UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

ANÁLISIS JURÍDICO DE LOS DELITOS INFORMÁTICOS ESTABLECIDOS EN EL CÓDIGO PENAL FEDERAL

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

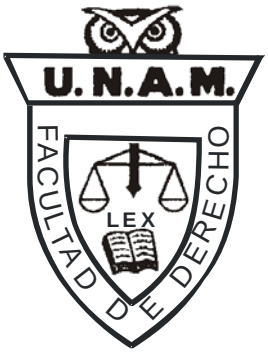
LICENCIADO EN DERECHO

P R E S E N T A:

SAÚL MARTÍNEZ CADENAS

ASESOR:

MTRO. ISRAEL TRUJILLO MÁRQUEZ



MÉXICO, D. F. **2010**

A mis padres,

A mis hermanos,

A mi hija Karen.

ÍNDICE

ANÁLISIS JURÍDICO DE LOS DELITOS INFORMÁTICOS ESTABLECIDOS EN EL CÓDIGO PENAL FEDERAL

CAPÍTULO PRIMERO

Conceptos generales para la comprensión del derecho informático

CAPÍTULO SEGUNDO

Nociones básicas del derecho informático y del delito informático

CAPÍTULO TERCERO

Bases jurídicas para la regulación del delito informático

CAPÍTULO CUARTO

Análisis jurídico de los delitos informáticos establecidos en el Código Penal Federal

INTRODUCCIÓN

El desarrollo de las tecnologías de la información y de las comunicaciones ha sido desenfrenado en los últimos 50 años, tanto que permitió gestar en la actualidad una sociedad de la información en donde todo el mundo vive una conectividad total y el intercambio de información es constante.

De igual manera, los avances de la cibernética e informática permitieron el desarrollo ininterrumpido de las computadoras y provocaron el nacimiento y despliegue mundial de las redes informáticas.

Todo esto se ha traducido en un avance para la humanidad, ya que los beneficios que acarrean los medios informáticos son bastantes y en la actualidad la infraestructura de un Estado se sostiene con estos medios e incluso todos los servicios que prestan los sistemas bursátil, financiero, bancario, comercial, etcétera, se apoyan con las computadoras y las redes informáticas.

Ahora bien, con el devenir de estas tecnologías han surgido nuevos comportamientos y nuevas relaciones que no deben escapar al mundo del derecho, so pena de quedar imposibilitado para resolver la problemática que se presente.

Muchos son los temas que surgen con estas nuevas tecnologías y que deben ser regulados por el derecho, entre los que destacan: el comercio electrónico, la firma digital, el teletrabajo, la protección de datos personales, el valor probatorio de los medios informáticos, los derechos de autor de los programas de cómputo, lo delitos informáticos, etcétera.

Es necesario que estos avances tecnológicos queden regulados, para que el Estado controle jurídicamente estos sucesos que son de suma importancia para la sociedad.

Las computadoras y las redes informáticas aportan mucho a la humanidad entera y a los juristas, ya que facilitan las comunicaciones, el acceso a la información y han logrado automatizar la vida diaria del hombre e incluso se ha forjado en todo el mundo la idea de la sociedad de la información, como ya lo mencionamos.

Pero dentro de las redes informáticas, Internet, revolucionará las comunicaciones y la información entre los hombres, así como las relaciones entre los mismos, ya que trajo como resultado el surgimiento de nuevos comportamientos, que antes eran desconocidos y que algunos de ellos se tradujeron en conductas antisociales que violentan bienes jurídicos que es necesario salvaguardar para el bienestar de la sociedad.

Por ende, lo que más preocupa a los estudiosos de la sociedad de la información, es el surgimiento y desarrollo de los llamados “delitos informáticos” que son aquellas conductas tipificadas por el legislador que utilizan a la computadora como un objeto o instrumento del delito y que pueden violentar bienes jurídicos.

No olvidemos que el derecho penal surge para proteger aquellos valores que el Estado considera fundamentales para la sociedad, por ende, debemos utilizar el ius puniendi con que cuenta el Estado para tratar de evitar los excesos y aberraciones que se han producido con motivo de los avances tecnológicos en materia de sistemas y redes informáticas, que provocan el surgimiento de conductas antisociales que atentan contra bienes jurídicos que el Estado está obligado a proteger.

En México, todavía la respuesta a esta problemática es limitada porque existen pocas leyes que hacen referencia al fenómeno informático, por ejemplo, el Código de Comercio, el Código Civil Federal, la Ley Federal de Protección al Consumidor, la Ley Federal del Derecho de Autor, el Código Federal de Procedimientos Civiles, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, así como la tipificación de ciertas conductas en los Códigos Penales estatales y en el Federal; pero de la lectura de dichos Códigos Penales podemos deducir que aún faltan muchas conductas antisociales que no fueron tipificadas.

La presente tesis que lleva por título "ANÁLISIS JURÍDICO DE LOS DELITOS INFORMATICOS ESTABLECIDOS EN EL CÓDIGO PENAL FEDERAL" tiene como objeto de estudio precisamente a estos delitos que surgen con el uso de la computadora e Internet, pero se constriñe jurídicamente sólo al análisis de los delitos establecidos en el Código Penal Federal.

Esta tesis se divide estructuralmente en cuatro capítulos, el primero denominado "Conceptos generales para la comprensión del derecho informático", en donde se establece el marco conceptual propio de los temas informáticos y las redes de computación.

En el segundo capítulo intitulado "Nociones básicas del derecho informáticos y del delito informático", se establecen los parámetros doctrinales del derecho informático como rama del derecho que permite la regulación de todos estos temas y del delito informático haciendo alusión a su concepto, clasificación, orígenes y características doctrinales.

En el tercer capítulo denominado "Bases jurídicas para la regulación del delito informático" se debaten los temas jurídicos más álgidos del derecho informático, ya que se hace un estudio sobre la necesidad de regular los medios

informáticos e Internet a la luz de los artículos 6º, 7º y 16º de la Constitución Política de los Estados Unidos Mexicanos.

En el capítulo cuarto intitulado "Análisis jurídico de los delitos informáticos establecidos en el Código Penal Federal" se hace un estudio del título noveno del Código Penal Federal en su libro segundo, en específico en los artículos 211 Bis-1, 211 Bis-2, 211 Bis-3, 211 Bis-4 y 211 Bis-5 del Código Penal Federal, para conocer cuáles son las deficiencias de los delitos informáticos establecidos en dicho Código Penal.

CAPITULO PRIMERO

INFORMÁTICO CONCEPTOS GENERALES PARA LA COMPRENSIÓN DEL DERECHO

1. Las nuevas formas de información y comunicación

Desde sus orígenes, el ser humano cuenta con un conjunto de necesidades básicas, pero también posee otro tipo de requerimientos que se derivan de su calidad social, en este sentido, surgen otra serie de necesidades relacionadas con el conocimiento, la dominación, la comunicación, la negociación y la información.[1]

De esta manera, la información y la comunicación existen desde los orígenes de la propia humanidad como necesidades fundamentales del ser humano y de los grupos sociales donde se desarrolla, pero a medida que avanza la humanidad van surgiendo nuevas formas de información y comunicación, de ahí que en la actualidad se hable de una revolución tecnológica que favorece entre otras cosas el surgimiento de las tecnologías de la información y comunicación. "Las capacidades ínsitas al ser humano para comunicarse ven aumentadas sus posibilidades con los diversos avances técnicos que jalonan la historia del hombre. Estos progresos técnicos generaron en su momento nuevas posibilidades de comunicación."[2]

---

[1] Cfr. Temas Selectos de Derecho Informático. coord. Eduardo Castellanos Hernández, Editorial Secretaría de Gobernación, México, 2006, p. 14.

[2] FERNANDEZ RODRIGUEZ, José Julio. Lo público y lo privado en Internet. Editorial Universidad Nacional Autónoma de México, México, 2004, p. 31.

En esta revolución tecnológica, la computadora y sobre todo los sistemas y redes de información han logrado una conexión total entre todos los países del mundo, de ahí que se afirme que hoy en día trabajamos y vivimos en un mundo de conectividad global, en donde podemos tener conversaciones informales o llevar a cabo transacciones monetarias de muchos millones de dólares, con personas que se encuentran al otro lado del planeta de forma rápida y barata, esto bajo la proliferación de las computadoras personales y la facilidad de acceso a Internet.

"Entre la infinidad de nuevos términos surgidos desde la incorporación de la informática a la vida cotidiana, la palabra Internet por su contenido conceptual ha causado en la mayoría de las personas un sentimiento mágico pues brinda la posibilidad de lograr una comunicación total con otras personas en cualquier parte del mundo. Diversas proyecciones estiman que en diez años, quinientos millones de personas emplearán esta que es una extraordinaria y a la vez polémica herramienta de comunicación humana, producto del desarrollo tecnológico en las áreas de la microelectrónica, la fotónica y en general, en los sistemas de redes de telecomunicación."[3]

Indudablemente que la computadora y las redes informáticas aportan mucho a la humanidad entera, ya que facilitan las comunicaciones, el acceso a la información y han logrado automatizar la vida diaria del hombre e incluso se ha forjado en todo el mundo la idea de una sociedad de la información.

En la Cumbre Mundial sobre la Sociedad de la Información llevada a cabo en Ginebra en el año de 2003 se reconoció que la información y la comunicación son esenciales para el progreso, la iniciativa y el bienestar de los seres humanos, de igual manera, se señaló que las tecnologías de la información y las comunicaciones (TIC) tienen inmensas repercusiones en todos los aspectos de la

[3] BARRIOS GARRIDO, Gabriela (et al) Internet y Derecho en México. Editorial Mc Graw-Hill, México, 1998, p. XVII.

vida, pero también afirmaron que estas tecnologías no deben considerarse como un fin sino como un medio para el desarrollo de la humanidad.

Ahora bien, estas nuevas tecnologías de información y comunicación se desarrollan día a día y seguirán creciendo, con todo lo que ello implica para la humanidad, por ello, Julio Téllez Valdés afirma que en este entorno tecnológico "la sociedad se desarrolla en una nueva forma y sus actores se transforman: el Estado, la relación ciudadano-Estado, las organizaciones, el sistema productivo, comercio y la creación y difusión del conocimiento, entre otros importantes rubros."[4]

1.1. La llamada sociedad de la información

En el mundo contemporáneo la información adquiere un papel fundamental en la vida de los seres humanos e incluso se habla de una revolución de la información en donde las nuevas tecnologías de la información y las comunicaciones juegan un papel primordial al permitir el intercambio de conocimiento e información entre los individuos de todo el mundo de manera fácil y rápida.

"La sociedad se encuentra inmersa en un proceso de cambio global en el que las viejas estructuras han sido transformadas y en el que la información ha adquirido una importancia vital para todos los aspectos de la sociedad, incluido el económico. La Revolución de la información supone un reflejo de los cambios que alteraron la sociedad durante la Revolución industrial del siglo XVIII, pero con la salvedad de que ésta se ha producido en mucho menos tiempo."[5]

Este proceso revolucionario de la información surgió con la llegada de los primeros ordenadores en la década de los cuarentas del siglo pasado, en donde

---

[4] TÉLLEZ VALDÉS, Julio, Derecho Informático, 3ª edición, Editorial Mc Graw Hill, México, 2004, p. 6.
[5] GONZÁLEZ LÓPEZ, Óscar Rodrigo, Internet para la empresa, Editorial Anaya Multimedia, España, 2003, p. 23.

se transformaron procesos ya existentes, al lograr la automatización de los mismos; posteriormente, con el surgimiento y desarrollo de las computadoras y de las redes informáticas se vislumbró una verdadera sociedad de la información en donde el uso masivo de las nuevas tecnologías de la información y de las comunicaciones permitió un intercambio global de la información entre los seres humanos.

Para Héctor Fix Fierro la sociedad de la información es consecuencia de un vasto y complejo proceso de transformación de las sociedades industriales, por lo que dicho concepto pretende indicar la importancia fundamental que tiene la información para la vida social actual, en donde la información se convierte en una materia prima de la acción social.[6]

Por su parte, Gabriel Andrés Cámpoli señala que es inexacto hablar de la sociedad de la información, ya que los nuevos sistemas informáticos se han convertido en una herramienta de control social, por ende, es más viable hablar de una sociedad informatizada o de una sociedad tecnificada.[7]

Coincidimos con el criterio sostenido por Julio Téllez Valdés cuando afirma que la sociedad de la información comprende el uso masivo de las Tecnologías de la Información y Comunicación (TIC) para difundir el conocimiento y los intercambios en una sociedad; pero esta nueva sociedad debe ser totalmente incluyente sin distinciones de ninguna especie, por lo que también debe contribuir a eliminar las desigualdades de la brecha digital, entendida ésta como el desequilibrio en el acceso al uso de las computadoras entre los diversos países, sobre todo entre los países desarrollados y en vías de desarrollo.

---

[6] Cfr. FIX FIERRO, Héctor, Informática y documentación jurídica, Segunda edición, Editorial UNAM, México, 1996, p. 46.

[7] Cfr. CÁMPOLI, Gabriel Andrés, Delitos informáticos en la legislación mexicana, Editorial Instituto Nacional de Ciencias Penales, México, 2005, p. 27.

En diciembre de 2003 se llevó a cabo la primera fase de la Cumbre Mundial sobre la Sociedad de la Información celebrada en Ginebra, en donde los diversos países que participaron acordaron construir una Sociedad de la Información centrada en la persona y orientada al desarrollo, en donde todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.[8]

Es importante mencionar que la visión de la Sociedad de la Información que se tuvo en la Cumbre Mundial de Ginebra tuvo como base el derecho a la libertad de opinión y de expresión, el cual tiene su fundamento en el artículo 19 de la Declaración Universal de Derechos Humanos.

Asimismo, se reconoce que la comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social, por ende, constituye el eje central de la Sociedad de la Información.

Es importante mencionar que en esta Cumbre Mundial sobre la Sociedad de la Información se gestaron ciertos principios fundamentales que rigen el desarrollo de esta nueva sociedad basada en las tecnologías de la información y de las comunicaciones, a saber:

a) Una sociedad de la información para todos, en donde las tecnologías de la información y de las comunicaciones redunden en beneficio de todos.

[8] Cfr. Cumbre Mundial sobre la Sociedad de la Información Ginebra 2003. http://www.itu.int/wsis/index-es.html Consultado el día 25 de marzo de 2007 a las 18:00 horas.

b) La función de los gobiernos y de todas las partes interesadas, debe consistir en la promoción de las TIC para el desarrollo de los pueblos.

c) La infraestructura de la información y las comunicaciones: fundamento básico de una Sociedad de la Información integradora.

d) El acceso a la información y al conocimiento de manera masiva.

e) Fomento de la confianza y seguridad en la utilización de las nuevas tecnologías de la información y de las comunicaciones.

f) Las tecnologías de la información y de las comunicaciones deben traer beneficios en todos los aspectos de la vida.

g) Se debe reconocer en esta Sociedad de la Información la diversidad e identidades culturales, la diversidad lingüística y el contenido local.

h) Se debe reconocer una dimensión ética de la Sociedad de la Información.

En la segunda fase de la Cumbre Mundial sobre la Sociedad de la Información celebrada en Túnez en noviembre de 2005 se reafirmó la voluntad de los pueblos para construir una Sociedad de la Información centrada en la persona y orientada al desarrollo, con arreglo a los objetivos y principios de la Carta de las Naciones Unidas, el derecho internacional y el multilateralismo, respetando plenamente la Declaración Universal de los Derechos Humanos.[9]

1.2. Cibernética e informática

[9] Cfr. Cumbre Mundial sobre la Sociedad de la Información Túnez 2005. http://www.itu.int/wsis/index-es.html Consultado el día 25 de marzo de 2007 a las 20:00 horas.

Antes de entrar al estudio de la computadora, es necesario establecer los conceptos de cibernética e informática para la comprensión de los temas siguientes, ya que son el origen de todos los temas que se analizarán con posterioridad.

El término cibernética proviene del vocablo griego kybernetes que hace alusión al arte de pilotear un navío, aunque Platón la uso para significar el "arte de dirigir a los hombres". Actualmente se entiende que la cibernética es el estudio del control y comunicación en los sistemas complejos: organismos vivos, máquinas y organizaciones.[10]

Por su parte, Julio Téllez Valdés señala que la cibernética es la ciencia de la comunicación y control entre el hombre y la máquina, la cual se puede aplicar a cualquier campo de estudio.

Es importante destacar que esta concepción del término cibernética tuvo su origen en 1948, cuando Norbert Wiener utiliza dicho léxico para hacer alusión a la comunicación y el control del hombre sobre la máquina, en su obra "Cybernetics or control and communication in the animal and machine".

Posteriormente, el mismo Norbert Wiener en 1950 popularizó las implicaciones sociales de la cibernética, al establecer analogías entre los sistemas automáticos y las instituciones humanas en su obra "Cibernética y sociedad."[11]

Estas aseveraciones nos permiten entender porque la cibernética es la base de la relación hombre-máquina y el fundamento para la creación de la computadora y las nuevas tecnologías de la información y de las comunicaciones.

[10] Cfr. Cibernética. http://es.wikipedia.org/wiki/Cibern%C3%A9tica Consultado el 27 de marzo de 2007.
[11] Idem.

Por otra parte, la informática viene a cerrar el círculo hombre-máquina al lograr el tratamiento lógico y automatizado de la información, principalmente a través de la computadora, para que el ser humano pueda tomar decisiones.

El termino informática “es un préstamo léxico del francés informatique derivado de la conjunción de las palabras information y automatique, para dar idea de la automatización de la información que se logra con los sistemas computacionales. Esta palabra se usa sobre todo en España, computación se usa principalmente en América y proviene de cómputo (o cálculo) afín al término Computer Science utilizado en el mundo anglosajón.”[12]

Para Héctor Fix Fierro la informática es la ciencia del tratamiento automático o automatizado de la información, a través de las computadoras como medio principal, pero es enfático al establecer las diferencias entre cibernética e informática, ya que la primera se centra en los fenómenos de control y comunicación, mientras que la segunda se centra en el tratamiento de la información.

En la actualidad la informática incluye un amplio campo de acción que tiene que ver con los fundamentos teóricos de las computadoras, su diseño, el uso y la programación de las mismas, de ahí la importancia que tiene para nuestro estudio, ya que es la base para el entendimiento de los temas posteriores, ya que los delitos informáticos tiene como objeto material o instrumento a las computadoras

1.3. La computadora

No cabe duda que en la actualidad las computadoras son una herramienta fundamental para el desarrollo de los pueblos e incluso podemos afirmar que esta

[12] Informática. http://es.wikipedia.org/wiki/Portal:Inform%C3%A1tica Consultado el 29 de marzo de 2007, a las 19:00 horas.

máquina es una necesidad básica del hombre que le permite desarrollarse en todos los aspectos de su vida.

El término computadora "proviene del vocablo latino "computare" que significa calcular, aunque también es denominada como ordenador o computador."[13]

En la literatura hay un gran número de definiciones sobre la computadora, pero en términos generales coinciden en establecer que es una máquina electrónica diseñada para la manipulación y procesamiento de datos, capaz de desarrollar complejas operaciones a gran velocidad.[14]

Esta máquina se puede utilizar en cualquier campo de la actividad humana, ya que es de propósito general, por ejemplo, en las finanzas, la investigación, edición de imágenes, edición de textos, cálculos matemáticos, administración de pequeñas y grandes bases de datos, etcétera.

La computadora tiene tres características fundamentales: "1) Capacidad de almacenar instrucciones e información; 2) Gran rapidez y exactitud en la ejecución de instrucciones y cálculos; 3) Programabilidad (capacidad de comparar letras o números y decidir una acción)."[15]

A este respecto, debemos mencionar que es relevante la gran rapidez y exactitud en la ejecución de instrucciones y cálculos, ya que el tiempo que ocupa una computadora para que ejecute una operación varía en microsegundos, por ende, estas máquinas pueden realizar varias operaciones en unos segundos y

---

[13] Computadora. http://es.wikipedia.org/wiki/computadora Consultado el 3 de abril de 2007 a las 21:00 horas.

[14] Cfr. CHAVEZ TORRES, Anivar. http://www.monografias.com/trabajos11/curinfa/curinfa.shtml Consultado el 4 de abril de 2007 a las 18:00 horas.

[15] HERNÁNDEZ, Ricardo y Luz María DEL POZO. Informática en Derecho. Editorial Trillas, México, 1992, p. 134.

trabajar por horas o días de manera ininterrumpida, sin cometer errores, salvo que tenga en su sistema virus informáticos.

Por otra parte, la capacidad de comparar letras o números y decidir una acción es lo que marca la diferencia entre las computadoras y una simple calculadora, ya que un programa le permite a la computadora realizar determinadas acciones ordenadas por un usuario.

Como podemos observar, por muy compleja que sea la computadora, no deja de ser una máquina que realiza diversas funciones programadas, las cuales son ordenadas por un usuario.

1.3.1. Breve referencia histórica de las computadoras

Se ha dicho que la computadora es una colección de circuitos integrados y otros componentes relacionados que puede ejecutar con exactitud y rapidez acciones ordenadas por el usuario, pero si nos remontamos a la época antigua, podremos darnos cuenta que el hombre tuvo la necesidad de contar los objetos que poseía, por ende, comenzó a utilizar los medios que tenía a su alcance. Como podemos observar una necesidad del hombre es lo que va a dar origen a las computadoras, ya que éstas entre otras cosas procesan datos y realizan un gran número de operaciones programadas y eso es lo que necesitaba el hombre.

"La computadora es un invento reciente, que no ha cumplido ni los cien años de existencia desde su primera generación. Sin embargo es un invento que ha venido a revolucionar tecnológicamente. Actualmente su evolución es continua, debido a que existen empresas en el campo de la tecnología que se encargan de presentarnos nuevas propuestas en un corto tiempo."[16]

[16] Historia computadora. http://www.maestrosdelweb.com/editorial/compuhis/ Consultado el 6 de abril de 2007 a las 19:00 horas.

Para conocer esta pequeña evolución de las computadoras es menester remontarnos a sus antecedentes más alejados y posteriormente seguir con la secuencia histórica hasta llegar a las generaciones de computadoras (criterio que utilizan los científicos informáticos para dividir a las computadoras).

Se ha dicho que el origen de las máquinas de calcular se presenta con el ábaco chino, que era una tablilla dividida en columnas que permitía realizar operaciones de adicción y sustracción, posteriormente, dicho instrumento fue utilizado y perfeccionado por los griegos y los romanos.

Será hasta el siglo XVII cuando el francés Blas Pascal realizará una máquina calculadora, pero con la limitante de hacer sólo sumas y restas, sin embargo, este dispositivo servirá para que el alemán Leibnitz desarrolle una máquina que realice operaciones de adicción, sustracción, multiplicación y división.

En el siglo XIX el inglés Charles Babbage construyó la máquina denominada “máquina analítica” la cual podía realizar cualquier operación matemática, además disponía de una memoria que podía almacenar 1000 números de 50 cifras, pero dicho invento estaba aún muy limitado.[17]

Pasarían más de cien años para que la humanidad viviera el gran desarrollo de las computadoras, después de la segunda guerra mundial.

En 1944 se construyó en la Universidad de Harvard la “MARK I”, la cual fue diseñada por un equipo que estaba encabezado por Howard H. Aiken, no obstante, dicha máquina no fue considerada como una computadora electrónica ya que no era de propósito general y su funcionamiento estaba basado en dispositivos electromecánicos llamados relevadores; posteriormente en 1947 en la

[17] Cfr. Breve historia de la informática. http://www.monografias.com/trabajos10/recped/recped.shtml Consultado el 6 de abril de 2007 a las 21:00 horas.

Universidad de Pennsylvania se construyó una máquina denominada “ENIAC”, la cual fue la primera computadora electrónica construida por un equipo dirigido por John Mauchly y John Eckert; dicha máquina ocupaba todo un sótano en la universidad y tenía 18000 tubos de vacío, consumía 200 kw de energía eléctrica y requería todo un sistema de aire acondicionado, pero tenía la capacidad de realizar 5000 operaciones aritméticas por segundo.[18]

Este nuevo proyecto fue apoyado por el Departamento de Defensa de los Estados Unidos, el cual tuvo como nuevo integrante al ingeniero Von Neumann, cuya idea fundamental fue permitir que en la memoria coexistieran datos con instrucciones, para que la computadora pueda ser programada en un lenguaje y no por medio de alambres, de esta idea va a surgir la computadora denominada “EDVAC” que tenía 4000 bulbos y usaba una memoria basada en tubos de mercurio.

A partir de este momento y hasta nuestros días, los científicos de las computadoras han dividido la historia de la computadora en generaciones, las cuales vamos a señalar a continuación:

a) Primera generación.- esta generación cubrió la década de los cincuentas y las máquinas generadas durante este periodo estaban construidas por medio de tubos de vacío y eran programadas en lenguaje de máquina, no obstante, estas máquinas eran grandes y costosas.

Dentro de esta generación aparece la computadora “UNIVAC”, que fue la primera computadora comercial; después IBM desarrolló la “IBM 701”; siendo la “IBM 650” la computadora más exitosa ya que usaba un esquema de memoria secundaria llamado tambor magnético, que es el antecesor de los discos actuales.

[18] Cfr. Historia de la computación. http://www.monografias.com/trabajos/histocomp/histocomp.shtml Consultado el 6 de abril de 2007 a las 22:00 horas.

b) Segunda generación.- esta generación cubrió la década de los sesentas y las computadoras estaban construidas con circuitos de transistores, además, se empiezan a definir las formas de comunicación entre el usuario y la máquina, las cuales reciben el nombre de programación de sistemas.[19]

En esta generación las computadoras reducen su tamaño y el costo, además, empiezan a surgir los primeros programas de aplicación como el Word Star y la hoja de cálculo. Dentro de los modelos más importantes en este periodo tenemos a la "Philco 212", la "UNIVAC M460" y la "IBM 7090".

c) Tercera generación.- "La aparición del IBM 360 marca el comienzo de la tercera generación. Las placas de circuito impreso con múltiples componentes pasan a ser reemplazadas por los circuitos integrados."[20]

Además el manejo de dichas computadoras es por medio de los lenguajes de control de los sistemas operativos.

d) Cuarta generación.- en esta generación aparecen los microprocesadores que son circuitos integrados de alta densidad con gran velocidad. Las computadoras basadas en los microprocesadores son pequeñas y baratas, además, de que su venta masiva coadyuva al amplio desarrollo de las computadoras personales.

Por otra parte, el software y los sistemas que se manejan con la computadora han tenido un considerable avance porque han hecho más interactiva la comunicación con el usuario.

e) Quinta generación.- "En vista de la acelerada marcha de la microelectrónica, la sociedad industrial se ha dado a la tarea de poner también a

---

[19] Idem.
[20] Historia de la computación. http://es.wikipedia.org/wiki/Historia_de_la_computaci%C3%B3n Consultado el 8 de abril de 2007 a las 21:00 horas.

esa altura el desarrollo del software y los sistemas con que se manejan las computadoras.[21]

En esta etapa destacan los circuitos de gran velocidad, en donde el lenguaje hombre-máquina es más cotidiano y no tan especializado, además de que surgen los sistemas de inteligencia artificial.

En la actualidad, vivimos todavía en la quinta generación de las computadoras, en donde los avances en software son los que marcan el desarrollo generacional de las computadoras en el mundo.

1.3.2. Elementos de la computadora

Una computadora para cumplir sus funciones está formada por un conjunto de equipos, dispositivos y periféricos utilizados como infraestructura para el procesamiento y almacenamiento de información.

"Aunque las tecnologías empleadas en las computadoras digitales han cambiado mucho desde que aparecieron los primeros modelos en los años 40, la mayoría todavía utiliza la arquitectura Eckert-Mauchly, publicada a principios de los años 1940 por John Von Neumann pero que fue creada por John Presper Eckert y John William Mauchly."[22]

Históricamente dentro de esta arquitectura podemos encontrar 4 elementos fundamentales: la unidad central de proceso, la memoria, los dispositivos de entrada y de salida.

---

[21] Historia de la computación. http://www.monografias.com/trabajos/histocomp/histocomp.shtml Consultado el 8 de abril de 2007 a las 21:00 horas.

[22] Arquitectura (elementos básicos de una computadora) http://es.wikipedia.org/wiki/computadora Consultado el 11 de abril de 2007 a las 19:00 horas.

La unidad central de proceso (CPU) es el verdadero cerebro de la máquina, ya que se encarga de recibir los datos de las unidades de entrada, para procesarlos y posteriormente enviar los resultados a las unidades de salida. Para cumplir esta función el procesador cuenta con dos partes: la unidad control y la unidad lógica-aritmética (ALU). [23]

La unidad de control se encarga de identificar y ejecutar las distintas instrucciones codificadas en los programas, utilizando para ello el resto de los elementos del equipo.

La unidad lógica-aritmética se limita a realizar cálculos aritméticos y operaciones lógicas.

La memoria es una secuela de celdas de almacenamiento numeradas, donde cada una es un bit o unidad de información. En este dispositivo se almacenan tanto la información como las instrucciones que constituyen los distintos programas que se van a ejecutar. En una computadora podemos identificar dos tipos de memoria: la memoria interna o principal y la memoria externa o de almacenamiento secundario.

“En la memoria interna residen los datos que están siendo procesados en un determinado momento, así como el código de los programas que se encuentran en ejecución. Esta memoria interna se divide en memoria ROM (que no puede ser modificada –memoria de solo lectura- y que conserva su contenido de forma permanente, incluso en ausencia del suministro eléctrico) y memoria RAM (sobre la que se puede realizar operaciones de lectura y de escritura y que depende de la existencia de suministro eléctrico para su funcionamiento, ya que se trata de una memoria volátil. La memoria externa o de almacenamiento secundario tiene una mayor capacidad y se utiliza para guardar la información que

[23] Cfr. GÓMEZ VIEITES, Álvaro y Manuel, VELOSO ESPIÑEIRA. Redes de computadoras e Internet. Editorial Alfaomega-Rama, México, 2003, p. 39.

se quiere conservar de forma permanente en el sistema. La constituyen los discos duros, los discos flexibles, cintas magnéticas, CD-ROMs, etc."[24]

Los dispositivos de entrada son los elementos que sirven a la computadora para obtener información del mundo exterior. Entre los dispositivos de entrada más comunes tenemos: el teclado, el ratón, los scanners y los lectores de códigos de barras.

Los dispositivos de salida permiten comunicar los resultados del procesamiento al mundo exterior. Los dispositivos más comunes son: los monitores, las impresoras, plotters, tarjetas de sonido y altavoces.

Ahora bien, estructuralmente la computadora se compone de dos partes principales: el hardware y el software.

El hardware es el aspecto físico de la computadora y está conformado por todos los elementos materiales que la integran. El software se integra por todos los programas que permiten el funcionamiento de la computadora.[25]

1.4. Las redes informáticas

A medida que surgen las computadoras personales y que se van perfeccionando con el avance de la tecnología, nace la necesidad de conexión entre las computadoras para el uso y manejo de datos entre ellas, de ahí se plantea la idea de una interconexión de ordenadores para el aprovechamiento de los recursos.

Algunos autores han conceptualizado a la red de computadoras, señalando que: "es un conjunto de ordenadores conectados entre sí (a través de teléfono,

[24] Ibídem, p. 40.
[25] Cfr. Informática. http://www.monografias.com/trabajos11/curinfa/curinfa.shtml Consultado el 11 de abril de 2007 a las 18:00 horas.

microondas, satélites, etcétera) que emplean un mismo lenguaje o protocolo. Un protocolo es una descripción formal de formatos de mensaje y de reglas que los ordenadores deben seguir para intercambiar dichos mensajes.”.[26]

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de computadoras o dispositivos conectados entre sí, para compartir información, recursos y servicios.[27]

Cuando se comparte información, recursos y servicios a través de una red informática se optimiza el desarrollo de una empresa, de un giro comercial, de una oficina pública o privada y de cualquier área en donde funcione un conglomerado de equipos informáticos, por ende, podemos afirmar que son muchas las ventajas que nos brindan las redes informáticas, entre las que destacan las siguientes:

a) Mayor facilidad en la comunicación entre usuarios.

b) Reducción en el presupuesto para software y hardware.

c) Posibilidad de organizar grupos de trabajo.

d) Mejoras en la administración de los equipos y programas y en la integridad de los datos.

e) Mayor seguridad para acceder a la información.[28]

Sin entrar a mayores cuestiones técnicas, ya que no es materia de la presente tesis, se puede señalar que una red tiene tres niveles de componentes,

---

[26] GONZÁLEZ LÓPEZ, Oscar Rodrigo, Ob. Cit., p. 30.
[27] Cfr. Red de computadoras. http://es.wikipedia.org/wiki/Red_de_computadoras Consultado el 12 de abril de 2007, a las 19:00 horas.
[28] Cfr. http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/redes.htm Consultado el 12 de abril de 2007 a las 22:00 horas.

sin los cuales no puede funcionar: a) software de aplicaciones, b) software de red y c) hardware de red.

El software de aplicaciones está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información y recursos; por su parte, el software de red consiste en programas informáticos que establecen protocolos o normas para que las computadoras se comuniquen entre si; por lo que respecta al hardware de red está formado por los componentes materiales que unen las computadoras.

Es importante señalar, que dos componentes fundamentales en las redes informáticas son los medios de transmisión que transportan las señales de los ordenadores (cable estándar, fibra óptica o infrarrojos y radiofrecuencias) y el adaptador de red, que permite acceder al medio que conecta a las computadoras, así como recibe paquetes desde el software de red y transmite instrucciones y peticiones a otras computadoras.[29]

Otro de los puntos que no debemos olvidar cuando hablamos de redes, es la gestión de la red y la administración del sistema, ya que es una parte crucial para que esta conexión de computadoras pueda funcionar adecuadamente; de esta manera tenemos que el gestor de la red es una persona o el equipo responsable de configurar la red para que opere de forma eficiente y el administrador del sistema es la persona o el equipo responsable de configurar las computadoras y el software para emplear la red.

Ahora bien, no debemos olvidar que las redes pueden ser objeto de un acceso ilegal, como siempre ha sucedido desde que se crearon las redes informáticas, por ende, es importante que una conexión de computadoras cuente

[29] Cfr. Redes informáticas. http://es.encarta.msn.com/encyclopedia_761567995_2/Red_(informática).html Consultado el 15 de abril de 2007 a las 21:00 horas.

con las medidas de seguridad necesarias para evitar estos accesos ilícitos, los cuales serán objeto de estudio de los temas siguientes.

1.4.1. Clasificación de las redes informáticas

En el mundo de la informática existen un gran número de criterios para clasificar a las redes informáticas; en el presente rubro haremos mención de algunos de estos criterios.

Por su posibilidad de acceso, las redes suelen dividirse en redes públicas y redes privadas. Una red pública es aquella que puede usar cualquier persona, ya que no requiere claves de acceso personal, y una red privada será aquella red que solo pueden usar ciertas personas que cuentan con su clave de acceso personal.

Por el ámbito de cobertura o espacio geográfico que ocupan pueden ser redes locales, red de área del campus, red de área metropolitana y red de área amplia.[30]

Las redes locales, también llamadas LAN, se limitan a un área relativamente pequeña, tal como un cuarto, un edificio, una nave o un avión.[31]

La red de área del campus (CAN) permite la conexión de dos o más redes locales y pueden estar conectadas en un área geográfica específica, como los campus universitarios, un complejo industrial o una base militar.

La red de área metropolitana (MAN) permite la conexión de redes locales juntas, pero no extiende su área fuera de los límites de la ciudad o del área metropolitana.

---

[30] Cfr. Red de computadoras. http://es.wikipedia.org/wiki/Red_de_computadoras Consultado el 12 de abril de 2007, a las 22:00 horas.
[31] Cfr. GONZÁLEZ LÓPEZ, Oscar Rodrigo, Ob. Cit., p. 31.

Por último, la red de área amplia (WAN) es una red de comunicaciones de datos que cubre un área geográfica muy amplia, incluso internacional y para ello, puede utilizar las instalaciones de transmisión proporcionadas por los portadores comunes, como las compañías de teléfono.

1.4.2. Evolución histórica de las redes informáticas

El nacimiento y evolución de las redes informáticas es reciente y han llegado a su punto más alto con la instauración de Internet la llamada "red de redes"; pero esta gran red de computadoras fue consecuencia de las aportaciones que hicieron científicos, ingenieros e investigadores.

En 1960 Joseph Carl Robnett Licklider escribió un artículo llamado "Simbiosis hombre-computadora" en el cual prevé la posibilidad de formar una red multiusuario denominada "centro pensante" en un plazo no mayor a 15 años, por ende, es considerado uno de los pioneros en las redes informáticas, ya que fragua el surgimiento de una red global que permita interconectar diversos ordenadores.[32]

"Solo unos meses más tarde, Licklider se convirtió en la cabeza del programa de investigación de computación de la Agencia de Investigación Avanzada de Proyectos del Departamento de Defensa de los Estados Unidos (Advanced Research Project Agency: ARPA) institución que fundó y lanzó el desarrollo de Internet."[33]

Después de años de trabajo, dicha agencia de investigación avanzada logró desarrollar "ARPANET", una red que unía redes de cómputo del ejército y de laboratorios universitarios que hacían investigaciones militares.

---

[32] Cfr. Historia de Internet. http://es.wikipedia.org/wiki/Historia_de_Internet Consultado el 20 de abril de 2007 a las 19:00 horas.
[33] PARDINI, Anibal A. Derecho de Internet Editorial La Roca, Buenos Aires, 2002, p. 42.

"En la década de los sesenta nació el proyecto que gestó Internet en sus primeros pasos: el programa de investigación DARPA (Defense Advanced Research Projects Agency) a resultas del cual, se crea la Red ARPANET que conectaba las redes de ordenadores de su propietarios, fundamentalmente del ejército, las empresas de la industria militar y laboratorios de universidades. Esta red fue creciendo hasta conectar a unos 100 ordenadores a principios de los ochenta, pero siempre con un carácter cerrado, circunscrito a la comunidad científica y militar."[34]

Durante la década de los setentas del siglo pasado, se crearon redes cooperativas descentralizadas, como UUCP, una red de comunicación mundial basada en UNIX y USENET, la cual daba servicio a la comunidad universitaria y posteriormente a diversas organizaciones comerciales.

"En 1980, las redes más coordinadas, como CSNET (red de ciencias de cómputo) y BITNET empezaron a proporcionar redes de alcance nacional a las comunidades académicas y de investigación, las cuales hicieron conexiones especiales que permitieron intercambiar información entre las diferentes comunidades. En 1986 se creó la NSFNET (red de la Fundación Nacional de Ciencias) la cual unió en cinco macro centros de cómputo a investigadores de diferentes estados de Estados Unidos. De este modo la NSFNET se expandió con gran rapidez, conectando redes académicas a más centros de investigación, remplazando así a ARPANET en el trabajo de redes de investigación. ARPANET se da de baja en marzo de 1990 y CSNET deja de existir en 1991, cediendo su lugar a Internet."[35]

De esta manera, surge Internet, una red mundial cuyo objetivo fue crear una serie descentralizada y autónoma de uniones de redes de cómputo, con la

[34] SANCHEZ ALMEIDA, Carlos y Javier A. MAESTRE RODRÍGUEZ. La Ley de Internet. Editorial SERVIDOC S.L., España, 2002, p. 29.
[35] BARRIOS GARRIDO, Gabriela, (et al) Ob. Cit., p. 9.

capacidad de trasmitir información sin necesidad de contar con un control humano y disponible para todas las personas.

México fue el primer país latinoamericano en conectarse a Internet, lo cual hizo en 1989, a través de los medios de interconexión de Teléfonos de México, pero en sus inicios dicha red se utilizó para fines académicos en diversas entidades educativas como el Instituto Tecnológico de Estudios Superiores de Monterrey, el Instituto Politécnico Nacional, la Universidad Nacional Autónoma de México, la Universidad de Guadalajara y la Universidad de las Américas; posteriormente, se empezó a utilizar para fines comerciales y es cuando realmente se masifica su utilización.[36]

1.4.3. Generalidades sobre Internet

En la actualidad, Internet se erige como un medio de información y comunicación masivo, de la llamada sociedad de la información, que experimenta grandes y rápidos avances desde su creación, sin embargo, estos avances también traen consigo nuevos comportamientos en la sociedad en sus diversos aspectos sociales, económicos y culturales que se deben regular, ya que algunos de estos comportamientos que se despliegan en el ciberespacio se tornan antisociales y contrarios a las normas jurídicas.

“Internet es en la actualidad una utilidad empleada de forma cotidiana por cientos de millones de personas. Es un sistema de comunicación que, desde sus inicios relativamente cercanos en el tiempo, ha experimentado una evolución extraordinaria que ha ido derivando en una modificación de las costumbres comunicativas y culturales de una amplia parte de la sociedad. Herramientas como el correo electrónico o la mensajería instantánea sirven en muchas

[36] Cfr. Ibídem, pp. 17-20.

ocasiones como alternativas aventajadas del correo postal o las llamadas telefónicas tradicionales."[37]

Como podemos observar, Internet, se erige como la red de redes, ya que es la más importante en extensión y número de usuarios en el mundo, además de que es una red pública a la cual todos podemos acceder.

Por otro lado, es acertado el comentario que hacen Carlos Sánchez Almeida y Javier Maestre Rodríguez en el sentido de que el término Internet es el más aceptado por las comunidades informáticas, ya que esta red de redes tiene una conexión universal, toda vez, que conecta entre sí una infinidad de redes que existen en el mundo, de forma que los ordenadores cambian información de manera continua y rápida; no obstante, se pueden encontrar otras denominaciones para hacer referencia a esta red universal, tales como: autopista de la información, ciberespacio, etcétera.[38]

Ahora bien, el término Internet surge de la contracción de inter-network que significa entre redes.

Oscar Rodrigo González López afirma que no es viable establecer una definición de Internet, ya que cuenta con muchas dimensiones entre las que destacan las siguientes:

a) Es un conjunto de máquinas conectadas entre sí, posee una jerarquía de tres niveles formados por redes de eje central (backbones) redes de nivel intermedio y redes aisladas (stub networks).

b) Es un conjunto de recursos y herramientas a los que se tiene acceso.

---

[37] Historia de Internet. http://es.wikipedia.org/wiki/Historia_de_Internet Consultado el 20 de abril de 2007 a las 19:00 horas.
[38] Cfr. SÁNCHEZ ALMEIDA, Carlos y Javier A., MAESTRE RODRIGUEZ, Ob. Cit., p. 24.

c) Puede entenderse como una comunidad de personas y organizaciones que se sirven de ella para realizar todo un conglomerado de actividades.[39]

Es importante mencionar que la Federal Networking Council (FNC) de los Estados Unidos definió en 1995 a Internet señalando que es un sistema global de información que está lógicamente unido por un espacio global único de dirección basado en el protocolo de Internet TCP/IP o sus extensiones o continuaciones subsecuentes, además es capaz de soportar comunicaciones usando la serie de protocolos Transmisión Control Protocol/Internet Protocol (TCP/IP) y sus extensiones o continuaciones subsecuentes u otros protocolos IP –compatibles, asimismo, ofrece, usa o hace accesibles pública o privadamente servicios de alto nivel soportados en las comunicaciones e infraestructura mencionada.[40]

Esta definición que nos ofrecen en los Estados Unidos es demasiado especializada para efectos de la presente tesis, por ende, nos concretaremos a entender a Internet como la red más grande del mundo, que pretende conectar a todas las redes existentes.

Esta conexión se puede llevar a cabo a través de un lenguaje o protocolo que nació en 1983 denominado protocolo TCP/IP (Transmission Control Protocol/Internet Protocol.

Por una parte, el protocolo TCP (Transmisión Control Protocol) se encarga de descomponer en el origen la información en paquetes que viajan por la red de forma separada hasta llegar a su destino, donde vuelven a reagruparse; por otra parte, el protocolo IP (Internet Protocol) se encarga de dirigir adecuadamente la información por la red. De esta manera, las computadoras de cualquier red informática pueden estar conectadas y comunicadas para el intercambio de

[39] Cfr. GONZÁLEZ LÓPEZ, Oscar Rodrigo, Ob. Cit., pp. 29-30.
[40] Cfr. FERNANDEZ DELPECH, Horacio. Internet: su problemática jurídica. Editorial Abeledo-Perrot, Argentina, 2001, pp. 12-13.

información; estos protocolos o lenguajes son muy importantes para Internet ya que se engloban a todas las redes del mundo.

Ahora bien, se ha dicho que Internet tiene ciertas características que le permiten distinguirse de otras redes informáticas, primeramente, su carácter global y dinámico, ya que Internet llega a todos los rincones del mundo; su magnitud, ya que Internet tiene un gran número de servidores y usuarios conectados; por último, Internet es una veta inagotable de información disponible para los usuarios.

Como lo hemos visto, Internet se erige como la red mundial que favorece el desarrollo de la sociedad de la información, al convertirse en una tecnología de la información y comunicación de alcance mundial.

1.4.4. Principales servicios que proporciona Internet

Se ha dicho que una de las características de Internet es su capacidad para concebir un gran número de servicios de diferente naturaleza y posibilidades de uso.[41]

Esta red de redes, nos ofrece una gama de servicios, que indudablemente coadyuvan al desarrollo de la comunicación e información en el mundo, pero también son los medios a través de los cuáles se cometen los llamados delitos informáticos, como se verá en los próximos capítulos. Entre los servicios más importantes que nos ofrece Internet tenemos los siguientes:

1) La World Wide Web (WWW) es el servicio más importante que ofrece Internet, ya que es una red articulada en torno a documentos, conocidos como sitios o páginas Web, dichas páginas se encuentran alojadas en un servidor y pueden incluir no sólo documentos de texto, sino también imágenes y sonido.

[41] Cfr. SÁNCHEZ ALMEIDA, Carlos y Javier A., MAESTRE RODRIGUEZ, Ob. Cit., p. 30.

Cabe señalar que una página Web es un documento escrito en un lenguaje especial denominado HTML.

Es importante mencionar que dentro de las páginas encontramos enlaces o links internos, a otros sitios de la propia página o externos a otras páginas, de esta manera, el que accede a una página Web puede ir de un documento a otro contenido en la página o fuera de ella en otra página, dando lugar a lo que se conoce como navegación.[42]

2) El e-mail o correo electrónico es el medio de comunicación más utilizado que nos brinda la red, ya que permite el envío y recepción de mensajes entre los usuarios de Internet en pocos segundos.

Ahora bien, lo más interesante del correo electrónico es que es una forma de comunicación sencilla, rápida y barata, además de que no exige que emisor y receptor coincidan en tiempo y espacio.

3) El sistema Telnet permite la conexión con un ordenador remoto para utilizar los programas que éste dispone desde el primero.

4) El servicio File Transfer Protocol permite la transmisión de archivos entre un ordenador y otro. Para poder hacer uso de este servicio se requiere un nombre de usuario (login) y una contraseña (password) para acceder. Una vez que se produce la conexión, el programa permitirá al usuario navegar en los directorios para obtener el archivo deseado.

5) El servicio Usenet o NetNews es un tablón de anuncios electrónico que incluye temas de debate y distribución de información, a través de este medio,

[42] Cfr. FERNANDEZ DELPECH, Horacio, Ob. Cit., p. 22.

Usenet permite a los usuarios establecer contactos con otras personas con intereses similares.[43]

6) El Internet Relay Chat (IRC) permite mantener conversaciones escritas on line con cualquier otro usuario, para ello, se requiere la instalación de un programa de Chat, pero a diferencia del correo electrónico, en el Chat se requiere que los participantes coincidan en tiempo para que puedan entablar comunicación. Cabe señalar que a través de este sistema se pueden llevar a cabo videoconferencias que es un servicio más de Internet.

7) La tecnología Wap posibilita el acceso a Internet sin la necesidad de un ordenador y un módem, pudiéndose realizar la conexión y el ingreso a la red mediante un teléfono celular móvil. “Esta tecnología permite también el envío y recepción de e-mails a través de ciertos sitios determinados (servicio de wapmail).”[44]

Estos servicios que mencionamos no son los únicos que presta Internet, pero si los más utilizados en el mundo, además, la tecnología avanza todos los días, por ende, irán surgiendo mayores posibilidades para hacer uso de Internet y en estas nuevas posibilidades surgirán otras formas para delinquir.

1.5. Los virus informáticos

Sin duda uno de los grandes problemas que acarrea el uso de la computadora y sobre todo de Internet, son los virus informáticos, ya que genera avatares para todo aquel que tiene una computadora personal y para las empresas representa un golpe devastador por la pérdida de información o daños a los sistemas, además de que tienen que invertir grandes recursos en la

[43] Cfr. GONZALEZ LOPEZ, Oscar Rodrigo, Ob. Cit., p. 49.
[44] FERNANDEZ DELPECH, Horacio, Ob. Cit., p. 26.

localización y eliminación de los virus informáticos que han infectado a sus sistemas.

El virus informático es un fenómeno que surgió con el desarrollo de la computadora y se ha extendido con el surgimiento de Internet, pero lo más grave es que los virus dañinos se convierten en una amenaza real para los sistemas informáticos y para el mundo del derecho penal una nueva forma de conducta antisocial.

"Hay miles de variedades de virus, pueden hacer cualquier cosa, desde que aparezca una ventana diciendo "Hola" hasta borrar todos los contenidos del disco duro de un ordenador. La proliferación de los virus ha llevado a la aparición del fenómeno de los virus de engaño (virus hoax) que no son más que un aviso generalmente distribuida por correo electrónico o sitios Web sobre un virus que no existe o que no hace exactamente lo que dice el aviso. Sin embargo, los virus reales presentan una amenaza real para la red. Empresas como Symantec y McAffe desarrollan software antivirus con el fin de detectar y eliminar estos de los sistemas. Pero como cada día se crean nuevos virus es esencial mantener actualizada la aplicación y descargar frecuentemente los llamados archivos de definición de virus."[45]

Para que podamos entender qué es un virus, debemos fijar algunos de sus elementos más comunes:

a) Es un programa de computadora.

b) Su principal cualidad es la de poder auto replicarse.

c) Intentan ocultar su presencia hasta el momento de la explosión.

---

[45] LITTLEJOHN SHINDER, Debra. Prevención y detección de delitos informáticos. Editorial Anaya Multimedia, España, 2002, p. 411.

d) Producen efectos dañinos en el huésped.[46]

Con estos elementos podremos darnos cuenta porque los virus informáticos tienen gran similitud con los virus biológicos que sufren los seres humanos, y porqué se utilizó la denominación de "virus" a un programa informático que se introduce en una computadora para reproducirse y dañar el equipo que lo aloja.

Hay muchas definiciones sobre lo que es un virus informático, las cuales hacen alusión a los elementos que hemos señalado con antelación, pero veamos algunas de ellas:

"Los virus informáticos son programas diseñados expresamente para interferir en el funcionamiento de una computadora, registrar, dañar o eliminar datos, o bien para propagarse a otras computadoras y por Internet, a menudo con el propósito de hacer más lentas las operaciones y provocar otros problemas en los procesos."[47]

Por su parte, Jesús de Marcelo Rodao sostiene que: "Básicamente un virus sería un programa que posee la capacidad de reproducirse a sí mismo e introducir variantes y copias suyas en otros programas, infectándolos. Luego podrá ser más o menos maligno, reproducirse de una forma u otra y copiarse siguiendo diversas técnicas."[48]

Ahora bien, dependiendo de cada tipo de virus, su forma de atacar el equipo será distinta, pero en términos generales el funcionamiento de un virus informático es simple ya que al ejecutarse un programa que está infectado, el código del virus queda alojado en la memoria RAM de la computadora, aun

---

[46] Cfr. ¿Qué es exactamente un virus? http://www.geocities.com/ogmg.rm/QueSon.html Consultado el 25 de abril de 2007 a las 22:00 horas.
[47] http://www.microsoft.com/latam/ahtome/security/viruses/intro_viruses_what.mspx Consultado el 25 de abril de 2007 a las 23:00 horas.
[48] RODAO, Jesús de Marcelo. Virus de Sistemas Informáticos e Internet. Editorial Alfaomega, México, 2000, p. 13.

cuando el programa que lo contenía haya terminado de ejecutarse, de esta manera el virus toma el control de los servicios básicos del sistema operativo, infectando cualquier archivo que sea ejecutable, por último, el código del virus se añade al programa infectado y se graba en los diversos discos que contiene el equipo, asegurando con ello su reproducción.

Una vez que se ha infectado cualquier equipo informático, el virus está listo para hacer daño y cada virus está diseñado para hacer un tipo distinto de daño en la computadora que lo aloja.

Es importante mencionar que no todos lo virus causan daño, ya que hay algunos cuyo propósito no es dañar sino molestar al usuario; de cualquier forma un virus es un programa que se inserta en un equipo informático sin la voluntad del usuario.

1.5.1. Evolución histórica de los virus informáticos

Uno de los grandes teóricos de la computadora, como lo es Von Neumann también fue precursor de los virus informáticos, ya que con su teoría de la organización de autómatas complejos, que presentó en 1939, se gestó la idea de desarrollar pequeños programas que pudiesen tomar el control de otros programas de similar estructura.

A principios de 1950 en los laboratorios Bell, los programadores Robert Thomas Morris, Douglas Mcllory y Victor Vysottsky crearon un juego denominado “CoreWar” que consistía en introducir en la memoria de un equipo dos computadoras virtuales que lucharan entre ellas para apoderarse de la memoria disponible y bloquear al contrario.[49]

[49] Cfr. Ibídem, p. 4.

Según la literatura, en 1972 Robert Thomas Morris elabora el primer programa dañino denominado “Creeper” que atacaba a la computadora IBM 360, emitiendo una leyenda en la pantalla, para este problema se creó otro programa llamado “Reaper”.[50]

En 1984 el doctor Fred Cohen escribió un libro denominado “Virus informáticos: teoría y experimentos” en donde define a los virus informáticos y señala que son un grave peligro para la seguridad nacional de los Estados Unidos.

En 1986 se dieron a conocer los virus Brain, Bouncing, Ball y Marihuana que fueron los primeros virus de infección masiva, pero sólo se constriñeron a infectar el sector de arranque de los discos.

Uno de los sucesos históricos que ha marcado la evolución de los virus informáticos se presentó el 2 de noviembre de 1988, cuando Robert Tappan Morris ingreso un virus en la red Arpanet logrando infectar a 6000 servidores conectados a la red, partiendo de una computadora del Instituto Tecnológico de Massachussets; más tarde fue descubierto y condenado a cumplir 400 horas de trabajo en favor de la comunidad.

En 1988 aparece en el mercado el antivirus denominado “FLUSHOT” creado por Ross Greenberg, de igual manera, aparece el VIRUSCAN, creado por John McAfee.[51]

En 1995 aparecen los llamados macro virus, que es una nueva familia de virus que no solo infecta documentos, sino que puede auto-copiarse para infectar otros documentos sin ser un archivo ejecutable. En 1997 se diseminó por Internet un macro virus denominado “Laroux” que infectó hojas de cálculo del programa MS-Excel de muchos equipos.

---

[50] Cfr. Historia del virus. http://www.perantivirus.com/sosvirus/general/histovir.html Consultado el 30 de abril de 2007 a las 18:00 horas.
[51] RODAO, Jesús de Marcelo, Ob. Cit., p. 6.

En 1999, se propagaron masivamente en Internet virus adjuntos a mensajes de correo electrónico como el “Melisa” o el macro virus “Melissa”, así como el peligroso “CIH” y el “ExploreZip”. A finales de ese año, surgió el virus “BubbleBoy” primer virus que infecta los sistemas tan solo con leer el mensaje de correo electrónico y se muestra en formato HTML.

A partir del año 2000, los creadores de virus informáticos se han perfeccionado, sobre todo han mejorado sus técnicas para hacer indetectables sus programas malignos.

“Resultará imposible impedir que se sigan desarrollando virus en todo el mundo, por ser esencialmente una expresión cultural de “graffiti cibernético”, así como los crackers jamás se detendrán en su intento de “romper” los sistemas de seguridad de las redes e irrumpir en ellas con diversas intencionalidades. Podemos afirmar que la eterna lucha entre el bien y el mal ahora se ha extendido al ciberespacio.” [52]

1.5.2. Diversos tipos de virus informáticos

En el mundo de las computadoras e Internet existen muchas clases de virus, los cuales han ido cambiando a través del tiempo, ya que se han perfeccionado y seguirán avanzando a medida que los programas de cómputo y equipos informáticos vayan mejorando con la tecnología; por eso, los programas antivirus no proporcionan una protección completa ya que cada día van surgiendo nuevos virus informáticos.

Vamos a señalar una clasificación de virus informáticos y posteriormente haremos una breve semblanza de los virus más conocidos, dependiendo de su estructura y composición.

---

[52] MACHADO LA TORRE, Jorge. http://www.jorgemachado.net/content/view/52/1/ Consultado el 30 de abril de 2007 a las 20:00 horas.

Los virus del sector de arranque o de inicio, son los más hostiles ya que al infectar dicho sector dentro de un disco duro o flexible, se apodera del sistema en formal total e impide que la computadora pueda encender o pueda iniciar sus funciones.

Los virus de aplicaciones o programas, son programas ejecutables que cuando funcionan, infectan al sistema; estos virus también pueden presentarse adjuntos a otros programas denominados inocentes e instalarse al mismo tiempo que éstos.

Los virus de macros son programas que están incluidos en documentos o en programas de hojas de cálculo, los cuales se reproducen cuando se utiliza el documento o la hoja de cálculo. Este tipo de virus son los más recientes y de mayor expansión en el mundo informático.[53]

Entre los tipos más comunes de virus informáticos tenemos a: camaleón, caballo de Troya, gusanos, bomba de tiempo, mockinbird, polimórfico y el hoax.

El camaleón es un virus parecido al Caballo de Troya, ya que crea un programa maligno y lo disfraza como uno legal.

El Caballo de Troya es un programa diseñado para hacer que la computadora realice funciones ajenas a las solicitadas por el usuario, pero se disfraza de manera que no sea reconocido.

El gusano se introduce cuando inicia el sistema operativo de la computadora, ocupando la memoria del equipo, ya que se reproduce un gran número de veces, por lo que satura el sistema.

[53] LITTLEJOHN SHINDER, Debra, Ob. Cit.,p. 410.

La bomba de tiempo implica un virus que se activa cuando acaece una fecha determinada y puede tener una variante con la bomba lógica cuando se activa el virus ante una condición lógica.

Los Mockinbird son virus que se quedan fuera del sistema para esperar a que un usuario autorizado entre, de esta manera copia las claves de acceso para entrar posteriormente al sistema.

El polimórfico es un virus que intenta escapar de los antivirus produciendo mutaciones de sí mismo cuando se copia en el archivo.

El hoax no es un virus propiamente dicho, pero implica un mensaje de amenaza de virus, normalmente falso.

Estos son algunos ejemplos de los virus más conocidos, pero como lo mencionamos con antelación, día a día, van surgiendo nuevos virus informáticos por lo que es imposible hacer una buena sistematización de todos estos programas.

CAPÍTULO SEGUNDO

NOCIONES BÁSICAS DEL DERECHO INFORMÁTICO Y DEL DELITO INFORMÁTICO

2. El derecho y las nuevas tecnologías de la información y comunicación

Como lo mencionamos en el capítulo primero, en esta revolución tecnológica, la computadora, los sistemas y redes informáticas han provocado un enlace total entre todos los países del mundo, de ahí que los seres humanos estemos en un constante intercambio de información y comunicación de manera fácil y rápida.

Las computadoras y las redes informáticas aportan mucho a la humanidad entera, porque coadyuvan al desarrollo de las comunicaciones y la información, logrando automatizar la vida diaria del hombre, por ende, permitieron el nacimiento de una sociedad de la información, como también lo mencionamos en el capítulo anterior.

"La cultura informática representa todo un reto para el Estado y para la sociedad en general, una serie de datos nos permitirán establecer que en el presente siglo se ha creado más riqueza que cualquiera otra época anterior de la que se tenga noticia, con base en la informática y sus aplicaciones en la ciencia y la tecnología."[54]

[54] Temas Selectos de Derecho Informático, Ob. Cit., p. 30.

Ahora bien esta sociedad de la información y esta cultura informática provocan el surgimiento de nuevas formas de comportamiento y nuevas formas de interacción entre los seres humanos. “Sabemos por amargas experiencias, que los medios informáticos alteran, al menos en parte, los esquemas tradicionales de interacción social y ofrecen nuevas formas de relación interpersonal.”[55]

Por otro lado, el derecho es un producto social y para la sociedad, como lo sostiene Manuel Rivera Silva, por tanto, debe entender estas nuevas formas de interacción entre los seres humanos y actualizarse en la medida que estos avances tecnológicos se presenten en el mundo fáctico, para no quedar obsoleto e imposibilitado para resolver la problemática que surge con la utilización de la computadora e Internet.

Por eso es importante que estas nuevas tecnológicas de la información y las comunicaciones queden integradas en el mundo del deber ser, con el fin de que el Estado regule jurídicamente estos sucesos que son de importancia para la sociedad, de ahí que Héctor Fix Fierro sostenga que “donde hay sociedad, hay derecho y donde hay derecho hay personas que se ocupan de crear normas jurídicas, aplicarlas y explicarlas, se trata de funciones con tradición de siglos que en muchos aspectos han cambiado, con raíces tan profundas y sólidas, cabe preguntarse si la computadora y la informática –tecnología advenediza, casi- tienen algo que aportar al jurista aparte del manejo más rápido y eficiente de la información.”[56]

No tenemos duda en afirmar que estas tecnologías de la información y las comunicaciones han aportado mucho a la humanidad entera ya que facilitan las comunicaciones así como el acceso a la información y lograron automatizar la vida diaria del hombre, sin embargo, el uso de estas tecnologías y sobre todo de Internet generaron nuevos comportamientos que pusieron en tela de juicio a los

[55] CÁMPOLI, Gabriel Andrés, Ob. Cit., p. 17.
[56] FIX FIERRO, Héctor, Ob. Cit., p. 23.

actuales sistemas jurídicos, ya que se trastocaron ciertos principios rectores tales como: la libertad de expresión, el derecho a la información, el derecho a la intimidad, el patrimonio, la competencia de los tribunales, etcétera.

Peor aún, el uso de estas tecnologías de la información generaron un gran número de conductas antisociales que violentan bienes jurídicos que debemos salvaguardar, no olvidemos que el derecho penal, como la última ratio del derecho, surge para proteger aquellos bienes jurídicos que la sociedad y el Estado consideran importantes para la vida colectiva.[57]

"El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.[58]

Ahora bien, dichas conductas antisociales nunca fueron consideradas por el legislador, sino que surgieron con el devenir de la tecnología, por ello se ha gestado en el mundo jurídico la idea de un derecho penal informático que se encargue de analizar los delitos, penas y medidas de seguridad relacionados con el uso de las computadoras e Internet.

2.1. Orígenes del derecho informático

En la actualidad, los medios informáticos son una herramienta fundamental y necesaria para todo aquel que pretende practicar y ejercer el derecho de manera eficiente, aunado a que nuevos comportamientos surgen con el desarrollo de la informática que deben ser analizados por los juristas, por ende, debemos

[57] Cfr. GONZALEZ- SALAS CAMPOS, Raúl. La teoría del bien jurídico en el derecho penal. Segunda edición, Editorial Oxford, México, 2001, pp. 67-77.
[58] http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml Consultado 8 de agosto de 2007 a las 18:00 horas.

encontrar los puntos de unión entre el derecho y la informática, para conocer esta nueva rama del derecho denominada derecho informático.

"La informática concierne a todos los sectores de la vida económica y social en forma destacada. Esta expansión hace nacer problemas jurídicos nuevos de carácter general y muy técnicos. Los dominios del derecho se modifican así bajo la influencia de la informática en forma muy numerosa y sólo un trabajo de colaboración puede permitir abordar en su conjunto y al mismo tiempo un modo de actuar práctico y documentado."[59]

Luz María del Pozo y Ricardo Hernández sostienen que al relacionar el derecho con la informática surge la interdisciplina llamada derecho informático, dentro de la cual se desarrollan múltiples áreas relacionadas con el derecho, por ello los estudiosos del derecho deben atender a esta interdisciplina ya que los nuevos juristas, los del futuro inmediato, resolverán con esta técnica los problemas que ya actualmente se plantean.[60]

Por esto, el derecho informático es una nueva rama del derecho que se encuentra en pleno desarrollo, ya que actualmente la informática se relaciona con todas las actividades del ser humano, de donde surgen conductas que deben ser contempladas por el derecho.

Ahora bien, esta nueva rama del derecho tiene orígenes muy recientes "podemos decir que las alusiones más específicas sobre esta interrelación las tenemos a partir del año de 1949 con la obra de Norbert Wiener en cuyo capítulo IV, consagrado al Derecho y las Comunicaciones, expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico. Dicha interrelación se da a través de las comunicaciones, a lo que había

[59] AZPILCUETA, Hermilio Tomás. Derecho Informático. Editorial Abeledo-Perrot, Argentina, p. 33.
[60] Cfr. HERNÁNDEZ, Ricardo y Luz María, DEL POZO, Ob. Cit., p. 125.

que mencionar que si bien estos postulados tienen más de medio siglo, en la actualidad han adquirido matices que ni el mismo Wiener hubiera imaginado."[61]

Por su parte, el juez norteamericano Lee Loevinger mencionará que uno de los pasos más grandes en el progreso del hombre, será la aplicación de las computadoras al derecho, dando origen a la Jurimetría.

El italiano Mario Losano, al hablar propiamente de la informática jurídica, utilizará el término de Iuscibernética, criticando el término jurímetría, ya que no se busca medir el derecho, sino de aplicar la cibernética al campo de la informática jurídica.[62]

Se dice que el término "Derecho Informático" (Rechtinformatik) fue acuñado por el doctor Wilhelm Steinmûller, profesor de la Universidad de Regensburg en Alemania en los años setentas, sin embargo, se han acuñado un gran número de denominaciones, a saber: Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información, Iuscibernética, Derecho Tecnológico, Derecho del Ciberespacio, Derecho de Internet, etcétera.[63]

Por último, es importante mencionar las palabras de Enrique Cáceres, cuando menciona lo difícil que es investigar en estas disciplinas que están en proceso de formación, ya que no hay un cuerpo de doctrina bien definido que sirva de marco de referencia, toda vez, que apenas se están generando los conceptos, métodos y técnicas para la comprensión de dichas disciplinas; aunado a que el investigador debe manejar con fluidez los conceptos del derecho y de la informática, además, en México se presenta un problema mayúsculo ya que no hay muchos especialistas en la materia que inicien al nuevo investigador en estos temas.

---

[61] TÉLLEZ VALDÉZ, Julio, Ob. Cit., p. 17.
[62] Cfr. I Congreso Iberoamericano de Informática Jurídica, Santo Domingo, del 29 de octubre al 2 de noviembre de 1984, Editorial Centro Regional del IBI para la enseñanza del informática, p. 20.
[63] Cfr. Derecho Informático. http://es.wikipedia.org/wiki/Derecho_inform%C3%Altico Consultado el 30 de agosto de 2007 a las 21 horas.

2.1.1. Concepto y clasificación del derecho informático

El derecho informático, como una nueva rama del derecho que está en expansión, tiene ciertas particularidades que es menester mencionar, ya que al tener una relación directa con los medios informáticos, adquiere características especiales distintas al derecho común, como lo sostiene Luz María del Pozo y Ricardo Hernández:

a) Su campo de investigación es internacional, ya que busca consensos aplicables y es respetuoso de leyes nacionales.

b) Su herramienta principal es el estudio del derecho comparado.

c) Sus fuentes de información, generalmente no pueden ser los libros, porque su investigación se realiza antes de que éstos sean publicados, por ende, las fuentes de información son las revistas especializadas o los documentos y memorias de los Congresos nacionales e internacionales.

d) La información está en diversos idiomas, distintos al español.

e) Lo que busca el derecho informático es el diseño y justificación de estructuras nuevas o bien corregir las ya existentes sobre los principios de la Constitución del país de que se trate.

f) Sus fines serán siempre de orden público y de interés social.[64]

g) El uso y la utilización de los medios informáticos son el objeto y/o el medio de regulación.

[64] Cfr. HERNÁNDEZ, Ricardo y Luz María, DEL POZO, Ob. Cit., p. 128.

h) Es un derecho altamente tecnificado y especializado, con un lenguaje propio de los medios informáticos.

"El derecho informático es una disciplina como ya dije, reconocida en el extranjero y posee todas las características de un derecho especializado como centros de investigación rubricados con enciclopedias generales, trabajos jurídicos, etcétera. El estudio de este derecho da lugar a manifestaciones de todo orden: seminarios, artículos de periódicos, obras prácticas, publicaciones científicas, de manera que existe ya la creencia de hacer de la informática una cuestión misma."[65]

De esta manera, podemos identificar como el derecho informático se erige como una rama del derecho, que parte de supuestos distintos al derecho común, por ende, tratar de definirlo resulta un tanto complicado.

A pesar de lo anterior, el doctor Héctor Ramón Peñaranda Quintero sostiene que el derecho informático es 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 dos aspectos: a) Regulación del medio informático en su expansión y desarrollo y b) Aplicación idónea de los instrumentos informáticos.[66]

Por su parte, el doctor Julio Téllez Valdés sostiene que "el derecho informático es una rama de las ciencias jurídicas que considera a la Informática como instrumento (Informática Jurídica) y objeto de estudio (Derecho de la Informática)."[67]

---

[65] AZPILCUETA, Hermilio Tomás, Ob. Cit., p. 34.
[66] Cfr. PEÑARANDA QUINTERO, Héctor Ramón. Naturaleza jurídica del derecho informático como rama autónoma del derecho. http://www.monografías.com/trabajos23/juridica-informatica/juridica-informatica.shtml Consultado el 5 de septiembre de 2007 a las 19:00 horas.
[67] TÉLLEZ VALDÉS, Julio, Ob. Cit., p. 17.

De estas definiciones, podemos inferir que la relación entre derecho e informática se da en dos puntos, cuando el derecho regula a los medios informáticos y cuando el derecho utiliza a dichos medios informáticos como un instrumento para su desarrollo.

En este sentido se pronuncia Juan José Ríos Estavillo quien sostiene que la relación entre derecho e informática tiene dos líneas de investigación: "los aspectos normativos del uso de la informática desarrollados bajo el derecho de la informática y la aplicación de la informática en el tratamiento de la información jurídica, conocida como informática jurídica."[68]

Por ello, la clasificación del derecho informático obedece a estos dos puntos de unión entre el derecho y la informática, por un lado, la regulación de los medios informáticos que da origen al derecho de la informática, por otro lado, la utilización de la informática como un recurso para el desarrollo del derecho, dando cabida a la informática jurídica.

La doctrina será coincidente en mencionar que dentro del derecho informático podemos encontrar a la informática jurídica y al derecho de la informática, siendo que la primera es la más antigua, por ende, la más desarrollada y el segundo está aún en expansión.

2.1.2. La informática jurídica

A medida que las sociedades avanzan y las nuevas tecnológicas de la comunicación se globalizan, se hace imprescindible el uso de la informática en el ámbito jurídico, no obstante, es sabido que todavía muchos abogados son reacios a la utilización de cualquier tecnología, además de que una gran mayoría tiene un desconocimiento total de estos medios y de los beneficios que acarrean.

---

[68] RÍOS ESTAVILLO, Juan José. Derecho e Informática en México. Editorial UNAM, México, 1997, p. 45.

Es importante mencionar que en la literatura se confunde el derecho informático con la informática jurídica, no obstante, hemos visto en el punto anterior que el derecho informático es el género y una de las especies es la informática jurídica, ya que ésta abarca sólo un aspecto, es decir, la aplicación de los conocimientos de la informática al derecho, pero no se ocupa de las normas jurídicas que se crean y aplican a los fenómenos informáticos.

Ahora bien, esta sistematización del derecho informático es reciente, por ello, como hemos visto en los incisos anteriores, los primeros indicios de la relación entre la informática y el derecho dará como resultado el nacimiento de la informática jurídica, ya que desde 1949 Lee Loevinger propuso la utilización de dos ordenadores para la aplicación del derecho, dando origen a una disciplina que él denominó “jurimetrics”.

Posteriormente, en 1963 Hans Baade elabora una obra denominada “Jurimetrics: the Methodology of Legal Inquiry” en donde plantea que para desarrollar lo jurídico es necesario hacer tres tipos de investigación:

a) Aplicar modelos lógicos a las normas jurídicas.

b) Aplicar las computadoras a la actividad jurídica.

c) En lo futuro, por medio de dichas computadoras, prever los resultados judiciales.[69]

Será en 1968, cuando Mario Losano cambiará el nombre de Jurimetrics por el de “Iuscibernética”. No debemos soslayar que todos estos términos en mayor o en menor medida, dan cuenta de la informática jurídica, ya que denotan la aplicación de lo informático a lo jurídico.

[69] Cfr. Ibídem, p. 51.

Existen también otras denominaciones que implican la aplicación de lo informático en el derecho: computers and law, rechtsinformatique, jurismática, derecho cibernético e informática jurídica, éste último término derivado de la tradición francesa, el cual ha tenido mayor aceptación en el mundo.

"Esta área del conocimiento surgió en 1959 en Estados Unidos, la Informática Jurídica ha sufrido cambios afines a la evolución general de la misma Informática. Las primeras investigaciones en materia de recuperación de documentos jurídicos es forma automatizada se remontan a los años cincuenta, época en que comienzan a utilizar las computadoras no sólo con fines matemáticos sino también lingüísticos."[70]

En 1959, será en la Universidad de Pittsburg Pensylvania, bajo el auspicio de John Horty, que se grabarán diversos ordenamientos legales en cintas magnéticas, siendo esto la primera demostración de un sistema legal automatizado de búsqueda de información.

Posteriormente, esta automatización se irá perfeccionando con el tiempo hasta llegar a las grandes bases de datos en materia jurídica.

2.1.3. Concepto y clasificación de la informática jurídica

Como vimos en el punto anterior, hay una gran variedad de términos para señalar aquella rama del derecho informático, que se encarga de aplicar los conocimientos, técnicas y métodos de la informática al derecho; pero como lo sostiene el doctor Héctor Fix Fierro el término "informática jurídica" es el que se impone para delimitar la aplicación de la informática a lo jurídico, ya que es un concepto sintético, estricto y no da lugar a confusiones.

[70] TÉLLEZ VALDÉZ, Julio, Ob. Cit., p. 18.

Ahora bien, Luz María del Pozo y Ricardo Hernández mencionan que la informática jurídica tiene tres características: es una subárea del derecho informático, es una herramienta para el tratamiento de la materia jurídica y es una técnica o técnicas para la automatización de los datos jurídicos.[71]

En este sentido Enrique M. Falcón sostiene que "la informática ha sido caracterizada muy bien por Vaz Llore y Dall Anglio cuando dicen: la informática jurídica es el resultado del impacto de la tecnología (de la computación agregamos) en la ciencia del derecho. En ella tienen puntos de encuentro distintas disciplinas: la documentación, la ciencia de la información, las matemáticas, la lógica, la lingüística y el derecho."[72]

No dudamos por ningún motivo que la informática jurídica es una rama del derecho informático, de naturaleza interdisciplinaria en donde convergen distintas disciplinas para coadyuvar con el desarrollo del derecho.

Así el doctor Téllez Valdés define a la informática jurídica "como la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación."[73]

Por su parte, el doctor Fix Fierro señala que la informática es el conjunto de estudios e instrumentos derivados de la aplicación de la informática al derecho o más precisamente a los procesos de creación, aplicación y conocimiento del derecho.

---

[71] Cfr. HERNÁNDEZ, Ricardo y Luz María, DEL POZO, Ob. Cit., p. 133.
[72] FALCON, Enrique M. ¿Qué es la informática jurídica? Editorial Abeledo-Perrot, Argentina, 1992, p. 90.
[73] TÉLLEZ VALDÉZ, Julio, Ob. Cit., p. 19.

De esta manera, podemos decir sucintamente que la informática jurídica es la disciplina que permite la aplicación de los conocimientos de la informática al derecho, para su mejor comprensión, análisis y conocimiento, por ende, su utilización es una herramienta fundamental para todo jurista que pretende hacer ciencia jurídica.

Por otro lado, el común de la doctrina señala que la informática jurídica se divide en tres grandes disciplinas:

a) Informática jurídica documentaria: la cual se encarga de recopilar los textos jurídicos en bases de datos para su posterior consulta de manera eficiente y rápida. Para el doctor Héctor Fix Fierro la informática jurídica documentaria "se ocupa del tratamiento automatizado de los documentos jurídicos, principalmente los derivados de la legislación, la jurisprudencia y la doctrina."[74]

Es importante mencionar que la informática jurídica documentaria es la más antigua, ya que el uso primigenio de la computadora en el mundo del derecho fue la captación del mayor número de leyes para hacer más rápida su consulta.

b) Informática jurídica de control y gestión: conlleva la utilización de las computadoras en la organización y administración de los órganos encargados de crear y aplicar el derecho e incluso en la administración de oficinas públicas, Notarías y despachos jurídicos.

Esta rama de la informática está en continua evolución, ya que constantemente está abarcando mayores actividades en el campo del derecho.

c) Informática jurídica metadocumental: denominada así porque va más allá del tratamiento de documentos y textos jurídicos; su campo de acción se concentra en la toma de decisiones, educación e investigación. Es de inferirse que

[74] FIX FIERRO, Héctor, Ob. Cit., p. 56.

esta rama de la informática es la más reciente, ya que implica que la computadora con los programas idóneos pueda resolver los conflictos que se le planteen.

Como se puede observar, el campo de acción de la informática jurídica es muy basto, ya que va de la recopilación de documentos jurídicos en bases de datos, hasta la resolución de problemas y toma de decisiones.

2.1.4. El derecho de la informática

Otro de los aspectos que debemos analizar en la sociedad de la información, es el impacto negativo que se presenta en la utilización de los medios informáticos, ya que no sólo hay beneficios en estas tecnologías, por ende, surge otra rama del derecho informático que tiene a la informática como objeto de regulación.

Muchos son los problemas que surgen con el uso de las computadoras y sobre todo de Internet, y aunque a nivel internacional hay muchos cuerpos normativos al respecto, el fenómeno informático es muy amplio, por ello, no se puede abarcar toda la problemática que representa a nivel mundial la utilización de la computadora.

El doctor Fix Fierro logra sintetizar esta gran problemática que representa el uso de estas tecnologías informáticas, ya que menciona que la heterogeneidad de los ámbitos jurídicos que afecta la informática impide tener una legislación única, por otro lado, la insatisfacción de las formas de solución tradicionales se hace patente. [75]

De esta manera, surge el derecho de la informática, como una rama del derecho informático que se encarga de regular el fenómeno informático, para ello,

[75] Idem, p. 54.

es necesario entender toda la problemática que abarca, para posteriormente hacer una planeación, control y regulación de estos fenómenos.

El doctor Téllez Valdés define el derecho de la informática como “el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática. Es decir, es un conjunto de leyes en cuanto que, si bien escasos, existen diversos ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático.”[76]

Como podemos deducir, el derecho de la informática está en plena expansión ya que existen muchos temas de la informática que deben ser regulados y a pesar de que a nivel mundial se hace un esfuerzo por cubrir todos los fenómenos informáticos son muy bastos los tópicos que debemos tomar en consideración.

Horacio Fernández Delpech sostiene que múltiples son los temas relacionados con Internet que plantean debate en cuanto a sus implicaciones jurídicas, por ello, menciona enunciativamente los siguientes:

1) El régimen de registro de nombre de dominio.

2) El principio de la libertad de expresión y su vinculación con la libertad de contenidos en Internet.

3) Los ilícitos cometidos a través de Internet.

4) La responsabilidad de los proveedores que intervienen en la Red.

5) La afectación de los derechos a la propiedad intelectual de los autores, compositores e intérpretes.

[76] TÉLLEZ VALDÉZ, Julio, Ob. Cit., p. 21.

6) La afectación de la privacidad de los individuos.

7) La protección de los datos personales.

8) La defensa legal de los sitios Web.

9) La regulación del comercio electrónico y el uso de la firma digital

10) La jurisdicción aplicable a los conflictos planteados.[77]

A estos temas solo es menester agregar la protección de programas de cómputo y el teletrabajo.

Todos estos temas serán materia del derecho de la informática, que como rama del derecho informático, hará los planteamientos necesarios para buscar una buena regulación de esta variedad de fenómenos jurídicos de la informática, poniendo énfasis en aquellas conductas derivadas del uso de la computadora e Internet que se tornan antisociales.

En los próximos incisos haremos alusión al delito informático, materia del presente trabajo de investigación, ya que lo más deleznable del uso de estas tecnologías informáticas es el desarrollo de conductas que violentan bienes jurídicos que el Estado está obligado a salvaguardar a través de las normas jurídico penales.

2.2. El delito informático

Uno de los temas que más preocupa en la sociedad de la información es la regulación de los medios informáticos y de las conductas que se están desplegando con el uso de la computadora y sobre todo de Internet.

[77] Cfr. FERNÁNDEZ DELPECH, Horacio, Ob. Cit., pp. 13 y 14.

Vimos en el punto anterior que son muchos los aspectos que deben quedar enmarcados en el mundo del derecho, ya que con estos avances tecnológicos, nuevas necesidades de regulación resaltan a la vista, por ejemplo, el contrato informático, la protección de datos personales, el teletrabajo, los derechos de autor, etcétera; pero lo que más preocupa a los estudiosos de la informática es lo relativo a las conductas antijurídicas que surgen con el uso de los medios informáticos y que violentan bienes jurídicos que el Estado está obligado a proteger.

No olvidemos que el derecho penal surge para proteger valores fundamentales que la sociedad y el Estado consideran valiosos para la vida en sociedad, de ahí que Miguel Ángel García Domínguez señale que "el elemento fundamental para que sea admisible la tipificación de un delito es que exista una necesidad social digna de protegerse. Esa necesidad social es condición sine qua non para darle intervención al derecho penal. Si no nos encontramos ante un bien jurídico que merezca ser protegido penalmente estaría violando el principio de la intervención mínima penal."[78]

No tenemos duda de que la computadora e Internet se presentan como herramientas favorables para la sociedad, pero también se constituyen como verdaderos instrumentos utilizados por individuos para realizar actos ilícitos. "El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes…A las reconocidas ventajas que ello supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más que el mal no está en el medio utilizado sino en la persona que lo utiliza."[79]

---

[78] GARCÍA DOMÍNGUEZ, Miguel Ángel. Los Delitos Especiales Federales. Editorial Trillas, México, 1987, p. 23.

[79] RIBAS ALEJANDRO, Javier. Aspectos Jurídicos del Comercio Electrónico en Internet. 2ª. edición, Editorial Aranzadi, España, 2003, p. 127.

Podemos señalar que este tipo de comportamiento informático se encuentra desde los orígenes de la propia tecnología, ya que los medios informáticos facilitaron las actividades laborales, lo que propició que en un momento dado el usuario se encontrara en una situación de ocio, lo cual canalizó a través de la computadora cometiendo sin darse cuenta una serie de ilícitos; es de esta manera como surge el ilícito informático, como una acción no intencional, pero a medida que los sujetos informáticos se dan cuenta de los beneficios que pueden adquirir con esos ilícitos o por simple diversión para demostrar su inteligencia, es que el ilícito informático se va convirtiendo en la mayoría de las veces como intencional.

En la actualidad, los grandes sujetos activos en los delitos informáticos (hackers, phreaker, cracker, entre otros) cuentan con características propias que los distinguen de un sujeto activo convencional, primeramente porque estos delincuentes son considerados de cuello blanco, de ahí que en un apartado posterior hagamos una breve referencia a estas características.

Ahora bien, este tipo de ilícitos presenta ciertas peculiaridades, que son sintetizadas por Antonio Enrique Pérez Luño, quien sostiene que desde el punto de vista de la dogmática jurídico penal, la criminalidad informática obliga a revisar los elementos constitutivos de gran parte de los tipos penales tradicionales, aunado a que la delincuencia informática está en constante transformación en virtud de que los medios informáticos tienen día a día innovaciones tecnológicas, por último, la criminalidad informática se caracteriza por las dificultades para descubrirla, probarla y perseguirla. “Se ha hecho célebre la imagen de Parker de que los sistemas informáticos son como “queso de Gruyére” por las enormes oquedades y lagunas que quedan siempre abiertas a posibles atentados criminales.”[80]

Estas dificultades para descubrir, probar, perseguir y juzgar el ilícito informático, se presentan por una serie de situaciones que debemos mencionar:

[80] PEREZ LUÑO, Antonio-Enrique. Manual de informática y derecho. Editorial Ariel, España, 1996, p. 76.

a) Hay una gran carencia de delitos informáticos, por ello, hace falta una tipificación específica en la mayoría de las legislaciones, relativa exclusivamente a ilícitos informáticos.

b) La transnacionalidad de las conductas, que muchas veces se realizan en un país, pero cuyos resultados se producen en otro.[81]

c) La falta de consenso internacional para reprochar algunos ilícitos informáticos.

d) La utilización de los medios informáticos, provocan que dichas acciones sean virtuales

e) Las constantes innovaciones tecnológicas, permiten que el delincuente informático esté un paso adelante de las soluciones jurídicas.

f) Por que no decirlo, el sujeto activo en el delito informático es una persona inteligente que busca los medios para no ser detectado.

Ahora veamos algunas realidades del delito informático para que entendamos la trascendencia de este asunto:

Los medios informáticos son utilizados mundialmente para reproducir indebidamente miles de copias de software, discos, videos y películas, (todos ellos bajo la denominación coloquial de piratas) violentando los derechos de autor y causando daños económicos a todas las industrias relacionadas con estas producciones.

El espionaje informático se lleva a cabo a través de programas maliciosos conocidos como Caballos de Troya o Backdoors, los cuales permiten a su creador

[81] Cfr. FERNÁNDEZ DELPECH, Horacio, Ob. Cit., p. 149.

obtener información clasificada que se encuentra en un sistema informático protegido por sistemas de seguridad, que son violentados, para la divulgación ilícita de secretos industriales o comerciales, lo que puede llevar a una empresa a la quiebra.[82]

Los medios informáticos son utilizados para difundir imágenes y videos violentos, para el desarrollo de la pornografía infantil y pedofilia, para el comercio de mujeres para ser usadas sexualmente, para el tráfico de armas y para la comunicación de la delincuencia organizada.

La llamada técnica del salami permite al usuario infiltrarse en diversas cuentas bancarias del sistema financiero para obtener pequeñas cantidades de dinero, que al acumularse en la cuenta del delincuente suma una cantidad considerable.

La mayoría de las áreas de infraestructura de importancia crítica para un país (energía, transporte, seguridad, sistema financiero, etcétera) se encuentran automatizadas y controladas por medios informáticos, los cuales son protegidos por sistemas de seguridad; si en un momento dado estos sistemas son vulnerados ponen en riesgo el funcionamiento de estas áreas de importancia crítica para el país.

Estas y otras acciones ilícitas se han generado con el desarrollo de los medios informáticos, las cuales ponen en duda los beneficios de la computadora e Internet, “junto a esta realidad por demás alentadora del avance de la tecnología, han surgido una serie de comportamientos disvaliosos antes impensables (la manipulación fraudulenta de los ordenadores con fines de lucro, la destrucción de bancos de datos, la copia de soportes lógicos, etc.) que la doctrina ha

[82] Cfr. NAVARRO ISLA, Jorge. Tecnologías de la Información y de las Comunicaciones: aspectos legales. Editorial Porrúa-ITAM, México, 2005, p. 382.

denominado, en forma genérica, delitos relacionados con los ordenadores o delitos informáticos."[83]

2.2.1. Concepto de delito informático

En la historia del derecho penal se han vertido un gran número de conceptos sobre el delito, de esta manera, Francisco Carrara, principal exponente de la Escuela Clásica, define al delito como la infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso; por su parte, Rafael Garófalo, exponente de la Escuela Positiva, menciona que el delito es una violación de los sentimientos altruistas de probidad y de piedad, en la medida media indispensable para la adaptación del individuo a la colectividad.[84]

Posteriormente, los penalistas se esforzaron para elaborar conceptos jurídicos, de ahí que Edmundo Mezger señale que el delito es la acción típicamente antijurídica y culpable, por su parte Jiménez de Asúa menciona que el delito es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal.

Incluso nuestro Código Penal Federal define al delito como la acción u omisión que sancionan las leyes penales.

En la doctrina podemos encontrar algunas otras definiciones del "delito", las cuales son influenciadas por la Escuela, doctrina o teoría que maneje su autor.

Ahora bien, tomando en cuenta estas definiciones, debemos encontrar el concepto más adecuado para referirnos a estas conductas antisociales que hemos

---

[83] Delitos no convencionales, compilador Julio B.J. Maier, Editorial del Puerto, Argentina, p. 225.
[84] Cfr. CASTELLANOS TENA, Fernando. Lineamientos Elementales de Derecho Penal. Octava edición, Editorial Porrúa, México, 1974, pp. 125-128.

mencionado y que surgen con el desarrollo de los medios informáticos, lo cual no resulta nada fácil por el cúmulo de conductas que debemos englobar, por ejemplo, Anibal A. Pardini sostiene que “el alcance del delito en Internet es tan vasto como la red misma.”[85]

Por ende, el primer gran problema teórico radica en la amplitud de las conductas que se quieren englobar en la definición de delito informático, ya que algunos conceptos además de incluir propiamente delitos, incorporan otro tipo de conductas relacionadas con otras materias.

“En sentido estricto, se entiende por delito las conductas tipificadas como tales por la ley penal. No obstante, bajo el rótulo del delito informático se suelen incluir junto a las conductas criminales que, por su gravedad, encajan en los tipos delictivos, aquellas que por su menor trascendencia no rebasan la esfera de las meras faltas. Junto a estos tipos penales la expresión delito informático se utiliza muchas veces con referencia a las infracciones administrativas (por ejemplo, los atentados contra las normas de protección de datos personales informatizados) o los ilícitos civiles (tales como la consabida piratería del software)[86]

También existe un gran debate en cuanto a la denominación más apropiada para hacer referencia a estos delitos; el especialista Jorge Navarro Isla sostiene que la denominación de los delitos informáticos varía entre los autores y las legislaciones, por ende, hay quienes prefieren llamarles delitos computacionales, delitos electrónicos, delitos cibernéticos o delitos telemáticos.[87]

Ahora veamos algunas referencias que hacen los teóricos de la materia; por cibercrimen, sostiene Debra Littlejohn Shinder, debemos entender a los delitos cometidos utilizando Internet o bien cualquier otra red informática como componente del crimen, para ello, las computadoras y las redes informáticas se

[85] PARDINI, Aníbal A., Ob.Cit., p. 66.
[86] PÉREZ LUÑO, Antonio-Enrique, Ob. Cit., p. 69.
[87] Cfr. NAVARRO ISLA, Jorge, Ob. Cit., p. 392.

ven involucradas de la siguiente manera: a) La computadora o la red pueden ser las herramientas del crimen; b) La computadora o la red pueden ser los objetivos del crimen y c) La computadora o la red pueden ser utilizadas para propósitos incidentales relacionados con el crimen.[88]

Por su parte, la doctora María de la Luz Lima Malvido define al delito informático como cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.

El italiano Carlos Sarzana sostiene que los delitos informáticos "son cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo."[89]

El doctor Téllez Valdés menciona que los delitos informáticos "son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).[90]

En todas estas definiciones existen elementos en común, ya que la computadora es un instrumento para la comisión del delito informático, pero también puede ser el objeto material de dicho ilícito, por ende, coincidimos con los argumentos que sostiene el doctor Téllez Valdés, cuando afirma que el concepto típico del delito informático consiste en una conducta típica, antijurídica y culpable en que se tiene a las computadoras como instrumento o fin, agregando solamente que dicha acción debe violentar bienes jurídicos protegidos por la ley penal.

2.2.2. Diversas clasificaciones del delito informático

[88] Cfr. LITTLEJOHN SHINDER, Debra, Ob. Cit., p. 43.
[89] Delitos Informáticos. http://www.monografias.com/trabajos6/delin/delin.shtml Consultado el 10 de septiembre de 2007 a las 22:00 horas.
[90] Cfr. TÉLLEZ VALDÉS, Julio, Ob. Cit., p. 163.

En la doctrina se han vertido un gran número de clasificaciones relacionadas con el delito informático, las cuales tratan de aglutinar todos los ilícitos que se presentan con el uso de la computadora e Internet. A continuación vamos a señalar algunas clasificaciones que sustentan algunos autores, aclarando que no son limitativas.

Un número importante de autores sostiene que Ulrich Sieber es uno de los teóricos más importantes en materia de delitos informáticos, el cual señala que hay dos grandes grupos de delitos informáticos: los de carácter económico y los delitos contra la privacidad.

En el primer grupo se deben considerar todas aquellas acciones que tomando a la computadora como un instrumento o como un objeto material causan daños patrimoniales a terceros, por otra parte, los delitos contra la privacidad son aquellos que se presentan cuando se causa una afectación en la privacidad de las personas mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.

Para Andrés Palazzi, cualquier clasificación que se haga del delito informático tiene que tomarse en consideración el bien jurídico tutelado; de esta manera, sostiene que existen los siguientes tipos de delitos informáticos:

a) Delitos contra el patrimonio

b) Delitos contra la intimidad

c) Delitos contra la seguridad pública y las comunicaciones

d) Falsificaciones informáticas

e) Contenidos ilegales en Internet[91]

Por su parte, Anibal A. Pardini sostiene que dentro del catálogo de delitos informáticos o ciberdelitos, éstos pueden ser agrupados según el objeto de ataque del sujeto activo en:

a) Robo, intercepción y modificación de datos.

b) Sabotaje, interferencia, hacking y distribución de virus en las redes.

c) Mediante computadora en red (fraudes).[92]

Ahora bien, el doctor Téllez Valdés señala que la clasificación del delito informático depende de si utilizamos a la computadora como un instrumento del delito o como un objeto, por lo que trata de ser congruente con su definición de delito informático al establecer que los delitos relacionados con la computadora como un instrumento o medio son:

1) "Falsificación de documentos por medio de la computadora.

2) Variación de los activos y pasivos en la situación contable de las empresas.

3) Simulación de delitos convencionales.

4) Robo de tiempo de computadora.

5) Lectura o copiado de información confidencial.

[91] Cfr. PALAZZI, Pablo Andrés. Delitos Informáticos. Editorial Ad hoc, Argentina, 2000, pp. 43-47.
[92] Cfr. PARDINI, Aníbal A., Ob. Cit., p. 65.

6) Modificación de datos.

7) Violación de un código de seguridad para acceder a un sistema informático.

8) Desviación del destino de pequeñas cantidades de dinero hacia una cuenta bancaria.

9) Uso no autorizado de programas de cómputo.

10) Insertar instrucciones que provocan interrupciones en la lógica interna de los programas de cómputo.

11) Alteración en el funcionamiento de los sistemas.

12) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

13) Acceso a áreas informatizadas en forma no autorizada.

14) Intervención de las líneas de comunicación de datos."[93]

Aunado a este grupo de delitos, se encuentran los que tienen que ver con la computadora como objeto, entre los que destacan según este autor los siguientes:

1) Programación de instrucciones que producen un bloqueo total al sistema.

2) Destrucción de programas por cualquier método.

[93] TÉLLEZ VALDÉS, Julio, Ob. Cit., p. 165.

3) Daño a la memoria.

4) Atentado físico contra la máquina o sus accesorios.

5) Sabotaje político o terrorismo en que se destruya o se apoderen de los centros neurálgicos computarizados.

6) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje o pago de rescate.

Todas estas clasificaciones responden a diversos criterios y momentos históricos, por ende, sólo deben ser tomadas como ejemplos no limitativos del delito informático y del intento por tratar de ordenar esta gama de ilícitos que utilizan a la computadora como un instrumento u objeto material del delito, por lo mismo, no podemos constreñirnos a estas clasificaciones ya que el delito informático es tan vasto y sigue en aumento que quizá en un futuro no muy lejano sean obsoletas.

2.2.3. Características del delito informático

Desde sus orígenes el delito informático muestra ciertas características propias del carácter innovador de su tecnología, por ende, cuando empiezan a surgir estas conductas que utilizan a la computadora e Internet como instrumentos para delinquir se presenta en la realidad la falta de regulación de los Estados para combatir esta nueva forma de delincuencia.

De esta manera, como lo sostiene Antonio Pérez Luño, la criminalidad informática, reviste tres peculiaridades, ya que por una parte hay una nueva versión de la delincuencia, que implica revalorar los elementos constitutivos de gran parte de los tipos penales tradicionales, por otra parte, en virtud de que la tecnología informática cambia constantemente hace que los delitos informáticos

también cambien con regularidad, por último, se presenta el gran problema que entraña descubrir, probar y perseguir al delincuente informático.[94]

Por su parte, el doctor Tellez Valdés sostiene que el delito informático tiene once características, pero toma en cuenta tanto peculiaridades del sujeto activo como características y fenómenos particulares del ilícito informático.

Así considera al delito informático como una conducta de cuello blanco, ya que no cualquier persona puede cometer estos delitos, porque se requieren conocimientos técnicos sobre la materia informática, que solo algunas personas tienen, por otro lado, como en la actualidad los conocimientos sobre las computadoras es necesario, desde muy temprana edad los niños y jóvenes tienen acceso a los conocimientos informáticos, por ende, desde sus orígenes el delito informático es cometido por un gran número de menores de edad, esto también trae como consecuencia que el delito informático sea cometido de manera culposa, pero también dolosa.

También considera que son acciones ocupacionales, porque las conductas se realizan cuando el sujeto activo está en el trabajo, de igual manera, son acciones de oportunidad debido a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

Estas nuevas conductas delictivas también provocan serias pérdidas económicas para los pasivos y pueden generar grandes ganancias para los activos.

Por ser sumamente sofisticadas las conductas informáticas, hay muchas facilidades de tiempo y espacio, ya que sin la presencia física del sujeto activo pueden llegar a cometerse, esto trae como consecuencia que haya grandes

[94] Cfr. PÉREZ LUÑO, Antonio Enrique, Ob. Cit., p. 75.

dificultades para su investigación y comprobación, aunado a que tienden a proliferar las conductas o a modernizarse ha medida que avanzan los conocimientos tecnológicos en la materia.

Aunado a lo anterior, se ha presentado la situación de que son muchos los casos y pocas las denuncias, ya que las grandes empresas prefieren no denunciar antes que aceptar que un delincuente informático vulneró sus sistemas de seguridad.

Como se puede observar, estas características son muy propias de un ambiente informático, que irán aumentando a medida que surgen nuevos conocimientos en la materia.

2.2.4. Evolución histórica de los delitos informáticos

Entrar al estudio de la evolución de los delitos informáticos es analizar la historia de las computadoras mismas, ya que el delito informático no se da de un día para otro, pero se va perfeccionando a medida que van surgiendo nuevos avances tecnológicos en la materia.

"En cuanto se reconoció que los ordenadores almacenaban elementos valiosos (información) los criminales vieron una oportunidad. Pero al igual que es difícil robar a alguien que se queda todo el día encerrado en caso, los datos almacenados en ordenadores independientes son difíciles de robar. Sin embargo, cuando los datos comenzaron a moverse de un ordenador a otro por medio de las redes, como la víctima de un robo cuando va de un sitio a otro, los datos se hicieron más vulnerables. Las redes proporcionaron otra ventaja: un punto de entrada. Incluso aunque la información valiosa nunca se enviara a través de los cables, las entradas y salidas de otros bits de datos abrían una vía de entrada para que los intrusos se colaran en los ordenadores…"[95]

[95] LITTLEJOHN SHINDER, Debra, Ob. Cit., p. 91.

En los primeros días de las computadoras, las personas no contaban con la capacidad ni el conocimiento para tener una computadora personal, en virtud de que eran máquinas muy grandes y costosas, por ende, solo existían algunas de ellas en el mundo.

El problema del delito informático toma su auge cuando las computadoras personales se hacen más fáciles en su manejo y más baratas; lo que trae como consecuencia su uso masivo en el mundo y a medida que las redes informáticas enlazan las computadoras en el mundo, se genera un medio idóneo para el delincuente informático.

Cuando se generaliza el uso de la computadora en el mundo, se abren las puertas para los delincuentes informáticos, ya que la información y los programas almacenados en las computadoras se hacen más vulnerables.

En sus inicios el delincuente informático utilizó el sistema telefónico para realizar llamadas de larga distancia sin pagar por ellas, de esta manera, surge el término “phreakers” que hace referencia al sujeto que realiza este tipo de llamadas telefónicas.

Posteriormente se afianza la idea del “cracker” que es una persona que se dedica a romper sistemas de seguridad y el “hacker” que es una persona considerada como un verdadero programador, que domina los sistemas informáticos del momento y es capaz de manipular los programas para que hagan cosas diversas a las ordenadas por el usuario.

Con el surgimiento de las redes informáticas y su uso masivo en el mundo se abre la posibilidad para mayores ilícitos informáticos. En la actualidad, el surgimiento de nuevas tecnologías como la banda ancha y las conexiones inalámbricas abre aun más la posibilidad de delinquir.[96]

[96] Ibídem, pp. 106-107.

2.2.5. Características del sujeto activo en el delito informático

Analizar al sujeto activo en el delito informático es muy interesante, ya que parece ser que cuenta con características especiales que lo distinguen del delincuente habitual.

La maestra Griselda Amuchategui Requena sostiene que el sujeto activo "es la persona física que comete el delito, se llama también delincuente, agente o criminal…el sujeto activo es siempre una persona física, independientemente del sexo, la edad, la nacionalidad y otras características."[97]

En los inicios de la computación y las redes informáticas se hicieron algunos estereotipos relacionados con el delincuente informático, de esta manera, se sostuvo que el delincuente informático era una persona brillante pero socialmente inadaptado, también se señaló que tenía un coeficiente intelectual elevado y que la mayoría de los delincuentes son hombres y adolescentes.

No obstante, con la masificación de la computadora y de las redes informáticas, cualquier persona puede acceder a una computadora e iniciar su carrera delictiva en el mundo informático.

En su momento, como lo señalamos con anterioridad, el delito informático fue considerado como un delito de cuello blanco, es decir, que sólo aquellos con conocimientos profundos en computación podían delinquir con estos medios, sin embargo, un gran número de especialistas en la materia sostiene que en la actualidad estos mitos del delincuente informático han cambiado, ya que es tan generalizado el uso de la computadora e Internet que cualquiera puede cometer un ilícito de manera dolosa o culposa.

---

[97] AMUCHATEGUI REQUENA, Griselda I. Derecho Penal. Tercera edición, Editorial Oxford, México, 2005, p. 37.

Pablo Andrés Palazzi sostiene que es un mito que el delincuente informático deba forzosamente poseer conocimiento profundos en la materia, ya que la computación se halla tan extendida hoy en día que cualquier persona que posea conocimientos mínimos de informática y tenga acceso a un ordenador, incluso desde su casa, puede realizar un delito informático.

"En efecto, determinados ilícitos como el hacking requieren de un conocimiento especial en materia de informática, sin embargo, con la masificación de los servicios informáticos en línea, tales como los servicios gubernamentales, prácticamente cualquier persona puede acceder y utilizar con relativa facilidad servicios de telecomunicaciones y navegar en el ciberespacio de donde se pueden obtener sin mayor restricción sofisticadas herramientas de programación para cometer voluntaria o involuntariamente, determinados delitos, situación que incide en el creciente número de ataques llevados a cabo por legos o personas inexpertas."[98]

De esta manera, podemos afirmar que si bien es cierto para cometer algunos delitos informáticos sí se requieren conocimientos especializados en la materia, tan bien es cierto que en la actualidad, por la masificación en el uso de la computadora e Internet cualquier persona puede cometer alguna conducta que se encuadre como delito informático, de manera dolosa o culposa.

[98] NAVARRO ISLA, Jorge, Ob. Cit., p. 398.

CAPÍTULO TERCERO

BASES JURÍDICAS PARA LA REGULACIÓN DEL DELITO INFORMÁTICO

3. Necesidad de una regulación integral de los medios informáticos en México

Como lo comentamos en el capítulo primero, el mundo de hoy vive en una conectividad total gracias a la computadora y las redes informáticas, las cuales aportan mucho a la humanidad entera, ya que facilitan las comunicaciones, el acceso a la información y han logrado automatizar la vida diaria del hombre e incluso se ha forjado en todo el mundo la idea de una sociedad de la información.

Ahora bien, no cabe duda que en el ciberespacio se entablan procesos de comunicación interpersonales, que requieren reglas básicas de convivencia ya que en este medio de comunicación electrónico también es necesario regular el comportamiento entre los participantes para evitar un caos electrónico en los procesos de comunicación e incluso para inhibir la comisión de ilícitos que dañen o pongan en peligro bienes jurídicos, por ello, se plantea un debate en el uso de los medios informáticos y sobre todo en el uso de Internet, ya que por una parte se exige su regulación jurídica y por otra parte, se plantea la posibilidad de que los particulares establezcan sus propios códigos normativos de utilización.

La autorregulación de Internet es un tema que preocupa no sólo a los estudiosos del derecho, sino a toda la sociedad en general, toda vez, que el ciberespacio conlleva un conglomerado de temas que es necesario regular jurídicamente, pero el primer gran debate versa sobre el ámbito de aplicación

territorial o extraterritorial de la regulación que se pretenda elaborar por las propias características del ciberespacio.

Incluso, hay algunos juristas que plantean la posibilidad del surgimiento del "Derecho Internacional de la Informática como un medio adecuado para la regulación de Internet, en donde el Derecho Internacional podría reducirse a un gran sistema de reglas de elección de la ley a aplicar a la resolución de un caso, dadas ciertas circunstancias.".[99]

Bajo esta tesitura, es claro que no debemos dejar que el ciberespacio se controle sólo, por ende, las autoridades federales mexicanas tienen que tener una participación más activa en la elaboración de los distintos cuerpos normativos que regulen todos los ámbitos de la red, hasta en tanto aparezca el tratado internacional correspondiente.

Por eso, Julio Fernández Rodríguez sostiene que "el derecho no escapa a la incidencia de Internet en todos los órdenes, una incidencia que está exigiendo replantear muchas de las instituciones jurídicas al uso y que reclama aproximaciones teóricas que arrojen luz a las oscuridades conceptuales que nacen al abrigo de la red.".[100]

En México, algunos juristas han puesto su vista en el análisis de todos los temas que deben ser regulados, ya que en nuestro país la legislación sobre aspectos informáticos es muy limitada[101] aunque en los últimos años, se han modificado algunas leyes ya existentes para incorporar los temas informáticos en la legislación mexicana, tal es el caso del Código de Comercio, el Código Civil Federal, la Ley Federal de Protección al Consumidor, la Ley Federal del Derecho de Autor, el Código Federal de Procedimientos Civiles, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, así como la

[99] TELLÉZ VALDÉS, Ob. Cit., p. 87.
[100] FERNÁNDEZ RODRÍGUEZ, José Julio, Ob. Cit., p. 144.
[101] Cfr. FIX FIERRO, Héctor, Ob. Cit., p. 54

tipificación de ciertas conductas en los Códigos Penales estatales y en el Federal; pero de la lectura de dichos Códigos Penales podemos deducir que aún faltan muchas conductas antisociales que no fueron tipificadas.

Muchos son los temas que deben ser objeto de regulación por parte del legislador mexicano, por la gama de aristas que se observan en los medios informáticos y sobre todo en Internet, por ende, Julio Téllez Valdés nos muestra una lista de temas que deben ser tomados en consideración en una regulación integral de los medios informáticos en México:

1. Regulación de bienes informacionales

2. Protección de datos personales

3. Regulación de Internet

4. Propiedad intelectual (protección de programas de cómputo y regulación de nombres de dominio)

5. Delitos informáticos

6. Contratos informáticos

7. Comercio electrónico

8. Teletrabajo

9. Valor probatorio de los soportes modernos de información.[102]

[102] Cfr. TÉLLEZ VALDÉS, Julio, Ob. Cit., pp. 22-23.

Estos temas deben ser materia de regulación por parte del legislador mexicano, siendo pertinente que todo lo relacionado con la computación, informática e Internet sean legislados exclusivamente por el Congreso de la Unión, para ello, será menester establecer una reforma al artículo 73 Constitucional para establecer la facultad del Congreso de la Unión para legislar en materia de informática e Internet, con el fin de evitar contradicciones normativas o lagunas legales que pudiesen presentarse en las leyes locales.

Para lograr lo anterior, las autoridades mexicanas deben conformar un grupo interdisciplinario que haga las propuestas necesarias para una buena regulación de todos estos temas, en donde se vean todas las aristas que implica el uso de la informática e Internet en la sociedad mexicana.

3.1. La libertad de expresión y el derecho a la información

En la llamada sociedad de la información, se está presentando un debate que parece truncar el destino de los medios informáticos y sobre todo de Internet en todo el mundo, ya que dos principios fundamentales de todo estado democrático de derecho, se ven confrontados ante la exigencia de encauzar en los cuerpos legales a Internet.

Como lo hemos venido afirmando, Internet se ha convertido en un medio de expresión, difusión y comunicación excelso en todo el mundo, que se sostiene bajo dos pilares fundamentales del estado democrático globalizado, a saber: la libertad de expresión y el derecho a la información.

Estos principios fundamentales se encuentran reconocidos en nuestra norma constitucional en su artículo 6º y complementariamente en el artículo 7º que rezan respectivamente lo siguiente:

"La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso que ataque a la moral, 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…".[103]

"Es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.

Las leyes orgánicas dictarán cuantas disposiciones sean necesarias para evitar que so pretexto de las denuncias por delitos de prensa, sean encarcelados los expendedores, papeleros, operarios y demás empleados del establecimiento de donde haya salido el escrito denunciado, a menos que se demuestre previamente la responsabilidad de aquéllos.".[104]

De la interpretación de la propia norma constitucional mexicana se desprende que se reconoce la libertad de expresión y el derecho a la información que será garantizado por el Estado; ambos principios debemos entenderlos extensivamente en atención a que son garantías individuales que deben respetar todos los órganos del Estado; en este sentido, Internet como un medio a través del cuál los seres humanos se expresan en diversas formas y sirve también como un instrumento de comunicación e información entre los individuos, queda salvaguardado su uso dentro de los alcances de los preceptos constitucionales citados.

---

[103] Constitución Política de los Estados Unidos Mexicanos, 50ª edición, Editorial Sista, México, 2010, p. 20.
[104] Ibídem, p. 21.

De igual manera, existen diversos instrumentos internacionales que salvaguardan jurídicamente dichas libertades, tal es el caso de la Declaración Universal de los Derechos Humanos que en su artículo 19 menciona que: “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el difundirlas, sin limitaciones de fronteras, por cualquier medio de expresión”.[105]

Asimismo, el Pacto de San José de Costa Rica reconoce la libertad de pensamiento, expresión e información e incluso el Pacto Internacional de Derechos Civiles y Políticos señala que el derecho a la libertad de expresión comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística o por cualquier otro procedimiento de su elección.

Toda esta normatividad nacional e internacional ha permitido que el ejercicio de la libertad de expresión e información sea un pilar fundamental en los estados democráticos, tan es así que Horacio Fernández Delpech refiere que “el derecho a la libertad de expresión es hoy en día un derecho humano fundamental, receptado por la mayoría de los Estados democráticos en sus constituciones y afirmado en los principales acuerdos internacionales es la piedra angular de cualquier sistema democrático y no escapan a este principio de la libertad de expresión el carácter de los contenidos incorporados a la red Internet.”.[106]

Ahora bien, este reconocimiento nacional e internacional hacia dichos principios no es absoluto, ya que todas las normas son claras en establecer los límites a estas libertades, que para el caso del sistema jurídico mexicano, esta libertad de expresión e información no debe trastocar la moral, los derechos de terceros, ni perturbar el orden público o provocar algún delito, más aún, la libertad

---

[105] Cfr. Derecho Internacional de los Derechos Humanos, Editorial Oficina en Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Colombia, 2004, p. 655.
[106] FERNANDEZ DELPECH, Horacio, Ob. Cit., p. 123.

de imprenta debe respetar la vida privada y la paz pública, e incluso en la actualidad la norma constitucional mexicana ya reconoce la protección de datos personales.

En este mismo tenor se pronuncian los instrumentos internacionales que hemos señalado, ya que la Declaración Universal de los Derechos Humanos refiere que las libertades que otorga dicho instrumento sólo serán restringidas por la ley cuando se busque el respeto a los derechos y libertades de los demás, y se satisfagan las justas exigencias de la moral, del orden público y del bienestar general de una sociedad.

Lo anterior nos permite afirmar que si bien es cierto existe un reconocimiento normativo hacia la libertad de expresión e información, también es cierto que no es absoluto o irracional, ya que siempre se podrá ejercer cuando no se dañe a los demás en lo particular o a la sociedad en general.

Esta situación pone realmente en tela de juicio a estos derechos que se ejercen en la computadora e Internet, ya que en el uso de dichos medios se trastocan derechos y libertades de otros, se generan conductas antisociales y se puede menoscabar el orden público y el bienestar general de una sociedad, por ende, no es viable reconocer de manera extensiva estos derechos en el uso de tales tecnologías, sino más bien debemos pugnar por un sistema integral de regulación que norme todos los aspectos de la computadora y del ciberespacio.

La red es un producto social que requiere una regulación integral para beneficio del propio grupo social; y el sistema de autorregulación que proponen algunos usuarios de la red, que tiene que ver con las netiquettes,[107] es un sistema ambiguo, que no da certeza a los usuarios, ya que la red es un mundo que tiene muchas facetas de información y comunicación, que deben ser reguladas en

[107] http://www.albanet.com.mx/artículos/NETIQUETTE.html Consultado el 3 de septiembre de 2007 a las 17:00 horas.

específico, porque cada una tiene sus particularidades, de igual manera, debemos inhibir el desarrollo de las conductas delictivas que han puesto en jaque a la sociedad de la información, esto corresponde a cada una de las naciones en particular a través de la incorporación de diversas figuras delictivas en sus Códigos Penales que aseguren la prevención general y la prevención especial de la norma jurídico penal.

3.2. Violación a la intimidad y privacidad de las personas

Los conceptos de intimidad y privacidad han sido objeto de muchos debates por parte de los doctrinarios, pero por lo limitado de nuestro trabajo de tesis solo haremos algunas reflexiones.

La literatura distingue estos conceptos al considerar que la intimidad constituye la esfera en que se desarrollan las facetas únicas, exclusivas y reservadas de la vida de la persona, por el contrario, la privacidad es un concepto más amplio ya que “es el derecho que tiene una persona de no ser molestada o sufrir invasión a su persona o a su información personal, así como a sus relaciones y comunicaciones privadas, entre las que se cuentan las comunicaciones electrónicas.”.[108]

Derivado de lo anterior, consideramos que la norma constitucional no reconoce explícitamente el derecho a la intimidad, como lo hace con el derecho a la privacidad en diversos preceptos constitucionales, derivado esto de la regulación de los actos de molestia que prohíbe el artículo 16 Constitucional reformado el 18 de junio de 2008, que en lo conducente refiere:

“Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

[108] BARRIOS GARRIDO, Gabriela, Ob. Cit., p. 48.

…

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

…

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio.

…

La correspondencia que bajo cubierta circule por las estafetas, estará libre de todo registro y su violación será penada por la ley.”.[109]

Indudablemente, que toda persona que haga uso de la computadora e Internet queda salvaguardada bajo el derecho a la privacidad, que le va permitir no ser molestado en su persona, bienes o derechos, incluyendo en sus

[109] Constitución Política de los Estados Unidos Mexicano, Ob. Cit., pp. 23-25.

comunicaciones y correspondencia, salvo en los casos que la propia norma constitucional establece.

La misma Declaración Universal de los Derechos Humanos reconoce este derecho a la privacidad ya que refiere que: nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación

Sin embargo, a pesar de que existen estos ordenamientos jurídicos, que protegen el derecho a la privacidad desde un ámbito constitucional e internacional, tal protección es insuficiente, ya que los avances informáticos han provocado nuevos ataques a la privacidad de las personas, tan es así que uno de los temas más discutidos es la protección de datos personales.

Son muy variados los ataques a la privacidad de las personas a través de los medios informáticos e Internet, pero los más reconocidos por su constancia son:

a) La entrada en el disco duro de un sistema sin consentimiento del titular

b) La acumulación o registro de datos sin consentimiento

c) La transferencia de datos sin consentimiento

d) El empleo de una dirección IP asignada a otro ordenador

e) La intercepción de mensajes de correo electrónico y de las comunicaciones en general (Chat, video, etcétera)

f) Hostigamiento electrónico

g) Uso indebido de directorios de correo electrónico o listas de usuarios.

h) Alteración o destrucción de información

i) Interrupción del servicio[110]

j) El SPAM (envío de correo electrónico no deseado)

Por ende, se debe pugnar por la regulación integral de todos los temas relacionados con la computadora e Internet, para evitar estos ataques que se producen a la privacidad de las personas por estos medios tecnológicos.

3.3. ¿Debemos regular Internet?

Como lo hemos mencionado reiteradamente en los apartados anteriores, todos los temas relacionados con los medios informáticos e Internet deben quedar perfectamente regulados en la legislación, para evitar ataques a la privacidad de las personas e incluso para inhibir la vulneración de bienes jurídicos, so pretexto de la libertad de expresión y el derecho a la información.

Ahora bien, la red de redes cuenta en la actualidad con un sistema de reglas sociales que permiten regular las comunicaciones interpersonales entre los participantes activos de la red, denominadas netiquettes, que no son más que un conjunto de reglas de comportamiento que se utilizan en la red.[111]

Estas reglas de comportamiento se sujetan a diversos principios entre los que destacan los siguientes:

---

[110] Cfr. FERNANDEZ RODRIGUEZ, José Julio, Ob. Cit., pp. 99-100.
[111] http://www.albanet.com.mx/artículos/NETIQUETTE.html Consultado el 3 de septiembre de 2007 a las 17 horas.

a) Uno de los principios que nunca hay que olvidar es “respetar la privacidad de los demás”, ya que la información que nos comparten, sobre todo de datos personales, no debe transmitirse al mundo sin autorización del titular, ya que trastocamos el derecho a la intimidad de las personas.

b) El segundo principio, consiste en dejar siempre una buena impresión en los demás cibernautas, ya que no debemos utilizar un lenguaje ofensivo, sino cortés. Esto es muy importante, sobre todo en los Chat y correos electrónicos, ya que esto ha dado lugar a ciertas reglas más específicas en estos medios como son: no usar mayúsculas, dar un formato claro y corto al mensaje, no enviar propaganda, etcétera.

c) En la red, compórtate con los demás como te gustaría que los demás se comportasen contigo. Este principio engloba la esencia de las netiquettes, ya que lo que busca la autorregulación es un buen comportamiento ético por parte de los usuarios de la red.

Estas reglas de comportamiento en la red son convencionales, y han sido creadas por los propios usuarios y servidores de la red. Esto nos lleva a una gran problemática, toda vez, que no sabemos con certeza cuáles son todas las reglas que se utilizan, lo que genera falta de certeza y seguridad jurídica.

Por otro lado, las netiquettes varían de dominio a dominio, lo que genera ambigüedad en las reglas, ya que parece ser que cada dominio tiene sus propias reglas, tan específicas, que hacen imposible su conocimiento para una nueva persona que está explorando dicho dominio.

Ahora bien, estas reglas convencionales no tienen una sanción como tal para el caso de incumplimiento de las mismas, quizá la única sería el rechazo de los participantes en el dominio; más aún, la utilización de las reglas queda al arbitrio de los usuarios de la red.

Como podemos observar, las netiquettes, como se conoce a las reglas de comportamiento aceptables en la red, son convencionales y no dan ninguna certeza o seguridad al usuario, quedan al libre arbitrio de los usuarios y no existe ninguna sanción para el caso de incumplimiento.

Lo anterior nos lleva a pensar, que esta autorregulación de la red tiene muchas desventajas, ya que la falta de una completa y verdadera regulación jurídica de la red, ha generado el surgimiento de conductas delictivas en el desenvolvimiento del ciberespacio, por ende, es imperativo que Internet quede regulado jurídicamente para evitar la falta de certeza y seguridad en su funcionamiento, ya que no debemos de soslayar que en México y en el Mundo, las comunicaciones y la información fluyen en la actualidad a través de Internet, lo que ha generado un gran número de conductas positivas, pero también negativas para los que acceden a este sistema de comunicación.

3.4. Análisis del artículo 6º Constitucional

El artículo sexto Constitucional consagra dos de las garantías individuales más importantes del ciudadano en nuestro país, esto es, la libertad de expresión y el derecho a la información, con el correlativo derecho de acceso a la información pública, ya que en dicho precepto se señala lo siguiente:

“La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque la moral, los derechos de tercero, provoque algún delito o perturbe el orden público; el derecho de réplica será

ejercido en los términos dispuesto por la ley. El derecho a la información será garantizado por el Estado.

Para el ejercicio del derecho a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

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. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.[112]

Como se aprecia en el precepto constitucional citado, la norma fundamental en México reconoce dos derechos fundamentales en la vida de todo gobernado, ya que consagra la libertad de expresión y el derecho a la información con su correlativo actualizado y ampliado derecho de acceso a la información pública.

Como lo sostienen Emilio O. Rabasa y Gloria Caballero, lo más característico del hombre y que lo distingue de los demás seres de la naturaleza, es la facultad de concebir ideas y poderlas trasmitir a sus semejantes, por eso la libertad de expresión es el derecho más propiamente humano, el más antiguo y la base de otros derechos.[113]

Por su parte, sostienen que el derecho a la información fue consagrado en 1977 en la Constitución y comprende los siguientes derechos:

a) El derecho del particular y de los grupos a tener acceso a los medios de comunicación, en determinadas circunstancias y cuando se trate de asuntos de suma importancia para la sociedad.

b) El derecho a recibir información veraz.

---

[112] Constitución Política de los Estados Unidos Mexicanos, Ob. Cit., p. 20.
[113] Cfr. RABASA, Emilio O y Gloria, CABALLERO. Mexicano: esta es tú Constitución . Editorial Cámara de Diputados, México, 1984, pp. 37-39.

c) El derecho a obtener de los órganos públicos la información necesaria para salvaguardar los intereses particulares o de grupos.[114]

Ahora bien, como se ha mencionado con antelación, estos derechos fundamentales no se pueden ejercer arbitrariamente o sin ninguna restricción, ya que la norma constitucional establece los límites a que se sujetan los mismos, es decir, que se ejercerán siempre y cuando no ataquen la moral, los derechos de terceros, provoquen algún delito o perturben el orden público.

Visto lo anterior, podemos afirmar que la computadora e Internet son medios de expresión, información y comunicación masivos que unen a millones de personas en el mundo, por tanto, su uso se sustenta en el ejercicio de la libertad de expresión y el derecho a la información que se encuentran reconocidos tanto en las normas nacionales como internacionales, como lo hemos sostenido en los apartados anteriores.

Esta posición quedó perfectamente definida en la Cumbre Mundial sobre la Sociedad de la Información celebrada en Ginebra en 2003 y posteriormente en la Cumbre de Túnez de 2005, en donde se reconoció que la sociedad de la información se sustenta en el derecho a la libertad de opinión y de expresión.

Pero estas libertades que se pueden ejercer a través de los medios informáticos, también tienen límites, ya que la propia norma constitucional señala que estos derechos no podrán ejercerse cuando se ataque la moral, los derechos de terceros, se provoque algún delito o perturbe el orden público, de ahí que Emilio O. Rabasa y Gloria Caballero sostengan que los derechos del hombre, para ser respetados, deben ser respetables, por ende, la libertad de expresión ya no lo es si ataca la vida privada, la moral o la paz pública.

---

[114] Ibídem, p. 40.

Por tal motivo, no podemos soslayar que los sistemas informáticos e Internet, pueden ser utilizados, para violentar bienes jurídicos, so pretexto del ejercicio de la libertad de expresión, de opinión y de información, por ello, es imprescindible que reconozcamos que la sociedad de la información debe sujetarse a normas jurídicas bien definidas para evitar el desarrollo de conductas antisociales.

3.5. Análisis del artículo 7º Constitucional

El artículo 7º de la Constitución regula otro derecho fundamental del ser humano como lo es el derecho para publicar y difundir las ideas por cualquier medio gráfico, es decir, reconoce la libertad de imprenta, ya que dicho precepto reza lo siguiente:

"Es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.

Las leyes orgánicas dictarán cuantas disposiciones sean necesarias para evitar que so pretexto de las denuncias por delito de prensa sean encarcelados los expendedores, "papeleros", operarios y demás empleados del establecimiento de donde haya salido el escrito denunciado, a menos que se demuestre previamente la responsabilidad de aquellos.".[115]

Para Emilio O. Rabasa y Gloria Caballero la libertad de imprenta es solo una manifestación de la libre expresión y políticamente la libertad de expresar ideas, en forma verbal o por escrito, por ende, es de la mayor importancia para las democracias.

[115] Constitución Política de los Estados Unidos Mexicanos, Ob. Cit., p. 21.

Por su parte Jesús Orozco Henríquez y Jorge Madrazo mencionan que la libertad de imprenta, también llamada libertad de prensa, es una garantía del régimen democrático en tanto exterioriza el pluralismo político e ideológico y puede controlar los actos del gobierno denunciando sus errores y defectos, por lo que mediante esta garantía se establece la facultad de todos los individuos, independientemente de su condición, de publicar escritos sobre cualquier materia, en tanto que se obliga al Estado a abstenerse de coartar el ejercicio de dicha facultad fuera de las excepciones constitucionales señaladas, así como a no establecer censura previa a impreso alguno, ni a exigir garantías a los autores o impresores de cualquier publicación.[116]

Ahora bien, esta libertad para publicar y difundir ideas por cualquier medio gráfico también tiene limitantes, que se encuentran perfectamente reguladas en la constitución y que consisten en el respeto a la vida privada, la moral y la paz pública.

A este respecto, Jorge Madrazo sostiene que lamentablemente ni la legislación secundaria, ni la jurisprudencia, se han preocupado por fijar estos conceptos que adolecen de una excesiva vaguedad e imprecisión, lo cual ha provocado su aplicación arbitraria y caprichosa por parte de las autoridades judiciales y administrativas.

En este tenor, podemos decir que todas las ideas que plasmamos y difundimos de manera verbal o por escrito a través de un sistema informático tienen la protección de la Constitución, pero el ejercicio de esta garantía constitucional que se puede ejercer por cualquier medio informático e incluso por Internet también tiene limitantes, como lo es el respeto a la vida privada, a la moral y a la paz pública.

---

[116] Diccionario Jurídico Mexicano. Segunda edición, Editorial UNAM-PORRUA, México, 1988, p. 2008.

Lamentablemente, los medios informáticos han sido utilizados para dispersar información falsa a través de correos electrónicos o para denostar a la gente o para verter opiniones políticas, religiosas, sociales o económicas sin ningún respeto hacia la autoridad o los particulares o para intimidar o mostrar gráficos o impresos a través de las páginas Web que constituyen verdaderos ilícitos penales, por ello, es imprescindible que todos los medios informáticos e Internet tengan una buena regulación jurídica para evitar que bajo el pretexto de la garantía prevista en el artículo 7º de la Constitución se vulneren bienes jurídicos a través de los sistemas informáticos.

3.6. Análisis del artículo 16 Constitucional

El artículo 16 constitucional conglomera un conjunto de derechos fundamentales de suma importancia para todo individuo en un estado democrático como el nuestro, ya que regula diversos actos de molestia de la autoridad hacia las personas, pero por lo limitado de nuestra investigación, solo haremos alusión a los temas que tienen con ver con la protección de datos personales y las comunicaciones privadas, ya que los sistemas informáticos son instrumentos de comunicación y de captación de bases de datos personales.

De esta manera, el precepto constitucional mencionado reza en la parte conducente lo siguiente:

“Nadie puede ser molestado en su persona, familia, domicilio, papeles y posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de

seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

…

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estar autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

…

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio…”.[117]

De este precepto constitucional en su párrafo primero se desprenden un conjunto de derechos que tienen que ver con la legalidad y la seguridad jurídica,

[117] Constitución Política de los Estados Unidos Mexicano, Ob. Cit., pp. 23-25.

de ahí que Emilio O. Rabasa y Gloria Caballero sostengan que la garantía consignada en la primera parte de este artículo así como las que establece el artículo 14 Constitucional, son la base sobre la que descansa el procedimiento judicial protector de los derechos del hombre, por tal motivo, sostienen, que es absoluta la prohibición de ocasionar molestias a las personas, a sus familias, papeles o posesiones, si no es con una orden escrita, fundada y motivada en una disposición legal y expedida por una autoridad que de acuerdo con una ley en vigor tenga facultades para realizar esos actos.[118]

En este sentido, tomando en consideración el precepto constitucional mencionado, es imprescindible reconocer que toda persona que haga uso de los sistemas informáticos e Internet no puede ser molestada por ninguna autoridad, salvo que exista un mandamiento escrito de alguna autoridad competente que funde y motive la causa legal del procedimiento.

Este derecho a no ser molestado por la autoridad, salvo que concurran ciertas exigencias constitucionales, es importantísimo para el ejercicio de cualquier otro derecho, ya que permite un desarrollo pleno de la personalidad del individuo.

De esta manera, el uso de los sistemas informáticos, así como de Internet por parte de un particular debe ser respetado por todos los órganos del Estado, a no ser que en su ejercicio, el particular haga uso de dichos medios informáticos para violentar una norma jurídica.

Por otra parte, la protección de datos personales es un tema de suma importancia para cualquier sociedad moderna que tenga grandes flujos de información, de ahí que Julio Téllez Valdés reconozca que las computadoras han facilitado la concentración automática de datos referidos a personas, así como su

[118] Cfr. RABASA, Emilio O y Gloria, CABALLERO, Ob. Cit., p.59.

manejo rápido y eficiente, por ende, quién tiene esta gama de datos personales a su disposición puede ser un factor de poder.[119]

De ahí que surja la necesidad de que los datos personales queden regulados jurídicamente en sus diferentes facetas como lo ha concebido la doctrina y como se ha adoptado en diferentes países, en donde se reconocen cuatro aristas de la protección de datos personales:

A) Derecho de acceso: le permite al particular conocer quién tiene su información y que tipo de información tienen sobre su persona.

B) Derecho de rectificación: permite al particular modificar los datos que considere errados y que se encuentren en poder de un tercero.

C) Derecho de uso conforme al fin: consiste en que el particular puede exigir que sus datos sean utilizados sólo para el fin que fueron exigidos.

D) Derecho para la prohibición de interconexión de archivos: prohíbe que las distintas bases de datos se unan entre sí para intercambiar información de los particulares.[120]

La norma constitucional mexicana recoge dentro de esta gama el derecho de acceso y rectificación e incorpora la cancelación y la posibilidad de manifestar su oposición, además menciona las excepciones para esta protección de datos, las cuales son: por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Hoy en día la protección de datos personales adquiere mayor relevancia en un país como el nuestro en donde diversas instituciones públicas y privadas tienen

[119] Cfr. TELLEZ VALDÉS, Julio, Ob. Cit., p. 60.
[120] Ibídem, p. 63.

nuestros datos personales sin ningún control, de ahí que cuando proporcionamos datos para adquirir algún crédito bancario, resulta que dicha institución de crédito intercambia nuestros datos de manera electrónica con otras instituciones comerciales sin ninguna dificultad técnica o legal, por tanto, esas nuevas instituciones que tienen nuestros datos empiezan a ofrecernos productos o bien nos tienen perfectamente identificados para fines de mercado.

Esto se ha logrado gracias a los sistemas informáticos e Internet, ya que la computadora nos ha permitido crear grandes bases de datos y a través de Internet se pueden intercambiar estar bases, incluso por correo electrónico.

Con la incorporación a la constitución de este nuevo derecho en el artículo 16 se abre una gran posibilidad para que nuestros datos personales tengan una verdadera y real protección y no sean utilizados sólo para fines políticos o económicos, porque como dice Julio Téllez Valdés quien tiene acceso a la información de las personas y puede disponer de ella, está en la posibilidad de ser un factor de poder.

Ahora bien, el artículo 16 Constitucional también establece un derecho fundamental relacionado de manera íntima con los sistemas informáticos e Internet, ya que se reconoce en la norma fundamental que las comunicaciones privadas son inviolables.

Indudablemente que en los sistemas informáticos se resguarda información privada y a través de Internet se entablan por los medios más comunes como el Chat, el Messenger o el Correo Electrónico comunicaciones privadas, por ende, podemos afirmar que la comunicación que se entabla entre los particulares a través de los medios electrónicos e Internet queda protegida bajo el derecho fundamental de inviolabilidad de las comunicaciones privadas, previsto en el artículo 16 Constitucional.

E incluso queda reforzado ese principio bajo la premisa de que la ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, pero con motivo de la reforma constitucional del 18 de junio de 2008, en el artículo 16 Constitucional se abre la posibilidad de que las comunicaciones privadas sean aportadas por alguno de los participantes en forma voluntaria y no sea considerado como delito.

Como consecuencia de lo anterior se produjo en el Código Federal de Procedimientos Penales una serie de adiciones previstas en los artículos 278 Bis y 278 Ter al tenor de lo siguiente:

"Capítulo VIII Bis. Comunicaciones privadas entre particulares

Artículo 278 Bis: Las comunicaciones entre particulares podrán ser aportadas voluntariamente a la averiguación previa o al proceso penal, cuando hayan sido obtenidas directamente por alguno de los participantes en la misma.

El Tribunal recibirá las grabaciones o video filmaciones presentadas como prueba por las partes y las agregará al expediente.

Las comunicaciones que obtenga alguno de los participantes con el apoyo de la autoridad, también podrán ser aportadas a la averiguación o al proceso, siempre que conste de manera fehaciente la solicitud previa de apoyo del particular a la autoridad. De ser necesario, la prueba se perfeccionará con las testimoniales o periciales conducentes.

En ningún caso el Ministerio Público o el juez admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley ni la autoridad prestará el apoyo a que se refiere el párrafo anterior cuando se viole dicho deber.

No se viola el deber de confidencialidad cuando se cuente con el consentimiento expreso de la persona con quien se guarda dicho deber.

Las empresas concesionarias y permisionarias del servicio de telecomunicaciones o de Internet, estarán obligadas a colaborar con las autoridades para la obtención de dichas pruebas cuando así lo soliciten. Cualquier omisión o desacato a esta disposición será sancionada por la autoridad, en los términos del artículo 178 del Código Penal Federal.”.[121]

En este precepto del Código Federal de Procedimientos Penales, siguiendo la tesitura de la reforma constitucional mencionada, se permite que las comunicaciones privadas, incluso las que se llevan a cabo por medios informáticos e Internet, puedan ser aportadas en la averiguación previa o en el proceso penal como medios de prueba, e incluso obliga a los concesionarios de telecomunicaciones e Internet a facilitar estas comunicaciones a las autoridades ministeriales o judiciales.

Por ende, debemos reconocer que las comunicaciones privadas llevadas a cabo a través de un medio informático e Internet, pueden ser aportadas a una averiguación previa o a un proceso penal, cuando uno de los participantes de la comunicación, las ofrezca de manera voluntaria.

Ahora bien, siguiendo con el estudio del artículo 16 Constitucional, debemos reconocer que si bien es cierto que la norma constitucional establece como principio que las comunicaciones son inviolables, también es cierto que la propia norma establece las posibilidades de excepción, como el supuesto que vimos anteriormente en donde uno de los participantes puede aportar la comunicación privada y ser considerada válida la comunicación, pero, también se establece la posibilidad de que los jueces federales especializados en cateos, arraigos e intervención de comunicaciones privadas, creados con motivo de la reforma constitucional mencionada, intervengan una comunicación privada llevada a cabo por cualquier medio incluso a través de medios informáticos e Internet.

---

[121] Agenda Penal Federal, 26ª edición, Editorial ISEF, México, 2009, pp. 77-78.

Siguiendo con esta tesitura, de acuerdo al artículo 34 de la Ley de Seguridad Nacional, el Centro de Investigación y Seguridad Nacional está facultado para solicitar la intervención de comunicaciones privadas en materia de seguridad nacional al juez federal, ya que señala lo siguiente:

"Artículo 34. De conformidad con lo dispuesto por el párrafo noveno del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro deberá solicitar en los términos y supuestos previstos por la presente ley, autorización judicial para efectuar intervenciones de comunicaciones privadas en materia de Seguridad Nacional.".[122]

Por su parte, la Ley Federal contra la Delincuencia Organizada, establece toda una regulación sobre las solicitudes de intervención de comunicaciones privadas que puede hacer el Procurador General de la República o la Subprocuraduría de Investigación Especializada en Delincuencia Organizada, sin embargo, el estudio de dicha legislación se llevará a cabo en el siguiente punto.

Asimismo, en el artículo 8º fracción XXIX de la Ley de la Policía Federal se faculta a la policía federal para solicitar por escrito ante el juez federal la autorización para la intervención de comunicaciones privadas, ya que señala:

"Artículo 8. La policía federal tendrá las siguientes atribuciones y obligaciones siguientes:

Fracción XXIX.- Solicitar por escrito ante el juez de control, en términos del capítulo XI de la presente ley, la autorización para la intervención de comunicaciones privadas para la investigación de los delitos. La autoridad judicial competente deberá acordar la solicitud en un plazo no mayor de doce horas a partir de su presentación.".[123]

[122] Ibídem, p. 9.
[123] Ibídem, p. 3.

Como se observa, es muy amplia la posibilidad de intervenir una comunicación privada, incluso aquellas que se llevan a cabo por medios informáticos e Internet, toda vez, que tanto la Constitución como las leyes secundarias facilitan esa posibilidad a diversas autoridades, sobre todo cuando se trata de investigar delitos; no olvidemos que Internet y las computadoras son medios idóneos para la comisión de una gran gama de delitos que se están presentado en la actualidad, que van desde el fraude, la pederastia, la pornografía infantil e incluso el terrorismo, por ende, las autoridades federales en aras de inhibir la delincuencia organizada han abierto la posibilidad de abrir las comunicaciones privadas, con los riesgos que ello implica, porque quien tiene acceso a nuestras comunicaciones privadas tiene acceso a nuestra vida y puede ejercer poder sobre nosotros.

3.7. La Ley Federal contra la Delincuencia Organizada ante la posibilidad de intervenir comunicaciones privadas

La Ley Federal contra la Delincuencia Organizada fue publicada en el Diario Oficial de la Federación el 7 de noviembre de 1996 bajo el auspicio del entonces presidente de la república Ernesto Zedillo Ponce de León y parece ser que desde su creación dicho cuerpo normativo se ha erigido como un sistema de justicia penal totalmente independiente.

Augusto Sánchez Sandoval y Alicia Gónzalez Vidaurri al analizar dicho cuerpo normativo sostuvieron que la Ley Federal contra la Delincuencia Organizada “constituye la creación de una legislación aparte, que pone en acto este nuevo e inconstitucional fuero posmoderno, con principios de derecho que no estaban contenidos en la ley ordinaria.”.[124]

[124] SANCHEZ SANDOVAL, Augusto y Alicia GONZALEZ VIDAURRI. Criminología. México, 2005, p. 197.

Ahora bien, por lo limitado de nuestra investigación, solo haremos alusión a la intervención de comunicaciones privadas hecha en términos del presente cuerpo normativo.

En el título segundo capítulo cuarto de dicha ley se establece la regulación de las órdenes de cateo y de intervención de comunicaciones privadas en los artículos 15 al 28.

En el artículo 16 de la mencionada ley se establece la posibilidad de que el Procurador General de la República o el Subprocurador de Investigación Especializada en Delincuencia Organizada, soliciten la intervención de alguna comunicación privada, lo cual harán por escrito al Juez Federal Especializado en Cateos, Arraigos e Intervención de comunicaciones privadas, circunstanciando el motivo, tiempo, lugar y personas a quienes habrá de intervenirse su comunicación.

Pero es importante mencionar que dicho cuerpo normativo constriñe el objeto de la intervención de la comunicación privada, la cual se podrá realizar de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.[125]

Como se puede observar, la Ley Federal contra la Delincuencia Organizada, habla expresamente que podrán intervenirse comunicaciones privadas llevadas a cabo a través de sistemas o equipos informáticos.

Por su parte, el artículo 17 de dicha ley señala que el juez federal está obligado a resolver sobre la petición de intervención en el término de 12 horas, pero en ningún caso podrá autorizar las intervención cuando se trate de materias

[125] Cfr. Agenda Penal Federal, Ob. Cit., p. 7.

de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

El artículo 20 de dicho cuerpo legal señala que durante la intervención de la comunicación privada, el ministerio público de la federación ordenará la trascripción de aquellas grabaciones que resulten de interés para la averiguación previa y las cotejará en presencia del personal del cuerpo técnico de control de la unidad especializada en delincuencia organizada.

Asimismo, el artículo 22 de la ley menciona que de toda intervención de comunicación se levantará acta circunstanciada por el ministerio público de la federación, que contendrá las fechas de inicio y término de la intervención, un inventario pormenorizado de los documentos, objetos y las cintas de audio o video que contengan sonidos o imágenes captadas durante la misma, la identificación de quienes hayan participado en las diligencias, así como los demás datos que considere relevantes para la investigación.

El artículo 26 de la ley en comento obliga a los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención a colaborar eficientemente con la autoridad competente para el desahogo de dichas diligencias.

Por su parte, los artículos 27 y 28 establecen las sanciones penales para los servidores públicos que intervengan comunicaciones privadas sin la autorización judicial correspondiente o cuando divulguen información relacionada con la intervención de comunicación.

Como se puede apreciar, este cuerpo normativo, da la pauta para que en la investigación de la delincuencia organizada se puedan intervenir comunicaciones privadas que se lleven a cabo a través de sistemas o equipos informáticos, de ahí la importancia de comentar dicho cuerpo normativo.

3.8. Códigos Penales que regulan delitos informáticos en México

Pretender analizar todos los Códigos Penales de la república para ubicar los delitos informáticos en México es una labor muy compleja para un trabajo de investigación tan limitado como éste, por ende, trataremos de echar mano de dos obras que se encargan de analizar tales legislaciones, para observar los datos obtenidos durante sus investigaciones.

De acuerdo a Alberto Enrique Nava Garcés en 1992, el Congreso local del estado de Sinaloa legisló por vez primera en México, sobre los delitos informáticos al tenor de lo siguiente:

"Título Décimo:
Delitos contra el patrimonio
Capítulo V
Delitos Informático
Artículo 217 Comete el delito informático, la persona que dolosamente y sin derecho:

I. Use o entre a una base de datos, sistemas de computadoras 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.".[126]

[126] NAVA GARCÉS, Alberto Enrique. Análisis de los Delitos Informáticos. Editorial Porrúa, México, 2005, p. 76.

Posteriormente el 17 de mayo de 1999 se publicaron en el Diario Oficial de la Federación diversas reformas al Código Penal Federal en donde se incluyen dentro del título noveno capítulo segundo diversos delitos informáticos al tenor de lo siguiente:

“Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

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

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

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

Por su parte, Gabriel Andrés Cámpoli hace un análisis de los diversos Códigos Penales de las entidades federativas, para ubicar aquellas legislaciones que establecen delitos informáticos, resultando lo siguiente:

Código Penal para el Estado de Aguascalientes

Código Penal para el Estado de Baja California

Nuevo Código Penal para el Estado de Colima

Código Penal del Estado de México

Código Penal para el Estado de Guanajuato

Código Penal para el Estado Libre y Soberano de Jalisco

Código Penal para el Estado de Morelos

Código Penal para el Estado de Nuevo León

Código de Defensa Social para el Estado Libre y Soberano de Puebla

Código Penal para el Estado Libre y Soberano de Quintana Roo

Código Penal para el Estado de Sinaloa

Código Penal para el Estado de Tabasco

Código Penal para el Estado de Tamaulipas

Código Penal para el Estado de Yucatán

Código Penal para el Estado de Zacatecas

Nuevo Código Penal para el Distrito Federal[127]

Como se puede observar de este análisis, todavía no existe uniformidad en México sobre la necesidad de legislar los delitos informáticos, porque todavía en muchas entidades no se legisla en la materia, más aún, en las distintas legislaciones se tipifican conductas tan variadas que es difícil encontrar un tipo penal común en todas las legislaciones.

[127] Cfr. CÁMPOLI, Gabriel Andrés, Ob. Cit., p. 102.

CAPÍTULO CUARTO

ANÁLISIS JURÍDICO DE LOS DELITOS INFORMÁTICOS ESTABLECIDOS EN EL CÓDIGO PENAL FEDERAL

4. El derecho penal ante las conductas antisociales de la informática

Como se ha comentado en reiteradas ocasiones, la información y la comunicación existen desde tiempos remotos, como necesidades fundamentales del ser humano y de los grupos sociales donde se desarrolla, pero a medida que avanza la humanidad surgen nuevas formas información y comunicación, de ahí que en la actualidad se hable de una sociedad de la información, en donde la revolución tecnológica de la computadora y sobre todo de las redes informáticas han logrado una conexión total entre los seres humanos.

De ahí que en los últimos años se presente con gran auge en los foros nacionales e internacionales el debate sobre la regulación jurídica de los medios informáticos y sobre todo de Internet, ya que una gama de supuestos con consecuencias jurídicas se han presentado y requieren una regulación integral, por ejemplo, los contratos informáticos, el teletrabajo, la protección de datos personales, la protección de los programas de cómputo, el valor jurídico de los soportes de información, el comercio electrónico, etcétera, pero más aún, el conjunto de situaciones con efectos jurídicos que se pueden presentar en Internet es demasiado basta, por eso, hemos planteado la necesidad de regular todas o la mayoría de las aristas que se presentan con los medios informáticos e Internet.

Pero es la realización de conductas antisociales, a través de los medios informáticos, lo que nos debe preocupar y alarmar, ya que a través de estos medios de comunicación se realizan un gran número de delitos que ponen en tela de juicio los beneficios que traen a la humanidad las computadoras e Internet, por ende, Andrés Cámpoli sostiene que "sabemos por amarga experiencia que los medios informáticos alteran, al menos en parte, los esquemas tradicionales de interacción social y ofrecen nuevas formas de relación interpersonal."[128]

Asimismo, sostiene que esto ha traído como consecuencia necesaria que los medios informáticos sirvan como medios de comisión de delitos ya tipificados en la mayoría de los Códigos Penales, y pueden generar violaciones de bienes jurídicos protegidos, cuya vulnerabilidad, hasta la fecha, no se considera delito, pero que en el consciente popular violan al menos las reglas de convivencia pacífica en la sociedad.

En este contexto, surgen a la vista las palabras de Luis Rodríguez Manzanera quien sostiene que en el mundo actual, tan complejo y cambiante, nacen actitudes y actividades antisociales desconocidas con anterioridad.[129]

Lo anterior toma cabida, ya que si bien es cierto, que a través de los medios informáticos e Internet se pueden cometer delitos ya tipificados en las leyes penales como el fraude y la pornografía infantil, también es cierto que con estos medios de comunicación e información actuales se pueden realizar otras conductas que todavía no se encuentran tipificadas en los Códigos Penales como el acceso ilícito a un sistema de cómputo de un gobernado con el fin de sustraer su información personal o simplemente para dañar el propio equipo, esto a través de la gama de virus informáticos que se han creado.

---

[128] Ibídem, p. 17.
[129] Cfr. RODRIGUEZ MANZANERA, Luis, Criminología, Décimo Tercera edición, Editorial Porrúa, México, 1998, p. 503.

Ahora bien, no debemos pensar que todo lo nuevo o actual que tiene que ver con los medios informáticos, que choque con algunas estructuras actuales, deba ser considerado como delito, pero si debemos punir aquellas conductas que violenten valores fundamentales de una sociedad.

Es por ello que el Derecho Penal, que es considerado como la ultima ratio que tiene el Estado para inhibir el desarrollo de conductas antisociales, tiene que intervenir para proteger aquellos valores que la sociedad considera fundamentales para la convivencia pacífica.[130]

En este sentido, Fernando Castellanos Tena señala que la ley penal consigna los tipos y conmina con penas las conductas formuladas, por ser opuestas a los valores que el Estado está obligado a tutelar.[131]

Por ello, se debe utilizar al ius puniendi con que cuenta el Estado para tratar de contrarrestar el surgimiento de estas conductas antisociales que surgen con el desarrollo de los medios informáticos y que seguirán surgiendo a medida que estas tecnologías sigan avanzando, muestra de ello son los delitos previstos en los artículos 211 Bis-1, 211 Bis-2, 211 Bis-3, 211 Bis-4 y 211 Bis-5 del Código Penal Federal.

4.1. El título noveno del Código Penal Federal y los delitos informáticos

En el presente apartado, analizaremos como se encuentra estructurado el título noveno del Código Penal Federal en donde el legislador mediante reforma publicada en el Diario Oficial de la Federación el 17 de mayo de 1999 inserta el capítulo segundo denominado del “Acceso ilícito a sistemas y equipos de informática”.

---

[130] GARCÍA DOMINGUEZ, Miguel Ángel, Ob. Cit., p. 22.
[131] CASTELLANOS TENA, Fernando, Ob.Cit., p. 167.

De esta manera, tenemos que el título noveno del libro segundo del Código Penal Federal, denominado “Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática”, se integra con dos capítulos, el primero relacionado con la revelación de secretos y el segundo que tiene que ver con el acceso ilícito a sistemas y equipos de informática.

A este respecto, debemos comentar que desconocemos la razón del legislador para incorporar en el título noveno estos delitos informáticos, ya que no hay que soslayar que los diversos títulos que se encuentran en el libro segundo del Código Penal, engloban un conjunto de ilícitos penales que protegen bienes jurídicos en común, por ejemplo, los delitos de robo, fraude, extorsión, abuso de confianza se engloban en el título relacionado con los delitos patrimoniales, y los delitos de violación, abuso sexual, hostigamientos sexual, estupro e incesto se integran en el título denominado de los delitos contra la libertad y el normal desarrollo psicosexual.

Así, los Códigos Penales se ordenan y sistematizan, ya que en cada título se integran los delitos que protegen bienes jurídicos en común, sin embargo, se desconoce el motivo o la razón que tuvo el legislador para integrar dentro del título noveno a los delitos informáticos, ya que no es claro el bien jurídico que se pretende proteger, porque son supuestos totalmente distintos la revelación de secretos y el acceso ilícito a sistemas y equipos de informática.

Es por ello que Alberto Enrique Nava Garcés señala que “regularmente bajo el título que corresponda dentro del Código Penal, se establece el bien jurídico que tutela, por ejemplo, “Delitos contra la vida y la integridad corporal”, “Delitos contra la moral pública y las buenas costumbres” “Delitos contra la salud”, etc., en el caso que nos ocupa, el título señala: “Revelación de secretos y acceso ilícito a sistemas y equipos de informática”. Esto es, no deja en claro cuál es el bien jurídico tutelado, y esto ocurre porque si el fin fuera proteger el patrimonio,

entonces la ubicación de los delitos sería errónea, a pesar de que, dentro de los mismos se establece, entre otras conductas, el daño a los sistemas.”.[132]

Por eso de entrada la ubicación de estos delitos informáticos en la estructura del Código Penal Federal es confusa, porque no se sabe si dicha ubicación atiende a un aspecto práctico del legislador o a una verdadera sistematización que englobe a estos delitos informáticos dentro del título relacionado con la revelación de secretos y por ello, comparta el mismo bien jurídico.

A nuestro parecer, la revelación de secretos y el acceso ilícito a sistemas y equipos de informática, son distintos, por tanto, no comparten la protección del mismo bien jurídico.

De esta manera, con motivo de la reforma mencionada del 17 de mayo de 1999 se adicionan al Código Penal Federal siete preceptos que van del 211 Bis-1 al 211 Bis-7.

Es importante mencionar que con motivo de la reforma del 24 de junio de 2009 publicada en el Diario Oficial de la Federación se adicionó un párrafo al artículo 211 Bis-2 y al artículo 211 Bis-3, en donde se establece respectivamente lo siguiente:

“Artículo 211 Bis-2.- …

…

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

[132] NAVA GARCÉS, Alberto Enrique, Ob. Cit., pp. 81-82.

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

“Artículo 211 Bis-3.- . . .

. . .

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.”.

Como se puede observar, estos nuevos supuestos vienen a agravar la punibilidad de los delitos informáticos, porque ahora cuando se actualizan estos tipos penales la pena privativa de libertad va de cuatro a diez años de prisión, por el simple hecho de que los sistemas o equipos informáticos pertenecen a la seguridad pública.

4.2. El bien jurídico tutelado en los delitos informáticos del Código Penal Federal

Comúnmente se dice que la razón de ser del derecho penal es la protección de bienes jurídicos y que esta razón limita al ius puniendi con que cuenta el Estado, de ahí que un análisis sobre un delito en particular debe partir del estudio del bien jurídico que protege dicho delito.

De ahí la importancia del estudio de los bienes jurídicos, ya que de inicio nos muestra la razón por la cual el legislador crea un delito en particular, por eso

Miguel Ángel García Domínguez señala que el derecho penal, sólo debe utilizarse para la protección de los bienes jurídicos individuales o colectivos más importantes o esenciales para la vida ordenada en comunidad y para los demás bienes están las otras sanciones jurídicas, por ende, sostiene que el derecho penal se caracteriza por proteger los valores fundamentales del orden social.[133]

Por su parte Cesar Augusto Osorio y Nieto menciona que la protección de los bienes jurídicos se lleva a cabo por medio de las normas penales y en el sistema jurídico mexicano, estas normas se encuentran contenidas en el Código Penal Federal, en el Código Penal para el Distrito Federal, en los Códigos Penales de cada entidad federativa y en diversas leyes federales que tipifican conductas delictivas.[134]

Ahora bien, podemos mencionar que existen muchas definiciones sobre el bien jurídico, pero coincidimos con Cesar Augusto Osorio y Nieto cuando afirma que el bien jurídico "representa los valores, los intereses de las personas físicas o morales protegidas por la norma penal mediante la sanción correspondiente."[135]

También resulta interesante la postura de Von Liszt cuando afirma que el bien jurídico es un interés vital del individuo o de la comunidad que es protegido jurídicamente. [136]

Bajo este tenor podemos decir que los bienes jurídicos son intereses fundamentales que deben ser protegidos jurídicamente para mantener el orden social, por ello, si pretendemos analizar los delitos informáticos establecidos en el Código Penal Federal, debemos partir del estudio del bien jurídico que pretenden proteger dichos delitos.

---

[133] Cfr. GARCÍA DOMINGUEZ, Miguel Ángel, Ob. Cit., p. 23.
[134] Cfr. OSORIO Y NIETO, César Augusto. Delitos Federales. Séptima edición, Editorial Porrúa, México, 2005, p. 11.
[135] Ibídem, p. 10.
[136] Cfr. GONZALAZ-SALAS CAMPOS, Raúl, Ob. Cit., p. 23.

Ahora bien, desde que surgieron estos delitos informáticos en México, pocos han sido los autores que han analizado dichos ilícitos, por ello, no logramos vislumbrar algún jurista en nuestro país que nos de luz sobre el bien jurídico tutelado en los delitos previstos en los artículos 211 Bis-1, 211 Bis-2, 211 Bis-3, 211 Bis-4 y 211 Bis-5.

Por eso, con temor a equivocarnos en esta apreciación, lo que se pretende proteger con los delitos informáticos establecidos en el capítulo II del título noveno del Código Penal Federal denominado “Acceso ilícito a sistemas y equipos de informática” es la información contenida en los sistemas o equipos de informática de personas, del Estado, del sistema financiero y de la seguridad pública.

Como consecuencia de lo anterior, podemos decir que el bien jurídico tutelado en estos delitos es la información contenida en los sistemas o equipos de informática.

Lo anterior es así, ya que de la lectura de los cinco ilícitos informáticos se observa que el objetivo común es la protección de la información que se encuentra almacenada en los sistemas y equipos de informática, pero sólo cuando se encuentra protegida por un mecanismo de seguridad o cuando se está autorizado para acceder al sistema informático se realice de manera indebida la modificación, destrucción o pérdida de la información.

Ahora bien, el hecho de que algunos de estos tipos penales estén tan cerrados para proteger solo la información que se encuentra en sistemas o equipos de informática protegidos por un mecanismo de seguridad, es la mayor debilidad de estos ilícitos y es la mayor crítica que podemos hacer a estos tipos penales, porque solo protegen la información protegida por un mecanismo de seguridad, pero deja fuera la información de la mayoría de los gobernados que normalmente no contamos con un mecanismo de seguridad en nuestros equipos o sistemas.

En este sentido, Jesús Antonio Molina Salgado, citado por Alberto Enrique Nava Garcés, comenta al respecto que es tan absurdo que los tipos penales solo protejan la información de los sistemas informáticos protegidos por un mecanismo de seguridad, porque es como si dijéramos que para que se diera el delito de allanamiento de morada es necesario que la casa habitada cuente con un candado, llave, portón o cadena protectora, por ende, sostiene que la justicia no puede reducirse sólo a aquellos quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad y se pregunta ¿o qué acaso el que tu computadora esté conectada al Internet significa que cualquiera puede justificadamente borrar o destruir archivos, sólo porque no está protegida por algún mecanismo de seguridad?.[137]

Asimismo, continúa señalando que el Código Penal no define que debemos entender por mecanismo de seguridad, un password, un candado contra robo, un sistema criptográfico de llave pública, un firewall o simplemente tener la computadora encerrada en un cuarto bajo llave o con un guardia de seguridad, esto al final de cuentas traerá innumerables problemas de interpretación a la hora de que le toque a un juez analizar un caso concreto.

Como se aprecia, no es fácil analizar delitos de nueva creación y muchas hojas pueden llevarnos discutir tan solo el bien jurídico tutelado, cuando no es tan clara la ubicación sistemática de los delitos en algún título del Código Penal, como en el presente caso de los delitos informáticos.

4.3. Análisis del artículo 211 Bis-1 del Código Penal Federal

Como lo hemos comentado, analizar un delito de nueva creación puede resultar difícil, máxime sino hay un apoyo bibliográfico al respecto que coadyuve en el análisis, sin embargo, trataremos de ser lo más objetivos posibles, en este

[137] Cfr. NAVA GARCÉS, Alberto Enrique, Ob. Cit., p. 80.

somero estudio, apoyándonos en los conceptos teóricos de Fernando Castellanos Tena e Irma Griselda Amuchategui Requena, entre otros.

El artículo 211 Bis-1 reza lo siguiente:

"Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.".

En cuanto al párrafo primero, debemos iniciar con los sujetos y los objetos. De acuerdo a Amuchategui Requena el sujeto activo es la persona física que comete el delito y el sujeto pasivo es la persona física o moral sobre quien recae el daño o peligro causado por la conducta del sujeto activo. [138]

De igual manera, distingue al sujeto pasivo de la conducta y al sujeto pasivo del delito, señalando que el pasivo de la conducta es quien resiente la acción del sujeto activo y el pasivo del delito es el titular del bien jurídico afectado.

De esta manera, el sujeto activo que nos indica el tipo penal en estudio es un sujeto activo indeterminado porque menciona la palabra "al que" en este sentido al no establecer ninguna calidad del sujeto activo, cualquier persona física puede cometer dicho ilícito, ya que no señala si es hombre o mujer, o si es servidor público.

[138] Cfr. AMUCHATEGUI REQUENA, Irma Griselda, Ob. Cit., p. 38.

Por su parte, el sujeto pasivo de la conducta y del delito será la persona física o moral, dueña, propietaria o titular de la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

En cuanto a los objetos, jurídico y material, Fernando Castellanos Tena menciona que el objeto material lo constituye la persona o cosa sobre quien recae el daño o peligro y el objeto jurídico es el bien jurídico protegido por la ley.[139]

El tipo penal a estudio, tiene como objeto material los sistemas o equipos de informática que contienen información, porque serán las cosas sobre las que recae el daño.

El objeto jurídico y bien jurídico tutelado, como lo hemos comentado, será la información contenida en los sistemas o equipos de informática que se encuentra protegida por un mecanismo de seguridad.

En cuanto a los verbos núcleos del tipo, tenemos tres: modifique, destruya o provoque pérdida de información. En esta tesitura, tomando en consideración los verbos núcleos, podemos decir que es un delito de acción que genera un resultado material.

El medio comisivo o medio de ejecución, es importante para distinguir este supuesto de los otros ilícitos informáticos, ya que se pide que sea sin autorización.

Ahora bien, el hecho de que este tipo penal señale que la información se encuentre contenida en un sistema o equipo de informática, protegidos por algún mecanismo de seguridad, nos permite visualizar una circunstancia de modo que es difícil de precisar, como se comentó anteriormente, ya que no se señala que debemos entender por un mecanismo de seguridad.

---

[139] Cfr. CASTELLANOS TENA, Fernando, Ob. Cit., p. 152.

En cuanto a la punibilidad, es muy baja, ya que va de seis meses a dos años de prisión y de cien a trescientos días multa.

Con relación a los supuestos del párrafo segundo, lo único que va a variar son los verbos núcleos del tipo ya que son: conozca o copie información. De esta manera, tenemos que en este segundo párrafo, de acuerdo a los verbos núcleos del tipo, el delito va a ser de acción pero el resultado será formal.

También es importante mencionar que la punibilidad se atenúa ya que será de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa, es decir, la mitad de la sanción impuesta a los supuestos del párrafo primero del artículo en estudio.

Como se aprecia, la configuración de estos ilícitos informáticos es cerrada, porque sólo protege la información contenida en equipos o sistemas informáticos protegidos por algún mecanismo de seguridad, pero soslaya un gran número de sistemas informáticos que no cuentan con estos mecanismos de seguridad, además no se precisa que debemos entender por tales mecanismos, ya que no sabemos si son mecanismos físicos o electrónicos.

4.4. Análisis del artículo 211 Bis-2 del Código Penal Federal

El artículo 211 Bis-2 del Código Penal Federal contiene tres párrafos, los dos primeros creados desde la reforma del 17 de mayo de 1999 y el tercero adicionado el 24 de junio de 2009.

Es importante mencionar que los tipos penales de los primeros dos párrafos son casi idénticos con relación al artículo anterior, con la salvedad de que la información contenida en los sistemas y equipos de informática son del Estado, por este motivo la punibilidad será aumentada, como se verá a continuación.

El artículo 211 Bis-2 de la norma sustantiva penal menciona:

“Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.”.

En cuanto al primer párrafo del artículo mencionado tenemos que el sujeto activo es indeterminado porque señala la palabra “al que” y el sujeto pasivo de la conducta será el servidor público que tenga bajo su custodia los sistemas o equipos informáticos y el sujeto pasivo del delito será el Estado.

El objeto jurídico como se identifica con el bien jurídico es la información contenida en un sistema o equipo de informática del Estado protegido por un mecanismo de seguridad y el objeto material serán los sistemas o equipos de informática que contienen información del Estado, y que se encuentran protegidos por un mecanismo de seguridad.

Los verbos núcleos del tipo que establece este tipo penal son: modifique, destruya o provoque pérdida de información, de esta manera, tomando en consideración estos verbos núcleos, podemos decir que este delito puede cometerse vía acción generando un resultado material.

El medio comisivo o medio de ejecución, como ya lo comentamos es muy importante, porque se pide que sea sin autorización.

La circunstancia de modo que está presente en todos estos ilícitos es la protección de los sistemas o equipos informáticos del Estado por algún mecanismo de seguridad.

La punibilidad para estos supuestos se agrava, por el hecho de que los sistemas y equipos de informática pertenecen al Estado, ya que va de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Con relación al párrafo segundo del artículo en estudio también tenemos un sujeto activo indeterminado, un pasivo de la conducta que será el servidor público que tenga bajo su custodia los sistemas informáticos y el pasivo del delito que será el Estado.

Observamos también un objeto jurídico que se identifica con el bien jurídico que es la información contenida en sistemas o equipos de informática del Estado protegidos por algún mecanismo de seguridad, de igual manera, tenemos que el objeto material son los sistemas o equipos informáticos del Estado protegidos por algún mecanismo de seguridad.

Pero la gran variación con relación al párrafo primero son los verbos núcleos del tipo: conozca o copie información. De esta manera, con base en estos supuestos se puede afirmar que el delito será de acción generando un resultado formal.

De igual manera se observa un medio de ejecución o comisivo que es sin autorización y la circunstancia de modo que consiste en que los equipos deben estar protegidos por un mecanismo de seguridad.

La punibilidad será de seis meses a dos años de prisión y de cien a trescientos días multa, por lo que se atenúa con relación al párrafo primero.

Con relación al párrafo tercero, ya no sólo se pide que la información contenida en los sistemas o equipos de informática pertenezca al Estado, sino se exige que tenga que ver con la seguridad pública y por este hecho se va a agravar la punibilidad, como se verá a continuación.

El sujeto activo en este párrafo tercero es indeterminado ya que señala la palabra “a quien” y el sujeto pasivo de la conducta será el servidor público que tenga bajo su custodia los sistemas, equipos o medio de almacenamiento informático, por su parte, el sujeto pasivo del delito seguirá siendo el Estado al ser el titular de la seguridad pública.

El objeto jurídico que se identifica con el bien jurídico es la información en materia de seguridad pública contenida en sistemas, equipos o medios de almacenamiento informático. El objeto material tiene que ver con estos sistemas, equipos o medios de almacenamiento informático. Es importante mencionar que en este tipo penal, se agrega un objeto material, diferente a los otros ilícitos informáticos ya que también se habla del medio de almacenamiento informático y no sólo de sistemas o equipos.

En cuanto a los verbos núcleos del tipo tenemos que son: conozca, obtenga, copie o utilice información. Tomando en consideración estos verbos, podemos decir que los ilícitos se van a cometer vía acción y el resultado va a ser formal.

El medio comisivo o medio de ejecución también estará presente en este tipo penal: sin autorización. De igual manera, la circunstancia de modo: protegidos por algún medio de seguridad. Es menester señalar que en este tipo penal ya no se habla de mecanismo de seguridad sino de medio de seguridad.

En cuanto a la punibilidad se agrava fuertemente con relación a los otros ilícitos informáticos, ya que va de cuatro a diez años de prisión con multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. De igual manera, se establece otra sanción para aquellos sujetos activos que sean o hubieren sido servidores públicos ya que en estos casos también se decretará su destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

4.5. Análisis del artículo 211 Bis-3 del Código Penal Federal

El artículo 211 Bis-3 también se compone de tres párrafos, los primeros dos creados a virtud de la reforma del 17 de mayo de 1999 y el tercero adicionado el 24 de junio de 2009. En estos tipos penales se va a modificar el medio de ejecución y como consecuencia la circunstancia de modo, ya que no se requiere que se realice la acción sin autorización, sino que el sujeto activo va a estar autorizado para acceder a los sistemas y equipos informáticos del Estado, como consecuencia de esto, tampoco se pide en el tipo penal que los equipos y sistemas informáticos estén protegidos por algún mecanismo de seguridad. Esto es la gran diferencia con relación a los supuestos previstos en el artículo anterior.

El artículo 211 Bis-3 del Código Penal Federal señala entre otras cosas lo siguiente:

“Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de

información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación, por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.”.

El tipo penal previsto en el párrafo primero del precepto en estudio menciona un sujeto activo indeterminado porque señala la palabra “al que”. El sujeto pasivo de la conducta será el funcionario que tenga bajo su custodia los sistemas o equipos informáticos del Estado y el pasivo del delito será el propio Estado titular de la información contenida en los equipos o sistemas.

El objeto jurídico como se identifica con el bien jurídico es la información contenida en un sistema o equipo de informática del Estado y el objeto material serán los sistemas o equipos de informática que contienen información del Estado.

En cuanto a los verbos núcleos del tipo que establece este tipo penal son: modifique, destruya o provoque pérdida de información, por ende, estos ilícitos penales se pueden cometer vía acción generando un resultado material.

El medio comisivo o medio de ejecución, como ya lo comentamos, se va a modificar con relación a los tipos penales previstos en los artículos anteriores, ya que en este supuesto el sujeto activo está autorizado para acceder a los sistemas y equipos de informática del Estado.

Como consecuencia de lo anterior, la circunstancia de modo también se modifica, ya que no se exige que los sistemas o equipos informáticos del Estado tengan algún mecanismo de seguridad, sino que ahora se pide que la modificación, destrucción o la provocación de la pérdida de la información se realice de manera indebida.

En cuanto a la punibilidad, se agrava con relación a los preceptos anteriores ya que va de dos a ocho años de prisión y de trescientos a novecientos días multa.

Con relación al párrafo segundo del artículo en estudio, podemos señalar que las únicas diferencias con el tipo penal anterior es el verbo núcleo del tipo y la punibilidad, ya que se pide como verbo núcleo “copie” información y la punibilidad se atenúa porque va de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

En cuanto al párrafo tercero del artículo en comento, se agravará la punibilidad por el hecho de que la información contenida en los sistemas y equipos informáticos pertenece a la seguridad pública.

El sujeto activo en este párrafo tercero es indeterminado y el sujeto pasivo de la conducta será el servidor público que tenga bajo su custodia los sistemas, equipos o medio de almacenamiento informático, por su parte, el sujeto pasivo del delito seguirá siendo el Estado al ser el titular de la seguridad pública.

El objeto jurídico que se identifica con el bien jurídico es la información en materia de seguridad pública contenida en sistemas, equipos o medios de almacenamiento informático. El objeto material tiene que ver con estos sistemas, equipos o medios de almacenamiento informático. Es importante mencionar que en este tipo penal, también se agrega un objeto material, diferente a los otros ilícitos informáticos ya que se habla del medio de almacenamiento informático y no sólo de sistemas o equipos.

En cuanto a los verbos núcleos del tipo tenemos que son: obtenga, copie o utilice información, como consecuencia de lo anterior, podemos decir que los ilícitos se van a cometer vía acción y el resultado va a ser formal.

Con relación al medio comisivo o medio de ejecución, no olvidemos que se modifica con relación a los artículos anteriores, ya que en este supuesto el sujeto activo está autorizado para acceder a los sistemas, equipos o medios de almacenamiento.

Por ende, al estar autorizado, ya no se pide que el equipo o sistema informático tenga un mecanismo de seguridad, sino que ahora se exige como circunstancia de modo que las acciones se realicen indebidamente.

En cuanto a la punibilidad se agrava fuertemente con relación a los otros ilícitos informáticos, ya que va de cuatro a diez años de prisión con multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. De igual manera, se establece una agravante para aquellos sujetos activos que sean o hubieren sido servidores públicos en una institución de seguridad pública, toda vez, que se impondrá hasta una mitad más de la pena impuesta, además destitución e inhabilitación para desempeñarse en otro empleo, puesto, cargo o comisión pública, por un tiempo igual al de la pena impuesta.

4.6. Análisis del artículo 211 Bis-4 del Código Penal Federal

El presente artículo no va a variar mucho con relación a los ilícitos previstos en los artículos 211 Bis-1 y 211 Bis-2 de la norma sustantiva penal en comento, ya que solo se modifica el sujeto pasivo, porque ahora se exige que la información contenida en sistemas o equipos de informática pertenezcan a las instituciones que integran el sistema financiero.

De esta manera, tenemos que el artículo 211 Bis-4 señala lo siguiente:

"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.".

Por su parte, el artículo 211 Bis-6 del Código Penal Federal señala que para los efectos de los artículos 211 Bis-4 y 211 Bis-5, se entiende por instituciones que integran el sistema financiero las mencionadas en el artículo 400 Bis del propio código sustantivo penal.

Ahora bien, el artículo 400 Bis último párrafo señala que:

"Para los mismos efectos, el sistema financiero se encuentra integrado por las instituciones de crédito, de seguros y de fianzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades

financieras de objeto limitado, uniones de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradoras de fondos de retiro y cualquier otro intermediario financiero o cambiario.”.

De ahí la única diferencia con los tipos penales previstos en los artículos 211 Bis-1 y 211 Bis-2 de la norma sustantiva penal federal, ya que la información contenida en sistemas o equipos de informática protegidos por un mecanismo de seguridad pertenecen a las instituciones de crédito, de seguros y de fianzas, a los almacenes generales de depósito, a las arrendadoras financieras, a las sociedades de ahorro y préstamo, etcétera.

Ahora bien, con relación al primer párrafo del artículo 211 Bis-4 en análisis podemos decir que el sujeto activo es indeterminado porque menciona la palabra “al que” en este sentido al no establecer ninguna calidad del sujeto activo, cualquier persona física puede cometer dicho ilícito.

Por su parte, el sujeto pasivo de la conducta y del delito serán las instituciones que integran el sistema financiero, propietarias o titulares de la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

El tipo penal a estudio, tiene como objeto material los sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, porque serán las cosas sobre las que recae el daño.

El objeto jurídico y bien jurídico tutelado, será la información contenida en los sistemas o equipos de informática de las instituciones que integran el sistema financiero que se encuentra protegida por un mecanismo de seguridad.

En cuanto a los verbos núcleos del tipo, tenemos tres: modifique, destruya o provoque pérdida de información. En esta tesitura, tomando en consideración los verbos núcleos, podemos decir que es un delito de acción que genera un resultado material.

Al igual que algunos ilícitos informáticos el medio comisivo o medio de ejecución de este tipo penal es sin autorización.

La circunstancia de modo también está presente en este tipo penal ya que se pide que los sistemas o equipos de informática de las instituciones que integran el sistema financiero estén protegidos por algún mecanismo de seguridad.

En cuanto a la punibilidad, también es muy baja, ya que puede ir de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Con relación a los supuestos del párrafo segundo, lo único que va a variar son los verbos núcleos del tipo ya que son: conozca o copie información contenida en equipos informáticos de las instituciones que integran el sistema financiero, por ende, en este segundo párrafo, de acuerdo a los verbos núcleos del tipo, el delito va a ser de acción pero el resultado será formal.

También es importante mencionar que la punibilidad se atenúa en este supuesto ya que será de tres meses a dos años de prisión y de cincuenta a trescientos días multa, es decir, la mitad de la sanción impuesta a los supuestos del párrafo primero del artículo en estudio.

Como se aprecia, los tipos penales previstos en el artículo 211 Bis-4 del Código Penal Federal, tienen una gran similitud con los tipos penales de los artículos 211 Bis-1 y 211 Bis-2 del código en comento, ya que la única diferencia es que los sistemas o equipos de informática pertenecen a las instituciones que integran el sistema financiero.

4.7. Análisis del artículo 211 Bis-5 del Código Penal Federal

El último de los delitos informáticos es el previsto en el artículo 211 Bis-5 del Código Penal Federal, al cual también se le aplica lo previsto en el artículo 400 Bis de la norma sustantiva penal federal, ya que tiene que ver con la información contenida en sistemas y equipos de informática de las instituciones que integran el sistema financiero.

El mencionado artículo señala:

"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.".

Es importante mencionar que este tipo penal tiene gran similitud con las figuras delictivas previstas en el artículo 211 Bis-3 del propio Código Penal Federal, con la salvedad de que el tipo penal en estudio tiene como objeto material los sistemas y equipos de informática de las instituciones que integran el sistema financiero.

El tipo penal previsto en el párrafo primero del artículo 211 Bis-5 del Código Penal Federal establece un sujeto activo indeterminado porque señala la palabra “al que”. El sujeto pasivo de la conducta será aquella persona que tenga bajo su custodia los sistemas o equipos informáticos de las instituciones que integran el sistema financiero y el pasivo del delito serán las instituciones que integran el sistema financiero.

El objeto jurídico como se identifica con el bien jurídico es la información contenida en un sistema o equipo de informática de las instituciones que integran el sistema financiero y el objeto material serán los sistemas o equipos de informática de las instituciones que integran el sistema financiero.

En cuanto a los verbos núcleos del tipo que establece este tipo penal son: modifique, destruya o provoque pérdida de información, por ende, estos ilícitos penales se pueden cometer vía acción generando un resultado material.

El medio comisivo o medio de ejecución, se va a modificar con relación a algunos delitos informáticos, ya que en este supuesto el sujeto activo está autorizado para acceder a los sistemas y equipos de informática de las instituciones que integran el sistema financiero.

Como consecuencia de lo anterior, la circunstancia de modo también se modifica, ya que no se exige que los sistemas o equipos informáticos de las instituciones que integran el sistema financiero tengan algún mecanismo de seguridad, sino que se pide que la modificación, destrucción o la provocación de la pérdida de la información se realice de manera indebida.

En cuanto a la punibilidad, va de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

En el párrafo segundo del artículo en comento, encontramos que las únicas diferencias con el párrafo anterior es el verbo núcleo del tipo y la punibilidad, ya que se pide como verbo núcleo “copie” información y la punibilidad se atenúa porque va de tres meses a dos años de prisión y de cincuenta a trescientos días multa, pero también se establecen como elementos del tipo penal que el sujeto activo esté autorizado para acceder a los sistemas y equipos de las instituciones que integran el sistema financiero y que copie información de manera indebida.

En cuanto al párrafo tercero del artículo en comento, es aplicable para los dos párrafos anteriores, ya que establece una agravante al mencionar que si los sujetos activos son funcionarios o empleados de las instituciones que integran el sistema financiero, las penas se incrementarán en una mitad.

Por último, el artículo 211 Bis-7 establece otra agravante aplicable para todos los delitos informáticos ya que señala que las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Como se ha podido observar, son pocas las conductas tipificadas como delitos informáticos, pero lo más grave aún es que ninguna protege o tutela la información contenida en sistemas o equipos de cualquier gobernado que no esté protegido por algún mecanismo de seguridad, ya que en estos delitos los sujetos pasivos únicamente pueden ser las instituciones que integran el sistema financiero, el Estado o particulares cuando sus equipos informáticos están protegidos por mecanismos de seguridad.

CONCLUSIONES

PRIMERA: El mundo entero vive informado y comunicado gracias a los avances tecnológicos en materia de informática, tan es así que se presenta en la humanidad el fenómeno de la sociedad de la información en donde los seres humanos vivimos interconectados.

SEGUNDA: Actualmente, Internet se presenta como la red mundial, a la cual todos tenemos acceso y nos proporciona un gran número de servicios y beneficios a toda la humanidad, pero también es el instrumento para cometer un gran número de conductas antisociales en todo el mundo.

TERCERA: El derecho informático es una nueva rama del derecho, que tiene dos objetivos: la regulación de los medios informáticos que da origen al derecho de la informática y la utilización de la informática como un recurso para el desarrollo del derecho, dando cabida a la informática jurídica.

CUARTA: Muchos temas relacionados con los sistemas informáticos e Internet requieren una regulación integral, pero los delitos informáticos adquieren una relevancia importante, porque el desarrollo y surgimiento de conductas antisociales que dañan o ponen en peligro bienes jurídicos es constante en el mundo de los sistemas informáticos e Internet.

QUINTA: En nuestro país, la legislación sobre aspectos informáticos es muy limitada, aunque en los últimos años, se han modificado algunas leyes ya existentes para incorporar los temas informáticos en la legislación mexicana, tal es el caso del Código de Comercio, el Código Civil Federal, la Ley Federal de Protección al Consumidor, la Ley Federal del Derecho de Autor, el Código Federal de Procedimientos Civiles, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, así como la tipificación de ciertas conductas en los Códigos Penales estatales y en el Código Penal Federal, pero aún así son

muy bastas las aristas del mundo de los medios informáticos e Internet que requieren regulación.

SEXTA: En México, el uso de los sistemas informáticos e Internet está protegido por diversos derechos fundamentales establecidos en la norma constitucional como la libertad de expresión, el derecho a la información, a no ser molestado por la autoridad salvo que exista un mandamiento escrito por autoridad competente que funde y motive la causa de su actuar y a la inviolabilidad de las comunicaciones privadas, pero el ejercicio de esos derechos a través de los medios informáticos no puede ser absoluto, toda vez, que la propia norma constitucional los limita cuando atacan la moral, los derechos de terceros, provocan algún delito o perturban el orden público.

SÉPTIMA: El bien jurídico tutelado en los delitos informáticos previstos en el Código Penal Federal, es la información contenida en los sistemas y equipos de informática, según se desprende del análisis de los diversos supuestos que se mencionan en los artículos 211 Bis-1, 211 Bis-2, 211 Bis-3, 211 Bis-4 y 211 Bis-5 del propio cuerpo normativo y no se deduce de la ubicación de tales delitos en el título noveno libro segundo de dicho código.

OCTAVA: Los delitos informáticos previstos en el Código Penal Federal, solo protegen la información contenida en los sistemas y equipos informáticos de los particulares, del Estado y de las instituciones que integran el sistema financiero, pero cuando dichos equipos y sistemas se encuentran protegidos por algún mecanismo de seguridad, pero soslaya a todas las demás personas cuyos equipos o sistemas informáticos carecen de tal mecanismo de seguridad.

PROPUESTA

Es indudable que los medios informáticos causan un gran interés para los juristas, ya que los temas de regulación son bastante amplios y los mismos no han sido analizados con la amplitud que requieren, de ahí el gran interés por elaborar este trabajo de investigación, ya que los delitos informáticos son un tema de actualidad que deben ser analizados a la luz de las normas constitucionales y de los distintos Códigos Penales que hay en México.

Nuestra legislación penal ha pretendido regular estos delitos informáticos, pero su campo de acción ha sido muy limitado, tan es así que el Código Penal Federal establece solo siete artículos relacionados con la modificación, destrucción o pérdida de información contenida en sistemas informáticos y lo mismo sucede con los distintos códigos penales de los estados, ya que únicamente toman algunos aspectos relacionados con la delincuencia informática.

Por ende, proponemos la unificación de criterios para legislar los delitos informáticos y que sea el Congreso de la Unión el facultado para establecer los delitos relacionados con los equipos y sistemas informáticos e Internet en el Código Penal Federal, haciendo un estudio exhaustivo e integrador de todas aquellas conductas que violentan bienes jurídicos y que toman a la computadora como un instrumento u objeto del delito, esto con el fin de que los tipos penales en materia informática queden unificados y así evitar la diversidad normativa en la materia.

Ahora bien, muchos son los temas relacionados con los sistemas informáticos e Internet que requieren regulación, por ende, también se propone que todo lo relacionado con la computación, informática e Internet sean legislados exclusivamente por el Congreso de la Unión, para ello, será menester establecer una reforma al artículo 73 Constitucional para establecer la facultad del Congreso de la Unión para legislar en materia de informática e Internet, con el fin de evitar

contradicciones normativas o lagunas legales que pudiesen presentarse en las leyes locales.

Para lograr lo anterior, las autoridades mexicanas deben conformar un grupo interdisciplinario que haga las propuestas necesarias para una buena regulación de todos estos temas, en donde se vean todas las aristas que implica el uso de la informática e Internet en la sociedad mexicana.

Por último, proponemos que las conductas tipificadas en el Código Penal Federal en los artículos 211 Bis-1, 211 Bis-2 y 211 Bis-4 integren cualquier equipo o sistema de informática y no sólo a aquellos que se encuentren protegidos por un mecanismo de seguridad o que pertenezcan al Estado o a las instituciones que integran el sistema financiero, porque es indudable que la mayoría de los habitantes en este país, no contamos con ningún mecanismo de seguridad en nuestros sistemas o equipos de informática, por tanto, estamos fuera del marco de protección del Código Penal Federal y cualquiera pudiese modificar, destruir, perder, conocer o copiar nuestra información contenida en nuestros equipos o sistemas de informática y no se violentaría ningún bien jurídico.

También es importante que se presente una interpretación auténtica o legislativa por parte del legislador, para que mediante una adición al Código Penal Federal, señale con precisión que debemos entender como un mecanismo de seguridad en los sistemas o equipos de informática, ya que hasta este momento no sabemos si el legislador quiso hacer referencia a mecanismos físicos o electrónicos.

Estas propuestas aunque someras, son importantes para un mejor desarrollo de los sistemas informáticos e Internet.

BIBLIOGRAFIA

1. DOCTRINAL:

1.- AMUCHATEGUI REQUENA, Griselda I. Derecho penal. Editorial Oxford, México, 2005.

2.- AZPILCUETA, Hermilio Tomás. Derecho Informático. Editorial Abeledo-Perrot, Argentina.

3.- BARRIOS GARRIDO, Gabriela, (et al) Internet y derecho en México. Editorial Mcgraw-Hill, México, 1998.

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

5.- Delitos informáticos en la legislación mexicana. Editorial Instituto Nacional de Ciencias Penales, México, 2005, p. 27.

6.- CASTELLANOS TENA, Fernando. Lineamientos elementales de derecho penal. Octava edición, Editorial Porrúa, México, 1974.

7.- FALCON, Enrique M. ¿Qué es la informática jurídica? Editorial Abeledo-Perrot, Argentina, 1992.

8.- FERNANDEZ DELPECH, Horacio. Internet: su problemática jurídica. Editorial Abeledo-Perrot, Argentina, 2001.

9.- FERNANDEZ RODRIGUEZ, José Julio. Lo público y lo privado en Internet. Editorial UNAM, México, 2004.

10.- FIX FIERRO, Héctor. Informática y documentación jurídica, Segunda edición, UNAM, México, 1996.

11.- GARCÍA DOMÍNGUEZ, Miguel Ángel. Los Delitos Especiales Federales. Editorial Trillas, México, 1987.

12.- GENIS, Alfredo. Fraude ¿cibernético?. Política Criminal, Coordinador Augusto, SANCHEZ SANDOVAL, Editorial UNAM, 2003.

13.- GOMEZ VIEITES, Alvaro y Manuel, VELOSO ESPIÑEIRA. Redes de Computadoras e Internet. Editorial Alfaomega-Rama, México, 2003.

14.- GONZÁLEZ-SALAS CAMPOS, Raúl. La teoría del bien jurídico en el derecho penal. Segunda edición, Editorial Oxford, México, 2001.

15.- GONZÁLEZ LÓPEZ, Oscar Rodrigo. Internet para la empresa. Editorial Anaya multimedia, España, 2003.

16.- GUIBOURG, Ricardo A. (et al) Manual de informática jurídica. Editorial Astrea, Argentina, 1996.

17.- HERNÁNDEZ, Ricardo y Luz María del POZO. Informática en Derecho. Editorial Trillas, México, 1992.

18.- JIMENEZ DE ASÚA, Luis. Tratado de derecho penal. Tomo I, Quinta edición, Editorial Losada, Argentina.

19.- LITTLEJON SHINDER, Debra. Prevención y detección de delitos informáticos. Editorial Anaya, España, 2002.

20.- NAVA GARCÉS, Alberto Enrique. Análisis de los delitos informáticos. Editorial Porrúa, México, 2005.

21.- NAVARRO ISLA, Jorge. Tecnologías de la Información y de las Comunicaciones: aspectos legales. Editorial Porrúa-ITAM, México, 2005.

22.- OSORIO Y NIETO, César Augusto. Delitos Federales. Séptima edición, Editorial Porrúa, México, 2005.

23.- PALAZZI, Pablo Andrés. Delitos Informáticos. Editorial Ad hoc, Argentina, 2000.

24.- PARDINI, Anibal A., Derecho de Internet. Editorial La Rocca, Argentina, 2002.

25.- PÉREZ LUÑO, Antonio-Enrique. Manual de informática y derecho, Editorial Ariel, México, 1996.

26.- RABASA, Emilio O y Gloria CABALLERO. Mexicano: esta es tú Constitución. Editorial Cámara de Diputados, México, 1984.

27.- RIBAS ALEJANDRO, Javier. Aspectos Jurídicos del Comercio Electrónico en Internet. Segunda edición, Editorial Aranzadi, España, 2003.

28.- RÍOS ESTAVILLO, Juan José. Derecho e Informática en México. Editorial UNAM, México, 1997.

29.- RODAO, Jesús de Marcelo. Virus de Sistemas Informáticos e Internet. Editorial Alfaomega, México, 2000.

30.- RODRIGUEZ MANZANERA, Luis, Criminología. Décimo Tercera edición, Editorial Porrúa, México, 1998.

31.- SÁNCHEZ ALMEIDA, Carlos y Javier, MAESTRE RODRÍGUEZ. La ley de Internet. Editorial Servidoc, España, 2002.

32.- SANCHEZ SANDOVAL, Augusto y Alicia GONZALEZ VIDAURRI. Criminología. México, 2005.

33.- TELLEZ VALDEZ, Julio. Derecho informático, Tercera edición, Editorial Mc Graw Hill, México, 2005.

34.- I Congreso Iberoamericano de Informática Jurídica (memorias) Santo Domingo, 29 de octubre a 2 de noviembre de 1984, Editorial Centro Regional del IBI para la enseñanza de la informática.

35.- Delitos no convencionales. Compilador Julio B.J. Maier, Editorial del Puerto, Argentina.

36.- Derecho Internacional de los Derechos Humanos. Editorial Oficina en Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Colombia, 2004.

37.- Diccionario Jurídico Mexicano. Segunda edición, Editorial UNAM-PORRÚA, México, 1988.

38.- Temas Selectos de Derecho Informático. Coord. Eduardo Castellanos Hernández, Editorial Secretaría de Gobernación, México, 2006.

2. LEGISLACIÓN:

1. Agenda Penal Federal, Vigésimo Sexta edición, Editorial ISEF, México, 2009.
2. Código Penal Para el Estado de Aguascalientes, Editorial Sista, México, 2009.
3. Código Penal Para el Estado de Sinaloa, Editorial Sista, México, 2009.
4. Constitución Política de los Estados Unidos Mexicanos, 50ª edición, Editorial Sista, México, 2010.

3. FUENTES ELECTRÓNICAS:

1.- Arquitectura (elementos básicos de una computadora) http://es.wikipedia.org/wiki/computadora

2.- Breve historia de la informática. http://www.monografias.com/trabajos10/recped/recped.shtml

3.- COMPUTADORA http://es.wikipedia.org/wiki/computadora

4.- Cumbre Mundial sobre la Sociedad de la Información Ginebra 2003. http://www.itu.int/wsis/index-es.html

5.- Cumbre Mundial sobre la Sociedad de la Información Túnez 2005. http://www.itu.int/wsis/index-es.html

6.- Cibernética. http://es.wikipedia.org/wiki/Cibern%C3%A9tica

7.- CHAVEZ TORRES, Anivar. http://www.monografias.com/trabajos11/curinfa/curinfa.shtml

8.- Derecho Informático. http://es.wikipedia.org/wiki/Derecho_inform%C3%Altico

9.- Delitos Informáticos. http://www.monografias.com/trabajos6/delin/delin.shtml

10.- Historia de la computación. http://es.wikipedia.org/wiki/Historia_de_la_computaci%C3%B3n

11.- Historia de la computación. http://www.monografias.com/trabajos/histocomp/histocomp.shtml

12.- Historia computadora. http://www.maestrosdelweb.com/editorial/compuhis/

13.- Historia de Internet. http://es.wikipedia.org/wiki/Historia_de_Internet

14.- Historia del virus. http://www.perantivirus.com/sosvirus/general/histovir.html

15.http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/redes.htm

16.http://www.microsoft.com/latam/ahtome/security/viruses/intro_viruses_what.mspx

17.- http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml

18.- http://www.albanet.com.mx/artículos/NETIQUETTE.html

19.- Informática. http://es.wikipedia.org/wiki/Portal:Inform%C3%A1tica

20.- Informática. http://www.monografias.com/trabajos11/curinfa/curinfa.shtml

21.- MACHADO LA TORRE, Jorge. http://www.jorgemachado.net/content/view/52/1/

22.- PEÑARANDA QUINTERO, Héctor Ramón. Naturaleza jurídica del derecho informático como rama autónoma del derecho. http://www.monografías.com/trabajos23/juridica-informatica/juridica-informatica.shtml

23.- ¿Qué es exactamente un virus? http://www.geocities.com/ogmg.rm/QueSon.html

24.- Red de computadoras. http://es.wikipedia.org/wiki/Red_de_computadoras

25.- Redes informáticas. http://es.encarta.msn.com/encyclopedia_761567995_2/Red_(informática).html