener varias modalidades de conductas delictivas a través de estos medios, que han alcanzado un daño importante a nivel internacional, ya que cualquier persona o usuario de la tecnología de cualquier parte del mundo se encuentra expuesto a ser víctima de estas conductas ilícitas realizadas a través de un instrumento tecnológico o de una computadora.

por lo que es de suma importancia regular mediante un ordenamiento legal las conductas delictivas que se cometen día a día en cualquier parte del mundo a través del ciber espacio, tal y como se encuentran reguladas todas aquellas conductas ilícitas que se exteriorizan y que se materializan y que se encuentran tipificadas dentro de la rama penal del derecho.

Si bien es cierto que ya existen varios países que cuentan con una cierta normatividad en materia penal, y que tipifican los ciber delitos que se cometen a través de la red, también es cierto que a nivel internacional falta mucho por hacer para poder llegar a cubrir las necesidades que tiene este ámbito de la cibernética en materia delictiva.

Por lo que es de suma importancia darnos cuenta que esta problemática es cada vez más grave, y que día a día aqueja a más personas, por lo que es necesario que todos los países que faltan por regular las conductas ilícitas cometidas a través de la informática, tomen conciencia de proteger y tutelar bajo un estado de derecho todos los bienes con que cuentas los usuarios de la tecnología bajo una producción legislativa en materia de informática, ya

que algunos países se han quedado sin enfrentar los grandes problemas que se han presentado en materia de delincuencia a través de este tipo de medios.

Independientemente por cuanto a materia de ley y legislación en materia informática es importante mencionar que la criminología y la criminalística informática son ramas importantes para el derecho penal en la informática ya que son ciencias auxiliares para el derecho penal.

También es importante mencionar que debido a que la problemática que se ha presentado con las nuevas posibilidades de delincuencia a través de la red de internet y de las nuevas tecnologías de las que se ha hecho un mal uso, ha puesto al hombre en la necesidad de crear un cuerpo policiaco que se encargue principalmente de cuidar y velar por la seguridad de los usuarios de esta red, tanto en el nivel nacional e internacional pues como ya lo hemos venido mencionado este es una problemática que afecta al individuo que haga uso de la tecnología en cualquier parte del mundo donde sea utilizada.

Sin embargo es de gran importancia mencionar que la ciber delincuencia es cada vez más amplia y llega cualquier parte del mundo, por lo que es de suma importancia que todos los países que hacen uso de estos medios, pongan en marcha un efectivo método de control y protección para combatir cualquier tipo de delito que se cometa en el ciber espacio, ya que hoy en día esto se traduce en una gran amenaza tanto a nivel nacional como a nivel internacional.

Por lo que este problema obliga a las autoridades a ocuparse de la seguridad de todos los usuarios del internet, pero principalmente a brindarles los medios para tratar de erradicar o por lo menos disminuir el alto índice de delincuencia cibernética que vivimos hoy en día, que por su naturaleza no respeta frontera alguna y la gran habilidad que tienen los ciber delincuentes para poder ocultarse.

Tomando en cuenta esto sería de suma importancia que existiera un cuerpo tanto a nivel nacional como internacional que protegiera a los usuarios del internet pero que aparte permitiera la existencia de un internet libre, abierto y seguro a todos aquellos que quieran hacer uso de él, pero que sobre todo se preocupara por tener una amplia capacidad para luchar y contrarrestar el gran problema que vivimos hoy en día que es la ciberdelincuencia.

CAPÍTULO CUARTO

ESTUDIO Y ANALISIS DE LA LEGISLACION EN MATERIA DE DELITOS INFORMATICOS EN MEXICO

DERECHO POSITIVO MEXICANO

Una de las principales características del derecho mexicano, es que se encuentra compuesto de diversos cuerpos normativos, los cuales tienen como finalidad la prevención o en su caso la sanción de los delitos previstos en los ordenamientos legales que regulan la conducta de los individuos de manera coercitiva en el ámbito social.

"El proceso evolutivo de la sociedad obliga a que las normas que la rigen evolucionen a la par, obedeciendo a factores socioeconómicos, tecnológicos y políticos, entre otros. En consecuencia las leyes se encuentran en un constante cambio, por lo que para estar en condiciones de realizar una labor eficaz en la investigación y persecución de conductas delictivas por medio de las TICS se debe atender a las adecuaciones a la ley. "[120]

En México existen avances en materia de regulación de delitos informáticos, sin embargo no han sido suficientes para contrarrestar los efectos producidos por los mismos, los cuales se han incrementado de manera incontrolable sin que exista un método eficaz para atacar su acelerada proliferación.

En razón de lo anteriormente señalados es de vital importancia mencionar los diversos cuerpos normativos en los cuales se hace referencia de los delitos informáticos partiendo jerárquicamente de nuestra ley suprema en la

[120] op. cit. Lira Arteaga, Oscar Manuel, *Cibercriminalidad*, Instituto Nacional de Ciencias Penales. Primera edición México 2010. Pág. 26

cual encontramos la base para la regulación de la conducta externa de los hombres en un lugar y tiempo determinado.

CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS

Como señala el artículo 71 de la Constitución Política De Los Estados Unidos Mexicanos el derecho de iniciar leyes o decretos compete al presidente de la república, los diputados y senadores, al congreso de la unión y legislaturas de los estados, razón por la cual se debe poner en mesa de debates la legislación y regulación de los delitos informáticos.

En nuestra carta magna específicamente en el numeral 133 establece la jerarquía de la misma y su aplicación en relación con los convenios y tratados celebrados por México a través del presidente de la república, previamente aprobados por el senado de la república, en el cual faculta a las diversas autoridades a valorar los diversos convenios y tratados firmados por mexica en sus resoluciones.

Artículo 133. Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados.[121]

En materia de delitos informáticos en nuestro código penal federal se encuentra tipificado dicha conducta como acceso ilícito a sistemas y equipos de informática en el cual se observa que se pretende una regulación de las conductas en dicho tema pero el mismo no resulta totalmente aplicable a las

[121] Constitución Política De Los Estados Unidos Mexicanos

diversas conductas ilícitas que son generadas por medio de un ordenador y códigos maliciosos mejor conocidos como virus informáticos.

A continuación se realiza la transcripción de algunos artículos que hacen referencia a la regulación de los delitos informáticos con la finalidad de mostrar un panorama más amplio en relación con las conductas delictivas que se encuentran sancionadas por la legislación mexicana.

CODIGO PENAL FEDERAL

Capitulo II

Acceso ilícito a sistemas y equipos de informática

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.

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.

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.

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. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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.

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 ciento cincuenta a cuatrocientos cincuenta días multa.

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. Si el responsable es o hubiera sido 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.

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.

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.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema 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.

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.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.[122]

Como se puede advertir dicha conducta antijurídica únicamente se contempla de manera general a los delitos informáticos sin especificar de manera clara cuales son los mismos y cuáles son las penas para las personas que incurran en dichos delitos razón por la cual a lo largo de la presente tesis se pretende demostrar la necesidad de la creación de un cuerpo normativo a nivel federal el cual contemple las diversas figuras delictivas y las cuales a manera de sanción y prevención reduzca el avance de dichas conductas antijurídicas.

[122] Código Penal Federal

Del anterior análisis podemos apreciar que por medio del internet se hace más frecuente la comisión de delitos que si bien es cierto ya existen tipificados de manera concreta en la legislación penal como son*: rebelión, terrorismo, sabotaje, conspiración, delitos en vías de comunicación y correspondencia, delitos contra la salud, delitos contra el libre desarrollo de la personalidad, pornografía, trata de personas, lenocinio revelación de secretos, acceso ilícito a sistemas y equipos de informática, falsificación alteración y destrucción de moneda, falsificación y utilización indebida de títulos al portador documentos de crédito publico, falsificación de documentos en general, delitos contra la seguridad y paz de las personas, amenazas, homicidio, delitos contra el patrimonio, robo, fraude, extorsión, operaciones con recursos de procedencia ilícita, delitos electorales* y diversas leyes en específico que contemplan dichas conductas antijurídicas, de las cuales haremos una transcripción de lo referente a los delitos informáticos.

LEY FEDERAL DE TELECOMUNICACIONES

A través del estudio de la presente ley se puede inferir que de la regulación de delitos informáticos en materia de telecomunicaciones es de igual manera importante que los otros delitos en virtud de que se plantea el uso aprovechamiento y explotación de los medios de comunicación vía satelital para lo cual es necesario analizar su legislación como punto de partida.

Artículo 71. Las infracciones a lo dispuesto en esta Ley, se sancionarán por la Secretaría de conformidad con lo siguiente:

A. Con multa de 10,000 a 100,000 salarios mínimos por:

[…]

V. Interceptar información que se transmita por las redes públicas de telecomunicaciones, y

VI. No cumplir en tiempo y forma, con las obligaciones establecidas en las fracciones XII, XIII, XIV, XV, XVI y XVIII del artículo 44 de esta Ley, en materia de telefonía. [123]

CODIGO DE COMERCIO

Con el uso de los medios electrónicos y el aumento en la facilidad de realizar actividades inherentes al comercio en línea, aumenta la posibilidad de ser víctima de las conductas ilícitas en los diversos ámbitos, ya sean sociales, políticos, económicos a través del internet, es por ello la necesidad de regular, de igual forma dicha conducta al aumentar día con día a pasos agigantados.

A nivel internacional existen diversos organismos, para regular el comercio electrónico, pero no así por cuanto hace a los delitos por los que se ve afectada los diversos sujetos que participan en el comercio electrónico.

ARTICULO 96. Las disposiciones del presente código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una firma electrónica.

ARTICULO 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 comunico ese mensaje de datos.
La firma electrónica se considerara avanzada o fiable si cumple por lo menos los siguientes requisitos:
I. los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
II. los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

[123] Ley Federal de Telecomunicaciones

III. es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma, y
IV. respecto a la integridad de la información de un mensaje de datos, es posible detectar cualquier alteración de esta hecha después del momento de la firma.
Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una firma electrónica; o presente pruebas de que una firma electrónica no es fiable.

ARTICULO 98. Los prestadores de servicios de certificación determinaran 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.

La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos.
Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado. [124]

De los Delitos en Materia de Derechos de Autor

Existen diversos materiales que pueden ser robadas y distribuidas sin el consentimiento de su autor por medio de las tecnologías de la información y comunicación y los cuales pueden ser muy amplios desde culturales hasta de entretenimiento, sin embargo los programas de cómputo son los más susceptibles en este aspecto, por lo cual citamos algunos de los artículos más relacionados con dichas conductas ilícitas a fin de atender la problemática en la que nos encontramos trabajar de manera conjunta con las diversas autoridades a fin de que dichas conductas ilícitas disminuyan.

[124] Código de Comercio

Artículo 424.- Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa:

I. Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Pública;

II. Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos;

III. A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor.

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, video gramas 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.

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, video gramas o libros a que se refiere el párrafo anterior, o

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.[125]

De los Programas de Computación y las Bases de Datos

Si bien es cierto como hemos señalado con anterioridad de igual forma es de vital importancia atender a los delitos que son cometidos en contra de un ordenador ya sea por la facilidad de actuar o el acceso a ellos.

[125] Ley Federal de Derechos de Autor

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.

Determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

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.

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.

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.

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 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.

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:

I. Sea indispensable para la utilización del programa, o

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.

Artículo 106.- El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y

IV. La de compilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

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.

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.

Artículo 109.- El acceso a información de carácter privado relativo a las personas contenidas en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

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.

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:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

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.

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.

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.[126]

[126] Ley Federal de Derechos de Autor

LEY DE LA PROPIEDAD INDUSTRIAL

Se puede inferir básicamente que con la ley de propiedad industrial se busca el proteger obras artísticas científicas industriales y comerciales en los campos de servicios, marcas y patentes, dicha ley va encaminada a la protección de modelos de utilidad, diseños industriales, secretos industriales, signos distintivos, marcas avisos, nombres comerciales y denominaciones de origen, los cuales pueden ser susceptibles de apropiación y pero aun de manera ilícita.

En México para la regulación de dicha propiedad industrial contamos con el Instituto Mexicano de Propiedad Industrial, pero los alcances de dicho organismo son muy limitados en el ciber espacio ya es prácticamente imposible la protección o reconocimiento de los derechos que establece esta ley, que a continuación se transcriben los artículos más referentes a dichas cuestiones en materia de delitos informáticos.

Artículo 2o.- Esta ley tiene por objeto:

I.- Establecer las bases para que, en las actividades industriales y comerciales del país, tenga lugar un sistema permanente de perfeccionamiento de sus procesos y productos;

II.- Promover y fomentar la actividad inventiva de aplicación industrial, las mejoras técnicas y la difusión de conocimientos tecnológicos dentro de los sectores productivos;

III.- Propiciar e impulsar el mejoramiento de la calidad de los bienes y servicios en la industria y en el comercio, conforme a los intereses de los consumidores;

IV.- Favorecer la creatividad para el diseño y la presentación de productos nuevos y útiles;

V. *Proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de invención; registros de modelos de utilidad, diseños industriales,*

marcas, y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen, y regulación de secretos industriales;

VI. Prevenir los actos que atenten contra la propiedad industrial o que constituyan competencia desleal relacionada con la misma y establecer las sanciones y penas respecto de ellos, y

VII. Establecer condiciones de seguridad jurídica entre las partes en la operación de franquicias, así como garantizar un trato no discriminatorio para todos los franquiciatarios del mismo franquiciante.

LEY DE INSTITUCIONES DE CRÉDITO

La presente ley se encuentra íntimamente ligada a la regulación de la banca y crédito, las cuales a su vez son el blanco principal para aquellas personas infractoras conocidas como delincuentes de cuello blanco, los cuales tienen altos conocimientos en cuestiones informáticas o bien se encuentran en un lugar de oportunidad al contar con todas las facilidades para la comisión de dichos delitos.

Artículo 1o.- La presente Ley es de orden público y observancia general en los Estados Unidos Mexicanos y tiene por objeto regular el servicio de banca y crédito, la organización y funcionamiento de las instituciones de crédito, las actividades y operaciones que las mismas podrán realizar, su sano y equilibrado desarrollo, la protección de los intereses del público y los términos en que el Estado ejercerá la rectoría financiera del Sistema Bancario Mexicano.

Artículo 2o.- El servicio de banca y crédito sólo podrá prestarse por instituciones de crédito, que podrán ser:

I. Instituciones de banca múltiple, y

II. Instituciones de banca de desarrollo.

Capítulo IV De los Delitos

Artículo 112.- Se sancionará con prisión de tres meses a dos años y multa de treinta a dos mil días de salario cuando el monto de la operación, quebranto o perjuicio patrimonial, según corresponda, no exceda del equivalente a dos mil días de salario.

Cuando el monto de la operación, quebranto o perjuicio patrimonial, según corresponda, exceda de dos mil y no de cincuenta mil días de salario; se sancionará con prisión de dos a cinco años y multa de dos mil a cincuenta mil días de salario.

Cuando el monto de la operación, quebranto o perjuicio patrimonial según corresponda, exceda de cincuenta mil, pero no de trescientos cincuenta mil días de salario, se sancionará con prisión de cinco a ocho años y multa de cincuenta mil a doscientos cincuenta mil días de salario.

Cuando el monto de la operación, quebranto o perjuicio patrimonial según corresponda, exceda de trescientos cincuenta mil días de salario, se sancionará con prisión de ocho a quince años y multa de doscientos cincuenta mil a trescientos cincuenta mil días de salario.

Considerando el monto de la operación, quebranto o perjuicio patrimonial, las sanciones previstas en este artículo se impondrán a:

I. Las personas que con el propósito de obtener un crédito, proporcionen a una institución de crédito, datos falsos sobre el monto de activos o pasivos de una entidad o persona física o moral, si como consecuencia de ello resulta quebranto o perjuicio patrimonial para la institución;

Serán sancionados hasta en una mitad más de las penas previstas en este artículo, aquéllos funcionarios, empleados o comisionistas de terceros intermediarios o de constructoras, desarrolladoras de inmuebles y/o agentes inmobiliarios o comerciales, que participen en la solicitud y/o trámite para el otorgamiento del crédito, y conozcan la falsedad de los datos sobre los montos de los activos o pasivos de los acreditados, o que directa o indirectamente alteren o sustituyan la información mencionada, para ocultar los datos reales sobre dichos activos o pasivos;

II. Las personas que para obtener créditos de una institución de crédito, presenten avalúos que no correspondan a la realidad, resultando como consecuencia de ello quebranto o perjuicio patrimonial para la institución;

III. Los consejeros, funcionarios, empleados de la Institución de crédito o quienes intervengan directamente en la autorización o realización de operaciones, a sabiendas de que éstas resultarán en quebranto o perjuicio al patrimonio de la institución.

Se consideran comprendidos dentro de lo dispuesto en el párrafo anterior y, consecuentemente, sujetos a iguales sanciones, los consejeros, funcionarios, empleados de instituciones o quienes intervengan directamente en lo siguiente:

a) Que otorguen créditos a sociedades constituidas con el propósito de obtener financiamientos de instituciones de crédito, a sabiendas de que las mismas no han integrado el capital que registren las actas constitutivas correspondientes;

b) Que para liberar a un deudor, otorguen créditos a una o varias personas físicas o morales, que se encuentren en estado de insolvencia, sustituyendo en los registros de la institución respectiva unos activos por otros;

c) Que otorguen créditos a personas físicas o morales cuyo estado de insolvencia les sea conocido, si resulta previsible al realizar la operación, que carecen de capacidad económica para pagar o responder por el importe de las sumas acreditadas, produciendo quebranto o perjuicio patrimonial a la Institución;

d) Que renueven créditos vencidos parcial o totalmente a las personas físicas o morales a que se refiere el inciso anterior si resulta previsible al realizar la operación, que carecen de capacidad económica para pagar o responder por el importe de las sumas acreditadas, produciendo quebranto o perjuicio patrimonial a la Institución, y

e) Que a sabiendas, permitan a un deudor desviar el importe del crédito en beneficio propio o de terceros, y como consecuencia de ello, resulte quebranto o perjuicio patrimonial a la institución;

Para efectos de lo previsto en el primer párrafo de la presente fracción, no se considera que causen un quebranto o perjuicio al patrimonio de la institución las operaciones que se celebren como parte de procesos de reestructuración de operaciones de pago que se realicen en términos del artículo 65 de esta Ley.

IV. Los deudores que no destinen el importe del crédito a los fines pactados, y como consecuencia de ello resulte quebranto o perjuicio patrimonial a la institución, y

V. Los acreditados que desvíen un crédito concedido por alguna institución a fines distintos para los que se otorgó, si dicha finalidad fue determinante para el otorgamiento del crédito en condiciones preferenciales.

Artículo 112 Quáter.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:

I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o

II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

Artículo 113.- Serán sancionados con prisión de dos a diez años y multa de quinientos a cincuenta mil días de salario, los consejeros, funcionarios o empleados de las instituciones de crédito o quienes intervengan directamente en el otorgamiento del crédito:

I. Que omitan u ordenen omitir registrar en los términos del artículo 99 de esta Ley, las operaciones efectuadas por la institución de que se trate, o que alteren u ordenen alterar los registros para ocultar la verdadera naturaleza de las operaciones realizadas, afectando la composición de activos, pasivos, cuentas contingentes o resultados;

II. Que presenten a la Comisión Nacional Bancaria y de Valores datos, informes o documentos falsos o alterados sobre la solvencia del deudor o sobre el valor de las garantías que protegen los créditos;

III. Que, conociendo la falsedad sobre el monto de los activos o pasivos, concedan el crédito;

IV. Que conociendo los vicios que señala la fracción II del artículo 112 de esta Ley, concedan el crédito, si el monto de la alteración hubiere sido determinante para concederlo;

V. Que proporcionen o permitan que se incluyan datos falsos en los documentos, informes, dictámenes, opiniones, estudios o calificación crediticia, que deban presentarse a la Comisión Nacional Bancaria y de Valores en cumplimiento de lo previsto en esta Ley;

VI. Que destruyan u ordenen que se destruyan total o parcialmente, los sistemas o registros contables o la documentación soporte que dé origen a los asientos contables respectivos, con anterioridad al vencimiento de los plazos legales de conservación, y

VII. Que destruyan u ordenen que se destruyan total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de impedir u obstruir los actos de supervisión y vigilancia de la Comisión Nacional Bancaria y de Valores.

Artículo 113 bis.- A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de recursos o valores de los clientes de las instituciones de crédito, se le aplicará una sanción de tres a diez años de prisión y multa de quinientos a treinta mil días de salario.

Si quienes cometen el delito que se describe en el párrafo anterior son funcionarios o empleados de las instituciones de crédito o terceros ajenos pero con acceso autorizado por éstas a los sistemas de las mismas, la sanción será de tres a quince años de prisión y multa de mil a cincuenta mil días de salario.

Artículo 113 bis 1.- Los consejeros, funcionarios, comisarios o empleados de una institución de crédito que inciten u ordenen a funcionarios o empleados de la institución a la comisión de los delitos a que se refiere la fracción III, del artículo 112 y los artículos 113 y 113 Bis, serán sancionados hasta en una mitad más de las penas previstas en los artículos respectivos.

Artículo 113 bis 2.- Serán sancionados los servidores públicos de la Comisión Nacional Bancaria y de Valores, con la pena establecida para los delitos correspondientes más una mitad, según se trate de los delitos previstos en los artículos 111 a 113 Bis y 114 de esta ley, que:

a) Oculten al conocimiento de sus superiores hechos que probablemente puedan constituir delito;

b) Permitan que los funcionarios o empleados de la institución de crédito alteren o modifiquen registros con el propósito de ocultar hechos que probablemente puedan constituir delito;

c) Obtengan o pretendan obtener un beneficio a cambio de abstenerse de informar a sus superiores hechos que probablemente puedan constituir delito;

d) Ordenen o inciten a sus inferiores a alterar informes con el fin de ocultar hechos que probablemente puedan constituir delito, o

e) Incite u ordene no presentar la petición correspondiente, a quien esté facultado para ello.[127]

[127] Ley De Instituciones De Crédito

LEY FEDERAL DE JUEGOS Y SORTEO

En dicho ámbito de igual manera se encuentra expuesta la tecnología de sufrir atentados como se ha presentado con casos prácticos en el capítulo tercero de la presente investigación.

Articulo 1.- Quedan prohibidos en todo el territorio nacional, en los términos de esta Ley, los juegos de azar y los juegos con apuestas.

LEY DE SEGURIDAD NACIONAL

UNICO

Artículo 3. Para efectos de esta Ley, por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven ha:

I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país;

II. La preservación de la soberanía e independencia nacionales y la defensa del territorio;

III. El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;

IV. El mantenimiento de la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

V. La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional, y

VI. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes.

Artículo 4. La Seguridad Nacional se rige por los principios de legalidad, responsabilidad, respeto a los derechos fundamentales de protección a la

persona humana y garantías individuales y sociales, confidencialidad, lealtad, transparencia, eficiencia, coordinación y cooperación.

Artículo 5. Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:

I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;

II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;

III. Actos que impidan a las autoridades actuar contra la delincuencia organizada;

IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;

VI. Actos en contra de la seguridad de la aviación;

VII. Actos que atenten en contra del personal diplomático;

VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;

IX. Actos ilícitos en contra de la navegación marítima;

X. Todo acto de financiamiento de acciones y organizaciones terroristas;

XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y

XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos. (DR)IJ

Artículo 6. Para los efectos de la presente Ley, se entiende por:

I. Consejo: Consejo de Seguridad Nacional.

II. Instancias: Instituciones y autoridades que en función de sus atribuciones participen directa o indirectamente en la Seguridad Nacional.
III. Red: Red Nacional de Investigación.
IV. Centro: Centro de Investigación y Seguridad Nacional, y
V. Información gubernamental confidencial: los datos personales otorgados a una instancia por servidores públicos, así como los datos personales proporcionados al Estado Mexicano para determinar o prevenir una amenaza a la Seguridad Nacional.

LEY FEDERAL CONTRA LA DELINCUENCIA ORGANIZADA

ARTÍCULO 2.- Cuando tres o más personas se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos de los delitos siguientes, serán sancionadas por ese solo hecho, como miembros de la delincuencia organizada:

I. Terrorismo, previsto en los artículos 139 a 139 Ter y terrorismo internacional previsto en los artículos 148 Bis al 148 Quáter; contra la salud, previsto en los artículos 194 y 195, párrafo primero; falsificación o alteración de moneda, previstos en los artículos 234, 236 y 237; el previsto en la fracción IV del artículo 368 Quáter en materia de hidrocarburos; operaciones con recursos de procedencia ilícita, previsto en el artículo 400 Bis; y el previsto en el artículo 424 Bis, todos del Código Penal Federal;

II. Acopio y tráfico de armas, previstos en los artículos 83 bis y 84 de la Ley Federal de Armas de Fuego y Explosivos;

III. Tráfico de indocumentados, previsto en el artículo 159 de la Ley de Migración;

IV. Tráfico de órganos previsto en los artículos 461, 462 y 462 bis de la Ley General de Salud;

V. Corrupción de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo previsto en el artículo 201; Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, previsto en el artículo 202; Turismo sexual en contra de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tiene capacidad para resistirlo, previsto en los artículos 203 y 203 Bis; Lenocinio de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, previsto en el artículo 204; Asalto, previsto en los artículos 286 y 287; Tráfico de menores o personas que no tienen capacidad para comprender el significado del hecho, previsto en el artículo 366 Ter, y Robo de vehículos, previsto en los artículos 376 Bis y 377 del Código Penal Federal, o en las disposiciones correspondientes de las legislaciones penales estatales o del Distrito Federal;

VI. Delitos en materia de trata de personas, previstos y sancionados en el Título Segundo de la Ley General para Combatir y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos, excepto en el caso de los artículos 32, 33 y 34 y sus respectivas tentativas punibles.

LEGISLACIONES LOCALES

CODIGO PENAL PARA EL ESTADO DE MORELOS

DE LOS DELITOS INFORMATICOS

ARTÍCULO 148 quarter.- Comete el delito informático, la persona que dolosamente y sin derecho:

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;

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;

III. Haga uso de la red de Internet utilizando cualquier medio para realizar actos en contra de las personas o cosas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para perturbar la paz pública o que atente contra el orden constitucional; y

IV. Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

CODIGO PENAL PARA EL ESTADO DE SINALOA
CAPITULO V
DELITTO INFORMATICO

Artículo 217.- Comete delito informático, la persona que dolosamente sin derecho:

I.- Use o entre a una base de datos, sistema de computadores de red de computadoras o a cualquier parte de la misma, con el propósito 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

II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programas de computadora o los datos contenidos en la misma, a en la base sistema o red.

Al responsable del delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días de multa.

CODIGO PENAL PARA EL DISTRITO FEDERAL
CAPITULO III

Artículo 230. Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán:

I. De veinticinco a setenta y cinco días multa, cuando el valor de lo defraudado no exceda de cincuenta veces el salario mínimo, o no sea posible determinar su valor;

II. Prisión de cuatro meses a dos años seis meses y de setenta y cinco a doscientos días multa, cuando el valor de lo defraudado exceda de cincuenta pero no de quinientas veces el salario mínimo;

III. Prisión de dos años seis meses a cuatro años y de doscientos a quinientos días multa, cuando el valor de lo defraudado exceda de quinientas pero no de cinco mil veces el salario mínimo;

IV. Prisión de cuatro a seis años y de quinientos a ochocientos días multa, cuando el valor de lo defraudado exceda de cinco mil pero no de diez mil veces el salario mínimo; y

V. Prisión de seis a once años y de ochocientos a mil doscientos días multa, cuando el valor de lo defraudado exceda de diez mil veces el salario mínimo.

Cuando el delito se cometa en contra de dos o más personas, se impondrá además las dos terceras partes de las penas previstas en las fracciones anteriores.

CODIGO PENAL PARA EL ESTADO DE VERACRUZ

CAPITULO III

DELITOS INFORMATICOS

Artículo 181.- Comete delito informático quien, sin derecho y con perjuicio de tercero:

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

II.- Intercepte, interfiera, use, altere, dañe o destruya un soporte o programa informático o la información contenida en el mismo o en la base, sistema o red.

Al responsable de este delito se le impondrá de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementan en una mita

PROPUESTAS

Acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.

Acuerdos globales en la definición legal de dichas conductas delictivas.

Especialización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

Creación de tratados de extradición, de acuerdos de ayuda mutua y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile por ejemplo; en virtud de lo anterior crear tratados o convenios con dichos países con la finalidad de homologar criterio y leyes.

Se destine de acuerdo a lo establecido en el Presupuesto de Egresos de la Federación a la profesionalización y equipamiento de los cuerpos de seguridad pública en los municipios y demarcaciones territoriales del Distrito Federal, mejoramiento de la infraestructura de las corporaciones.

Capacitación de los ministerios públicos y peritos a nivel federal y nacional para atender la problemática de los diversos delitos realizados por medio de un ordenador.

Desarrollo de políticas públicas para informar a la población en general de la diversidad de delitos y así prevenir dichas conductas.

BIBLIOGRAFIA

Awad M. Elías, Procesamiento Automático de Datos, 18ª ed. Ed. Mc Graw Hill, México, 1982.

Azaola Calderón, Luis, Delitos informáticos y derecho Penal, 1ª Ed. México, Ed. Ubijus, 2010.

Barriuso Ruiz, Carlos, La contratación electrónica, Madrid, Dykison, S.L., 2002, p. 37.

Cámpoli, Gabriel. Delitos Informáticos en la Legislación Mexicana. INACIPE. México 2005.

Castrillón y Luna, Víctor Manuel, La Protección Constitucional de los Derechos Humanos. Ed. Porrúa México 2006.

M. Correa, Carlos, Derecho Informático 5ª ed. Buenos Aires, Ed. Depalma.

Correa, Carlos, y otros. Derecho Informático, Buenos aires, Argentina, Ed. Depalma.

Fernando Castellanos, Lineamientos Elementales del Derecho penal 39ª Ed. México, Ed. Porrúa,1998.

Fix Fierro, Héctor, Informática y documentación jurídica, México, UNAM, Facultad de Derecho, 1990.

Flores Salgado, Lucerito, Derecho Informático.

Franco Guzmán, Ricardo, Análisis de los delitos informáticos. Ed. Porrúa. México 2005.

Franco Guzmán, Ricardo. Análisis de los delitos informáticos. Ed. Porrúa. México 2005..

Lima Malvado, María de la Luz. Delitos Electrónicos, Criminalia. México, Ed. Porrúa No. 1-6. Año L, Enero-Junio, 1984.

Lira Arteaga, Oscar Manuel CIBERCRIMINALIDAD, Instituto Nacional de Ciencias Penales. Primera edición México 2010.

Livas, Javier, Cibernética, Estado y Derecho, México, Gernika.

López Betancourt, Eduardo, Delitos en particular, México, Porrúa, 2004.

Losano, Mario G., Introducción a la Informática Jurídica, España, Universidad de Palma de Mallorca, Facultad de Derecho, 1982.
M. Correa, Carlos, Derecho Informático 5ª ed. Buenos Aires, Ed. Depalma.

Manual de los Derechos Humanos en México, Emilio Álvarez Icaza Longoria, Primera edición: Nostra Ediciones, 2009.

Molina Salgado, Jesús Antonio, Breviarios Jurídicos, 1ª ed., Editorial Porrúa, S.A. de C.V., México, D, F, 2003.

Montero Zendejas, Daniel, Derecho Penal y Crimen Organizado: Crisis de la Seguridad, 1ª Ed. México, Ed. Porrúa 2008.

Montiel Sosa, Juventino: CRIMINALÍSTICA. Editorial Limusa. Segunda edición México 2007.

Muñoz Torres, Ivonne. “Delitos Informáticos. Diez Años Después”.

Nava Garcés, Alberto, Delitos Informáticos, México, Porrúa, 2007.

Orts Berenguer, Enrique y Margarita Roig Torres, Delitos informáticos y delitos comunes cometidos a través de la informática, Tirant lo Blanch, “colección de delitos”, Valencia España, 2001.

Palazzi, Pablo A. Delitos Informáticos, 1ª ed. Ad Hoc, Buenos Aires, 2000.
Pérez Luño, Antonio Enrique, Ensayos de Informática Jurídica, ed. Coyoacán, 2009.

Ríos Estavillo, Juan José, Derecho e informática en México, Instituto de Investigaciones Jurídicas, Serie E: varios, numero 83, Universidad Nacional Autónoma de México, México, 1997.

Rodríguez Gilberto. Revista y Computación. 17° ed. SEP. México, 1987

Rojas Amandi, Víctor Manuel “El uso de internet en el derecho” ed. Oxford .

Sanders Donald, Informática Presente y Futuro, 4ª ed. Ed. Mc Graw Hill, México, 1985.

Sarzana, Carlos. Criminalita e Tecnología Computer Crimes, Resegna Penitenziaria e Criminología Nos. 1-2. 1, Gennaio-Geugno, 1979, Roma, Italia.

Simón Hocsman, Heriberto, Negocios en Internet, Editorial Astrea, Cd. Buenos Aires, Argentina.

Ulbarri Millan J. Manuel y otro, Computación 6ª ed. Sep México, 1988. UNESCO Organización de las Naciones Unidas para la educación, la Ciencia y la Cultura .

Zabale, Ezequiel, “La competencia en materia de acciones civiles o penales derivadas del uso de la red Internet”, Derechos Informáticos, Argentina, 2002.

LEYES CONSULTADAS

Código de Comercio

Código Penal Federal

Constitución Política De Los Estados Unidos Mexicanos

Ley De Instituciones De Crédito

Ley Federal de Derechos de Autor

Ley Federal de Derechos de Autor

Ley Federal de Telecomunicaciones

FUENTES CONSULTADAS

Área del Derecho civil de la Universidad de Girona, España. http://civil.udg.es/normacivil/estatal/contract/LSSI.htm

Consulta Virtual en: http://www.ecured.cu/index.php/Cracker.

Consulta Virtual: Acurio Del Pino, Santiago. *La delincuencia Informática transnacional y la UDIMP* en http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/acurio.pdf

Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de Junio de 2000, www.mityc.es/NR/rdonlyres/62C8DF55-516E-4294-90A2-69F754C8AAE0/0/3Directiva_2000_31_CE.pdf.

Eur-LEx, Directiva 93/34CE. Http: //eur-lex.europa.eu/ LexUriServ/ site/ es/oj/ 1998/l_204/ l_20419980721es00370048.

http://books.google.com.mx/books?id=mWk1VSOpmA8C&pg=PA112&lpg=PA112&dq=clasificaci%C3%B3n+de+Uhlrich+Sieber&source=bl&ots=pigTqHh4jC&sig=8Z4gX6Ie0H7crDySy5AbKgb80AQ&hl=es-419&sa=X&ei=IP6jUM3CNaHJyAGP9oHABQ&sqi=2&ved=0CBwQ6AEwAA#v=onepage&q=clasificaci%C3%B3n%20de%20Uhlrich%20Sieber&f=false
http://comunidad.derecho.org/mjviega/deli_inf.htm,

http://criminologiausco.blogspot.mx/2005/08/concepto-de-criminologa.html.

http://delitosinformaticos.com/legislacion/espana.shtml.

http://delitosinformaticos.weebly.com/policia-cibernetica.html.

http://es.wikipedia.org/wiki/Convenio_sobre_cibercriminalidad.

http://europa.eu/rapid/press-release_IP-13-13_es.htm.

http://justiciaforense.com/material/ARCHIVOS%20FORENSES/CRIMINALISTICA%20GENERAL%20Y%20DE%20CAMPO/ARCHIVOS%20PDF/NOCIONES%20DE%20CRIMINALISTICA.pdf.

http://translate.google.com.mx/translate?hl=es&sl=en&u=http://www.fbi.gov/&prev=/search%3Fq%3Dfbi%26biw%3D1366%26bih%3D667.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf.
http://www.disc.unam.mx/2005/presentaciones/delitos_menores.pdf.
http://www.elsiglodetorreon.com.mx/noticia/18839.las-funciones-de-la-policia-cibernetica-de-me.html consultada.

http://www.intelpage.info/web/europol.htm.

http://www.interpol.int/es/Acerca-de-INTERPOL/Estructura-y-gobernanza.

http://www.interpol.int/es/Criminalidad/Delincuenciainform%C3%A1tica/Cibe

http://www.nacion.com/2012-09-10/Opinion/adhesion-al-convenio-europeo-sobre-ciberdelincuencia.aspx.

http://www.oem.com.mx/oem/notas/n1875272.htm

http://www.revista.unam.mx/vol.4/num4/art7/ago_art7.pdf.

http://www.ssp.gob.mx/application?pageid=pcibernetica.
Levine Gutierrez Guillermo, Ulibarri Milan. J. Manuel y otros. Computación Óp. Cit.

http://www.unesco.org/new/es/www.taringa.net/posts/info/9270756/Los-10-hackers-mas-famosos.html

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

DIVISIÓN DE ESTUDIOS SUPERIORES DE POSGRADO

Daniel Montero Zendejas

Doctor en Derecho de la Facultad
De Derecho de la UAEM.

Emite el siguiente:

VOTO RAZONADO

Otorgado al trabajo de tesis titulado:

"PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS"

Que para optar el grado de Maestro en Derecho, programa
Educativo incorporado al programa Nacional de Posgrado de
Calidad del Consejo Nacional de Ciencias y Tecnología
Presenta el alumno: LIC. OSCAR MANUEL VENCES SANCHEZ

FUNDAMENTO

En primer termino es de vital importancia resaltar el avance tecnológico, del cual hemos sido participes, el cual nos ha cambiado la vida, trayendo consigo una evolución en los diversos ámbitos en los que nos encontramos involucrados, pero a la vez dichos avances traen consigo una modalidad de delitos, el cual no solo requiere de un análisis jurídico local, sino en un contexto nacional globalizado.

Atendiendo a la importancia del tema así como de su estrecha vinculación con la vida cotidiana de las personas, es que el tema expuesto por el Lic. Oscar Manuel Vences Sánchez, es de vital importancia para su estudio así como los métodos de prevención que en el mismo se atendieron

gracias a las aportaciones que en el realizó el Dr. Daniel Montero Zendejas, para el beneficio de una sociedad en pleno desarrollo tecnológico.

ESTRUCTURA Y CONTENIDO

Por lo que respecta a la estructura y contenido de la presente investigación se puede apreciar que el alumno durante la misma, la estructura es cuatro capítulos, los cuales se encuentran detallados de una manera adecuada; iniciando los mismos en el primer capítulo con una familiarización con el método de análisis, así como los conceptos, de os cuales se abarcaron durante el desarrollo de la presente tesis; de igual manera se contempla un capítulo de antecedentes para poder ubicarnos en la historia de los avances tecnológicos, posteriormente se realiza un estudio comparado con las diversas legislaciones a nivel nacional para poder emitir una conclusión debidamente estructurada respecto del tema en cuestión.

VALORACION

Una vez analizada la presente tesis, su metodología así como sus conclusiones y propuestas que para obtener el grado de maestro debe de contener las mismas, se puede afirmar que una vez analizada y valorada la presente investigación, cuenta con los requisitos para su aprobación. Por lo tanto a manera de conclusión el alumno el Lic. Oscar Manuel Vences Sánchez, ha elaborado una investigación cuyas conclusiones son acordes a un estudio detallado sobre el tema tratado, por lo que bajo mi criterio y previa revisión de los comités tutoriales del presente trabajo de investigación reúne el nivel y calidad que se requiere para una tesis de grado. Derivado de lo anterior es para mi un gran honor otorgar mi

VOTO APROBATORIO

Cuernavaca Morelos 27 de septiembre de 2019

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

Cuernavaca, Morelos a 2 de octubre del 2019.

MTRO. PEDRO HURTADO OBISPO
COORDINADOR DEL PROGRAMA EDUCATIVO
DE MAESTRIA DE LA FACULTAD DE DERECHO
Y CIENCIAS SOCIALES
P R E S E N T E.

Por medio de la presente me dirijo a usted para manifestarle que habiendo sido designado por usted como miembro de la comisión revisora en el desarrollo del trabajo de tesis tendente a la obtención del grado académico de Maestro en Derecho, dentro del programa de Maestría en Derecho, elaborado por el Licenciado en Derecho **OSCAR MANUEL VENCES SÁNCHEZ**, y que se intitula **"PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS"**, dicha investigación a mi parecer se ha concluido satisfactoriamente, por lo que otorgo mi **VOTO APROBATORIO**, ya que se trata de un trabajo de investigación original, en el cual el sustentante demuestra la hipótesis que plantea y en la que sigue métodos de investigación científica, y un sustento en el derecho interno, contrastado y analizado en relación al derecho internacional y en al derecho comparado, con una amplia y especializada fuente de consultas que refuerzan su aparato crítico, y que incluye también las conclusiones y propuestas con una propuesta legislativa aterrizada a un instrumento jurídico.

Por todo lo anterior, manifiesto a usted que, en mi carácter de revisor de la citada investigación, la apruebo plenamente a efecto de que la interesada pueda continuar con los trámites pertinentes para la celebración de su examen recepcional.

ATENTAMENTE

DR. RICARDO TAPIA VEGA
Profesor de Tiempo Completo "C" de
la Facultad de Derecho y Ciencias Sociales de la UAEM

Cuernavaca, Mor., septiembre 26 del 2019

C. DR. VICTOR MANUEL CASTRILLON Y LUNA,
COORDINADOR DE LA DIVISIÓN DE ESTUDIOS DE POSGRADO
FACULTAD DE DERECHO Y CIENCIAS SOCIALES,
UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS.
P R E S E N T E.

Muy Distinguido Doctor Castrillón Luna:

El C. LIC. OSCAR MANUEL VENCES SÁNCHEZ, alumno del programa de Maestría en Procuración y administración de justicia, ha presentado para su análisis al suscrito un trabajo de investigación que lleva por título, **"PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS"**, con el cual pretende optar por el grado de Maestro en Derecho.

El Lic. Vences Sánchez, concluyo el trabajo en cuestión y que, desde mi muy particular punto de vista, reúne los requisitos reglamentarios y estatutarios, establecidos por la Legislación Universitaria de nuestra alma mater, y por este conducto como revisor de tesis le otorgo mi voto aprobatorio.

El trabajo presentado por el Lic. Oscar Manuel Vences Sánchez, desde mi personal punto de vista, merece este voto, así como la autorización para que si usted no tiene inconveniente se le pueda conceder el derecho de presentar el exámen de grado de Maestro en Derecho.

Aprovecho la oportunidad para enviarle un afectuoso saludo y despedirme como siempre a sus respetables órdenes.

A T E N T A M E N T E.

DR. JULIO CABRERA DIRCIO
PROF. INVEST. T. C. DE LA FACULTAD
DE DERECHO Y CIENCIAS SOCIALES
DE LA U.A.E.M.

Av. Universidad 1001 Col. Chamilpa Cuernavaca, Mor. C.P. 62210
Tel (7)3297061 pagina web www.derecho.uaem.mx
dr.juliocabreradircio@hotmail.com

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

DIVISIÓN DE ESTUDIOS SUPERIORES DE POSGRADO

Héctor González Chevez

Doctor en Derecho de la Facultad
De Derecho y Ciencias Sociales de la UAEM.

Emite el siguiente:

VOTO RAZONADO

Otorgado al trabajo de tesis titulado:

"PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS"

Que para optar el grado de Maestro en Derecho, programa
Educativo Incorporado al Programa Nacional de Posgrado de
Calidad del Consejo Nacional de Ciencia y Tecnología
Presenta el alumno: LIC. OSCAR MANUEL VENCES SANCHEZ

FUNDAMENTO

En primer termino es de vital importancia resaltar el avance tecnológico, del cual hemos sido participes, el cual nos ha cambiado la vida, trayendo consigo una evolución en los diversos ámbitos en los que nos encontramos involucrados, pero a la vez dichos avances traen consigo una nueva modalidad de delitos, el cual no solo requiere de un análisis jurídico local, si no en un contexto nacional globalizado.

Atendiendo a la importancia del tema así como de su estrecha vinculación con la vida cotidiana de las personas, es que el tema expuesto por el Lic. Oscar Manuel Vences Sánchez, es de vital importancia para su estudio, así como los métodos de prevención que en el mismo se atendieron, para el beneficio de una sociedad en pleno desarrollo tecnológico.

Por lo que se puede destacar que el alumno, en la tesis que presenta ha llevado una metodología jurídica, asi como un estricto apego a la realidad jurídica, respecto a sus conclusiones y propuestas en la presente investigación.

ESTRUCTURA Y CONTENIDO

Por lo que respecta a la estructura y contenido de la presente investigación se puede apreciar que el alumno durante la misma, la estructura en cuatro capítulos, los cuales se encuentran detallados de una manera adecuada; iniciando los mismos en el primer capitulo con una familiarización con el método de análisis, así como los conceptos, de los cuales se abarcaron durante el desarrollo de la presente tesis; de igual manera se contempla un capitulo de antecedentes para poder ubicarnos en la historia de los avances tecnológicos, posteriormente se realiza un estudio comparada con las diversas legislaciones a nivel internacional y por ultimo un estudio comparativo a nivel nacional para poder emitir una conclusión debidamente estructurada respecto del tema en cuestión.

VALORACIÓN

Una vez analizada la presente tesis, su metodología, asi como sus conclusiones y propuestas, que para obtener el grado de maestro debe de contener las misma, se puede afirmar que una vez analizada y valorada la presente investigación, cuenta con los requisitos, para su aprobación. Por lo tanto podemos afirmar que el alumno el Lic. Oscar Manuel Vences Sánchez, ha elaborado una investigación cuyas conclusiones son acordes a un estudio detallado sobre el tema tratado, por lo que bajo mi criterio y previa revisión de los comités tutoriales del presente trabajo de investigación, reúne el nivel y calidad, que se requiere para una tesis de grado. Derivado de lo anterior es para mi un gran honor otorgar mi

VOTO APROBATORIO

Cuernavaca Morelos a 14 de mayo de dos mil catorce.

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS.
FACULTAD DE DERECHO Y CIENCIAS SOCIALES

Profesor Investigador de Tiempo Completo de la Facultad de Derecho y Ciencias Sociales

Cuernavaca, Morelos, a 14 de mayo de 2014.

DR. EDUARDO OLIVA GÓMEZ.
JEFE DE LA DIVISIÓN DE ESTUDIOS SUPERIORES DE LA FACULTAD DE DERECHO Y CIENCIAS SOCIALES.
P R E S E N T E

En relación con el trabajo de tesis desarrollado por el **LICENCIADO OSCAR MANUEL VENCES SÁNCHEZ intitulado "PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS"**, que presenta para obtener el grado de Maestro en Derecho, por la Facultad de Derecho y Ciencias Sociales de la Universidad Autónoma del Estado de Morelos, y que se me encomendó como miembro de la Comisión Revisora; me permito manifestarle lo siguiente:

En virtud de que la tesis contiene un serio trabajo de investigación y novedoso, aunado de una extensa bibliografía que apoya el contenido de la problemática que aborda; una hipótesis que responde al problema planteado y argumentando, con sustento jurídico; un marco teórico acorde a la legislación vigente; y una estructura capitular que responde a la hipótesis, con su consecuente desarrollo metodológico, reflejado en la lógica de los argumentos jurídicos, por lo que otorgo mi **VOTO APROBATORIO**, para que el trabajo de investigación desarrollado, sea sustentado como tesis en el correspondiente Examen de Grado.

A T E N T A M E N T E

Dr. Francisco Xavier García Jiménez
Profesor Investigador de Tiempo Completo de la Facultad de Derecho y Ciencias Sociales