UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

TITULO DE LA TESIS

LA NECESIDAD DE REGULAR EL DELITO INFORMÁTICO EN EL CÓDIGO PENAL PARA EL DISTRITO FEDERAL

T E S I S

QUE PARA OBTENER EL TÍTULO DE

L I C E N C I A D O E N D E R E C H O

P R E S E N T A:

JONÁS NOÉ GIRÓN DEL RÍO

ASESOR:
MTRA. MA. GRACIELA LEÓN LÓPEZ

Nezahualcóyotl, Estado de México, 28 DE AGOSTO 2014

ÍNDICE

CAPÍTULO PRIMERO MARCO TEÓRICO DE LA INFORMÁTICA

Página

1. Nociones y Concepto de Informática……..1

1.1.1 Orígenes de la computación…… ……..2
1.1.2 Concepto de computadora…… ……4
1.1.3 Estructura de una computadora……4
1.1.4 Nivel Operacional……5
1.1.5 Nivel Estructural……6
a. Hardware……6
b. Software……7
c. Lenguaje de programción……..7

CAPÍTULO SEGUNDO MARCO TEÓRICO DEL DELITO INFORMÁTICO

2. Relación entre Informática y Derecho……..9
2.1 Derecho Informático……10
2.2 Antecedentes del Derecho Informático……12
2.3 Orígenes de la Informática Jurídica……14
2.4 Concepto de Delito Informático……17

CAPÍTULO TERCERO ANÁLISIS DEL DELITO INFORMÁTICO

3. Análisis del Delito Informático……19
3.1 Elementos Jurídicos del Delito Informático……..19
3.2 Presupuestos del Delito Informático……20
3.2.1 Sujeto Activo……20

3.2.2 Sujeto Pasivo……21
3.2.3 Objeto Material……22
3.2.4 Bien Jurídico Tutelado……23
3.3 Clasificación del Delito Informático……24
3.4 Características del Delito Informático……26

CAPÍTULO CUARTO MARCO LEGAL DEL DELITO INFORMÁTICO

4.- Ámbito Internacional……27

4.1 ONU……28
4.2 UNESCO……32
4.3 OCDE……34
4.4 AIDP……36

4.5 Legislaciones de otros países respecto al Delito Informático……38
4.5.1 Alemania……39
4.5.2 Argentina……40
4.5.3 Austria……49
4.5.4 Brasil……50
4.5.5 Chile……51
4.5.6 Costa Rica……52
4.5.7 España……53
4.5.8 Estados Unidos de Norteamérica……54
4.5.9 Francia……55
4.5.10 Perú……56

4.6 Marco Jurídico Nacional del Delito Informático……56
4.6.1 Constitución Política de los Estados Unidos Mexicanos……57
4.6.2 Código Penal Federal……59
4.6.3 Código Penal del Estado de Aguascalientes……62
4.6.4 Código Penal para el Estado de Baja California……64
4.6.5 Código Penal para el Estado de Colima……65
4.6.6 Código Penal del Estado de México……68
4.6.7 Código Penal para el Estado de Guanajuato……71
4.6.8 Código Penal del Estado de Morelos……72
4.6.9 Código Penal del Estado de Sinaloa……74
4.6.10 Código Penal del Estado de Zacatecas……75
4.6.11 Código Penal para el Distrito Federal……76

PROPUESTA LA NECESIDAD DE REGULAR EL DELITO INFORMÁTICO**….79**

Conclusiones……..84

Anexos……86

A mi Familia:
Quiénes me han acompañado en mi vida,
tanto académica como en lo personal,
apoyándome incondicionalmente y quienes
han sido un pilar fundamental en mi persona,
no sería posible ser la persona que soy sin ellos.

A mi abuelo Martín Del Río Torres
y a mi Tío Mario Del Río Soto a quiénes
les dedico enteramente la presente, quién ya no
se encuentra físicamente pero están en nuestras vidas.

A mis compañeros y amigos:
Que estuvieron en mi vida y que hoy se encuentran
apoyándome y motivándome en cada etapa de mi vida
a quienes les agradezco siempre su estancia.

A mi estimada asesora:
Mtra. Ma. Graciela León López, quien
ha sido quien me guío en la licenciatura
y en la presente investigación, quién también
me ha motivado para llegar hasta donde hoy
estoy. GRACIAS.

A mis maestros y amigos:
Mónica Hernández Villegas y
José Luis Maldonado quienes
son unas personas muy especiales
en mi vida por estar ahí para escucharme.

A mi Alma Mater:
La Universidad Nacional Autónoma de México,
como la Institución que me permitió estudiar en
sus aulas y en las que permitió desarrollarme
como profesionista y quién me ha dado mucho
y con quién estoy en entera deuda.

INTRODUCCIÓN

En nuestras vidas la tecnología informática desempeña un papel muy importante, tanto en las nuevas formas de hacer llegar una carta o un mensaje, sustituyéndolo por un correo electrónico, el hacer un depósito bancario en una ventanilla de alguna institución financiera de su preferencia, esto hoy ha cambiado, ahora la forma a través de la cual se hace llegar dinero es mediante una transferencia en un sistema interbancario de pagos electrónicos.

El tener contacto con un familiar o amigo a través de una página web, por ejemplo Facebook o estar informando lo que nos parece relevante a través de un perfil en Twitter, lo anterior nos hace reflexionar acerca de la importancia del acercamiento que tú y yo tenemos con la Internet, por lo que me encontré en la necesidad de búsqueda de información acerca de los delitos que se cometen en la gran carretera de la información o también llamado el Cibermundo.

Sabemos que la tecnología avanza en gran medida a los descubrimientos que día a día se hacen, así también la ciencia del derecho es dinámica respecto a la creación y modificación de las normas que lo caracterizan, es por ello, que me permito realizar la presente investigación para profundizar en el campo de la ciberdelincuencia en redes sociales.

Quiero aclarar que no únicamente personas que tengan acceso a las redes sociales pueden ser víctimas de la delincuencia en internet, sino que también encontramos delitos como el fraude en portales bancarios o de pago, el acceso no autorizado a páginas gubernamentales y de empresas privadas.

El análisis que presento es con la finalidad de dar a conocer que deben contemplarse este tipo de delitos, porque afectan a terceros en la comisión de estas conductas y lo considero en cuatro capítulos:

En el primer apartado desarrollo la investigación a través de un marco teórico de la informática, para establecer un preámbulo y así posteriormente relacionarlo con la comisión de los delitos informáticos.

En el segundo capítulo denominado: marco teórico del delito informático, abordo la relación de que existe entre la Informática y el Derecho, n los que abordo temas acerca de las definiciones que realizan los teóricos acerca del tema, así como sus antecedentes históricos que han sido fundamentales en la construcción de esta nueva rama del derecho, el derecho informático.

Posteriormente en el tercer apartado intitulado: Análisis del delito informático, considero en el desarrollo de la investigación un análisis breve y claro del delito informático, así también tomo en cuenta los elementos jurídicos del delito informático y los presupuestos del delito informático para enfocarme en una clasificación del delito en comento.

En el cuarto capítulo considero el desarrollo del marco legal del delito informático, tomando en cuenta las opiniones vertidas acerca del tema de organismos internacionales como la Organización de Naciones Unidas, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, la Organización para la Cooperación y el Desarrollo Económicos y la Asociación Internacional de Derecho Penal. En el ámbito internacional también reviso las legislaciones acerca del tema en países de Europa y América, así también me adentro en el estudio de la legislación de algunos de los estados de la República Mexicana, su Distrito Federal y la Constitución Política de los Estados Unidos Mexicanos.

Finalmente realizo mi propuesta acerca de la necesidad de regular el delito informático en el código penal para el Distrito Federal, abordando desde una perspectiva jurídica y retomando algunas circunstancias del sistema jurídico local.

CAPÍTULO PRIMERO MARCO TEÓRICO DE LA INFORMÁTICA

1. Nociones y Concepto de Informática

La tecnología ha sido un pilar fundamental en el avance de la humanidad, misma que ha incursionado en todas las ramas del conocimiento, la computación y la informática han sido los ejes más importantes en estas últimas décadas.

La aparición de las tecnologías de la información ha sido un gran aporte de las nuevas generaciones que también auxilian a las generaciones que no se encuentran tan familiarizadas con la computación (o equipos de cómputo).

Por ello trato el tema de la informática retomando dos definiciones que considera Marco Antonio Tiznado:

"La informática es la ciencia que estudia el tratamiento automático de la información por medio de las computadoras".[1]

"La informática se refiere al uso de computadoras o dispositivos físicos electrónicos, por lo cual esta plantea a los usuarios de computadoras, una serie de interrogantes que se relacionan con la ética y los valores".[2]

Asimismo es importante señalar que la informática tiene una serie de características que hay que considerar, entre las que se encuentran:

Representa una de las áreas de la actividad humana que ha sufrido un mayor desarrollo en los últimos años, se ha venido expandiendo en los campos más importantes como en la medicina, telecomunicaciones, medio ambiente, alimentos, y también en el derecho.

[1] TIZNADO Santana, Marco Antonio. Informática, Mc Graw-Hill, 2da. Edición, México 2004 p.2
[2] *Ibídem*. p. 24

La computadora es el instrumento principal en esta rama del conocimiento, a lo que añadiría también sus derivados tales como, microcomputadoras, tabletas electrónicas, teléfonos inteligentes y pantallas táctiles con acceso a internet.

La informática puede considerarse simultáneamente como Ciencia y como Ingeniería, esto en consecuencia a las diferentes perspectivas de los ingenieros expertos en el tema, esto porque algunos consideran elementos esenciales y otros los excluyen.

La humanidad en el proceso histórico se ha aventurado en la creación de mecanismos para desempeñar sus actividades en la vida cotidiana y también para que sean más sencillas sus labores, en el caso específico de la inclusión de la informática ha beneficiado en gran parte éste desarrollo y lo ejemplifico con la transición de la máquina de escribir convencional a la computadora.

1.1.6 Orígenes de la computación

Los antecedentes históricos más relevantes de la informática son:

"En el año de 1833, el matemático e inventor inglés Charles Babbage diseñó una máquina a vapor que podía programarse, llamada máquina analítica. Babbage fue considerado el padre de la informática, ya que logró establecer el esquema formal de las computadoras que hoy se conocen: memorias, unidad de control, dispositivos de entrada y de salida y programas".[3]

Posteriormente en 1886, "el científico informático norteamericano Herman Hollerith creó una máquina censadora o tabuladora, la cual procesaba respuestas lógicas de tipo Sí o No."[4]

Entre 1937-1944, "Howard Aiken y un grupo de ingenieros de la IBM desarrollaron la primera computadora electromecánica que recibió el nombre

[3] TIZNADO Santana, Marco Antonio. Generalidades de la Informática e Internet, Colombia, Mc Graw Hill, 2004. p. 4
[4] *Ídem*

oficial de *AutomaticSequenceControllerCalculator* (ASCC), aunque se hizo famosa por el nombre de Mark I."[5]

En el año de 1946, "John W. Mauch y John Eckert, de la Universidad de Pensilvania, junto con un grupo de científicos desarrollaron, a petición del ejército estadounidense, la computadora ENIAC (*ElectronicNumericalIntegratoranCalculator*, Calculador e integrador numérico electrónico), construida con tubos al vacío. Se utilizó principalmente para el cálculo de la trayectoria de proyectiles."[6]

La comunidad experta de la computación agrupa la evolución de las computadoras en cinco generaciones a saber:

"La primera generación (1940-1952) reúne las computadoras de gran tamaño con lenguajes de programación de bajo nivel.

La segunda generación (1952-1964) se desarrollan el transistor y los circuitos electrónicos, con lo cual disminuye el tamaño de las computadoras y el uso de energía; los lenguajes de programación que se usan son *COBOL* (*COmmon Business Oriented lenguaje*) y *FORTRAN* (*FORmulaTRANslator*).

En la tercera generación (1964-1971) aparece el chip y con él las microcomputadoras; el lenguaje de programación utilizado es *BASIC* (*Beginner'sAll-purposeSymbolicInstructionCode*).

En la cuarta generación (1971-1981) se da origen a sistemas operativos como el *MS-DOS* (*Microsoft-Disk OperatingSystem*) y salen al mercado algunos programas como los procesadores de texto y las hojas de cálculo.

En la quinta generación (1981 en adelante) se perfeccionan los microprocesadores, aparecen las computadoras portátiles, la multimedia e

[5] *Ídem*
[6] *Ídem*

Internet. El software se hace más gráfico para un mayor entendimiento y se crean los disquetes de 3.5 pulgadas."[7]

1.1.7 Concepto de computadora

De acuerdo con Marco Antonio Tiznado, una computadora "es una máquina electrónica que tiene la capacidad para almacenar, recuperar y procesar datos e información".[8]

En una definición más específica se refieren a que "es una máquina capaz de aceptar unos datos de entrada, efectuar con ellos operaciones lógicas y aritméticas y proporcionar la información resultante a través de un medio de salida; todo ello sin intervención de un operador humano y bajo el control de un programa de instrucciones previamente almacenado en la propia computadora."[9]

1.1.8 Estructura de una computadora

En el análisis de la computadora es necesario conocer su estructura y componentes que la integran, dichos componentes pueden clasificar en las siguientes categorías: "dispositivos de entrada, por donde la máquina recibe la información; unidad central de procesamiento, *o CPU (Central ProcessingUnit)*, donde se ejecutan las instrucciones y los cálculos; y los dispositivos de salida, mediante los cuales se obtienen las respuestas proporcionadas por la computadora."[10]

---

[7] *Ibídem.* pp. 5-6
[8] *Ibídem.* p. 3
[9] PRIETO Espinosa, Alberto, et al, Introducción a la informática. Mc Graw Hill. Tercera Edición. Madrid 2002
[10] Informática. p.32

Todos los dispositivos se encuentran controlados por la unidad central la cual es la encargada de procesar y administrar el flujo de entrada y salida de la información, al igual ordena a cada dispositivo la tarea que realizará. Generalmente, "los dispositivos externos se conectan en los puertos que se ubican en la parte posterior de la computadora o a través de tarjetas."[11]

1.1.9 Nivel Operacional

En su nivel operacional encontramos en la computadora los siguientes componentes y unidades:

a. Dispositivos de entrada

En específico "son dispositivos que se conectan a la computadora, los cuales desempeñan una función específica", en el ingreso de información, entre este tipo de dispositivos podemos encontrar el teclado, el ratón, escáner, plotter, micrófono, cámara web, discos compactos, disco de 3.5 y memorias USB."[12]

b. Unidad Central de Proceso

En analogía con la anatomía humana puede decirse que es "el cerebro" de la computadora, es allí donde se procesa la información, se coordinan las tareas y se originan las respuestas que se transfieren a los dispositivos. Los elementos que la conforman son: la tarjeta principal, el procesador, la memoria, los puertos, las unidades de disco (disco duro, unidad de disquete, unidad de CD-ROM) y la fuente de energía.

[11] *Ídem*
[12] *Ídem*

c. Dispositivo de Almacenamiento

La función principal de la computadora es obedecer las instrucciones que son codificadas en los programas de cada ordenador. Sin embargo, "sólo puede manejar una instrucción y unos cuantos datos a la vez. La computadora tiene que colocar en algún lugar el resto del programa y los datos hasta que el procesador esté listo para usarlos. Para esto es la memoria interna o también conocida como memoria RAM."[13]

"El disco duro es el principal dispositivo de almacenamiento interno no removible de gran capacidad y alta velocidad. Un disco duro funciona de manera similar a los discos flexibles o disquetes: guarda la información en pistas divididas en sectores."[14]

d. Unidades de salida

En este tipo de unidades encontramos al monitor o pantalla en donde se visualizan los gráficos provenientes de las acciones que realizamos en la computadora, también en esta clasificación se encuentra la impresora, cuya función principal es la reproducción de información a una hoja de papel, y así obtener un registro impreso; por otra parte tenemos a los altavoces que son conectados a la computadora mediante una tarjeta de sonido, y cuya función es reproducir sonidos generados desde la computadora.

1.1.10 Nivel Estructural

a. Hardware

La palabra hardware se refiere a "los componentes físicos de un sistema informático incluyendo cualesquiera equipos periféricos, tales como impresoras, módems y ratones."[15]

---

[13] http://www.mailxmail.com/curso-componentes-pc-s/diferentes-dispositivos-almacenamiento 13 de Julio de 2014, 11:20 am

[14] Generalidades de la Informática e Internet p. 13

[15] Diccionario de Informática e Internet, Microsoft. Mc Graw Hill, segunda edición España 2005.

A través de los años se ha observado que avanza rápidamente el ramo computacional del Hardware, actualmente las computadoras poseen un Hardware más compacto y minimalista y más cercano a la portabilidad de los equipos de cómputo y dispositivos inteligentes.

b. Software

Se define al software como "un conjunto de instrucciones que permite que un sistema pueda ejecutar determinadas tareas. En una computadora el software constituye la parte lógica, es decir, los programas y las instrucciones que realizan las operaciones de cómputo y le ordena a la parte física, el hardware, qué se debe de hacer, dado que este último no puede realizar nada por sí solo. Básicamente, el software puede clasificarse en: sistemas operativos, lenguajes de programación, software de propósito general y software de propósito específico.

El software de propósito general incluye la mayor parte de los "paquetes" que se comercializan en cajas que van acompañadas de un manual de usuario y por lo general en un disco compacto."[16]

Cabe mencionar que el software puede ser empaquetado o gratis en algunas páginas de internet oficiales para su descarga desde un equipo de cómputo en una casa, oficina o empresa.

c. Lenguajes de programación

"El lenguaje de programación de bajo nivel es lo que se denomina código de máquina, que no es otra cosa que un conjunto de ceros y unos, es decir señales binarias que, por ejemplo, un procesador podrá "entender" a una alta velocidad.

[16] Informática. p.12, 21.

Los lenguajes de programación de alto nivel son un conjunto de palabras u órdenes que poseen una determinada sintaxis, es decir, una norma predefinida para escribir un programa.

Existen mucho programas de bajo nivel que se utilizan esencialmente para generar otros programas, algunos ejemplos representativos son: Pascal, Cobol, C, C++ y Java, entre muchos."[17]

Podemos concluir en este apartado que un lenguaje de programación es un conjunto de signos que reconoce la máquina para recibir y aplicar instrucciones, ya sean éstas sencillas o complejas.

La aplicación de éste tipo de lenguajes tiene su función para la representación de valores lógicos (verdadero y falso) para emplear un solo bit asignando de manera arbitraria el 1 y el 0 a cada uno de esos valores.

Sin embargo, por cuestiones de eficiencia, los ordenadores no manipulan bits individuales sino bytes por lo que la representación de los valores lógicos emplea siempre un byte.

La cuestión fundamental es que un ordenador no puede representar cualquier valor sino un valor perteneciente al rango de valores representables.

Sirve este tipo de lenguajes para codificar los números reales se utiliza el formato exponencial, así también para codificar un número en este formato se utilizan una parte de los bits para la representación de unidades de almacenamiento.

[17] Informática p. 19

CAPÍTULO SEGUNDO MARCO TEÓRICO DEL DELITO INFORMÁTICO

2. Relación entre Informática y Derecho

Antes de dar una respuesta, es necesario mencionar que la Informática es "la ciencia del tratamiento automático o automatizado de la Información, primordialmente mediante computadoras, es decir, cuando hablamos de la Información estamos refiriéndonos a información."[18]

La relación Derecho – Informática tiene dos factores o aspectos: la aplicación del Derecho, es decir, la Informática Jurídica; y la Informática como objeto de regulación jurídica, lo que da origen al llamado Derecho de la Informática o Derecho Informático.

Lo anterior nos permite visualizar claramente que la Informática Jurídica, no es más que un elemento de clasificación de la relación Derecho e Informática, igual que el Derecho de la Informática. El Derecho de la informática es la información desde el punto de vista jurídico y la Informática Jurídica es la información automatizada al servicio del Derecho.

Vinculando estos campos del conocimiento que son totalmente diferentes, los dos son producto y consecuencia del desarrollo y difusión de la tecnología de las computadoras. Ejemplificando en el caso de la Informática se desarrolla rápidamente la tecnología tanto en computadoras (Fijas y Portátiles), Sistemas Complejos de Cómputo y Dispositivos Móviles.

[18]FIX FIERRO, Héctor. Informática y Documentación jurídica. S.f., México, Tesis (Licenciado en Derecho), Universidad Nacional Autónoma de México, p.29.

2.1 Derecho Informático

La aparición en la sociedad actual de las nuevas formas de conductas ilícitas no reconocidas o tipificadas en las legislaciones penales, implica el riesgo de caer en el elemento negativo de la Tipicidad: la atipicidad; problema que el Derecho ha tratado de solucionar mediante la adecuada regulación clara y específica de dichas conductas, en un marco legal bien estructurado. Por lo tanto es necesario introducir nuevas figuras delictivas para dar respuesta a los problemas que le aquejan a la sociedad en el ámbito penal.

Considero a propio juicio que la sociedad y la tecnología avanzan conjuntamente para lograr un desarrollo y relativamente en su beneficio, debido a que algunas conductas pueden ser perjudiciales para su convivencia en concordia.

El derecho como una ciencia que se adapta a las necesidades que tiene una sociedad por caracterizarse como una forma de organización dinámica, es decir, en constante cambio y que paralelamente las normas cambian atendiendo al flujo social y por ende a las conductas que surgen contrarias al normal desarrollo de la sociedad, o que simplemente le provocan un conflicto.

Julio Téllez define al derecho informático como "una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática)."[19]
El derecho informático posee una importancia particular, debido a que en la actualidad se han llevado a la práctica nuevas formas de delinquir a través de internet, lo que nos afecta como sociedad y en particular a los cibernautas, es decir a los usuarios de internet.

[19]TÉLLEZ Valdés, Julio. *Op cit*. p. 13

Ahora con la presencia jurídica de una nueva rama del derecho, como lo es el derecho informático intenta en gran medida de estudiar, analizar y de integrar las nuevas formas de delinquir por individuos que la ciencia los denomina como hackers.

El Derecho Informático es considerado como una "ciencia y rama autónoma del Derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en aspectos como la regulación del medio informático en su expansión y desarrollo, y la aplicación idónea de los instrumentos informáticos." [20]

La rama del Derecho informático no se dedica al estudio del uso de los aparatos informáticos como ayuda al Derecho, sino que constituye un conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática. Es decir, que la informática en general desde este punto de vista es objeto regulado por el Derecho.

Asimismo, se le denomina también al Derecho Informático como "la universalidad de problemas que surgen de las transformaciones que el derecho ha ido realizando como imposición de ciertas actividades novedosas que se desarrollan en el ámbito social y que requieren nuevas regulaciones o una reinterpretación de las regulaciones ya existentes a fin de dar respuestas en el sentido de la justicia."[21]

[20] http://www.ecured.cu/index.php/Derecho_inform%C3%A1tico 10 de Julio de 2014, 13:15 hrs.
[21] PEÑA, Carlos, Docente de Ingeniería en la Universidad de Palermo. Documento disponible en línea: http://www.palermo.edu/ingenieria/downloads/pdfwebc&T8/8CyT05.pdf 08 de Julio de 2014, 11:00 hrs.

2.2 Antecedentes del Derecho Informático

El Derecho Informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, teniendo en su haber (al menos hasta la fecha) incipientes antecedentes a nivel histórico; sin embargo, podemos decir que las alusiones más específicas sobre esta interrelación, las tenemos a partir del año 1949 con la obra de Norbert Wiener, en cuyo capítulo IV, consagrado al derecho y a las comunicaciones, nos expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.[22]Dicha interrelación se da a través de las comunicaciones, a lo que habría que mencionar que aún la antigüedad de estos postulados tienen acerca de cuarenta años, en la actualidad han adquirido matices que probablemente superan las ideas e investigaciones de los teóricos que expusieron sus ideas acerca de este interesante tema.

En la obra "Derecho Informático de Julio Téllez"[23] menciona que en el año de 1959 en los Estados Unidos de América, la informática jurídica ha sufrido cambios afines a la evolución general de la misma informática.

La nueva disciplina ha dado lugar a numerosas denominaciones, entre las cuales tenemos:

Jurimetrics(en español jurimetría) creada por el juez norteamericano Lee Loevinger en el año de 1949.

Giuscibernetica (En español juscibernética) del profesor italiano Mario G. Losano, quien sostiene que la cibernética aplicada al derecho produce una depuración no sólo en términos cuantitativos, sino también cualitativos.

Computersand Law. (Denominación empleada en los países anglosajones).

Informátiquejurique. (Francia)

[22]Téllez Valdés, Derecho Informático, p.21.
[23] *Ibid*. p.1119

Jurismática, o más explícito: informática jurídica (denominaciones empleadas en México)

De acuerdo a su clasificación, se muestra que en sus primeros años, la informática jurídica se presentó como una informática documentaria de carácter jurídico, es decir, creación y recuperación de información que contenían datos principalmente jurídicos (compilaciones legislativas, jurisprudencias, doctrina, etc.).

En estos últimos años, se considera que la informática jurídica ha permitido un mejor conocimiento de los fenómenos jurídicos, por lo que muchos juristas, anteriormente que no mostraban algún interés o simplemente se mostraban indiferentes, han encontrado en la computadora un instrumento muy útil a la hora de desarrollar sus actividades.

En Europa entre 1966 y 1969 con la denominación de "cibernética y derecho" se utilizaron las funciones y las aplicaciones informáticas en el derecho tanto en el campo de las personas que al entrar en el mundo tecnológico tocan las normas y leyes que la regulan como de las investigaciones en el Derecho que recurren a elementos de la cibernética.

En 1968 el investigador del tema Mario Lasono propusó sustituir el término de jurimetria por el de "iuscibernética".[24]

En el año 1996 se creó la Ley Modelo de la CNUDMI sobre Comercio Electrónico, siendo este uno de los mayores esfuerzos jurídicos a nivel internacional para regular lo concerniente al denominado "comercio electrónico" proponiendo a los demás estados el fortalecimiento de la legislación regidora de estos medios.[25]

[24] https://docs.google.com/document/d/17SpYB0L0IuCkHacZpmIh325v2FEMv0JlDejhym1B4bE/edit
20 de Julio de 2014, 14:10 hrs.
[25] http://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf
20 de Julio 2014, 14:25 hrs.

Esta disciplina influye además a campos como el de las Ciencias Sociales, en el instante que es usada la tecnología de la información para la integración de las personas. Es posible ser más humanos con la ayuda de la informática jurídica, está reflexión histórica con dimensiones filosóficas es una de las tareas de la fenomenología hermenéutica.

Los sistemas de información están inmersos en contextos culturales diversos. El estudio de los procesos de información incluye aspectos retóricos, éticos y políticos. La ciencia de la información puede ser concebida como una disciplina retórica y la hermenéutica existencial puede proporcionar un antídoto al mentalismo en la ciencia de la información.

2.3 Orígenes de la Informática Jurídica

Los progresos mundiales de las computadoras, el creciente aumento de la capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información"[26], a lo que con más propiedad, podríamos decir que más bien estamos frente a la también conocida como "ERA DE LA INFORMÁTICA".

La informática ha sido considerada como uno de los fenómenos más importantes de los últimos tiempos, y lo que ha dado origen a que se encuentre involucrándose en la mayoría de las áreas del conocimiento humano, entre las cuales el derecho no puede ser la excepción, por lo que nace la informática jurídica.

[26] http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf 25 de junio de 2014 13:20 hrs.

En un sentido amplio, podemos decir que la informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del derecho, nacida en Estados Unidos (1959), la informática jurídica ha evolucionado de acuerdo con los avances de la misma informática.

"Las primeras investigaciones en materia de recuperación de documentos jurídicos en forma automatizada se remontan a los años de la década de 1950, cuando se comienzan a utilizar las computadoras no sólo con fines matemáticos, sino también lingüísticos. Estos esfuerzos fueron realizados en el HealthLaw Center (HLC) de la Universidad de Pittsburgh, Pensilvania. El entonces director del centro, John Horty, estaba convencido de la necesidad de encontrar, medios satisfactorios para tener acceso a la información legal."[27]

El profesor italiano Mario Losano en 1968, propuso el término Iuscibernética con el objetivo de sustituir al comúnmente utilizado hasta entonces jurimetría, pero reformulando sus alcances en cuanto comprendía una aproximación cibernética del derecho, esto es, concebía al derecho como un subsistema del sistema social susceptible de ser regulado y controlado, proponiendo así mismo el desarrollo de las técnicas necesarias para emplear la computadora precisamente en el ámbito jurídico, además del estudio sobre la lógica y técnicas de formalización del derecho a fin de lograr un óptimo tratamiento informático.[28]

Posteriormente, en el año de 1963, Hans Baade edita la obra *Jurimetrics: the Methodolog y 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, y

[27] *Ibídem.* p. 9
[28] LOSANO, Mario. Curso de Informática Jurídica. Madrid, Tecnos. 1987, pág.45.

- En tercero, llegar a prever futuras sentencias de los jueces.

No quedaron satisfechos por los resultados concretos brindados por la jurimetría y la presencia de instrumentos teóricos atractivos, como los ofrecidos por la cibernética teórica, lograron que en Europa los estudios puramente empíricos de tipo loevingeriano se unieran con estudios de tipo puramente teórico, con el resultado de que, entre 1966 y 1969, con la denominación de cibernética y derecho.[29]

En 1976, durante las Primeras Jornadas italo-Latinoamericanas de Informática Jurídica, realizadas en Lima-Perú, en la UNMSM, el Prof. Vittorio Frosini, propuso la denominación "GIURITECNICA"[30], como un nuevo símbolo semántico que no pretendía sustituir otros precedentemente registrados, sino que pudiera resumir las instancias que emergen del dominio de la nueva experiencia jurídica y que sea de fácil funcionabilidad, en vista de que la

Informática Jurídica no designaba un nuevo modelo del procedimiento operativo jurídico, debido a que no resaltaba el tratamiento tecnificado, más elaborado, de los datos jurídicos dentro de una metodología lógico-operativa.

En las jornadas de informática jurídica señaladas, tenían la preocupación cuando se manifestaba que en la Informática Jurídica se observaba una tendencia casi exclusiva para el uso de métodos de almacenamiento y búsqueda de información, lo que se perfilaba a constituir el simple uso de productos prefabricados de aplicación tanto para la información jurídica como para cualquier otra información con lo que se tenía el riesgo de lograr la temprana fosilización, estancamiento o seriamente el carácter obsoleto de la informática jurídica.

---

[29] http://www.segobver.gob.mx/sispdf/directorios/Directorio_SEGOB.pdf Antecedentes de la Informática Jurídica. 22 de Junio de 2014, 23:10 hrs.

[30] Vittorio Frosini no proponía un nuevo vocablo sino una nueva instancia de comprensión del problema de ausencia de un nuevo modelo jurídico lógico-operativo más acorde con las posibilidades operativas que debería fundar la Informática Jurídica.

2.4 Concepto de Delito Informático

Inicialmente debemos tener en consideración el significado jurídico del delito, por lo que Castellanos Tena refiere que: "La palabra delito, deriva del verbo latino *delinquere*, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley. El delito, está íntimamente ligado a la manera de ser cada pueblo y a las necesidades de cada época, los hechos que en determinado momento han tenido ese carácter, lo han perdido en función de situación diversas y, al contrario, acciones no delictuosas, han sido erigidas en delitos."[31]

Por su parte, Rafael Garófalo, exponente del Positivismo, lo define de la siguiente manera: "Es la violación de los sentimientos altruistas de probidad y de piedad en la medida indispensable para la adaptación del individuo a la colectividad."[32]

Previo a analizar la conceptualización que se tiene de los delitos informáticos enunciaré las percepciones de algunos autores que han expuesto sus posturas acerca del tema que tratamos.

Gabriel Campoli nos refiere que:

"Los delitos informáticos son todos aquellos 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."[33]

Para la presente investigación es importante el realizar una definición, porque posteriormente se propondrá el que se establezca la regulación del delito informático en el Código Penal para el Distrito Federal.

---

[31] CASTELLANOS Tena, Fernando. Lineamientos elementales de Derecho Penal. Porrúa, México 1984,p.125.
[32] Ibidem, p.p. 125-126.
[33] CAMPOLI, Gabriel Andrés. Derecho penal informático en México. INACIPE, 2004. p.14

Respecto al tema tratado, la ahora extinta Secretaría de Programación y Presupuesto contemplaba que el Derecho Informático "…constituye o constituiré más bien un cuerpo jurídico y articulado en cuanto a su tema real: el uso de la informática y tecnologías de la información a fines con todos los aspectos y conflictos jurídicos que implica".[34]

Los delitos informáticos implican actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como fraudes, robos, sabotajes, lesiones, etcétera. Sin embargo, debe destacarse que el uso de las tecnologías y en específico el uso de las computadoras con acceso a internet ha propiciado las posibilidades del uso indebido de estas nuevas tecnologías lo que paralelamente ha originado la necesidad de regular a través del campo del Derecho.

Por su parte, el "Convenio de Ciberdelincuencia del Consejo de Europa"[35] define a los delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".[36]

[34]Secretaría de Programación y Presupuesto, La Informática y el Derecho, INEGI, México 1983, p.23.
[35] Publicado por el Consejo de Europa, Ministerio de Asuntos Exteriores en Budapest (2001) consultado en línea: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf 16 de junio de 2014, 14:15 hrs.
[36] http://delitosinformaticos.info/delitos_informaticos/definicion.html 16 de junio de 2014, 15:10 hrs.

CAPÍTULO TERCERO ANÁLISIS DEL DELITO INFORMÁTICO

3. Análisis del Delito Informático

Es destacable analizar concretamente el Delito Informático desarrollando sus elementos para identificarlos y así lograr su caracterización de esa conducta antijurídica y posteriormente conjuntarlos para su estudio.

3.1 Elementos Jurídicos del Delito Informático

Varios elementos concurren en el delito. Se habla de presupuestos generales y especiales, datos positivos (aspecto positivo del delito) y datos o circunstancias negativos (aspectos negativos del delito). Si aquéllos se reúnen sin que nada los excluya, existe el comportamiento punible. Empero, puede suceder que, habiendo delito, se haya extinguido la pretensión punitiva.

El delito es un fenómeno unitario, que se integra de una vez, no por adición de componentes que acudan sucesivamente. Empero es pertinente estudiarlo en cada uno de sus elementos, mediante un ejercicio de abstracción. De las teorías que se ocupan en este asunto, la más conocida entre nosotros es la heptatómica, que sostiene la existencia de siete elementos: conducta o hecho, tipicidad, antijuricidad, imputabilidad, culpabilidad, condiciones objetivas de punibilidad, y punibilidad. Cada uno de estos datos puede ser eliminado por circunstancias o causa excluyente. Hay diversas corrientes doctrinarias que examinan estos temas, cada una a su manera y con sus propias conclusiones. Todas difieren notablemente.

En tanto que el Código Penal no contiene una definición del delito que muestre todos sus elementos, tema que concierne a la doctrina, ese ordenamiento regula las excluyentes. El capítulo VI del título primero del Código

Penal se dedica a lo que originalmente – y hasta la reforma de 1993- se denominó “circunstancias excluyentes de responsabilidad”, y hoy se designa “causas de exclusión del delito”.

3.2 Presupuestos del Delito Informático

Para la existencia de un delito se requiere la concurrencia de determinados sujetos y circunstancias, tanto de hecho como de jurídicas.

Se ha dividido a los presupuestos del delito en generales y especiales. Los generales son cuando necesariamente deben concurrir para la configuración de cualquier delito, pues su ausencia implica la imposibilidad de integrarlo, como presupuestos generales, podemos señalar: la norma penal, el sujeto activo y pasivo, la imputabilidad, el bien tutelado y el instrumento del delito. Los especiales son los condicionantes de la existencia de un delito concreto y cuya ausencia origina la no aplicación del delito, es decir no se encuentra en el tipo penal.

3.2.1 Sujeto Activo

“Es el autor de la conducta típica”[37] por su parte en relación a este mismo elemento el Jurista Celestino Porte Petit expresa que: “El que interviene en la realización del delito como autor, coautor o cómplice.”[38]

En sentido estricto es quien realiza una acción típica y antijurídica que puede serle personalmente reprochada. Sólo el hombre puede ser sujeto activo. Esta afirmación, sin embargo, constituye un logro del actual Derecho penal y supone la superación de pasadas épocas históricas. En ellas los procesos

[37] Zafarroni, Eugenio Raúl. Tratado de Derecho Penal –Parte General- Tomo III. Editorial Cárdenas. Editor y Distribuidor, Primera Reimpresión. México 1991.
[38] Porte Petit, Celestino. Apuntamientos de la Parte General de Derecho Penal. Porrúa, Sexta edición.

contra cosas y contra animales eran frecuentes, y son reveladores de que entonces se confundían las ideas de d. y de daño. En la actualidad la exigencia de capacidad de culpabilidad para ser sujeto activo de d. ha hecho desaparecer tanto a los animales como a las cosas de la posibilidad de serlo. En este punto es unánime la opinión de la doctrina.

"Solo el hombre es sujeto activo del delito, porque únicamente él se encuentra provisto de capacidad y voluntad y puede, con su acción, infringir el ordenamiento jurídico penal. Se dice que de una persona es sujeto activo cuando realiza la conducta o el hecho típico, antijurídico, culpable y punible, ya sea como autor intelectual, material, participe, cómplice o encubridor."[39]

3.2.2 Sujeto Pasivo

Es el titular del interés jurídico lesionado o puesto en peligro por la conducta del sujeto activo. Puede serlo la persona individual (antes de su nacimiento y después de él hasta su muerte), las personas jurídicas, el Estado y la colectividad social. Del sujeto pasivo puede diferenciarse la figura del perjudicado que es quien, por la comisión del d., sufre un daño patrimonial o de otra clase.

El sujeto pasivo "Es el titular del bien jurídico protegido por la ley"[40], y en la presente investigación, el sujeto pasivo sería la persona o personas en quién sean afectadas por la comisión del delito informático, quienes serían lesionadas en su esfera jurídica.

[39] PAVÓN Vasconcelos, Francisco. Derecho Penal Mexicano, Décima edición, S.A., Porrúa, México, 1991 p. 17.
[40] Ibidem, p.436.

Dentro de los llamados “Delitos Informáticos, el sujeto activo de la conducta no es un sujeto de rasgos comunes, sino de un especialista que tiene conocimientos amplios de la ciencia informática y computacional.

3.2.3 Objeto Material

El objeto material lo constituye la persona sobre la que recae el daño o peligro; la persona o cosa sobre la que se concreta la acción delictuosa.[41]

El objeto material es la cosa o sujeto sobre la que se realiza el delito. En este sentido debe decirse que precisamente el procedimiento o el proceso sujeto al conocimiento del servidor público, constituye dicho objeto.

Es considerado como aquel sobre el que recae el daño causado o producido como consecuencia de la realización de un delito.

En ocasiones nos encontramos que el objeto material puede ser fusionado dentro del sujeto pasivo, ya que en el catálogo de delitos con que cuentan nuestras legislaciones penales, existen delitos en los cuales se considera que el daño recae directamente en una persona por ejemplo, el delito de lesiones o de violación, por mencionar algunos.

Habrá situaciones en las cuales el sujeto pasivo esté separado totalmente del objeto material, y que existen delitos en los que sus consecuencias van a recaer sobre bienes muebles o inmuebles, incluyendo dentro de los primeros a los derechos.

[41] Castellanos, Fernando. Op. Cit. 436

3.2.4 Bien Jurídico Tutelado

No se concibe que exista una conducta típica sin que afecte un bien jurídico, el cual es indispensable para la configuración de la tipicidad. Se puede definir al bien jurídico penalmente tutelado como: “la relación de disponibilidad de un individuo como un objeto, protegido por el Estado, que revela su interés mediante la tipificación penal de conductas que le afectan.”[42]

En general la expresión “bien jurídico”, o alguna equivalente, no está utilizada en las legislaciones penales contemporáneas; no obstante, la dogmática refiere que en los códigos penales se hacen menciones sistemáticas a distintos bienes jurídicos.

Para Carlos Nino: la dogmática penal todo delito lesiona un bien jurídico. No es concebible un delito que no lesione un bien jurídicamente protegido. De este modo la lesión a un bien pareciera ser definitoria del concepto de delito. [43]

El bien jurídico que se lesiona con el delito es distinto, para la dogmática penal, del objeto material afectado por el delito.

Los distintos bienes jurídicos presentan una gran heterogeneidad. Evidentemente la vida, la propiedad, el honor, la honestidad, la administración pública, la tranquilidad pública, la fe pública, etcétera, son conceptos con notables diferencias categoriales entre sí.

[42] Zaffaroni, Eugenio Raúl. Op cit. 410

[43] NINO, Carlos Santiago. Consideraciones sobre la dogmática jurídica (Con referencia particular a la dogmática penal). UNAM, Instituto de Investigaciones Jurídicas. México, 1989, .56

3.3 Clasificación del Delito Informático

Dentro de este rubro, logro identificar delitos contra el patrimonio, contra la intimidad, contra la seguridad pública y las comunicaciones, falsificaciones informáticas y contenidos ilegales en internet.

Julio Téllez Valdés clasifica a estos delitos, de acuerdo a dos criterios:

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

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
b) Variación de los activos y pasivos en la situación contable de las empresas.
c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
d) Lectura, sustracción o copiado de información confidencial.
e) Modificación de datos tanto en la entrada como en la salida.
f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
h) Uso no autorizado de programas de cómputo.
i) Introducción de Instrucciones que provocan “interrupciones” en la lógica interna de los programas.
j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.
l) Acceso a áreas informatizadas en forma no autorizada.
m) Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por Ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.
b) Destrucción de programas por cualquier método.
c) Daño a la memoria.
d) Atentado físico contra la máquina o sus accesorios.
e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)

3.4 Características del Delito Informático

"Los delitos informáticos son acciones de tipo ocupacional, ya que en la mayoría de los casos, se realizan cuando el sujeto está trabajando o en su puesto de trabajo."[44]

Cabe mencionar que en la mayor parte de las ocasiones, presentan grandes dificultades a la hora de comprobar quien cometió el ilícito debido a la gran expansión de Internet y a al carácter técnico de estos hechos.

También su perpetración es relativamente fácil en cuanto a tiempo y espacio se refiere, ya que pueden llegar a consumarse en poco tiempo y sin necesidad de presencia física del delincuente.

Son delitos que provocan grandes pérdidas económicas para los afectados y grandes "beneficios" para el que comete el delito.

Por último, señalar que en su mayoría, sólo pueden ser cometidos por personas con unos determinados conocimientos técnicos.

Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.

Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

[44] http://www.usc.es/export/sites/default/gl/institutos/criminoloxia/descargas/Los_Delitos_Informxticos.pdf 18 de Julio de 2014, 10:35 hrs.

CAPÍTULO CUARTO MARCO LEGAL DEL DELITO INFORMÁTICO

4.- Ámbito Internacional

La inexistencia de una ley informática imposibilita que la persecución y castigo de los autores de delitos informáticos sea efectiva. Aunado a esto las autoridades no poseen el nivel de experiencia requerido en estas áreas ni la capacidad instalada para desarrollar actividades de investigación, persecución y recopilación de pruebas digitales y electrónicas. Por lo que todo tipo de acción contra los delincuentes informáticos quedaría prácticamente en las manos de la organización que descubre un delito y el tipo de penalización sería más administrativa que de otro tipo (si el delito proviene de fuentes internas).

Al tratar de resumir la red de redes computacionales podría ocasionar que se omitiera una parte muy importante del mismo: el Ciberespacio, y es que Internet posee una naturaleza biforme. Por un lado, es la red mundial de redes computacionales conectadas entre sí -a través de millones de kilómetros de cableados terrestres, marítimos, ondas satelitales entre otros conductos-, que permite la obtención de información y la comunicación entre usuarios. La otra parte hace referencia al lugar donde millones de personas se reúnen diariamente para comprar, divertirse, informarse o comunicarse. Es el Ciberespacio, espacio virtual que ha llegado a convertirse en la manzana de la discordia jurídica.

Por ello es necesario que se tomen medidas adecuadas a través de legislaciones, normas y otros instrumentos jurídicos para la efectiva regulación en el ámbito internacional debido a que se encuentra desarrollado la red a nivel mundial.

4.1 ONU

La Organización de las Naciones Unidas (O.N.U.) “es una organización de Estados soberanos. Los Estados se afilian voluntariamente a las Naciones Unidas para colaborar en pro de la paz mundial, promover la amistad entre todas las naciones y apoyar el progreso económico y social. La Organización nació oficialmente el 24 de octubre de 1945”.[45]

La O.N.U. tiene entre sus objetivos: “promover el estado de derecho en los planos nacional e internacional es uno de los aspectos esenciales de la misión de las Naciones Unidas.”[46] También es relevante mencionar que impulsa mecanismos para establecer el respeto del estado de derecho, el cual es fundamental para lograr una paz duradera posterior a un conflicto, para salvaguardar los derechos humanos.

En relación al tema de la presente investigación, la O.N.U. tiene entre sus actividades en el ámbito del estado de derecho: “apoyar el desarrollo, la promoción y la aplicación de normas y principios internacionales en la mayoría de los ámbitos del derecho internacional”.[47]

La Organización de las Naciones Unidas (O.N.U.) refuerza su labor de promoción del estado de derecho en los ámbitos nacional e internacional. En el tema en particular de los delitos informáticos, en específico a través del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal fue asistido por el Gobierno de Brasil (celebrado en Salvador de Bahía), del 12 al 19 de abril de 2010. Los congresos de las Naciones Unidas sobre Prevención del Delito se han venido celebrando cada cinco años, desde 1955, en distintas partes del mundo y en torno a una amplia variedad de temas.

---

[45] http://www.cinu.mx/onu/onu/ ,09 de abril de 2013,13: 25hrs.
[46] http://www.un.org/es/ruleoflaw/,09 de abril de 2013,13: 47hrs.
[47] Portal de la ONU citado anteriormente (Inmediato)09 de abril de 2013,14: 28hrs.

Éstos han tenido una considerable repercusión en la esfera de la prevención del delito y la justicia penal a escala internacional y han influido en las políticas y prácticas profesionales de los países.

"Como plataforma mundial, los congresos posibilitan el intercambio de información y de mejores prácticas entre los Estados y profesionales que trabajan en este sector. Su objetivo global es el de promover políticas de prevención del delito y medidas de justicia penal más eficaces en todo el mundo."[48]

La O.N.U. en su 12º Congreso sobre Prevención del Delito y Justicia Penal celebrado en la localidad del Salvador en Brasil del 12 al 19 de abril de 2010 le otorga un papel destacable al tema de los delitos cibernéticos, esto, porque este tema se ha convertido en un reto, ya que desde hace 50 años se ha tratado debido a que la tecnología ha ganado terreno día a día en nuestra interacción en la sociedad.

El 12º Congreso sobre Prevención del Delito ofreció una oportunidad singular para estimular el debate a fondo y propuestas de medidas a lo largo de tres vertientes principales, para lo cual fue necesario:

Establecer firmemente el sistema de justicia penal como pilar central del sistema del Estado de Derecho;

Destacar el papel fundamental del sistema de justicia penal en el desarrollo;

Subrayar la necesidad de un enfoque holístico respecto de la reforma del sistema judicial penal con objeto de reforzar la capacidad de los sistemas de justicia penal en la lucha contra el delito;

[48] http://www.un.org/es/conf/crimecongress2010/ 22 de Junio de 2014, 13:25 hrs

Determinar nuevas formas de delincuencia que planteen una amenaza a las sociedades de todo el mundo y analizar los medios para prevenirlas y controlarlas.

Hay ocho temas sustantivos en el programa que abarcan las cuestiones siguientes:

Los niños, los jóvenes y la delincuencia;

El terrorismo;

La prevención del delito;

El tráfico de emigrantes ilegales y la trata de personas;

El blanqueo de dinero;

El delito cibernético;

La cooperación internacional en la lucha contra la delincuencia;

y la violencia contra los emigrantes y sus familiares.

En este orden de ideas consideran que a pesar de las mejoras tecnológicas y de las investigaciones serias realizadas, el grado en que la tecnología de la información se utiliza para fines ilegales se mantiene estable o tal vez esté incluso aumentando.

En este congreso señalan algunos puntos para combatir este delito entre ellos se encuentran:

COMPATIBILIDAD DE LA LEGISLACIÓN. Esto se refiere a que debe existir una mejor cooperación internacional para desarrollar y normalizar la legislación adecuada.

RESTRICCIÓN DE SITIOS. Se refiere a que algunos gobiernos y organizaciones internacionales han comenzado a prestar atención a las obligaciones de los proveedores de servicios de Internet de boquear el acceso a los sitios web que contengan pornografía infantil.

APLICACIÓN DE LA LEY. Además de necesitar instrumentos s jurídicos, la aplicación de la ley depende en gran medida de la disponibilidad de instrumentos de investigación tales como programas informáticos forenses (para reunir pruebas, registrar las pulsaciones de teclado y descifrar o recuperar ficheros suprimidos) y programas informáticos o bases de datos de gestión de la investigación (por ejemplo, con valores “hash” para imágenes de pornografía infantil conocidas).

CAPACITACIÓN. Este rubro es importante, porque se debe de impartir capacitación a los funcionarios encargados de hacer cumplir la ley, los fiscales y los jueces.

En este orden de ideas, la Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC), en su calidad de órgano encargado de establecer normas en relación con la prevención del delito y la justicia penal, ofrecerá una plataforma multilateral en que se prestará atención preferente a los países en desarrollo

La UNODC trabajará con los expertos y los instrumentos adecuados, incluidos los del sector privado (en particular los proveedores de servicios de Internet) para combatir el problema en un determinado país o región. Se concederá prioridad a la prestación de asistencia técnica a los Estados miembros que la necesiten, con vistas a subsanar la falta de capacidad y competencia técnica y a asegurar la sostenibilidad a largo plazo de la lucha contra los delitos informáticos.

Es importante para la ONU el participar, ya que es una institución de orden mundial en el que se integran los países para establecer reglas, en este caso en materia de Derecho Penal y en específico en materia de los delitos informáticos.

4.2 UNESCO

Se define como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, su integración fue aprobada por la Conferencia de Londres de noviembre de 1945 y entró en vigor el 4 de noviembre de 1946, una vez que 20 Estados hubieron depositado sus instrumentos de aceptación, en la actualidad tiene 195 Miembros y ocho Miembros Asociados.

El principal objetivo de la UNESCO es contribuir al mantenimiento de la paz y la seguridad en el mundo promoviendo, a través de la educación, la ciencia, la cultura y la comunicación, la colaboración entre las naciones, a fin de garantizar el respeto universal de la justicia, el imperio de la ley, los derechos humanos y las libertades fundamentales que la Carta de las Naciones Unidas reconoce a todos los pueblos sin distinción de raza, sexo, idioma o religión.

Para cumplir este mandato, la UNESCO desempeña cinco funciones principales:

Estudios prospectivos: es decir, las formas de educación, ciencia, cultura y comunicación para el mundo del mañana

El adelanto, la transferencia y el intercambio de los conocimientos, basados primordialmente en la investigación, la capacitación y la enseñanza

Actividad normativa, mediante la preparación y aprobación de instrumentos internacionales y recomendaciones estatutarias.

Conocimientos especializados, que se transmiten a través de la "cooperación técnica" a los Estados Miembros para que elaboren sus proyectos y políticas de desarrollo.

En afinidad a los delitos informáticos, el 18 de marzo de 2004, se llevó a cabo y se ratificó en Lituania la Convención Internacional sobre la Delincuencia Cibernética, la cual entró en vigor el 1º de julio del mismo año.

La Convención es el primer tratado internacional sobre delitos cometidos por Internet u otras redes informáticas, que atentan especialmente contra los derechos de autor y derechos conexos.

La Convención aspira a impulsar una política penal común contra la delincuencia cibernética. Uno de sus principales objetivos es armonizar el derecho penal de los distintos países. Además, los Estados signatarios tienen la obligación de promulgar una ley procesal penal de alcance nacional que permita la investigación y el encausamiento de delitos cometidos por medio de un sistema informático. Por último, este instrumento prevé un régimen efectivo de cooperación internacional.

Entre los países que a han firmado la Convención, 27 son Estados Miembros del Consejo de Europa (Albania, Alemania, Armenia, Austria, Bélgica, Bulgaria, Croacia, Chipre, España, Estonia, Finlandia, Francia, Grecia, Hungría, Italia, la ex República Yugoslava de Macedonia, Moldavia, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, Rumania, Suecia, Suiza, Turquía y Ucrania), a los que se suman Estados Unidos, Japón y Sudáfrica, que también participaron en la preparación de la Convención.

4.3 O.C.D.E.

La Organización Europea de Cooperación Económica (OCDE) se creó en 1948 para ejecutar el Plan Marshall con financiación para la reconstrucción de un continente devastado por la guerra. Al hacer que los distintos gobiernos reconocen la interdependencia de sus economías, que allanó el camino para una nueva era de cooperación que iba a cambiar la faz de Europa. Animado por su éxito y la perspectiva de la realización de su trabajo hacia adelante en un escenario global, Canadá y los EE.UU. se unieron a los miembros la OECE en la firma del nuevo Convenio de la OCDE el 14 de diciembre de 1960. La Organización para la Cooperación y el Desarrollo Económico (OCDE) nació oficialmente el 30 de septiembre de 1961, cuando la Convención entró en vigor.

Otros países se unieron, empezando por Japón en 1964. Hoy en día, 34 países miembros de la OCDE en todo el mundo recurren regularmente entre sí para identificar problemas, discutir y analizar, y promover políticas para resolverlos. El historial es impresionante. Los EE.UU. ha sido testigo de la riqueza nacional, casi el triple que en las cinco décadas desde que la OCDE ha creado, calculado en términos de producto interno bruto per cápita de la población.

Así, también, que los países que hace unas décadas eran todavía los jugadores de menor importancia en el escenario mundial. China, India y Brasil se han convertido en los nuevos gigantes económicos. La mayoría de los países que formaban parte de la antigua Unión Soviética o bien se han unido a la OCDE o adoptado sus normas y principios para lograr nuestros objetivos comunes. Rusia está negociando para convertirse en miembro de la OCDE, y ahora tiene una estrecha relación con Brasil, China, India, Indonesia y Sudáfrica, a través de nuestro "mayor compromiso" del programa. Junto a ellos, la OCDE lleva alrededor de su mesa de 40 países que representan el 80% del comercio mundial y las inversiones, dándole un papel fundamental para hacer frente a los desafíos que enfrenta la economía mundial.

En 1983 la (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación. Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos.

En 1986 la OCDE publicó un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

Respecto a México, "ocupa el último lugar en materia de ciberseguridad entre los países que conforman la OCDE, va rezagado en la tipificación de delitos informáticos y no cuenta con recursos humanos preparados (agentes del MP, policías investigadores y jueces conocedores) para hacer frente a fraudes electrónicos, clonación de tarjetas, robo de base de datos, bloqueo de portales o jaqueo de cuentas de correo, entre otros ilícitos de este tipo"[49]

[49] http://www.eluniversal.com.mx/cultura/69843.html 18 de Junio de 2014, 12:30 hrs.

4.4 A.I.D.P.

La Asociación Internacional de Derecho Penal (A.I.D.P.) constituye la más antigua organización mundial que reúne especialistas de las ciencias penales y una de las sociedades culturales más antiguas del mundo.

Desde 1924 la A.I.D.P. ha adquirido en sus ámbitos de competencia un estatus especial entre las otras organizaciones y entre la doctrina, los expertos, las autoridades gubernamentales y los profesionales. Estos ámbitos son: 1) La política criminal y la codificación del Derecho penal, 2) El Derecho penal comparado, 3) El Derecho penal internacional (especialmente la justicia penal internacional) y 4) Los Derechos humanos en la administración de justicia penal.

Esta asociación internacional emitió un documento denominado "***Principales lineamientos político-criminales de la Asociación Internacional de Derecho Penal en un mundo globalizado***" en el que considera en un apartado a los delitos informáticos y otros delitos relativos a la tecnología de la informática.

En el Congreso…….se manifestó a favor de la inclusión de nuevas disposiciones penales con objeto de hacer frente a esas insuficiencias (principio de subsidiaridad), destacando la necesidad de evitar la sobrecriminalización y asegurar su incriminación con precisión y claridad.

Desde esta perspectiva, y siguiendo el contenido de la Recomendación núm. R(89)9, adoptada por el Consejo de Europa el 13 de septiembre de 1989, se entendió que el listado mínimo de actos a criminalizar vendría constituido por los siguientes:

– fraude en el campo de la informática,

– falsificación en materia informática,

– daños causados a datos o programas informáticos,

– sabotaje informático,

– acceso no autorizado,

– interceptación no autorizada,

– reproducciones no autorizadas (de un programa informático protegido, de una topografía).

El Congreso subrayó la importancia de la cooperación internacional en la prevención y persecución de los delitos informáticos, acentuada por "la movilidad de los datos informáticos en los sistemas de telecomunicación internacionales y la naturaleza altamente interrelacionada de la sociedad de información moderna", a cuyo efecto, es clara la necesidad de una adecuada armonización del derecho penal material y el otorgamiento de poderes coercitivos adecuados en todos los Estados miembros. A juicio de la AIDP, la cooperación internacional debería igualmente alcanzar a otros ámbitos, como:

– la elaboración de "normas internacionales de seguridad para los sistemas informáticos";

– la aplicación de "medidas adecuadas para la resolución de las cuestiones relativas a la competencia jurisdiccional en el ámbito de los delitos informáticos transfronterizos, así como otros delitos informáticos internacionales";

– el logro de "acuerdos internacionales entre los Estados que se sirven de la nueva tecnología de la información para hacer sus investigaciones más efectivas; esto incluye acuerdos que prevean medidas transfronterizas de investigación y aprehensión efectivas, inmediatas y legales en el campo de los sistemas informáticos interconectados, así como otras formas de cooperación internacional, protegiendo al mismo tiempo los derechos y libertades individuales".

4.5 Legislaciones de otros países respecto al Delito Informático

Indiscutiblemente continúa siendo el Derecho la principal fuente inagotable de adaptación social en la Comunidad Mundial de Naciones. Resulta fantástico apreciar como la Humanidad ha ido insertando los adelantos científico-tecnológicos en aras de perfeccionar los principales mecanismos de comunicación y avances hacia el desarrollo.

La comunidad de Estados de la O.N.U. ha presenciado los adelantos tecnológicos y lo que trae consigo, en este caso el uso o aplicación de los sistemas computacionales y el acceso a Internet para la comisión de delitos (por ejemplo mal uso del correo electrónico, la pornografía infantil en Internet etc.); lo que implica además un seguimiento continuo a conductas sociales que transgreden la voluntad política de los Estados Nacionales y, en su caso, la respuesta punitiva de quien es, junto al Estado, la más antigua y necesaria institución mundial.

Los países que se enfrentan a este problema socio-jurídico y claramente tecnológico se encuentran en la postura de efectuar modificaciones en sus legislaciones internas para armonizarlas con las disposiciones que emite la O.N.U., lo que se refleja en disminuir las conductas delictivas y así controlar para que se dispare el índice de delitos informáticos cometidos por los ciberdelincuentes como se muestra en el cuadro comparativo en el presente trabajo de investigación en la sección de anexos.

4.5.1 Alemania

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que se refiere a los siguientes delitos:

a) Espionaje de datos

Párrafo 202.a "I. Quien consiga sin autorización, para sí o para otro, datos que no le competan y que estén especialmente protegidos contra el acceso ilegítimo será castigado con pena privativa de la libertad de hasta tres años o con multa.
II. Datos, a efectos del apartado I, serán sólo aquellos que sean almacenados, transmitido electrónica, magnéticamente, o de forma no inmediatamente accesible".

b) Fraude informático

Párrafo 263.a "I. Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medio de una errónea configuración del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso, será castigado con pena de privación de libertad de hasta cinco años o con multa.
II. Procede aplicar el 263, apartados II a V.

c) Alteración de datos

Párrafo 269. I. Quien, para engañar en el tráfico jurídico, almacene o altere datos probatorios relevantes de manera que en el momento de su recepción existiría un documento no auténtico o falsificado, o utilice datos almacenados o alterados de ese modo será castigado con pena de privación de libertad de hasta cinco años o con multa.
II. La tentativa es punible.
Deberá aplicarse el x 267, apartado III".

d) Sabotaje informático

Párrafo 303b. “Quien destruya una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad,

1. cometiendo el hecho de acuerdo al párrafo 303.a.II, o

2. destruyendo, dañando, inutilizando, eliminando o alterando una instalación de elaboración de datos o un soporte de datos, será castigado con pena de privación de libertad de hasta cinco años o con multa.

II. La tentativa será punible”.

La finalidad de la legislación alemana, al crear el tipo de sabotaje informático diferenciado del tipo de alteración de datos, es clarificar y sancionar con mayor severidad las acciones que atentan contra procesos de datos que sean de importancia esencial para una empresa o establecimiento industrial ajenos o para la administración. Dichas acciones pueden recaer en equipos de procesamiento de datos, soportes y en los datos mismos.

4.5.2 Argentina

En la ley que trata los Delitos Informáticos, no hay una definición de delito informático, sin embargo, se ha llegado a definir como: “Hecho ilícito que se comete mediante la utilización de medios o sistemas informáticos”[50]

Normativa Argentina

- Ley 26388 de Delitos Informáticos

Texto de la ley de reforma del código Penal en materia de delitos informáticos Ley 26388

Art. 1°.- Incorpórense como últimos párrafos del artículo 77 del Código Penal, los siguientes:

[50] http://www.bcra.gov.ar/pdfs/eventos/Delitos_Pres_Antonio_Travieso.pdf 16 de Junio de 2014, 13:20 hrs.

"El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente. "

Art. 2°.- Sustitúyese el artículo 128 del Código Penal, por el siguiente:

"Artículo 128.- Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años."

Art. 3°.- Sustitúyese el epígrafe del Capítulo III, del Título V, del

Libro II del Código Penal, por el siguiente:

"Violación de Secretos y de la Privacidad."

Art. 4°.- Sustitúyese el artículo 153 del Código Penal, por el siguiente:

"Artículo 153.- Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su

destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena."

Art. 5°.- Incorpórase como artículo 153 bis del Código Penal, el siguiente:

"Artículo 153 bis.- Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. "

Art. 6°.- Sustitúyese el artículo 155 del Código Penal, por el siguiente:

"Artículo 155.- Será reprimido con multa de pesos UN MIL QUINIENTOS ($1.500) a PESOS CIEN MIL ($100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público."

Art. 7°.- Sustitúyese el artículo 157 del Código Penal, por el siguiente:

"Artículo 157.- Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos."

Art. 8°.- Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:

"Artículo 157 Bis.- Será reprimido con la pena de prisión de un mes a dos años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años."

Art. 9°.- Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente:

"Inciso 16.- El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos."

Art. 10.- Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:

"En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños."

Art. 11.- Sustitúyese el artículo 184 del Código Penal, por el siguiente:

"Artículo 184.- La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2. Producir infección o contagio en aves u otros animales domésticos;

3. Emplear substancias venenosas o corrosivas;

4. Cometer el delito en despoblado y en banda;

5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público."

Art. 12.- Sustitúyese el artículo 197 del Código Penal, por el siguiente: "Artículo 197.- Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida. "

Art. 13.- Sustitúyese el artículo 255 del Código Penal, por el siguiente:

"Artículo 255.- Será reprimido con prisión de un mes a cuatro años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de SETECIENTOS CINCUENTA PESOS a DOCE MIL QUINIENTOS PESOS."

Art. 14.- Deróganse el artículo 78 bis y el inciso 1° del artículo 117 bis del Código Penal.

Acerca de la confidencialidad de los datos encontramos la siguiente legislación:

LEY DE CONFIDENCIALIDAD SOBRE INFORMACION Y PRODUCTOS QUE ESTEN LEGITIMAMENTE BAJO CONTROL DE UNA PERSONA Y SE DIVULGUE

INDEBIDAMENTE DE MANERA CONTRARIA A LOS USOS COMERCIALES HONESTOS.

LEY Nº 24.766

Promulgada: Diciembre 20 de 1996.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTICULO 1°- Las personas físicas o jurídicas podrán impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honesto, mientras dicha información reúna las siguientes condiciones:

a) A, sea secreta en el sentido de que no sea, como cuerpo o en la configuración, reunión precisa de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y

b) Tenga un valor comercial por ser secreta; y

c) Haya sido objeto de medidas razonables, en las circunstancias, para mantenerla, secreta, tomadas por la persona que legítimamente la controla.

Se considerará que es contrario a los usos comerciales honestos el incumplimiento de contratos, el abuso de confianza, la instigación a la infracción y adquisición de información no divulgada por terceros que supieran o no, por negligencia grave, que la adquisición implicaba tales prácticas.

ARTICULO 2°- La presente ley se aplicará a la información que conste en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros elementos similares.

ARTICULO 3°- Toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a una información que reúna las condiciones enumeradas en el artículo 1° y sobre cuya confidencialidad se los haya prevenido, deberá abstenerse de usarla y de revelarla sin causa justificada o sin consentimiento

de la persona que guarda dicha información o de su usuario autorizado.

II

Protección de la información solicitada por la autoridad sanitaria como requisito para la aprobación de productos

ARTICULO 4°- Para los casos en que se solicite la aprobación del registro o autorización de comercialización de productos que utilicen nuevas entidades químicas que no tengan registro previo ni en la Argentina ni en cualquier otro país, deberá presentarse a la autoridad sanitaria local información que acredite la eficacia e inocuidad del producto. En la medida que esta información reúna los requisitos del artículo 1° y sea resultado de un esfuerzo técnico y económico significativo, será protegida contra todo uso comercial deshonesto tal como se define en la presente ley y no podrá ser divulgada

ARTICULO 5°- Para el caso de productos que tengan registro o autorización de comercialización en la Argentina o en países del anexo I, incluido el caso señalado en el artículo anterior una vez que se haya otorgado el registro en la Argentina o en alguno de esos países del anexo I, la autoridad sanitaria local procederá a la aprobación o autorización de comercialización de productos similares. A esos efectos la autoridad sanitaria local, para otorgar la inscripción de especialidades medicinales o farmacéuticas similares a las que se encuentran autorizadas en el país o en países del anexo I, solicitará que se presente únicamente la siguiente información, distinta a la mencionada en el artículo anterior:

a) Del producto: nombre propuesto para el mismo; fórmula (definida y verificable); forma o formas farmacéuticas en que se presentara; clasificación farmacológica, haciendo referencia al número de código -si existiere- de la clasificación internacional de medicamentos de la Organización Mundial de la Salud (OMS); condición de expendio;

b) Información técnica: método de control; periodo de vida útil; método de elaboración de acuerdo con prácticas adecuadas de fabricación vigente y datos sobre bioequivalencia o biodisponibilidad del producto respecto de los similares;

c) Proyecto de rótulos y etiqueta que deberán contener las siguientes inscripciones: nombre del laboratorio, dirección del mismo, nombre del Director Técnico, nombre del producto y

nombre genérico en igual tamaño y realce, fórmula por unidad de forma farmacéutica o porcentual, contenido por unidad de venta, fecha de vencimiento, forma de conservación y condición de venta, número de partida y serie de fabricación; y la leyenda MEDICAMENTO AUTORIZADO POR EL MINISTERIO DE SALUD Y ACCION SOCIAL, Certificado N°;

d) Proyecto de prospectos que reproducirá; las inscripciones no variables de los rótulos y etiquetas; la acción o acciones farmacológicas y terapéuticas que se atribuyen al producto con indicaciones clínicas precisas y con advertencias, precauciones y, cuando corresponda, de antagonismos, antidotismos e interacciones medicamentosas y de los efectos adversos que puedan llegar a desencadenar, posología habitual y dosis máximas y mínimas, forma de administración, presentaciones y riesgo de habituación adictiva en caso de determinadas formas de uso indebido;

e) En el caso de especialidades medicinales o farmacéuticas importadas de los países incluidos en el Anexo II que forma parte integrante de la presente, además de la información requerida en los incisos precedentes, deberá acompañarse un certificado de la autoridad sanitaria del país de origen. Previa a la solicitud de registro o importación ante la autoridad sanitaria local, el producto en cuestión deberá estar comercializado en el país de origen.

La elaboración de las especialidades medicinales o farmacéuticas a que se refiere, el presente artículo deberá llevarse a cabo en laboratorios farmacéuticos cuyas p1antas se encuentren aprobadas por entidades gubernamentales de países de alta vigilancia sanitaria o por el Ministerio de Salud y Acción Social, que cumplan con las normas de elaboración y control de calidad, exigidas por la autoridad sanitaria nacional.

Una vez presentada la información solicitada en este artículo, el Ministerio de Salud y Acción Social tendrá un plazo de 120 días corridos para expedirse, contados a partir de la presentación de la solicitud de inscripción de la especialidad medicinal o farmacéutica. La aprobación del registro o de la autorización de comercialización establecida al amparo de los procedimientos de aprobación para productos similares establecidos en este artículo, por parte de la autoridad administrativa local, no implica el uso de la información confidencial protegida por la presente ley.

El régimen del presente artículo será comprensivo para:

I. Las solicitudes de registro de especialidades medicinales a elaborarse en nuestro país y aquellas a importarse de países incluidos en el Anexo II que resulten similares a otras ya inscriptas en el Registro; y

II. Las solicitudes de registro de especialidades medicinales a elaborarse en nuestro país, similares a las autorizadas para su consumo público en al menos uno de los países que integran el Anexo I, aún cuando se tratara de una novedad dentro del Registro de la Autoridad Sanitaria

ARTICULO 6°- En los casos que se enumeran más abajo además de la información requerida en el artículo 5°, deberá presentarse a la autoridad sanitaria local, información que acredite la eficacia e inocuidad del producto. Los casos referidos son los siguientes:

a) Elaboración en el país de productos que no tengan registro previo en la Argentina, salvo la excepción prevista en el artículo anterior, para las especialidades medicinales autorizadas en algunos de los países del Anexo 1;

b) Importación desde un país del Anexo II de esta ley que no tuviera similares inscriptos en el registro de la autoridad sanitaria local aún cuando estuviera autorizada y comercializada en el país de origen;

c) Importación de productos manufacturados en países no incluidos en los Anexos I y II de la presente ley, y no autorizados para su consumo en alguno de los países del Anexo I.

ARTICULO 7°- Cuando la comercialización de los productos a registrar requiera la autorización del Instituto Argentino de Sanidad y Calidad Vegetal y del Servicio Nacional de Sanidad Animal o los nuevos organismos a crearse dependientes de la Secretaría de Agricultura, Pesca y Alimentación del Ministerio de Economía y Obras y Servicios Públicos, dicho organismo fijará la normativa administrativa correspondiente, creando un sistema de clasificación, archivo y reserva de documentación que asegure la protección de la propiedad intelectual, de acuerdo al artículo 1° de la presente ley, de la información científica y técnica que le fuera suministrada para la inscripción de productos fitosanitarios y zoosanitarios.

ARTICULO 8°- Cuando se trate de un producto o procedimiento protegido por una patente de invención, cualquier tercero podrá utilizar la invención antes del vencimiento de la patente, con fines experimentales y para reunir la información requerida para la aprobación de un producto o procedimiento por la autoridad competente para su comercialización con posterioridad al vencimiento de la patente.

ARTICULO 9º- La información a que se refiere este Capítulo, será protegida mientras reúna los requisitos del artículo 1°; por lo tanto no estará protegida la información que hubiera caído en el dominio público en cualquier país, por la publicación de cualquiera de los datos protegidos, la presentación de todos o partes de los mismos en medios científicos o académicos, o por cualquier otro medio de divulgación.

ARTICULO 10.- Quedará exceptuado de la protección del artículo 4°, la información cuya publicación sea necesaria para proteger al público o cuando se adopten medidas para garantizar la protección de dicha información contra todo uso comercial deshonesto.

4.5.3 Austria

La Ley de reforma del Código Penal, sancionada el 22 de Diciembre de 1987, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática 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 contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

Ley de reforma del Código Penal de 22 de diciembre de 1987

Esta ley contempla los siguientes delitos:

Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática 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 contempla sanciones para quienes cometen este hecho utilizando su profesión.

Puedo referir en cuanto a esta legislación que, no contempla la figura del delito informático, que lograría agrupar diferentes modalidades del mismo y no enfocarse a una figura delictiva o forma de operar.

4.5.4 Brasil

En Brasil el Derecho Penal Informático se caracteriza por su absoluta pobreza legislativa acerca del tema. La Parte Especial del Código Penal data de 1940 y las normas punitivas corresponden a una época en que no existían computadoras, de modo que las normas vigentes solamente pueden ser aplicadas a los delitos informáticos de forma incidental a tales hipótesis. El legislador brasileño solamente se preocupó del uso indebido de los ordenadores, en el momento en que la legislación existente se dirige específicamente a la piratería de "software", jamás al crimen informático, por excelencia.

A partir del 2 de abril comenzó a regir la ley contra delitos informáticos, sancionada por la Presidente Dilma Rousseff en diciembre de 2012. La legislación, hasta ahora inédita, tipifica diversos crímenes relacionados con la información personal almacenada en computadoras y prevé penas de seis meses a dos años de prisión por violar correos electrónicos que contengan información y datos de carácter confidencial, ya sean de naturaleza privada o comercial.

Entre otras disposiciones, también prevé la pena de tres meses a un año de prisión, además de multa, para quien “invada sistemas informáticos ajenos con el fin de obtener, adulterar o destruir datos o información sin autorización explícita”. Se aplicará la misma pena a quien produzca, ofrezca o venda programas que permitan la invasión de sistemas y computadoras ajenas. Para los casos en los que se interrumpan servicios, como sucedió en el año 2011, en el mayor ataque sufrido por órganos gubernamentales en el país que incluyó a sitios de la Presidencia de la República y del Ejército, la pena varía de uno a tres años de prisión.

El proyecto de ley comenzó luego de un episodio ocurrido en mayo de 2012 en el que una actriz brasileña, Carolina Dieckmann, fue víctima de chantaje, luego de que 36 de sus fotos personales fueran hackeadas de su computadora y exhibidas en distintos sitios.[51]

Antes de esta ley, los delitos informáticos perpetrados en Brasil no estaban tipificados pero, por analogía, se trataban como crímenes de violación de la comunicación.

4.5.5 Chile

LEY RELATIVA A DELITOS INFORMATICOS
Ley No.:19223

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

[51] http://dialogoamericas.com/es/articles/rmisa/features/regional_news/2013/04/16/feature-ex-4076 21 de Julio de 2014 13: 10 hrs.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

4.5.6 Costa Rica

La Asamblea Legislativa de la República de Costa Rica contempla en el Título VII del Código Penal (y su reforma del Artículo 9 de la Ley No. 7425) una sección denominada Delitos Informáticos y Conexos.

En la sección citada con antelación se encuentra el artículo 217 bis que ubica el tipo penal de Estafa informática el cual menciona: “Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

“Artículo 229 bis.- Daño informático

Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de tres a seis años de prisión si la información suprimida, modificada, destruida es insustituible o irrecuperable.

Acerca de las redes sociales y la suplantación de identidad:

“Sección VIII

Delitos informáticos y conexos

Artículo 230.- Suplantación de identidad

Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien utilizando una identidad falsa o inexistente cause perjuicio a un tercero.

La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz.

4.5.7 España

En el Nuevo Código Penal de España, el artículo 264-2 dispone que se aplicará la pena de prisión de uno a tres años y 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.

El código mencionado sanciona en forma detallada esta categoría delictual (violación de secretos/espionaje/divulgación), al aplicar pena de prisión y multa, agravadas cuando existe una intensión dolosa, y cuando el hecho es cometido por funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, el nuevo Código Penal de España, en su artículo 248, sólo tipifica las estafas con ánimo de lucro cuando el infractor se vale de alguna manipulación informática, pero no detalla las penas a aplicar en el caso de la comisión del delito.

4.5.8 Estados Unidos de Norteamérica

Este país adoptó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos exageradamente técnicos acerca de qué es y qué no es virus, un gusano, un “caballo de Troya” y en qué difieren de los virus, la nueva acta prohíbe la transmisión de un programa, información, códigos o comandos que causen daños a la computadora, a los sistemas informáticos, a las redes, información, datos programas 18 U.S.C. Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

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

a) Para los que intencionalmente causen un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.
b) Para los que lo transmitan sólo 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 al no definir los virus, sino al describir el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos de cualquier forma que se realicen. La nueva ley diferencia los niveles de los delitos y da lugar a que se considere qué debe entenderse por acto delictivo..

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa a la persona que defraude a otra mediante la utilización de una computadora o red informática.

4.5.9 Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

Acceso fraudulento a un sistema de elaboración de datos (462-2). En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionario del sistema.

Sabotaje informático (462-3). En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos (462-4). En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados (462-5). En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6). En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

4.5.10 Perú

En su Código Penal establece en el Capítulo X la modalidad del Delito Informático, específicamente en el artículo 207-A que expresa lo siguiente:

"El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas".

4.6 Marco Jurídico Nacional del Delito Informático

En este apartado considero el Código Penal Federal y las legislaciones de las entidades federativas de nuestro país que regulan de forma directa o en su caso regulen aproximadamente la figura del delito informático, contemplo las legislaciones penales de los siguientes estados de la República: Aguascalientes, Baja California, Colima, Estado de México, Guanajuato, Morelos, Sinaloa, Zacatecas y Distrito Federal.

Asimismo, relaciono la Constitución Nacional, debido a que es la Carta Magna que es la máxima ley de nuestro país, la cual rige la estructura y composición de nuestro sistema jurídico fundamentalmente.

En la actualidad, con el avance de la tecnología en sus diferentes campos de acción y su aplicación específica en nuestras vidas es cotidiano ver a las personas con un dispositivo de telefonía celular en las calles de la ciudad o a bordo del transporte público o privado los pasajeros se entretienen con aplicaciones específicas o dan lectura a libros en formatos digital.

Lo anterior lo vínculo con la ciencia del Derecho, porque así como la tecnología avanza, también el Derecho es dinámico y tiene que estar a la vanguardia con las nuevas conductas de la sociedad en las que se encuentra inmersa, por ejemplo no es la misma sociedad de México en el año de 1917 en donde el constituyente creaba las normas para la sociedad de esa época, hoy en día es importante darle esa vanguardia a la Constitución Política y en particular a las normas de carácter secundario para armonizar la convivencia de la colectividad.

4.6.1 Constitución Política de los Estados Unidos Mexicanos

Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Específicamente en su apartado A contempla:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos que se sustanciarán ante los organismos autónomos especializados e imparciales que establece esta Constitución.

B. En materia de radiodifusión y telecomunicaciones:

I. El Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales.

II. Las telecomunicaciones son servicios públicos de interés general, por lo que el Estado garantizará que sean prestados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin injerencias arbitrarias.

III. La radiodifusión es un servicio público de interés general, por lo que el Estado garantizará que sea prestado en condiciones de competencia y calidad y brinde los beneficios de la cultura a toda la población, preservando la pluralidad y la veracidad de la información, así como el fomento de los valores de la identidad nacional, contribuyendo a los fines establecidos en el artículo 3o. de esta Constitución.

IV. Se prohíbe la transmisión de publicidad o propaganda presentada como información periodística o noticiosa; se establecerán las condiciones que deben regir los contenidos y la contratación de los servicios para su transmisión al

público, incluidas aquellas relativas a la responsabilidad de los concesionarios respecto de la información transmitida por cuenta de terceros, sin afectar la libertad de expresión y de difusión.

Nuestra Constitución Política, enmarca el derecho a la libertad de expresión en su artículo sexto en el que señala que la manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley, dicho artículo nos indica qué sino en el caso de ataquen la vida privada o los derechos de terceros; por lo que es importante este señalamiento en el momento que el Estado debe proteger de la afectación que hagan terceros a la moral, la vida privada o a los derechos de las personas, así como garantizar el uso adecuado de los datos personales y confidenciales de quienes lo proporcionen.

4.6.2 Código Penal Federal

En esta legislación considera en el Título Noveno (Revelación de secretos y acceso ilícito a sistemas y equipos de informática) en su capítulo segundo en su 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.*

En su artículo 211 bis 2 expresa: "*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."

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.

En el anterior título intitulado Revelación de secretos y acceso ilícito a sistemas y equipos de informática, considera el legislador la prioridad hacia los equipos informáticos del Estado a la persona que tenga la intención de provocar

un daño o simplemente copie la información será sancionado, sin embargo se debe especificar en un título diferente, ya que se contempla como un delito informático que debe atender a características especiales para su comisión.

Siendo el Código Penal Federal un eje legislativo en materia penal para contemplar las figuras delictivas, debe considerarse y dedicársele importancia respecto a la regulación de los delitos informáticos como se ha venido dando en algunas entidades federativas, ya que es necesario establecer sanciones a las conductas delictivas de individuos que poseen las herramientas y conocimientos para vulnerar la privacidad, intimidad y mal uso de los datos que se incluyen en los perfiles de cuentas de redes sociales, correos electrónicos, sistemas de mensajería instantáneas, etcétera.

4.6.3 Código Penal del Estado de Aguascalientes

ARTÍCULO 180.- Violación de correspondencia. La Violación de Correspondencia consiste en abrir o interceptar en forma dolosa, una comunicación escrita, electrónica, magnética, óptica o informática que no esté dirigida al inculpado.

Al responsable de Violación de Correspondencia se le aplicarán de 3 a 6 meses de prisión y de 5 a 20 días multa, y al pago total de la reparación de los daños y perjuicios ocasionados.
Esta punibilidad no se aplicará si el responsable ejerce la patria potestad, tutela o custodia, y la comunicación escrita se dirige a las personas bajo su tutela o guarda.

ARTÍCULO 181.- Acceso informático indebido. El Acceso Informático Indebido consiste en:

I. Acceder a la información contenida en un aparato para el procesamiento de datos o cualquier dispositivo de almacenamiento de información sin autorización de su propietario o poseedor legítimo; o

II. Interferir el buen funcionamiento de un sistema operativo, programa de computadora, base de datos o cualquier archivo informático, sin autorización de su propietario o poseedor legítimo.

Al responsable del Acceso Informático Indebido se le aplicará de 1 a 3 meses de prisión, de 150 a 300 días multa así como el pago de la reparación de los daños y perjuicios ocasionados. Si quien realiza el Acceso Informático Indebido es el responsable del mantenimiento o seguridad del sistema de información sobre el que se perpetra, se le aplicará de 2 a 6 meses de prisión, de 300 a 600 días multa así como el pago de la reparación de daños y perjuicios ocasionados.

En el numeral anterior, contempla la violación de correspondencia. La cual se describe la conducta en que consiste en abrir o interceptar en forma dolosa, una comunicación escrita, electrónica, magnética, óptica o informática que no esté dirigida al inculpado, por lo que se acerca a un delito informático, debido a que al referirse a la interceptación de una comunicación escrita, electrónica- informática se adecua al correo electrónico o a la bandeja de entrada proveniente de las redes sociales en los portales de la Internet.

4.6.4 Código Penal para el Estado de Baja California

CAPITULO III
VIOLACION DE CORRESPONDENCIA

ARTÍCULO 257.- Tipo y punibilidad.- Al que dolosamente abra o intercepte una comunicación escrita que no esté dirigida a él, se le impondrá de veinte a cuarenta días multa.

Exclusión de pena, por razón de la patria potestad, tutela o custodia.- No se impondrá pena a los que ejerciendo la patria potestad, la tutela o custodia, abran o intercepten las comunicaciones escritas a sus hijos menores de edad o a las personas que se hallen bajo su tutela o guarda.

En el presente artículo, no se hace una aclaración acerca del medio en el que se tenga la comunicación, es decir, no se especifica si en un medio impreso, un medio electrónico, lo que a mi consideración sugeriría que se considere ese aspecto, porque en la actualidad se manejan frecuentemente comunicaciones electrónicas.

En éste ordenamiento jurídico, no se presenta la figura del delito informático, por lo que carece de la sanción a conductas que vulneren la privacidad y el manejo de datos de los usuarios de redes sociales o de forma general a quienes tengan acceso a internet, quienes deben tener seguridad al accesar a los portales de internet, sin que sufran un daño o menoscabo en el uso de sus datos personales.

La legislación penal de Baja California carece de la descripción de los delitos informáticos, lo que desde mi particular punto de vista es relevante tratar estas conductas porque el uso de la tecnología es constante, en específico de dispositivos móviles con acceso a internet y equipos de cómputo en los que existe un flujo de información de gran cantidad.

4.6.5 Código Penal para el Estado de Colima

CAPITULO III.

VIOLACION DE CORRESPONDENCIA.

ARTÍCULO 146.- Se aplicarán de seis meses a un año de prisión y multa hasta por 15 unidades:

I.- Al que abra indebidamente una comunicación escrita que no esté dirigida a él; y

II.- Al que indebidamente intercepte una comunicación escrita que no le esté dirigida, aunque no se imponga de su contenido.

CAPITULO IV

USO INDEBIDO DE LLAMADAS TELEFONICAS

ARTICULO 153 Bis.- Al que por cualquier medio de comunicación que se encuentre bajo su control o radio de acción, envíe mensajes obscenos, o a manera de broma o sin existir necesidad que lo justifique, realice llamadas de alerta, emergencia o ayuda a un particular o sistema de respuesta de llamada telefónica de emergencia o su equivalente, se le impondrá de uno a seis meses de prisión o multa hasta por 200 unidades.

En caso de reincidencia, se impondrá de seis meses a un año de prisión y multa hasta por 300 unidades.

Cuando como consecuencia de la llamada o mensaje indebido se produzca un daño, pérdida o alteración de cualquier índole o distracción, independientemente del resultado se le impondrá la pena de uno a 3 años prisión y multa hasta por 500 unidades.

CAPITULO VII

DELITO INFORMATICO

ARTÍCULO 240 Bis.- Se le impondrá una pena de seis meses a seis años de prisión y multa de trescientos a mil unidades al que de manera dolosa y sin derecho alguno, ni autorización de quien pueda otorgarlo conforme a la Ley, utilice o tenga acceso a una base de datos, sistemas o red de computadoras o a cualquier parte de la misma, con el firme propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información en perjuicio de otro.

De igual forma, la misma sanción del párrafo anterior se impondrá, a quien 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.

CAPÍTULO VIII

USO INDEBIDO DE INFORMACIÓN SOBRE ACTIVIDADES DE LAS INSTITUCIONES DE SEGURIDAD PÚBLICA, DE PROCURACIÓN E IMPARTICIÓN DE JUSTICIA, ASÍ COMO LAS DEL SISTEMA PENITENCIARIO.

ARTÍCULO 115 BIS.- Al que con objeto de planear o ejecutar un delito, u obstruir la función de seguridad pública, realice actos tendientes a obtener o trasmitir mediante cualquier medio, información sobre las

actividades propias de las instituciones de seguridad pública, de procuración e impartición de justicia, y de ejecución de las penas, de cualquier ámbito, o sobre cualquier servidor público, se le impondrá de dos a quince años de prisión y multa de hasta quinientas unidades.

Cuando el sujeto activo sea miembro de cualquiera de las instituciones de seguridad pública del Municipio, Estado o de la Federación, de procuración de justicia y de ejecución de las penas, federal o estatal, o haya pertenecido a cualquiera de éstas, o sea agente de seguridad privada que realice actividades de custodia o vigilancia hacia servidores públicos, se le impondrá de cinco a quince años de prisión y multa de hasta ochocientas unidades.

Igualmente, se sancionará con una pena de tres a siete años de prisión y multa de hasta doscientas unidades, a cualquier elemento perteneciente a las instituciones de seguridad pública que con la intención de cometer el delito a que se refiere el párrafo anterior, porte tres o más teléfonos celulares, o cualquier sistema de comunicación electrónica o de radiocomunicación, o bien, no justifique su propiedad o legitima posesión.

Además de la pena y sanción que corresponda por la realización de la conducta descrita en los dos párrafos anteriores, el servidor público será destituido del empleo, cargo o comisión, e inhabilitado por el mismo tiempo de la pena de prisión impuesta.

4.6.6 Código Penal del Estado de México

CAPITULO II

Utilización de imágenes y/o voz de personas menores de edad o personas que no tienen la capacidad para comprender el significado del hecho para la pornografía

Artículo 206.- Comete el delito de utilización de imágenes y/o voz de personas menores de edad o personas que no tienen la capacidad para comprender el significado del hecho para la pornografía, el que realice las siguientes conductas:

I. Produzca, fije, grabe, videograbe, fotografíe o filme e imprima de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.

II. Reproduzca, publique, ofrezca, publicite, almacene, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.

III. Posea intencionalmente para cualquier fin, imágenes, sonidos o la voz de personas menores de edad o de personas que no tengan la capacidad de comprender el significado del hecho o de resistirlo, sea en

forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.

IV. Financie, dirija, administre o supervise cualquiera de las actividades anteriores con la finalidad de que se realicen las conductas previstas en las fracciones anteriores.
Al autor de los delitos previstos en las fracciones I y II se le impondrá pena siete a doce años de prisión y de quinientos a tres mil días multa. Al autor de los delitos previstos en la fracción III se le impondrá la pena de seis a diez años de prisión y de quinientos a mil días multa. A quien cometa el delito previsto en la fracción IV, se le impondrá pena de prisión de diez a catorce años y de mil a dos mil días multa

En este capítulo se expresa la intención del legislador para sancionar el uso de imágenes y/o voz de personas menores de edad o personas que no tienen la capacidad para comprender el significado del hecho para la pornografía, lo que también debe contemplarse es el posible escenario de que se traslade al campo de las redes sociales, ya que se difunde el material en grupos de carácter cerrados, en el que los usuarios participan en cargar videos y fotos pornográficas de menores.

Asimismo, nos indica la fracción primera del artículo 206 que a quién Produzca, fije, grabe, videograbe, fotografíe o filme e imprima de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas, nos realiza la especificación de que si aquellas conductas las realiza de forma directa, informática, audiovisual, virtual o por cualquier otro medio,

por lo que considero un avance al contemplar estos medios que al utilizar el sujeto activo puedan sancionarse.

Capítulo V

Usurpación de Identidad

Artículo 264.- Se le impondrán de uno a cuatro años de prisión y de cien a quinientos días multa, a quien ejerza con fines ilícitos un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.

Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el párrafo que precede prevista en el presente artículo a quienes:

I. Cometan un hecho ilícito previsto en las disposiciones legales con motivo de la usurpación de la identidad;

II. Utilicen datos personales, sin consentimiento de quien deba otorgarlo;

III. Otorguen el consentimiento para llevar a cabo la usurpación de su identidad; y

IV. Se valgan de la homonimia para cometer algún ilícito.

Las sanciones previstas en este artículo se impondrán con independencia de las que correspondan por la comisión de otro u otros delitos.

Artículo 265.- Las penas señaladas en el artículo anterior se incrementarán hasta en una mitad, cuando el ilícito sea cometido por un

servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su profesión o empleo para ello.

Realizando el análisis del delito de usurpación de identidad, nos encontramos en un problema, ya que también en redes sociales se puede hacer mal uso de los datos que son proporcionados a los servidores de red, en los que se crean perfiles con nombres falsos, seudónimos, por lo que es una conducta muy común en perfiles de Facebook y Twitter, originando la comisión de este delito.

Lo anterior origina que algunos perfiles con estas características contengan información apócrifa, mismo que propicia la comisión del delito de suplantación de identidad al utilizar una imagen de identificación que no corresponde al usuario, así como la intromisión a otros perfiles que pueden sufrir el robo de su identidad, involucrando en primer tiempo su imagen o fotografía y en segundo la utilización de sus datos personales y por último el acceso a los perfiles de sus amigos o familiares que están incluidos en dichas redes sociales.

4.6.7 Código Penal para el Estado de Guanajuato

CAPÍTULO II
VIOLACIÓN DE CORRESPONDENCIA

Artículo 231.- Se aplicará de diez días a dos años de prisión y de diez a cuarenta días multa, a quien indebidamente:

I.- Abra, intercepte o retenga una comunicación que no le esté dirigida.

II.- Accese, destruya o altere la comunicación o información contenida en equipos de cómputo o sus accesorios u otros análogos.

No se impondrá pena alguna a quienes ejerciendo la patria potestad o la tutela, ejecuten cualquiera de las conductas antes descritas, tratándose de sus hijos menores de edad o de quienes se hallen bajo su guarda.

Se requerirá querella de parte ofendida cuando se trate de ascendientes y descendientes, cónyuges o concubinos, parientes civiles o hermanos.

Como hemos reiterado, el delito de violación de correspondencia, en concreto el Código Penal para el Estado de Guanajuato contempla en su fracción II del artículo 231 la destrucción del contenido (datos y/o información) que se encuentren almacenados en equipos de cómputo, por lo que es un parteaguas en contemplar en la compilación penal de Guanajuato un apartado específico acerca de los delitos informáticos.

4.6.8 Código Penal del Estado de Morelos

*CAPITULO *VIII*
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.

CAPÍTULO IV
VIOLACIÓN DE CORRESPONDENCIA

ARTÍCULO 241.- Al que abra o intercepte una comunicación escrita que no esté dirigida a él, se le impondrá de cincuenta a cien días multa.
No se sancionará a quienes ejerzan la patria potestad, la tutela o la custodia de menores de edad o incapacitados, en relación con las comunicaciones dirigidas a quienes se hallen bajo su potestad, tutela o guarda.

A diferencia de otras legislaciones de carácter penal, en el Estado de Morelos encontramos la regulación de los delitos informáticos en el capítulo VIII del citado código.

La figura del delito informático en este ordenamiento implica que la persona actúe de forma dolosa y sin derecho para el manejo de esos datos, a lo que se contemplan tres supuestos jurídicos:

a) Use o entre a una base de datos, sistema de computadores o red de computadoras.
b) 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.

c) 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.

Estos tres escenarios son importantes, al contemplarse las conductas señaladas para sancionarse, sin embargo, es necesario agregar por ejemplo: la suplantación de identidad en redes sociales, el envío masivo de archivos infectados con algún tipo de virus informático, amenazas de causar daño a la persona y/o al honor de la misma a través de internet.

4.6.9 Código Penal del Estado de Sinaloa

En este texto legislativo se encuentra en el Título Décimo denominado Delitos contra el patrimonio es su capítulo V contempla el Delito Informático (Artículo 217):

ARTÍCULO 217. Comete 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; o

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.

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.

Mi opinión acerca de este precepto legal, es que encontramos una definición aproximada en relación al delito informático y también observamos las características para la comisión del mismo, lo que nos acerca a evitar encontrarnos lagunas legislativas para esta figura delictiva.

En la legislación penal de Sinaloa se observa que se contempla la figura del delito informático en sus dos fracciones del numeral 217, sin embargo, no ponen a consideración la diversidad de conductas en las que puede considerarse el delito informático.

4.6.10 Código Penal del Estado de Zacatecas

Artículo 257.- Comete el delito de amenazas, el que valiéndose de cualquier medio, intimide a otro con causarle un mal en su persona, en su honor, en su prestigio, en sus bienes o en la persona, honor, prestigio o bienes de alguien con quien esté ligado con cualquier vínculo.

El delito de amenazas se sancionará con prisión de tres meses a un año o multa de cinco a veinte cuotas, o trabajo en favor de la comunidad hasta por quince días, a juicio del juzgador.

Artículo 258.- Al que por medio de amenazas de cualquier género trate de impedir que otro ejecute lo que tiene derecho a hacer, se le aplicarán las mismas sanciones a que se refiere el artículo anterior.

Artículo 259.- Se exigirá solamente caución de no ofender:
I.- Si los daños con que se amenaza son leves o evitables;
II.- Si la amenaza tiene por condición que el amenazado no ejecute un hecho ilícito en sí.

En este caso también se exigirá caución al amenazado, si el juez lo estima necesario.

Al que no otorgare la caución de no ofender, se le impondrá multa de cinco a diez cuotas.

En su numeral 257, contempla el delito de amenazas el cual consiste en intimidar a otro con causarle un mal en su persona, en su honor, en su prestigio, en sus bienes o en la persona, honor, prestigio o bienes de alguien con quien esté ligado con cualquier vínculo a través de cualquier medio; lo que deja abierta la posibilidad que se haga a través de internet y en específico en redes sociales, por lo que sugiero de forma breve, que se tiene contemplar de forma clara y concreta para no dejar laguna legislativa alguna para sancionar esas conductas que dañan la esfera de la colectividad.

4.6.11 Código Penal para el Distrito Federal

USURPACIÓN DE IDENTIDAD

Artículo 211 Bis.- Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.

Se aumentaran en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.

EXTORSIÓN

ARTÍCULO 236. Al que obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro causando a alguien un perjuicio patrimonial, se le impondrán de dos a ocho años de prisión y de cien a ochocientos días multa.

Cuando el delito se cometa en contra de persona mayor de sesenta años de edad, las penas se incrementarán en un tercio. Las penas se aumentarán en dos terceras partes cuando el delito se realice por servidor público o miembro o ex-miembro de alguna corporación de seguridad pública o privada. Se impondrán además al servidor o ex-servidor público, o al miembro o exmiembro de corporación de seguridad pública o privada, la destitución del empleo, cargo o comisión público, y se le inhabilitará de uno a cinco años para desempeñar cargos o comisión públicos; también se le suspenderá el derecho para ejercer actividades en corporaciones de seguridad privada.

Además de las penas señaladas en el primer párrafo, se impondrá de dos a seis años de prisión, cuando en la comisión del delito:

I. Intervenga una o más personas armadas, o portando instrumentos peligrosos; o

II. Se emplee violencia física.

Asimismo, las penas se incrementarán en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica.

VIOLACIÓN DE CORRESPONDENCIA

ARTÍCULO 333. Al que abra o intercepte una comunicación escrita que no esté dirigida a él, se le impondrá de treinta a noventa días multa.

No se sancionará a quien, en ejercicio de la patria potestad, tutela o custodia, abra o intercepte la comunicación escrita dirigida a la persona que se halle bajo su patria potestad, tutela o custodia.

Los delitos previstos en este artículo se perseguirán por querella.

El presente ordenamiento jurídico aplicable para el Distrito Federal carece de un título expreso o un artículo que tipifique la conducta de delito informático, lo que provoca un vacío legal y por lo tanto, en la sociedad se encuentren individuos que realizando conductas que vulneran la esfera privada de las demás personas queden sin sanción alguna.

PROPUESTA LA NECESIDAD DE REGULAR EL DELITO INFORMÁTICO EN EL CÓDIGO PENAL PARA EL DISTRITO FEDERAL

I. Exposición de Motivos

Considerando que de acuerdo con las cifras del Estudio de Hábitos de los Usuarios de Internet en México 2012[52], el número de internautas se incrementó un 14 por ciento, con lo que llegó a 40.6 millones de usuarios, podemos afirmar que en la legislación penal para el Distrito Federal no existe el tipo penal para proteger a estos usuarios de las conducta que afecten su acceso a internet.

En el caso de las redes sociales, principalmente Facebook y Twitter, es muy común que los usuarios agreguen fotos personales en su cuenta, aun existiendo algunos mecanismos para evitar que se haga mal uso de las fotos es perceptible que los ciberdelincuentes hagan uso de sus herramientas para hackear (violar mecanismos de seguridad) para accesar al perfil del usuario, a su información personal y a sus fotos.

Sumemos la falta de conocimiento de las políticas de privacidad y seguridad que emiten las redes sociales en el momento en que se crea el perfil del usuario de la red social que le agrade, simplemente no se les da una total importancia lo que se transforma en un problema serio para el titular de la cuenta al ser víctima de una suplantación de identidad, un robo de imágenes privadas, mal uso de datos personales que en un futuro puede convertirse en una extorsión.

Lo anterior demuestra que es necesario y urgentemente que se contemple la figura de delito informático en el que se haga mención de las características fundamentales para que sea considerado como una conducta de carácter delictiva y por ende sea castigada atendiendo su forma de comisión y las herramientas de las cuales se ha auxiliado el sujeto activo para externar su conducta.

---

[52] http://nuevaweb.com.mx/blog/estudio-de-habitos-y-percepciones-de-los-mexicanos-sobre-internet-2012/ 28 de agosto de 2014, 10:20 hrs.

II. Crítica al delito informático

La difusión y el crecimiento de las nuevas tecnologías han traído consigo en el ámbito jurídico nuevas formas de cometer delitos, lo que origina a la nueva creación de normas para que se sancionen estas conductas delictivas.

Contemplar el delito informático en nuestra legislación es un punto que también requiere de la opinión de los expertos en la materia informática, porque si se trabaja este tema en su conjunto podemos obtener un acercamiento más real, lo que nos proporcionará menos margen de errores en la legislación de esta conducta.

Es necesario promover las reformas adecuadas para el ofrecimiento de las pruebas electrónicas en los procesos penales, lo que nos ayudará a evitar que existan inconsistencias y deficiencias en estos aspectos.

En el Distrito Federal, se cuenta con una policía cibernética, sin embargo, con una legislación penal atrasada en este ámbito debido a que existe un desfase y una total incongruencia entre lo instrumental y la praxis, porque no hay una norma que contemple delitos informáticos pero si existe un órgano que persigue estas conductas.

La policía cibernética en el Distrito Federal considera la comisión de los delitos informáticos dentro del ámbito de la Cibercriminalidad.

El delito informático debe de contemplar varias conductas como: el acceso no autorizado a un equipo de cómputo, la usurpación de identidad en redes sociales, el apoderamiento ilícito de datos personales, fraude a través de medios informáticos, acceso no autorizado de correo electrónico, daño de equipos de cómputo por virus informáticos, robo de bases de datos (empresas e instituciones de gobierno), entre otros.

Lamentablemente, en México se tiene una deficiente estructura legislativa acerca de este tipo de conductas, lo que deja un vacío ocasionando impunidad, no atendiendo la afectación del sujeto pasivo, vulnerando su esfera jurídica.

La impartición de justicia en el Distrito Federal se ha caracterizado en estos últimos años con más transparencia, y más seriedad en las investigaciones, sin embargo considero el que exista una regulación de estas conductas antijurídicas que lesionan a la colectividad respecto a su privacidad, patrimonio y libertad en el uso de dispositivos que tengan conexión a internet.

III. La necesidad de la regulación del Delito Informático en el Código Penal para el Distrito Federal

Los usuarios de internet no tienen en específico un rango de edad promedio, tanto pueden accesar niños, adolescentes, adultos y personas de la tercera edad, lo que nos invita a reflexionar en el tema de la vulnerabilidad que sufren los niños y las personas de la tercera edad porque en general, son quienes están adentrándose en la red por primera vez sin algún familiar o conocido que los auxilie para ingresar a portales de internet que no cuentan con las normas de seguridad principales o portales que carecen de certificados de confidencialidad de datos, lo que provoca que se haga mal uso de estos datos y que en la mayoría de las ocasiones son de carácter personal.

La importancia de regular el delito informático radica en que evitará que las conductas delictivas permanezcan sin sanción y disminuyan estas modalidades, así como el dejar claro sus características para que sea considerado o no como delito.

El desarrollo constante de las nuevas tecnologías y en especial de la Informática ha dado origen a nuevas posibilidades de delincuencia que antes nunca fueron imaginadas, mediante los cuales es probable obtener en gran medida pérdidas económicas o causar importantes daños materiales o morales.

La Asamblea Legislativa del Distrito Federal como órgano enteramente legislativo con la facultad de crear y modificar las leyes que le competen al Distrito Federal, en este caso, el Código Penal para el Distrito Federal es fundamental que se contemple el Delito Informático, debido a que la sociedad tiene cada vez más un acceso frecuente a los medios de comunicación, específicamente a la red de redes, es decir, Internet.

IV. Beneficios de regular el Delito Informático

Actualmente se ven vulnerados los derechos de acceso de usuarios, en este caso de redes sociales de gran presencia internacional como Facebook y Twitter, posteriormente con la regulación en el Código Penal para el Distrito Federal se observará un precepto que castigue la comisión de este tipo de delitos.

Por lo que el regular el delito informático brindará mejor seguridad jurídica, en cuanto a la privacidad de sus datos a los usuarios de internet y en especial a las personas que cuentan con perfiles en redes sociales.

Protegerá los derechos y en específico, los bienes jurídicos patrimoniales, de privacidad, de propiedad intelectual.

En el caso de los bienes jurídicos encontramos el caso de la afectación que tienen los cuentahabientes bancarios, por el simple hecho de serlo son invadidos sus derechos a la privacidad de sus cuentas bancarias y que la mayoría de las veces son retirados los fondos que se encontraban “asegurados” por las instituciones bancarias.

De lo anterior también se desprende que no solo los cuentahabientes son víctimas de este tipo de delitos, ya que, las instituciones bancarias han sido despojadas de grandes capitales al ser violados todos sus mecanismos de seguridad para proteger los fondos que les son encargados, sin embargo, el abordar el campo de aplicación de los delitos que afectan a las instituciones bancarias implicaría el atender diferentes visiones del problema.

Habrá sanciones establecidas en la ley, lo que originará que no existan más delitos impunes, aportando los datos necesarios para valorar y considerar de qué se trata de un delito de ésta naturaleza.

Se adoptarán medidas nacionales y de ser posible medidas en el ámbito internacional para que se evite la comisión de estos delitos, es decir, habrá mecanismos para la cooperación en el ámbito penal internacional para la disminución del impacto del delito en el país y en específico en el Distrito Federal.

Existirá un avance en la legislación, lo que sentará precedente para las demás legislaciones de las entidades federativas acercándose a un mejor planteamiento del delito y así consideren adecuar las características de la figura del delito informático.

Con la regulación en específico de este delito se evitaría la confusión del impartidor de justicia a la hora de interpretar las conductas cercanas a la descripción legal que planteo.

En otro orden de ideas, lo pertinente sería la capacitación del personal de las Agencias del Ministerio Público para recibir y atender a las víctimas de este tipo de delitos, así también a Jueces del Tribunal Superior de Justicia del Distrito Federal para que tengan conocimiento de las nuevas modalidades de delincuencia en las redes informáticas para evitar el desconocimiento de estas nuevas formas de delinquir y a su vez cuenten con los elementos teóricos que les permitan una aplicación correcta de la ley en el caso concreto.

CONCLUSIONES

PRIMERA. Con la aparición de nuevas tecnologías y sus principales herramientas las computadoras y dispositivos móviles, la ciencia del Derecho ha tenido que incorporarse a este campo normativo, es decir el abordar estos nuevos temas para proteger a la sociedad de eventuales delitos informáticos, para lograr un avance en la legislación penal para sancionar este tipo de conductas ilícitas que vulneran la convivencia entre los individuos.

SEGUNDA. El surgimiento del campo de la informática ha contribuido a la aparición de ramas del derecho (Derecho Informático e Informática Jurídica) consideradas como emergentes al suscitarse nuevos problemas jurídicos, los cuales deben darse solución para evitar una problemática que pueda considerarse como situaciones no atendidas por la ciencia jurídica y que en algún momento dado se salga de control del Estado.

TERCERA. Los delitos Informáticos son considerados como una nueva especie de delitos, como los que ya conocemos pero que no pueden ser tratados de la misma manera, esto porque no se cuenta con una misma naturaleza normativa, ya que en otros delitos se encuentran tipificados cada uno de los elementos de su descripción en las legislaciones penales Federal y de cada una de las Entidades Federativas de México.

CUARTA. En la presente investigación se indicó que la comisión de los delitos informáticos, deben efectuarse por individuos que tengan conocimientos especializados o en su caso dominen conocimientos técnicos de la informática para que puedan realizarse, por lo que es claro que una persona que no posea los conocimientos adecuados para manipular un equipo de cómputo o un dispositivo con acceso a Internet, no puede ser sujeto activo del delito informático.

QUINTA. El delito informático en México es aún un tema que se encuentra en un estado de reposo, es decir, no se encuentra actualmente en las legislaciones penales de las entidades federativas que integran la República Mexicana (a excepción de Colima, Morelos y Sinaloa que se encuentra expreso en el Código Penal local, pero aún no se contemplan específicamente los delitos).

SEXTA. Un problema central de la comisión de los delitos informáticos es el establecer las medidas para sancionar a los sujetos activos del delito, ya que debe atenderse de acuerdo a la magnitud del daño causado por la manipulación de los sistemas informáticos, la mayoría de las veces es grave su impacto en personas físicas y personas jurídicas.

SÉPTIMA. Actualmente, en este rubro se habla de ciberdelincuencia, una forma de delincuencia que se ha trasladado al espacio paralelo de la Internet, en la cual en ocasiones el sujeto activo mantiene el anonimato, lo que no puede ser identificado físicamente, sin embargo, a través de estudios técnicos y en específico peritajes en la ciencia de la Informática es posible identificar sus direcciones o en su caso ubicaciones espaciales en determinado país o zona que cuentan un código denominado IP (el

cual es un protocolo de internet único para identificar la computadora o en su caso un dispositivo móvil).

OCTAVA. En el Distrito Federal, el Código Penal no se menciona el Delito Informático, sin embargo, existe un órgano policial que atiende denuncias acerca de delitos que se cometen a través de Internet denominada Policía Cibernética, misma que pertenece a la Secretaría de Seguridad Pública del Distrito Federal, lo que me considero que es una incongruencia que persiga delitos que aún no están establecidos en la norma penal, por lo que considero que es de suma importancia el que se contemplen los delitos informáticos en el la Ciudad de México.

NOVENA. Finalmente sugiero la adición de un capítulo expreso en el Código Penal para el Distrito Federal intitulado ***"DE LOS DELITOS INFORMÁTICOS"*** en el que se describa las conductas antijurídicas: de accesar sin autorización a equipos de cómputo, interceptación de comunicaciones en internet, suplantación de identidad en redes sociales y en servicios de mensajería, uso indebido de datos personales en redes sociales, daño en el honor y dignidad de las personas en redes sociales.

ANEXOS

Cuadro Comparativo Legislaciones América Latina respecto a los delitos informáticos.

País	Legislación	Características Generales
Argentina	Código Penal, Ley 26.388 (2008), Ley 25.326 (2000)	A partir de Junio de 2008, la Ley 26.388 conocida como la "ley de delitos informáticos" ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388.
Bolivia	Código Penal, Ley 1.768 (1997), Ley 3325 (2006)	La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". Dentro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos.
Brasil	Ley 12.737 (2012), Ley 11.829 (2008)	La Ley 12.737 es una ley reciente (año 2012), en la cuál se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet.
Chile	Ley 19.223 (1993), Ley 20.009 (2005), Ley 18.168 (2002)	La Ley 19.223 es una ley "Relativa a Delitos Informáticos" de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos. La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.
Colombia	Ley 1.273 (2009), Ley 1366 (2009)	La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cuál regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general "si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos".
Costa Rica	Ley 9.048 (2012)	La Ley 9048 es una modificación importante del Código Penal de este país. Inicialmente reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley Nº 4573. Por otro lado adiciona el inciso 6) al artículo 229 y un artículo 229 ter. Finalmente modifica la sección VIII del título VII del Código Penal, titulándolo "Delitos informáticos y conexos", donde regula desde el art. 230 hasta el art. 236. En esta modificación bastante integral, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231).

Fuentes de Consulta:

Bibliografía

CASTELLANOS Tena, Fernando. Lineamientos elementales de Derecho Penal. Porrúa, México 1984

CAMPOLI, Gabriel Andrés. Derecho penal informático en México. INACIPE, 2004.

PRIETO Espinosa, Alberto, et al, Introducción a la informática. Mc Graw Hill. Tercera Edición. Madrid 2002

Diccionario de Informática e Internet, Microsoft. Mc Graw Hill, segunda edición España 2005.

FIX FIERRO, Héctor. Informática y Documentación jurídica. S.f., México, Tesis (Licenciado en Derecho), Universidad Nacional Autónoma de México.

LOSANO, Mario. Curso de Informática Jurídica. Madrid, Tecnos. 1987

NINO, Carlos Santiago. Consideraciones sobre la dogmática jurídica (Con referencia particular a la dogmática penal). UNAM, Instituto de Investigaciones Jurídicas. México, 1989.

PAVÓN Vasconcelos, Francisco. Derecho Penal Mexicano, Décima edición, S.A., Porrúa, México, 1991

PORTE PETIT, Celestino. Apuntamientos de la Parte General de Derecho Penal. Porrúa, Sexta edición.

Secretaría de Programación y Presupuesto, La Informática y el Derecho, INEGI, México 1983.

TIZNADO Santana, Marco Antonio. Informática, Mc Graw-Hill, 2da. Edición, México

TIZNADO Santana, Marco Antonio. Generalidades de la Informática e Internet, Colombia, Mc Graw Hill, 2004

ZAFARRONI, Eugenio Raúl. Tratado de Derecho Penal –Parte General- Tomo III. Editorial Cárdenas. Editor y Distribuidor, Primera Reimpresión. México 1991.

Sitios de Internet

http://delitosinformaticos.info/delitos_informaticos/definicion.html

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

http://www.mailxmail.com/curso-componentes-pc-s/diferentes-dispositivos-almacenamiento

http://www.ecured.cu/index.php/Derecho_inform%C3%A1tico

http://www.palermo.edu/ingenieria/downloads/pdfwebc&T8/8CyT05.pdf

https://docs.google.com/document/d/17SpYB0L0IuCkHacZpmIh325v2FEMv0JlDejhym1B4bE/edit

http://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

http://www.segobver.gob.mx/sispdf/directorios/Directorio_SEGOB.pdf

http://www.usc.es/export/sites/default/gl/institutos/criminoloxia/descargas/Los_Delitos_Informxticos.pdf

http://www.cinu.mx/onu/onu/

http://www.un.org/es/ruleoflaw/

http://www.un.org/es/conf/crimecongress2010/

http://www.eluniversal.com.mx/cultura/69843.html