UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"ACATLAN"

ANALISIS DE LA NORMATIVIDAD INTERNACIONAL SOBRE EL CIBERCRIMEN Y LA POSTURA MEXICANA

T E S I S

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

ERIKA CERVANTES GALICIA

ASESOR: LIC. SAUL MANDUJANO RUBIO

MARZO DE 2003

AGRADEZCO:

A Dios, por permitirme culminar este sueño, dándome la fuerza que me inspira a superarme y a luchar por lo que quiero. Gracias por tu amor y ayuda incondicional.

A mis PADRES, por el amor, apoyo y sacrificio que en todo momento me han brindado sin reserva y que hacen posible que el día de hoy pueda concluir satisfactoriamente una etapa importante en mi vida.

Deseo dedicar especialmente el presente trabajo a mis hermanas, NANCY, AUREA y MONTSE, por estar conmigo siempre y ser mis mejores amigas. Gracias por el apoyo, cuidados y cariño que siempre me han manifestado.

A todos aquellos amigos que siempre han tenido para mí buenos deseos y palabras de aliento, que comparten conmigo los triunfos y fracasos y que de alguna forma me ayudaron para alcanzar esta meta. Gracias por su amistad.

Al Lic. SÁUL MANDUJANO RUBIO, por su tiempo, apoyo y conocimientos en la realización del presente trabajo de investigación.

A los miembros de mi Sínodo:

Lic. MARIO ROSALES BETANCOURT
Lic. SAUL MANDUJANO RUBIO
Lic. JOSE ARTURO ESPINOZA RAMIREZ
Lic. MARTIN GARCIA MARTINEZ
Lic. JUAN JOSE LOPEZ TAPIA

Por la disposición, asesoría y atención brindada.

A la UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, por darme la oportunidad de adquirir una formación académica integral, concediéndome la posibilidad de servir a la sociedad.

ÍNDICE

INTRODUCCIÓN

En la sociedad contemporánea, la tecnología se ha convertido en imperativo. Vivimos la era de la información, en ese sentido, la información ha cambiado fundamentalmente a la sociedad y seguramente continuara haciéndolo en el futuro. Si bien, originalmente, sólo algunos sectores específicos de la sociedad habían racionalizado sus procedimientos de trabajo con la ayuda de la tecnología de la información, en la actualidad, prácticamente todos los sectores de la sociedad, han sido afectados. La tecnología de la información, de un modo o de otro, ha invadido la mayoría de los aspectos de las actividades humanas. El uso generalizado del correo electrónico y del acceso a través de Internet a numerosos sitios Web son ejemplos de estos desarrollos.

Precisamente, debido al uso generalizado de los medios informáticos se suscitaron conductas indebidas vinculadas a ellos, dando lugar a nuevos tipos de delitos, así como a la comisión de delitos tradicionales mediante el uso de las nuevas tecnologías. Por otra parte, las consecuencias del comportamiento delictivo llegan más lejos que antes, no están restringidas por límites geográficos o fronteras nacionales. La reciente difusión de virus informáticos, perjudiciales para todo el mundo, constituye una prueba de esta realidad. Ante ese panorama, las medidas técnicas para proteger los sistemas informáticos necesitan ser implementadas

PAGINACION

DISCONTINUA

conjuntamente con las de carácter legal para prevenir e impedir los comportamientos delictivos.

Indudablemente, el desafío de las nuevas tecnologías para el campo del derecho es más apremiante, principalmente debido a factores como: la información y las comunicaciones fluyen más fácilmente alrededor del mundo; las fronteras no constituyen límites para este caudal; los delincuentes se encuentran cada vez menos en los lugares donde sus actos producen efectos; las leyes nacionales en general están confinadas a un territorio específico. Consecuentemente, las soluciones a los problemas planteados deben ser abordadas por el derecho internacional y necesitan de la adopción de instrumentos legales internacionales.

En el ámbito del derecho internacional, el tema de los delitos informáticos es atendido en diversos foros internacionales, en ellos se discute la manera de normar la tipificación y persecución de tales ilícitos. Debido a representar uno de los instrumentos jurídicos más acabados en la materia, la presente investigación se apoyará particularmente en el Convenio Preliminar sobre Delitos Informáticos auspiciado por el Comité para la Prevención del Delito dependiente del Consejo Europeo.

Conviene señalar que este trabajo recepcional no es de corte penalista, si son abordados aspectos generales de los delitos informáticos y su tipificación en el

derecho mexicano, no es suficiente para ubicarlo en el terreno del derecho penal, la referencia obedece a la necesidad de brindar los elementos necesarios para comprender la magnitud del problema y entender la finalidad de los convenios internacionales específicos.

Parte medular de la investigación, es describir las características de la normatividad internacional alusiva a los delitos informáticos. Considerando que algunos sistemas jurídicos muestran mayores avances que otros, sobresaliendo la tarea de naciones europeas, durante el desarrollo del trabajo se exponen aspectos trascendentes de dicha regulación. Sin buscar elaborar un estudio de derecho comparado, la sola mención de elementos jurídicos extranjeros permite visualizar el rezago aún presente en la legislación nacional.

Precisamente, para ubicar el reto del derecho mexicano en cuanto a los delitos informáticos, la revisión del convenio internacional mencionado, indicará las circunstancias que deberán tomarse en cuenta para tipificar y castigar los ilícitos electrónicos. Originado en Europa, el instrumento materia de análisis, revela de manera sobresaliente la labor de las naciones del viejo continente, una de las más destacadas en el planeta.

No cabe duda que en el derecho nacional, importantes logros se han conseguido respecto a la tipificación y persecución de los delitos informáticos. Por

supuesto, lo mismo que sucede en otras naciones, la tarea está muy lejos de concluirse en virtud de la dinámica de las conductas ilícitas relacionadas con los medios electrónicos. Recientemente, se anunció la creación en nuestro país de una instancia dentro de la Policía Federal Preventiva encargada de perseguir los delitos informáticos, la denominada Ciberpolicía, requerirá para su adecuado funcionamiento, que la normatividad interna se desarrolle aún más efectivamente.

CAPITULO I

SOBRE LA PROBLEMATICA DEL USO INDEBIDO DE LOS MEDIOS ELECTRONICOS.

CAPITULO I.- SOBRE LA PROBLEMATICA DEL USO INDEBIDO DE LOS MEDIOS ELECTRONICOS.

1.1. ASPECTOS GENERALES DEL USO INDEBIDO DE LOS MEDIOS ELECTRONICOS.

Como medio propicio para realizar los delitos informáticos, se encuentra la red de redes ya que Internet es un recurso para intercambiar información que puede ser empleado con fines diversos. Igual que hay quienes insultan y amenazan por vía telefónica, el correo electrónico puede ser empleado para amagar y atemorizar. De la misma manera que en la radio o la televisión es posible anunciar artículos cuya venta llega a constituir un fraude a los consumidores, en la red de redes hay estafas, a través de ella, pueden presentarse faltas que hace tiempo son padecidas en nuestras sociedades y, de manera más amplia, por el género humano.

El correo electrónico, por ejemplo, puede ser utilizado para vender estupefacientes o como vía para el lavado de dinero. En las tiendas electrónicas, con su tarjeta bancaria, los compradores pueden pagar artículos que luego resultan de mala calidad o que nunca reciben. Ésos no son delitos debidos a Internet, la cual simplemente es empleada para ilícitos que, quizá de todos modos, serían realizados o

han sido tipificados antes de que existiera la tecnología que hace posible la comunicación.

Internet, igual que todo medio de comunicación y todo espacio abierto a la interacción pública, ha sido empleada para propagar contenidos cuya divulgación, y antes su creación, son delictivos (por ejemplo y de manera destacada, la utilización de niños y niñas en imágenes de carácter pornográfico). Hay delitos que aparentemente sólo se cometen a través de las redes electrónicas, como la desviación de fondos de una cuenta bancaria a otra mediante la intromisión de algún especialista en informática en las bases de datos de una institución financiera. Pero aunque tecnológicamente sofisticadas, ésas son transgresiones que ya ocurrían con otros métodos, antes de Internet. El fraude y el robo siempre han existido.

De constante cambio, el mundo se transforma permanentemente. Para algunos está en marcha una tercera revolución, semejante a la agraria (primera) con 10,000 años de antigüedad que permitió al hombre hacer vida sedentaria, la industrial (segunda) con 200 años facilitó la producción en masa: la tercera consiste en la revolución informática, tiene por signo la computadora y muy probablemente dirigida

a crear la sociedad del conocimiento. Apenas comienza y se desarrollará en el siglo XXI.[1]

Sin necesidad de exhaustivo análisis, podemos percibir una aceptación generalizada de la informática como una de las conquistas decisivas de la sociedad post-industrial de nuestro tiempo. Las últimas tres décadas han sido espectadoras privilegiadas de una verdadera revolución en el desarrollo tecnológico, trastocando estilos de vida, derrumbando virtualmente fronteras estatales y potencializando las posibilidades del hombre en todos sus ámbitos de actuación, todo ello de la mano del nacimiento de las computadoras y su desarrollo astronómico.

Como herramienta, la computadora es instrumento extraordinario. Cualquier individuo provisto de una computadora personal, una línea telefónica, un modem, esta conectado al mundo y accede a los sistemas de redes de compañías, bancos, organismos de seguridad, organizaciones internacionales, dependencias públicas y otros. El empleo de la computación ofrece enormes ventajas al usuario, el decide la finalidad perseguida con el uso de la computadora.

Con multiplicidad de campos de actuación, el empleo de los sistemas informáticos puede realizarse en forma benéfica o nociva. Precisamente el uso

[1]ZAVALA, Antelmo. "El impacto social de la informática jurídica en México". Tesis. México. UNAM. 1996.

generalizado e indiscriminado de los sistemas telemáticos ha puesto en escena un amplio catálogo de abusos, propiciando el empleo indebido de este medio. El desarrollo de los medios informáticos ha permitido la generación de nuevos comportamientos antisociales y criminales sustentados ante el vigoroso avance de la tecnología informática que, por la magnitud de los valores e intereses en juego, exige que el Estado, en la formulación de sus políticas criminales, se vea en la necesidad de definir nuevos delitos.

En los tiempos que corren, no se pone en tela de juicio la existencia sofisticada de complejas relaciones entre el avance del campo informático y las dificultades que acarrea nuestra normatividad. Ha hecho su aparición un moderno tipo de delincuencia capaz de generar problemas adicionales al derecho penal y la administración de justicia. Se trata de una delincuencia inteligente con posibilidad de poner en jaque la seguridad pública y económica de un país, con el simple hecho de invadir dolosamente las redes informáticas.

Por sus particulares características, el uso indebido de los medios informáticos significa un auténtico desafío jurídico. Ese empleo indebido de la informática involucra a personas de alto nivel de inteligencia y educación, sujetos activos versátiles y escapadizos para los tradicionales medios de persecución del

delito. Por otra parte, la extraterritorialidad e intemporalidad de las acciones requeridas por el uso indebido de los medios informáticos, habida cuenta de las amplias posibilidades de la tecnología como coadyuvante para la perfección de conductas delictivas, revelan inadaptados los métodos y medios hasta ahora aplicados en la investigación, persecución y represión de actividades ilícitas.

En manos de potenciales delincuentes, el cúmulo de información produce una seducción irrefrenable para la comisión de ilícitos. La metodología delictual casi indetectable para los organismos de control y seguridad, se ha convertido en el medio para la comisión de añejos delitos regulados desde hace tiempo en el ordenamiento penal. Pero eso no es todo, las modalidades delictivas se manifiestan en acciones que inciden sobre nuevos ilícitos. Este último tipo de modalidad delictual se encuentra en un estado de auge peligroso, la manipulación indebida de los medios informáticos ha convertido a la computadora en objeto del delito. Igualmente, su utilización como medio para la perpetración de delitos la ha transformado en herramienta delictual abandonada al libre albedrío de los seducidos delincuentes.[2]

Ante la situación actual, deben analizarse las elaboraciones teóricas que sostienen el nacimiento de una nueva categoría delictual. La tipicidad previa y la

[2] GARELLI, M., La ley Actualidad, La delincuencia informática, Año LXIII, No. 49, Buenos Aires 1999.

prohibición de la analogía en materia penal, imponen acuñar una tipología especial delictiva que enmarque a la delincuencia informática como una realidad delictiva autónoma. Autores sudamericanos sostienen la elaboración de una teoría general del delito informático y legislación complementaria del Código Penal que en forma específica contemple los mismos.

Debido a que una gran porción de la criminalidad informática revela estructura similar a la de tipos delictivos ya contemplados en la legislación penal, apareciendo en todo caso el ordenador como instrumento para la comisión de delitos, entre la doctrina, aún existen opiniones que entienden a la ilicitud en los sistemas informáticos como el nacimiento de nuevas formas de perpetrar viejos ilícitos. Niegan se trate de una nueva categoría delictiva, refiriéndose a la comisión de ilícitos con caracterización y existencia autónoma desde tiempo considerable. No obstante, los partidarios de esta idea se han bifurcado en la estimación de la solución conveniente para el tratamiento de estas nuevas modalidades de ilicitudes antiguas. Algunos afirman que la actual estructura de la legislación penal es suficiente para contener los embates del avance técnico en el campo de los sistemas informáticos. Otros, por la ausencia de elasticidad en el marco jurídico preexistente, consideran

conveniente sancionar normas legales específicas que contemplen con precisión la actividad delictiva dentro del sector informático.[3]

Apreciando la metodología delictual casi indetectable para los organismos de control y seguridad, la informática ha propiciado la comisión de ilícitos que carecen de antecedente en la legislación penal vigente. La existencia de conductas penalmente reprochables, solo concebidas en relación a un sistema informático, ha generado en la doctrina posiciones disidentes a las manifestadas en el párrafo anterior. Por ese motivo, un grupo importante de autores entiende aconsejable la tipificación específica del accionar del delincuente informático.

Criminológicamente, la delincuencia informática presenta dificultades adicionales para su persecución en relación con la delincuencia tradicional. La rapidez en la comisión del ilícito, su realización a distancia, la complejidad para fijar la autoría, la facilidad para encubrir el hecho y borrar las pruebas pertinentes, los contratiempos para determinar el daño y su cuantificación, la dificultad en la fijación de los elementos del cuerpo del delito y la determinación del bien jurídico tutelado, que a la postre conllevan a las absoluciones o violación del principio de legalidad,

[3] ARTEGA S., Alberto. "El delito informático: algunas consideraciones jurídicas penales" Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela. 1987. Caracas, Venezuela. P. 125-133.

obligan a estimar que la informática no solo es medio utilizado por el sujeto para la comisión del delito, es acaso más, objeto de la perpetración del ilícito.[4]

Partidarios de una concepción amplia del delito informático y su regulación específica, estimando a la informática medio y objeto en la comisión de ilícitos, apreciamos altamente recomendable generar ágil respuesta del sistema jurídico para la prevención y punición de la delincuencia telemática. Desarrollar una teoría general del delito informático que brinde definición integral del ilícito y comprenda la singular estructura de un sistema informático, de los sujetos activos de esta clase de delito y las modalidades técnicas para la realización de ilícitos, los caracteres que asume la ilicitud informática respecto su contrariada fase probatoria, la intemporalidad y extraterritorialidad propias de estas conductas, la descripción de tipos específicos de imposible confusión a las figuras tradicionales, incluso la interpretación correcta del resultado legislativo y su atinada persecución, es requerimiento inaplazable.

1.2. CONCEPTO Y CARACTERÍSTICAS DEL DELITO INFORMATICO.

[4] CEBALLOS DE LA MORA, C., El delito informático, Estudios Jurídicos, Universidad Intercontinental, Revista semestral, No.14/15, México 2001, p.p. 109-130.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar en México, el autor Julio Téllez Valdez menciona, "Dar un concepto sobre delitos informáticos puede no resultar fácil. En su acepción tradicional, la denominación "delitos" alude a acciones típicas contempladas en textos jurídicos-penales, de tal suerte, se requeriría que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, no ha sido objeto de tipificación aún; sin embargo, por la necesidad, emplearemos dicha alusión, aunque se distinga lo típico y atípico".

Dependiendo del caso, los delitos informáticos son actitudes ilícitas que tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico).[5]

[5] TELLEZ Valdez, Julio. **Derecho Informático.** Edit. Mc Graw Hill. 2ª ed. México, 1996. Pp. 103-104.

Ciertos autores consideran que el delito informático, no es más que el delito cometido bajo el empleo de medios informáticos, es decir, constituyen nuevas formas de comisión de conductas ya descritas penalmente, rechazando la existencia de un bien jurídico autónomo para esta clase de delitos. Otro sector de la doctrina, estima que el delito informático tiene un contenido propio, afectando así un nuevo interés social cuyo reconocimiento legislativo urge, diferenciando así entre delitos computacionales, como nuevas formas comisivas de delitos; y delitos informáticos, aquellos que afectan el novísimo bien jurídico penal propuesto, "la información". Finalmente, existe una tercera vertiente, defendida por la doctrina de habla inglesa, que hace una diferencia tripartita en que la informática aparece como medio para cometer delitos tradicionales, como fin en sí misma y como medio de prueba.

Es el segundo sector, es decir, el que diferencia entre delitos computacionales y delitos informáticos en el que se ubica la postura mayoritaria y en ese sentido, "el delito electrónico es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin. En un significado estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[6]

[6]LIMA, Ma. de la Luz. "Delitos Electrónicos" Criminalia, México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984. Pp.100.

La definición aportada por la actual Subprocuradora María de la Luz Lima Malvido, se adhiere a la de otros autores como Pérez Luño, Jijena Leiva y Téllez Valdez, quienes hacen una distinción entre el uso de la informática como medio novedoso para afectar bienes jurídicos reconocidos penalmente, lo que se ha denominado "delito computacional" y el "delito informático", que en sentido estricto, es aquella conducta que afecta un nuevo interés social, íntimamente ligado al tratamiento de la información.

Existen otras definiciones en las que el llamado delito informático no constituye una nueva categoría delictiva, los hechos ilícitos que se cometen mediante el empleo del ordenador son, en principio, los mismos que desde hace milenios las sociedades han castigado de una forma o de otra. Esta postura es propuesta por autores como Guibourg, Alende, Campanella, Viega Rodríguez y Núñez Ponce.

Un tercer sector minoritario, donde destacan autores como Charney, Alexánder, Steele, Parker y Holder, consideran que el uso de computadoras se puede manifestar de tres maneras: en la primera, el ordenador puede ser objeto de la ofensa; en la segunda, la computadora puede ser "herramienta" del delito, esto ocurre, según indican los autores afiliados a esta posición, cuando el sujeto activo utiliza el

ordenador para facilitar la comisión de delitos tradicionales, finalmente, en la tercera, las computadoras resultan incidentales en los delitos, en la medida que contienen evidencias de los delitos.

Pretendiendo precisar el significado de los delitos informáticos, es conveniente destacar sus características principales, encontrando las siguientes:

1.- La delincuencia informática se comete en el ciberespacio, no se detiene ante las fronteras nacionales o convencionales, generando con esto la extraterritorialidad e intemporalidad de las acciones cometidas por el uso indebido de los medios electrónicos.

2.- Se requieren segundos para obtener los resultados deseados, sin importar sus consecuencias, las repercusiones pueden darse en la casa del vecino o en el otro lado del mundo.

3.- Puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador en el mundo.

4.- Existe dificultad para la investigación y persecución de dichos ilícitos debido al grado de sofisticación empleado, siendo posible eliminar cualquier evidencia o sospecha.

5.- Conforme las computadoras, la informática, los sistemas computacionales y las telecomunicaciones son más accesibles al común de la población, cualquier persona con aceptables conocimientos de informática y una computadora, es capaz de cometer desde el más simple hasta el más complejo de los actos ilícitos, tipificado o no en la legislación nacional, extranjera o internacional.

Otro aspecto sobresaliente a considerar, es el sujeto que realiza la conducta delictiva. Anteriormente, se estimaba que el sujeto activo en los delitos informáticos debía ser experto en la materia y dotado de cierta genialidad. Ese atributo ha desaparecido, cualquier persona con ciertos conocimientos informáticos puede delinquir, le basta con la intención de hacerlo.

Existe división en los criterios sobre las actitudes y características del sujeto activo, unos hacen alusión a conocimientos en el manejo de los sistemas informáticos, su actividad laboral gira alrededor de la informática, o bien tiene cierto

grado de habilidad en el manejo de las computadoras, el software y los sistemas computacionales, cuyas actividades no tienen relación con su desarrollo profesional o laboral.

Es importante conocer quién comete el crimen cuando la conducta es atípica, o el delito, cuando es tipificada, pero más trascendente es encontrar las causas generadoras de ésos actos y los factores que favorecen el fenómeno informático criminal, los cuales pueden ser: ociosidad, reto intelectual, ocasión, necesidad, venganza, deseo, exhibicionismo, búsqueda de reconocimiento, descuido, falta de seguridad o desconocimiento.

Siendo una postura subjetiva considerar al criminal informático como una persona lista, decidida, motivada y dispuesta a aceptar un reto tecnológico, de aquél que busca la venganza o reivindicarse de alguna situación o por descuido ingresa a un banco de datos del gobierno.

Por otra parte el sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias,

gobiernos, etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

Las modalidades delictivas se manifiestan en acciones que inciden dolosamente sobre el hardware o software del ordenador. La incidencia sobre el hardware se configura cuando el hecho antijurídico recae sobre los elementos que forman el equipo informático (teclado, visor y/o pantalla, C.P.U., impresora, etc.); en cambio recae sobre el software cuando el delincuente intercepta en forma dolosa y premeditada un sistema informático para apoderarse, dañar, alterar, destruir e interferir los programas informáticos.

El sujeto pasivo, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él se puede conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que

protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, alertar a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la impartición, procuración y administración de justicia para atender e investigar estas conductas ilícitas, con lo que se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

1.3. CLASIFICACIÓN DEL DELITO INFORMÁTICO.

Como en la mayoría de los casos, existen varias clasificaciones para referirse a los delitos informáticos, una de ellas es la propuesta por el Doctor Julio Téllez Valdez[7] quien los clasifica en atención a dos criterios:

1. Como instrumento o medio. Se encuentran las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.
2. Como fin u objetivo. Están las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

Xavier Ribas tiene una postura similar a la anterior, sólo que él tiene la siguiente denominación:

1. Los delitos cometidos contra el sistema.
2. Los delitos cometidos mediante el uso de sistemas informáticos.

María de la Luz Lima[8] los clasifica en tres categorías:

[7] TELLEZ Valdez, Julio, op. cit. p.55.
[8] LIMA, Ma. de la Luz. op. cit. p. 10.

1. Los que utilizan la tecnología electrónica como método. Conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. Los que utilizan la tecnología electrónica como medio. Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. Los que utilizan la tecnología electrónica como fin. Conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Dentro de la definición aportada por Pedro Zamora Sánchez[9] se puede obtener una clasificación:

1. conductas que involucran actividades delictivas por el mal uso de la computadora.
2. conductas que involucran actividades delictivas por el abuso de la computadora.

Toda clasificación obedece un objetivo; precisar la naturaleza del objeto clasificado; determinar la gravedad de una conducta; establecer las condiciones de

[9] ZAMORA SÁNCHEZ, Pedro, **Marco jurídico del lavado de dinero**, Colección Estudios Jurídicos, Editorial Oxford, México, D. F., 1999.p. 110.

realización de un acto; diferenciar la clase de actos, entre otros. En el caso que nos ocupa, la clasificación de los delitos informáticos nos permite conocer si los medios electrónicos fueron empleados como método o fin, determinando de ese modo, si se trata de un delito común realizado a través de medios informáticos o si se refiere a un delito atentatorio de un nuevo bien jurídico como la información.

De la misma clasificación de los delitos informáticos, se derivan los tipos de delitos informáticos. Atendiendo la opinión de Téllez Valdez, los delitos pueden ser:

1.Como instrumento o medio:

a. Planeación o simulación de delitos convencionales;
b. Lectura, sustracción o copiado de información confidencial;
c. Alteración de datos tanto en la entrada como en la salida;
d. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas;
e. Uso no autorizado de programas de cómputo;
f. Alteración en el funcionamiento de los sistemas;

g. Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios;
h. Acceso a áreas informatizadas en forma no autorizada;
i. Intervención en las líneas de comunicación de datos;
j. Desviación en el destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa;

2.Como fin u objetivo:

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

Por otra parte, existen diversos tipos de delitos que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.
- Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
- Estafas electrónicas: A través de compras realizadas haciendo uso de la red.
- Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

De la misma forma, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

- Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- Otros delitos: Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Desde el punto de vista de la Organización de las Naciones Unidas[10], reconoce los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras.

   - Manipulación de los datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos, representa el delito

[10] NACIONES UNIDAS. **Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de delitos informáticos.** Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. No.43 y 44. Naciones Unidas, Nueva York.1994.

informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

- Manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

- Manipulación de los datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la

falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2. Falsificaciones informáticas.

- Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.

- Como instrumento. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando

empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

3. Daños o modificaciones de programas o datos computarizados.

- Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Virus. Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos. Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba.

- Acceso no autorizado a servicios y sistemas informáticos. Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

- Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

- Reproducción no autorizada de programas informáticos de protección legal. La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase

de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Hemos destacado que el presente trabajo de investigación no se enfoca penalmente, esta dirigido a conocer la normatividad internacional relativa al cibercrimen, sin embargo, haber detallado la clasificación y tipos de los delitos informáticos, facilita la apreciación del tema y un mejor entendimiento del mismo.

1.4. LOS DESAFÍOS JURÍDICOS FRENTE AL DELITO INFORMÁTICO.

Cada vez que surge o se desarrolla un nuevo espacio de relación entre los individuos o una nueva actividad humana, el espíritu reglamentista de algunos abogados conduce al intento para dotarlo de nuevas pautas jurídicas. Desde luego, la existencia de normas es uno de los rasgos de una sociedad civilizada. Internet que se debe a uno de los desarrollos tecnológicos más intensos en los últimos veinte años, no podría estar al margen de ese rasgo de la civilización que son las reglas. Pero en muchos casos, antes de imaginar nuevas normas es pertinente revisar si no es más sencillo actualizar, para este espacio peculiar, las que ya tenemos.

Si se ha de atender a la singularidad de la red de redes, también es preciso recordar el inédito y hasta ahora casi siempre irrestricto ejercicio de las libertades que ha podido desplegarse, con propósitos y resultados de toda índole, en la red de redes.

En un trabajo reciente sobre el dilema entre legislar y no para Internet, se establece:

Decidir entre las restricciones represivas que atenten contra la libertad de expresión en Internet o convivir en ese espacio sin reglas donde las transgresiones sean cosa de todos los días, son los extremos que deben evitarse en una sociedad que necesita ser parte de los cambios, pero que es consciente de la importancia de garantizar el respeto y equilibrio en las nuevas "relaciones virtuales" que nos ofrece la cibercultura.

En virtud de los rápidos y constantes cambios tecnológicos, los legisladores no pueden comprender sus consecuencias y tampoco adaptar o, en este caso, plantear medidas reguladoras. Es fundamental recordar que uno de los problemas más graves en el establecimiento de normas en un medio cualquiera -con más razón en Internet donde cambia con rapidez la tecnología- es cómo proteger el

interés del público al tiempo que se obtiene el máximo de libertad posible para los ciudadanos, las compañías y otras entidades.

La opinión de los legisladores del mundo esta dividida, lo que está claro ya es que la ausencia de una estructura legal es una condición peligrosa para mantenerse a la altura del ritmo de innovación en la tecnología de la información y de la diversificación de necesidades de nuestra sociedad; también lo es la evidente urgencia de comprensión de las consecuencias tecnológicas y sociales con la llegada de Internet...[11]

Más severa, reclamando prudencia antes de abrir una nueva rama del derecho, es la posición de quienes recuerdan que no es la primera vez que los descubrimientos tecnológicos, especialmente aquellos que sirven para la comunicación, plantean viejos retos que parecen nuevos y por tal motivo no es necesario rehacer las leyes cada vez que se inventa algo nuevo.

Con la controversia si el ciberespacio es un territorio distinto que amerita una jurisdicción específica, o si simplemente se tienen que adecuar las leyes a los problemas actuales surgen una serie de preguntas que van desde, ¿Qué es, después de

[11] Bazaine Gallegos, Victoria Teresa, Legislar o no legislar: el dilema de Internet ignorado en México, México, UNAM, tesis de licenciatura en Ciencias de la Comunicación, Facultad de Ciencias Políticas y Sociales, p. 115.

todo, ese nuevo medio? ¿Constituye un espacio de expresión e intercambio con una materialidad suficiente para ser susceptible de regulación por parte de las leyes nacionales? ¿El tráfico de mensajes de un país a otro, requiere de una legislación multinacional, o al menos de convenios capaces de prever la persecución de delitos más allá de las fronteras de cada país?

O, desde otro punto de vista, ¿no puede pensarse que el espacio donde se despliega la información colocada en Internet es una zona distinta de la geografía hasta ahora conocida y reglamentada?

Una perspectiva así, indudablemente abre nuevos desafíos. Si se ha de legislar, tendría que ser reconociendo de manera amplia las singularidades de la red de redes. En contraposición con quienes sostienen que no hacen falta nuevas leyes para este medio, está la postura de aquellos que consideran que el Internet es un territorio distinto al de los estados nacionales y que, en consecuencia, requiere de un tratamiento jurídico también diferente.

De las anteriores reflexiones parecería desprenderse una contradicción entre la aplicación de las leyes actuales y la creación de nuevos ordenamientos para Internet. Pero no hay tal. Es posible ajustar la legislación hasta ahora vigente para

atender necesidades específicas como la protección de derechos de autor y la autentificación de transacciones mercantiles en la red, al mismo tiempo que se profundiza el debate sobre las nuevas fronteras del ciberespacio.

Las peculiaridades de Internet podían, también, provocar confusiones sobre la potestad de las autoridades locales y nacionales para examinar y, en su caso, perseguir delitos cometidos a través de la red de redes.

Si un aficionado a la pedofilia residente en la Gran Bretaña tiene fotografías de niños salvadoreños de los que se ha abusado sexualmente y las coloca en la red a través de un servidor ubicado en Alemania pero que es propiedad de una empresa estadounidense, ¿en que país debe castigarse ese ilícito? En casos como éste, hay que recordar que Internet es un medio: la persecución de esa falta correspondería, desde luego, a las autoridades inglesas si el delito que se persigue es la propagación de fotografías prohibidas debido a la edad de quienes aparecen en ellas. Si se trata de sancionar la utilización de menores de edad, la indagación sería del gobierno de El Salvador. Cuando ocasionan delitos aprovechándose de Internet, a los individuos se les castiga por la falta, independientemente del medio que hayan empleado y, por lo tanto, sin que sea sustantivo el sitio en donde esté materialmente depositada la información considerada como delictiva.

CAPITULO II

LA NORMATIVIDAD INTERNACIONAL SOBRE EL DELITO INFORMATICO.

CAPITULO II.- LA NORMATIVIDAD INTERNACIONAL SOBRE EL DELITO INFORMATICO.

2.1. TENDENCIAS NORMATIVAS INTERNACIONALES RESPECTO AL DELITO INFORMÁTICO.

Es objetivo de este capítulo presentar aquellos elementos considerados, tanto por organismos gubernamentales internacionales como por diferentes Estados, para enfrentar la problemática de los delitos informáticos. En este orden de ideas, debe mencionarse que durante los últimos años, se ha perfilado en el ámbito internacional cierto consenso en las valoraciones político-jurídicas de los problemas derivados por el mal uso de las computadoras, dando lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

En primer término, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio sobre la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el uso indebido de los programas computacionales.

Apreciar las implicaciones económicas de la delincuencia informática, su carácter internacional o transnacional, la disparidad en la protección jurídico-penal nacional y sus efectos perjudiciales sobre el flujo internacional de información, condujo a un intercambio de opiniones y propuestas de solución. Sobre la base de diversas posturas y deliberaciones, surgió un análisis y valoración comparativa de los derechos nacionales aplicables, así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

En 1986, la OCDE publicó un informe titulado **Delitos de Informática: Análisis de la Normativa Jurídica**, donde se reseñaban las normas vigentes y las propuestas de reforma en diversos Estados Miembros. Se recomendaba una lista mínima de situaciones sobre uso indebido, que los países podrían prohibir y sancionar en su legislación (Lista Mínima), por ejemplo el fraude y falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computo protegido.

Sobre el mismo particular, la Comisión Política de Información, Computadores y Comunicaciones, órgano de la OCDE, recomendó instituir

protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de finalizar la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema, a fin de elaborar directrices que contribuyan a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma como debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso merecedores de la regulación penal. El Comité Especial de Expertos sobre Delitos relacionados con el empleo de computadoras, del Comité Europeo para los Problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, entre ellas, la protección de la esfera personal, víctimas, posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado este proceso normativo a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que "recomienda a los gobiernos de los Estados miembros tener en cuenta, cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989. Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado a un consenso internacional en favor de su tipificación.

Adicionalmente, debe mencionarse que en 1992 la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos el mismo año.

En este contexto, consideramos que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con México y otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Cambiando de aires, considerando a las organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana Cuba[12], se sostuvo que la delincuencia relacionada con la informática, era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países, por ello se había difundido la comisión de actos delictivos.

Del mismo modo, la injerencia transnacional en los sistemas de proceso de datos de otros países, había atraído la atención de todo el mundo. Por tal motivo, si bien el problema principal —hasta ese entonces— era la reproducción y difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos,

[12] NACIONES UNIDAS. **Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana. 27 de agosto a 7 de septiembre de 1990.** (A/CONF. 144/28/Rev.1) Nueva York, Naciones Unidas. 1991.

no se habían difundido otras formas de delitos informáticos, siendo necesario adoptar medidas preventivas para evitar su aumento.

Partiendo del supuesto incremento de delitos informáticos no registrados, en vista de que los delitos informáticos eran un fenómeno nuevo y debido a la ausencia de medidas para contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Un estudio comparativo de las medidas adoptadas a nivel internacional para enfrentar esta problemática, permite afirmar que en la esfera del delito informático y el derecho penal, falta consenso sobre lo que son los delitos informáticos, no existe definición jurídica de la conducta delictiva, se carece de conocimientos técnicos en quienes hacen cumplir la ley, agregando dificultades de carácter procesal y falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, debe mencionarse la ausencia de la incorporación de estos delitos en los tratados internacionales de extradición.

Teniendo presente la situación descrita, es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario para solucionar los problemas derivados del incremento en el uso indebido de la informática, desarrollar un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. La elaboración de ese régimen, deberá considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal, durante un coloquio celebrado en Wurzburgo (Alemania) en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Contemplando las deficiencias del derecho penal tradicional, sugiere promover la modificación de la definición tradicional de los delitos o crear conceptos nuevos. Adicionalmente, recomienda que las nuevas disposiciones sean precisas, evitando una excesiva tipificación.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, la Asociación, recomendó que los Estados, de conformidad con sus tradiciones jurídicas y su cultura,

tipificaran como delito la conducta descrita en la "lista facultativa" a la que hemos hecho mención, especialmente la alteración de datos de computadora y el espionaje informático, el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares.

En general, se ha pretendido contribuir mediante recomendaciones a la uniformidad de las normas que sancionan los delitos informáticos en el ámbito internacional, sin dejar de observar la tradición jurídica de cada país.

2.2. LA PROTECCIÓN JURÍDICA INTERNACIONAL DE LOS MEDIOS ELECTRÓNICOS.

La legislación sobre protección de los medios electrónicos persigue acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos pueden contener datos e informaciones de carácter personal, y a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, a

un Estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje. No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello por parte de individuos poco conscientes e irresponsables con relación a los datos que dichos sistemas contienen.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

Ante la magnitud del problema, diversas formas puede adoptar la protección de los sistemas informáticos, podrá abordarse desde una perspectiva

penal, civil o comercial, incluso, de derecho administrativo. Estas distintas medidas de protección, no tienen porque ser excluyentes unas de otras, por el contrario, deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática, sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Indudablemente, la regulación jurídica de los ilícitos informáticos no pertenece de manera exclusiva al derecho interno de los estados, respondiendo a esa dimensión, en el ámbito del derecho internacional se realizan esfuerzos por conseguir una normatividad que regule el aspecto transfronterizo de tales delitos.

En la estructura de la Organización de las Naciones Unidas, se encuentran órganos vinculados con la normatividad referida a los delitos informáticos y su persecución. En el terreno normativo, la Comisión de las Naciones Unidas para el Derecho Mercantil (UNCITRAL), realiza tareas encaminadas a sugerir criterios orientadores de la regulación jurídica de los ilícitos informáticos. Mientras en el campo de la persecución de esos delitos, el Comité para la Prevención del Delito, dependiente del Consejo Económico y Social, hace lo propio.

Debido a que en presente trabajo de investigación, se aborda en diferentes incisos lo relativo a la regulación y persecución de los delitos informáticos en el terreno internacional, el propósito de éste, se concreta a establecer la necesidad de lograr una normatividad universal, aspectos que son discutidos en otros puntos de la investigación.

2.3. ASPECTOS RELEVANTES DE LA REGULACIÓN JURÍDICA INTERNACIONAL SOBRE EL CIBERCRIMEN.

Se ha sostenido que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para sancionar comportamientos merecedores de pena con los medios del derecho penal tradicional, al menos en parte, existen relevantes dificultades. En buena medida, las dificultades pueden deberse a la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De lo anterior, surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente, existe un amplio consenso sobre estas valoraciones que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema particular, a continuación se presentan casos específicos con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países:

Alemania

En Alemania para hacer frente a la delincuencia relacionada con la informática, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986, que produjo efectos a partir del 1 de agosto de 1986, en la que se contemplan los siguientes delitos:

Espionaje de datos (202 a);

Estafa informática (263 a);

Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273);

Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible;

Sabotaje informático (303 b), destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa;

Utilización abusiva de cheques o tarjetas de crédito (266 b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria.

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar el acceso no autorizado en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la

comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación a determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

Austria

La Ley de reforma del Código Penal de 22 de diciembre de 1987, contempla los siguientes delitos:

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

Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia

El 5 enero de 1988, este país dictó la Ley número 88-19, relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

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

modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

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

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

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

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

Estados Unidos

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. (18 U.S.C. Sec. 1030 [a][5][A]). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

Haciendo la aclaración que el creador de un virus no puede escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

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

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Consideramos importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de

sanciones pecuniarias de $10,000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios, y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias, gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándose aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir

datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

Gran Bretaña.

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría.

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

Holanda.

El 1° de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

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

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

España.

En el Nuevo Código Penal de España, el art. 263 establece que el que causare daños en propiedad ajena. En tanto, el artículo 264-2) establece que se aplicará la pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa y cuando el hecho es cometido por parte de funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, el nuevo Código Penal de España, en su artículo 248, solo tipifica las estafas con ánimo de lucro valiéndose de alguna

manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

Chile.

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993.

Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Esta ley prevé en el Art. 1°, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En tanto, el Art. 3° tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

En síntesis, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación

internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (chips, inteligencia artificial, nanotecnología, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Finalmente, debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

2.4. ANÁLISIS DE LA ESTRUCTURA INTERNACIONAL DIRIGIDA AL COMBATE DE LOS DELITOS INFORMÁTICOS.

Analizando la legislación internacional con respecto a los delitos informáticos, encontramos que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada

mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores.

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoria de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Sin embargo el nivel de criminalidad existente se debe a la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

Por su parte, el «Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos»[13] señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada.

Asimismo, la ONU resume de la siguiente manera los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

[13] NACIONES UNIDAS. **Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de delitos informáticos.** Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. No.43 y 44. Naciones Unidas, Nueva York.1994.

- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y su interconexión con otros medios, por supuesto, no es el único. Las ventajas y necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, prácticamente en todas las naciones, conlleva la posibilidad creciente de estos delitos; por ende, puede señalarse que la criminalidad informática constituye un reto considerable para los sectores afectados de la infraestructura crítica de un país, legisladores, autoridades policiales encargadas de las investigaciones y funcionarios judiciales.

En el continente americano, el Computer Security Institute de San Francisco asegura que, durante el año pasado, las pérdidas ocasionadas por la "ciberdelincuencia" en 186 empresas norteamericanas fueron de 376 millones de dólares aproximadamente (casi el doble de lo que se registró en el año 2000). Por otra parte, en cuanto a la pornografía infantil, los informes del Fondo de las Naciones

Unidas para la Infancia (UNICEF) señalan que, tan sólo en Estados Unidos, este negocio ilegal genera una cifra anual de entre 2,000 y 3,000 millones de dólares

Dadas estas cifras, y como consecuencia del crecimiento descontrolado de este fenómeno, en noviembre del año pasado, un total de 30 países firmaron en Budapest la Convención Internacional contra el "Cibercrimen", incluyendo a Estados Unidos, Japón, Canadá, Sudáfrica, y 26 de los 43 países miembros del Consejo de Europa.

Esta convención pretende coordinar la lucha para erradicar el crimen y terrorismo del ciberespacio, pero desafortunadamente a cambio de algunas garantías significativas para el hombre. Por ejemplo, las medidas que requerirán a los proveedores de accesos y servicios en Internet de mantener registros sobre las actividades de sus clientes (artículos 17, 18, 24, 25). Bajo la visión de algunos analistas, estas medidas suponen un riesgo considerable a la privacidad y otros derechos humanos de los usuarios de Internet, contrarios a principios establecidos en la Declaración Universal de los Derechos Humanos.

Casi de forma paralela a la Convención Internacional contra el "Cibercrimen" el gobierno estadounidense promueve la polémica *USA Patriot Act*, que incluye el propósito de "rediseñar Internet" para su mejor control, conduciendo el tráfico hacia unos servidores centrales donde agencias como la *Federal Bureau of*

Investigation FBI, puede instalar sus equipos para fiscalizar la navegación y el correo electrónico.

También en algunos países de Latinoamérica, se comienza a ver este tipo de acciones en contra del crimen en el ciberespacio. Por ejemplo, en Chile existe ya la Brigada Investigadora del "Cibercrimen" (BRICIB), que está adscrita a la Policía de Investigaciones de ese país. En México se encuentra la Policía Cibernética, área de la Policía Federal Preventiva, adscrita a la Secretaría de Seguridad Pública.

La Policía Cibernética vigila la red mediante sistemas convencionales para rastreo. Su patrullaje se centra sobre *hackers*, sitios de Internet, comunidades y *chat rooms* en los que promueven la pornografía y el turismo sexual infantil. Según este mismo organismo, se utiliza Internet como un instrumento para detectar a delincuentes que organizan sus actividades en algún lugar del ciberespacio. Además se realiza análisis sobre actividades de organizaciones locales e internacionales de pedofilia así como de redes de prostitución infantil y redes de tráfico de menores que los explotan en otros países.

Entre algunos de los ciberdelitos más comunes que persiguen las policías cibernéticas se encuentran: el acceso ilegal a sistemas propietarios, la intercepción ilegal, la interferencia y pérdida de datos, la interferencia de sistemas, la pornografía infantil, los delitos contra la propiedad intelectual, y el fraude electrónico. Sin

embargo, por diversas insuficiencias en materia de legislación, esta persecución tiene ciertas limitaciones.

En el caso de México, este tipo de actividades, como la que desempeña la Policía Cibernética, resulta muy delicada, pues en cierta medida, podría atentar contra las garantías individuales plasmadas en la Constitución Política de los Estados Unidos Mexicanos.

El gobierno mexicano, así como otros gobiernos del mundo, enfrentan actualmente el desafío de combatir enérgicamente el crimen en el ciberespacio, considerando aspectos de gran importancia como lo son la territorialidad, la privacidad de los ciudadanos, la seguridad nacional, el derecho a la información, la libertad de expresión, el desarrollo de nuevos mecanismos de seguridad, el adiestramiento constante de los órganos vigilantes, la legislación vigente, y la colaboración de la iniciativa privada, y la sociedad.

Combatir el crimen en el ciberespacio sin atentar contra garantías individuales significativas de los ciudadanos es un gran reto para los gobiernos.

CAPITULO III

ANALISIS DEL CONVENIO PRELIMINAR SOBRE DELITOS INFORMATICOS.

CAPITULO III.- ANALISIS DEL CONVENIO PRELIMINAR SOBRE DELITOS INFORMATICOS.

3.1. ORIGEN, ELABORACIÓN Y CONTENIDO DEL CONVENIO PRELIMINAR SOBRE DELITOS INFORMÁTICOS.

Sin duda alguna, en materia de regulación de delitos informáticos, los europeos se han colocado a la vanguardia. En gran medida, los logros en el viejo continente se deben a la labor de instancias comunitarias, cada vez más sólidas, un buen ejemplo, lo constituye el Comité Europeo para los Problemas de la Delincuencia.

Debido al auge de los delitos informáticos y la necesidad de estructurar un adecuado marco normativo, los europeos entendieron bien la urgencia. Se encargó a un Comité Especial de Expertos sobre Delitos relacionados con el Empleo de Computadoras, elaborar un proyecto de convenio que permitiera a los estados interesados establecer una regulación sobre este tipo de ilícitos, mismo que fue sometido a consideración del Comité Europeo para los Problemas de la Delincuencia.

El Convenio Preliminar sobre Delitos Informáticos[14], busca satisfacer el desafío de contar con la normatividad adecuada para combatir los delitos relacionados con esos medios, procurando el respeto a los derechos humanos en la nueva sociedad de la información. A instancias del Comité Europeo para los Problemas de la Delincuencia (CDPC), en noviembre de 1996, se decidió establecer un Comité de Expertos para que se encargara de los delitos informáticos. El CDPC basó su decisión en las siguientes razones:

1. Los rápidos desarrollos en el campo de la tecnología de la información tienen una relación directa sobre todos los sectores de la sociedad moderna.

2. La integración de los sistemas de telecomunicaciones y de información, que posibilitan el almacenamiento y la transmisión, sin tener en cuenta la distancia, de todo tipo de comunicaciones, abren una amplia gama de nuevas posibilidades.

3. Estos desarrollos, aumentaron por el surgimiento de las redes y las superautopistas de la información, incluyendo Internet, a través de

[14] CONSEJO DE EUROPA, Comité Europeo para los Problemas de la Delincuencia, **Convenio Preliminar sobre Delitos Informáticos**, Estrasburgo, 25 de Mayo de 2001.

las cuales, virtualmente toda persona podrá tener acceso a cualquier servicio de información electrónica sin importar en que lugar del mundo se encuentre.

4. Al conectarse con los servicios de comunicaciones y de información, los usuarios crean una especie de espacio común denominado "ciberespacio", que es utilizado con fines legítimos pero que también puede ser objeto de un mal uso.

5. Los delitos que se realizan en el ciberespacio, son cometidos contra la integridad, la disponibilidad y la confidencialidad de los sistemas informáticos y las redes de telecomunicaciones o consisten en el uso de dichas redes o sus servicios para cometer delitos tradicionales.

6. El carácter transfronterizo de dichos delitos, cuando se cometen a través de Internet, está en conflicto con la territorialidad de las autoridades nacionales encargadas de hacer cumplir las leyes.

7. En opinión del CDPC, el derecho penal debe mantenerse al corriente de estos desarrollos tecnológicos que ofrecen oportunidades altamente sofisticadas para hacer mal uso de las facilidades del ciberespacio y perjudicar intereses legítimos. Dada la naturaleza transfronteriza de las redes de información, se necesita un esfuerzo internacional concertado para tratar dicho uso.

8. Únicamente un instrumento internacional de carácter obligatorio, puede asegurar la eficacia necesaria en la lucha contra estos nuevos fenómenos. En el marco de dicho instrumento, además de las medidas de cooperación internacional, se deberían abordar las cuestiones de derecho sustantivo y procesal, al igual que las cuestiones que estén estrechamente conectadas con el uso de la tecnología de la información.

Adicionalmente a las consideraciones vertidas, el CDPC tuvo en cuenta el Informe que, por encargo suyo, preparó el Profesor H.W.K. Kaspersen. En ese informe, se concluyó que "...habría de buscar otro instrumento legal más obligatorio que una Recomendación, tal como un Convenio. Dicho Convenio no debería abordar solamente las cuestiones de derecho penal sustantivo, sino también las cuestiones de

derecho procesal penal, así como los acuerdos y procedimientos del derecho penal internacional." Una conclusión similar había surgido del Informe adjunto a la Recomendación N° R (89) 9, concerniente al derecho sustantivo y la Recomendación N° R (95) 13, relativa a los problemas de derecho procesal con relación a la tecnología de la información.

Los puntos de consulta específicos del nuevo comité fueron los siguientes:

i. "Rever a la luz de las Recomendaciones N° R (89) 9, sobre los delitos relacionados con el uso de computadoras y N° R (95) 13, concerniente a los problemas de derecho procesal penal relacionados con la tecnología de la información, en particular los siguientes temas:

ii. Los delitos informáticos, en particular aquellos cometidos mediante el uso de las redes de telecomunicaciones, tales como las transacciones de fondos ilegales, la oferta de servicios ilegales, la violación de los derechos de autor, así como también los delitos que violen la dignidad humana y la protección de los menores;

iii. Otras cuestiones de derecho penal sustantivo donde puede ser necesario un enfoque común a los fines de lograr una cooperación internacional tales como definiciones, sanciones y la responsabilidad de los actores en el ciberespacio, incluyendo a los proveedores de servicios de Internet;

iv. El uso, incluyendo la posibilidad del uso transfronterizo y la aplicabilidad de los poderes coercitivos en un entorno tecnológico, como la interceptación de telecomunicaciones y la vigilancia electrónica de las redes de información a través de Internet, el allanamiento y el secuestro en los sistemas de procesamiento de información (incluyendo sitios de Internet), la prohibición de acceder a material ilegal y el requerimiento de que los proveedores de servicios cumplan con obligaciones especiales, teniendo en cuenta los problemas causados por ciertas medidas de seguridad de la información, como la encripción;

v. El problema de la jurisdicción, con relación a los delitos vinculados a la tecnología de la información, entre ellos, determinar el lugar donde se cometió un delito *(locus delicti)* y cuál es el derecho que corresponde aplicar, incluyendo el problema de *ne bis idem,* en el caso de múltiples

jurisdicciones y la cuestión de cómo resolver los conflictos de jurisdicción positiva y cómo evitar los conflictos de jurisdicción negativa;

vi. El problema de la cooperación internacional en la investigación de los delitos informáticos, en estrecha colaboración con el Comité de Expertos sobre el Funcionamiento de los Convenios Europeos en el Campo Penal (PC-OC).

Atendiendo las circunstancias, el Comité elaboraría el borrador del instrumento legal obligatorio, basándose, en la medida de lo posible, en los ítems i) a v), poniendo particular énfasis en las cuestiones internacionales y, de ser apropiado, en las recomendaciones accesorias respecto de problemas específicos.

Con relación a la decisión del CDPC, el Comité de Ministros estableció el nuevo comité denominado: "Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras (PC-CY)" por decisión nº CM/Del/Dec(97)583, tomada en la 583ª reunión de los Representantes de los Ministros (celebrada el 4 de febrero de 1997). El Comité PC-CY, inició su labor en abril de 1997 y efectuó negociaciones con respecto al borrador de un convenio internacional en materia de delitos informáticos.

Conforme a los puntos de consulta originales, el Comité debía terminar su trabajo para el 31 de diciembre de 1999. Para ese entonces, el Comité no se encontraba en posición de concluir totalmente sus negociaciones sobre ciertas cuestiones incluidas en el borrador del Convenio, los términos de referencia se extendieron, por la decisión nº CM/Del/Dec/679 de los Representantes de los Ministros, hasta el 31 de diciembre de 2000.

Apreciando las dificultades, los ministros de justicia europeos, manifestaron su apoyo con respecto a las negociaciones: mediante la Resolución Nº 1, aprobada en su 21ª Conferencia (Praga, junio de 1997), se recomendaba al Comité de Ministros que apoyara el trabajo llevado a cabo por el CDPC, relacionado con los delitos informáticos a fin de que las disposiciones internas en materia de derecho penal, fueran lo más parecidas posibles entre sí y posibilitar el uso de medios eficaces de investigación con respecto a dichos delitos. Mediante la Resolución Nº 3, aprobada en la 23ª Conferencia de Ministros de Justicia Europeos (Londres, junio de 2000), se alentó a las Partes negociadoras a continuar con sus esfuerzos para encontrar soluciones apropiadas y posibilitar la mayor cantidad posible de Estados que sean Partes del Convenio. De igual manera, reconoció la necesidad de contar con un rápido y eficiente sistema de cooperación internacional, que tenga debidamente en

cuenta, los requerimientos específicos de la lucha contra los delitos informáticos. Los Estados Miembros de la Unión Europea expresaron su apoyo al trabajo realizado por el PC-CY á través de una Opinión Conjunta, aprobada en mayo de 1999.

Entre abril de 1997 y diciembre del 2000, el Comité PC-CY celebró 10 reuniones plenarias y 15 reuniones de su Grupo de Redacción. Después del vencimiento de la extensión de su plazo, los expertos celebraron, bajo la tutela del CDPC, tres reuniones más para finalizar el borrador del Memorando Explicativo y el borrador del Convenio a la luz de la opinión de la Asamblea Parlamentaria. El Comité de Ministros, solicitó a la Asamblea en octubre de 2000, que emitiera su opinión respecto del borrador del Convenio, que adoptó en la segunda parte de su sesión plenaria en abril de 2001.

Con posterioridad a la decisión tomada por el Comité PC-CY, se levantó el secreto a una primera versión del borrador del Convenio y se publicó en abril de 2000, seguida por posteriores borradores que fueron publicados después de cada reunión plenaria, con el fin de posibilitar que los Estados negociadores efectúen consultas con todas las partes interesadas. Este proceso de consulta resultó muy útil.

El borrador del Convenio, revisado y finalizado, así como su Memorando Explicativo, fueron sometidos para su aprobación al CDPC en su 50ª sesión plenaria en junio de 2001, después de lo cual, el texto del borrador del Convenio fue sometido al Comité de Ministros para su aprobación y quedar abierto para su firma.

Cabe destacar que hasta el momento, el Convenio Preliminar sobre Delitos Informáticos sigue abierto a la firma de los estados interesados, sin embargo, la fase de negociación ha concluido, estableciendo el texto final de este instrumento jurídico.

El documento comienza con un preámbulo dirigido a los Estados miembros del mencionado Consejo y demás países signatarios del convenio, en el cual se establecen la necesidad de alcanzar como una cuestión prioritaria una política criminal común dirigida a la protección de la sociedad contra los delitos informáticos, aprobando entre otras cosas una legislación que sea apropiada a tal fin y fomentando la cooperación internacional entre los Estados.

Atendiendo el texto del Convenio, consta de 48 artículos, estructurado en cuatro capítulos:

I. Uso de los términos;

II. Medidas que deben tomarse a nivel nacional: derecho sustantivo y derecho procesal;

III. Cooperación internacional;

IV. Disposiciones finales.

Capítulo I se refiere a las definiciones de los términos que se utilizaran en el resto del convenio.

Capítulo II, sección 1 (cuestiones de derecho sustantivo) abarca las disposiciones sobre delitos y otras disposiciones relacionadas referentes al área de los delitos informáticos o los delitos relacionados con el empleo de computadoras: primero define 9 delitos agrupados en 4 diferentes categorías, luego versa sobre la responsabilidad secundaria y las sanciones. En el capítulo se definen los siguientes delitos: acceso ilegal, interceptación ilegal, interferencia de los datos, interferencia del sistema, mal uso de los dispositivos, falsificación relacionada con el uso de computadoras, fraude relacionado con el uso de computadoras, delitos relacionados con la pornografía infantil y delitos relacionados con la violación de los derechos de autor y otros delitos relacionados.

Capítulo II, sección 2 (cuestiones de derecho procesal), cuyo alcance va más allá de los delitos definidos, ya que se aplica a cualquier delito cometido a través de un sistema informático o cuya evidencia se encuentre en formato electrónico, determina en primer lugar las condiciones y salvaguardas comunes aplicables a todas las facultades procesales contenidas en este Capítulo. Luego establece las siguientes facultades procesales: pronta preservación de datos almacenados; pronta preservación y revelación parcial de datos de tráfico; orden de suministrar; allanamiento y secuestro de datos informáticos; recopilación de datos informáticos en tiempo real; interceptación de datos de contenido. Finaliza con las disposiciones referentes a la jurisdicción.

Capítulo III contiene las disposiciones concernientes a la asistencia mutua con relación a los delitos tradicionales y a los delitos relacionados con el uso de computadoras, alude también a la extradición. Abarca la asistencia mutua tradicional en dos situaciones: cuando entre las partes no existen bases legales (tratados o legislación recíproca), en cuyo caso, corresponde aplicar sus disposiciones, o cuando existe dicha base, los acuerdos existentes se aplican a la asistencia que se concede en virtud del presente Convenio. De acuerdo con el capítulo, la asistencia específica relacionada con los delitos informáticos o con los delitos relacionados con el uso de computadoras, se aplica a ambas situaciones y abarca, sujeta a condiciones extra, la

misma serie de facultades procesales definidas en el Capítulo II. Además, el Capítulo III contiene una disposición sobre un tipo especial de acceso transfronterizo a datos informáticos almacenados que no requiere de la asistencia mutua (mediando un consentimiento o si están disponibles al público) y prevé, para asegurar una rápida asistencia entre las Partes, el establecimiento de una red que funcione las 24 horas y los 7 días de la semana.

Capítulo IV contiene las disposiciones finales, las cuáles, con ciertas excepciones, repiten las disposiciones convencionales de los tratados del Consejo de Europa.

3.2. ANALISIS DEL CONVENIO PRELIMINAR SOBRE DELITOS INFORMÁTICOS.

Empleando un método de interpretación sistemático, se realizará el análisis del Convenio. Para comprender el alcance de las obligaciones previstas a las Partes, no se describirá el contenido de cada artículo, sino se referirá a los capítulos sustantivos. De esta manera, es prudente destacar que dicho instrumento apunta principalmente a:

- Armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones relacionadas en materia de delitos informáticos.

- Establecer, conforme al derecho procesal penal de cada país, las facultades necesarias para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas relacionadas que se encuentren en formato electrónico.

- Establecer un régimen rápido y eficaz de cooperación internacional.

Revisando la tendencia adoptada en la elaboración del Convenio, se trata de un instrumento marco, es decir, los Estados partes no se obligan a uniformar su legislación, adoptando una regulación jurídica idéntica. De acuerdo con el texto, armonizar los elementos de los delitos, implica evitar contradicciones en la regulación de las conductas consideradas ilícitas.

Como regla general, los artículos del Convenio señalan el compromiso de cada Parte de adoptar las medidas legales y de otra índole necesarias para establecer

como delitos penales las conductas descritas, en virtud de sus leyes nacionales. Esto quiere decir, que la obligación adquirida es incorporar como delito la conducta prevista, sin embargo, cada Estado lo hará del modo que estime pertinente, aplicando igualmente la sanción que considere efectiva. En otras palabras, el Convenio se aparta del derecho uniforme.

Es evidente que el destinatario inmediato de las disposiciones del Convenio son los Estados. Las obligaciones se dirigen al compromiso de tipificar conductas ilícitas en los ordenamientos internos, brindar asistencia judicial recíproca, resolver cuestiones de jurisdicción, ofrecer cooperación entre sí, situaciones que por su naturaleza no pueden corresponder a particulares.

Respecto al ámbito territorial, el alcance del Convenio no se limita a Estados europeos. De conformidad con el artículo 37, después de la entrada en vigor, el Comité de Ministros del Consejo de Europa, consultando a los Estados Partes y con el consentimiento unánime de los mismos, puede invitar a cualquier Estado que no sea miembro del Consejo y que no haya participado en la elaboración del Convenio a adherirse al mismo.

Evidentemente, la intención de extender el ámbito territorial de aplicación persigue una mayor eficacia del instrumento. Mientras mayor sea el número de Estados Partes, la persecución de los delitos informáticos resultará eficaz.

Protector de la soberanía estatal, principio tradicionalmente incorporado a los tratados que comprometen la cooperación internacional, la inviolabilidad territorial obliga a las autoridades de un Estado a no realizar actividades en territorio de otro, bajo ningún pretexto. Correspondiendo al aspecto territorial de la soberanía, toda autoridad facultada a ejercer atribuciones en el territorio de un Estado, deberán ser carácter nacional y no extranjero.

Para que una autoridad extranjera pueda actuar en el ámbito espacial de otro Estado, requiere de autorización expresa. Figuras como la entrega vigilada, prevista en algunas convenciones internacionales, permiten que autoridades extranjeras se infiltren en el territorio de otros Estados a fin de concluir investigaciones tendientes a la persecución de delitos, ese operativo, amerita forzosamente el visto bueno de las autoridades del Estado Receptor.

En el caso del Convenio analizado en esta tesis, no se prevén alternativas similares a la descrita en el párrafo anterior. Revisando el texto, el instrumento

jurídico alude al respeto estricto de la jurisdicción de los Estados Partes, por esa razón, el principio de inviolabilidad territorial está plenamente justificado.

Consecuencia de todo acuerdo internacional vinculado a la cooperación, la reciprocidad es otro principio básico. Al señalar instituciones como la extradición y la asistencia judicial, los Estados Partes se obligan a actuar recíprocamente. En gran medida, la reciprocidad está señalada expresamente, pero en otros casos, se sobreentiende.

En el contenido del Convenio, se hace referencia repetidamente al principio de reciprocidad, los Estados Partes fortalecen la cooperación en la medida de dar cumplimiento cabal al principio. Prevista la asistencia unilateral, sin necesidad de mediar solicitud, los Estados que la ofrecen, lo hacen seguros de la reciprocidad en situaciones semejantes.

Al señalar la actuación de autoridades centrales en el capítulo relativo a la cooperación, el Convenio encuentra el modo de hacer más efectiva la reciprocidad. Una Autoridad Central que requiere la asistencia judicial de otra, debe ofrecer la reciprocidad en el caso contrario. Ello no significa que si no compromete la

reciprocidad carece del derecho a la asistencia, pero si lo hace garantiza la asistencia para situaciones posteriores.

3.3. DISPOSICIONES DE NATURALEZA SUSTANTIVA SOBRE DELITOS INFORMÁTICOS Y DELITOS RELACIONADOS CON EL EMPLEO DE COMPUTADORAS.

Hemos destacado que en el Convenio motivo de análisis, uno de los objetivos es orientar a los Estados partes en la tipificación de conductas ilícitas relacionadas con las computadoras. Del mismo modo, se ha señalado que no se trata de uniformar la legislación de los Estados, simplemente de avanzar en la sanción de los delitos informáticos.

Previo a describir las conductas ilícitas que los Estados se comprometen a tipificar en sus respectivas legislaciones, el Convenio describe una serie de términos considerados indispensables, en virtud que su significado es clave para orientar la tipificación respectiva. Si los Estados partes no consiguen armonizar el sentido de los términos empleados, difícilmente lograran una tipificación adecuada de los delitos informáticos, distorsionando el alcance de los tipos penales.

A continuación señalaremos el significado que se desprende de los términos empleados en el Convenio. Conocer su sentido facilitará entender el alcance del tipo penal y comprender el bien jurídico que se protege.

Sistema Informático. Conforme al Convenio, es un dispositivo que consta de hardware y software desarrollado para el procesamiento automático de datos digitales. Puede incluir facilidades de entrada (input), salida (output) y almacenamiento. Capaz de funcionar en forma independiente o estar conectado a una red con otros dispositivos similares. "Automático" significa sin intervención directa de un ser humano, "procesamiento de datos" significa que los datos que se encuentran en un sistema informático son operados mediante la ejecución de un programa de computación.

Un sistema informático en general consta de diferentes dispositivos, como el procesador o unidad de procesamiento central y periféricos. Un "periférico" es un dispositivo que ejecuta ciertas funciones específicas interactuando con la unidad de procesamiento, tales como una impresora, una pantalla de video, un medio para leer, escribir o almacenar datos en CDs.

Programa de Computación. Elemento del sistema informático, es una serie de instrucciones que pueden ejecutarse por medio de una computadora para alcanzar el resultado deseado. Una computadora puede operar diferentes programas.

Red. Es una interconexión entre dos o más sistemas informáticos. Internet es una red global que consta de muchas redes interconectadas que utilizan protocolos comunes.

Datos informáticos. Apoyada en la realizada por la ISO, esta definición contiene las palabras "que pueda ser procesado". Esto significa que los datos están en un formato tal que pueden ser directamente procesados por un sistema informático. Con el fin de aclarar el término datos, en este Convenio debe entenderse como datos en formato electrónico u otro formato que pueda procesarse directamente, se introduce el concepto de "datos informáticos".

Proveedor de Servicios. El término abarca una amplia categoría de personas que desempeñan un rol particular con respecto a la comunicación o el procesamiento de los datos, a través de los sistemas informáticos. Se aclara que quedan comprendidos tanto los entes públicos como los privados que proveen a los usuarios de su servicio, la capacidad para comunicarse por medio de un sistema

informático y cualquier otra entidad que procese o almacene datos informáticos en nombre de dicho servicio de comunicaciones o de los usuarios de dicho servicio.

Datos de Tráfico. Es una categoría separada de datos informáticos que está sujeta a un régimen legal específico. Estos datos son generados por las computadoras en la cadena de comunicación con el fin de encaminar una comunicación desde su punto de origen hasta su destino. Por lo tanto son datos auxiliares a la comunicación misma.

En caso de investigación de un delito cometido con relación a un sistema informático, los datos de tráfico son necesarios para rastrear la fuente de una comunicación, como el punto de partida para recopilar otras pruebas o como parte de las pruebas de un delito. Los datos de tráfico podrían ser efímeros, durar lo necesario para ordenar su inmediata preservación. Dichos datos indican el origen, destino, ruta, hora, fecha, tamaño, duración o el tipo de servicio subyacente.

Conviene aclarar que la definición, otorga a las legislaturas de cada país la capacidad de introducir alguna diferenciación respecto de la protección legal de los datos de tráfico de acuerdo a su sensibilidad.

Quienes redactaron el Convenio entendieron que las Partes no estarían obligadas a copiar literalmente en sus leyes nacionales los conceptos definidos, siempre que estas leyes abarcaran dichos conceptos de manera coherente con los principios contenidos y ofrecieran un marco equivalente para su implementación.

Entendida como una finalidad del Convenio, mejorar los medios para prevenir y evitar los delitos informáticos o los delitos relacionados con el uso de computadoras al establecer una norma mínima común con relación a los principales delitos, se establecen aquellas conductas que deberán incorporarse a la legislación penal de cada Estado. Precisamente, la parte sustantiva del Convenio se dedica a señalar las conductas que deberán tipificarse, clasificándolas por categorías, estas son:

Delitos relacionados con el empleo de computadoras: delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, que constituyen las amenazas básicas. Tal como se las identificó en los debates sobre la seguridad de los datos y de los sistemas informáticos, a las que están expuestos el procesamiento electrónico de datos y los sistemas de comunicaciones. El encabezamiento describe el tipo de delitos que abarca, que es el acceso no autorizado

a sistemas, programas o datos y la manipulación ilegal de dichos sistemas, programas o datos.

Esta categoría también comprende los delitos que por medios tradicionales, atacan intereses legales que ya están protegidos por el derecho penal, abarcan la falsificación y fraude.

Delitos relacionados con los contenidos: producción o distribución ilegal de pornografía infantil mediante el uso de sistemas informáticos. El Comité encargado de redactar el Convenio discutió la posibilidad de incluir otros delitos relacionados con los contenidos, tales como la distribución de propaganda racista a través de sistemas informáticos. Sin embargo, no pudo llegar a un consenso con respecto a que dichas conductas constituyeran un delito. Si bien hubo un apoyo significativo a favor de incluir esto como un delito penal, algunas delegaciones expresaron una fuerte preocupación respecto a la inclusión de una disposición tal, basándose en el derecho a la libertad de expresión.

Delitos relacionados con violaciones a los derechos de autor y otros derechos relacionados. fueron incluidos en el Convenio, porque las violaciones a los derechos de autor son una de las formas más difundidas de delitos informáticos o de

delitos relacionados con el empleo de computadoras y su escalamiento está causando preocupaciones a nivel internacional.

En el aspecto sustantivo, el Convenio también incorpora disposiciones respecto de la tentativa, la ayuda y la instigación. Así como lo referente a sanciones y medidas que se aplican a los responsables del delito, aclarando que no se uniforman penalidades.

3.4. DERECHO PROCESAL APLICABLE EN MATERIA DE JURISDICCIÓN NACIONAL.

Relativa al derecho procesal, la sección 2, describe ciertas medidas procesales que habrán de tomarse a nivel nacional con el fin de facilitar la investigación penal de los delitos establecidos en el Convenio, otros delitos cometidos mediante el uso de un sistema informático y la recopilación de pruebas de un delito penal en formato electrónico. De acuerdo con el Artículo 39, párrafo 3, ningún punto del Convenio requiere o invita a una Parte a establecer facultades o procedimientos distintos a los contenidos en el presente Convenio, ni impide que una Parte los establezca.

El Convenio adapta al nuevo entorno tecnológico medidas procesales tradicionales, tales como el allanamiento y secuestro. Además se crean otras, tales como la pronta preservación de los datos, con el fin de asegurar que las medidas tradicionales para reunir información, sigan siendo eficaces en el volátil entorno tecnológico. Como los datos en el nuevo entorno tecnológico no siempre son estáticos, sino que pueden estar en movimiento en el proceso de comunicación, otros procedimientos tradicionales de obtención de información relevantes para las telecomunicaciones, como la recopilación de los datos de tráfico en tiempo real y la interceptación de los datos de contenido, han sido adaptados con el fin de permitir la recopilación de los datos electrónicos que se encuentran en el proceso de la comunicación.

Todas las disposiciones a las que hace referencia esta Sección tienen como finalidad permitir la obtención o recopilación de datos a fin de realizar investigaciones o procedimientos penales específicos.

Los procedimientos en general, se refieren a todo tipo de datos, incluyendo tres tipos específicos de datos informáticos: datos del tráfico, datos de contenidos y datos sobre los abonados, que pueden encontrarse de dos formas; almacenados o en el proceso de la comunicación. La aplicabilidad de un

procedimiento a un tipo o formato particular de datos electrónicos depende de la naturaleza y del formato de los datos y de la naturaleza del procedimiento, como se describe específicamente en cada artículo.

Al adaptar las leyes procesales tradicionales al nuevo entorno tecnológico, en las disposiciones de esta sección surge el problema de elegir la terminología apropiada. Las opciones incluyeron mantener el lenguaje tradicional ('allanar' y 'secuestrar'), usar términos informáticos nuevos y más orientados hacia la tecnología ('acceder' y 'copiar'), como los adoptados en los textos de otros foros internacionales sobre el tema (tales como el subgrupo sobre Delitos Tecnológicos Graves del Grupo de los 8), o emplear un lenguaje combinado ('allanar o acceder de manera similar' y 'secuestrar o conseguir de manera similar'). Como existe la necesidad de reflejar la evolución de los conceptos en el entorno electrónico y de identificar y mantener también sus raíces tradicionales, se empleó el enfoque flexible de permitir que los estados utilicen tanto los antiguos conceptos de "allanar y secuestrar" como los nuevos conceptos de "acceder y copiar".

Todos los artículos incluidos en la Sección se refieren a "autoridades competentes" y a las facultades que les deben ser conferidas a los fines de llevar a cabo las investigaciones o procedimientos penales específicos. En algunos países,

sólo los jueces tienen la facultad de ordenar o autorizar la recopilación o producción de pruebas, mientras que en otros países los fiscales u otros funcionarios encargados de aplicar las leyes tienen las mismas o similares facultades. Consecuentemente, 'autoridad competente' se refiere a una autoridad de aplicación ya sea judicial, administrativa o de otra índole, facultada conforme a las leyes de cada país a autorizar o llevar a cabo la ejecución de medidas procesales a los fines de recopilar o producir pruebas con respecto a investigaciones o procedimientos penales específicos.

Otro aspecto importante, se contempla en el artículo 22, al determinar una serie de criterios en virtud de los cuales las Partes están obligadas a establecer jurisdicción respecto de los delitos penales enumerados en los artículos 2 a 11 del Convenio.

Se requiere a cada Parte castigue la comisión de los delitos establecidos en este Convenio cometidos en su territorio. Por ejemplo, una Parte haría valer su jurisdicción territorial si tanto la persona que ataca a un sistema informático como el sistema que es víctima del ataque están ubicados en su territorio y cuando el sistema informático atacado se encuentre en su territorio, aún si el atacante no lo está.

Es preciso que cada Parte establezca su jurisdicción penal respecto de los delitos que se cometan a bordo de buques de sus respectivas banderas o a bordo de aeronaves registradas conforme a sus respectivas leyes. Esta obligación, ya está implementada como un asunto general en las leyes de muchos estados, ya que dichos buques y aeronaves a menudo son considerados como una extensión de la jurisdicción de un Estado. Este tipo de jurisdicción, es principalmente útil cuando el buque o la aeronave no están ubicados en su territorio al momento de la comisión del delito. Si el delito se comete a bordo de un buque o aeronave que se encuentre fuera del territorio de la Parte de bandera, puede no haber ningún otro Estado que pudiera ejercer su jurisdicción de no ser por este requerimiento.

De igual modo, si un delito es cometido a bordo de un buque o aeronave que simplemente está atravesando las aguas o el espacio aéreo de otro Estado, el último Estado puede enfrentar impedimentos prácticos significativos para ejercer su jurisdicción y en consecuencia, es útil para el Estado donde está registrado el buque o la aeronave extendiendo su jurisdicción.

También se establece el principio de la nacionalidad, aplicado frecuentemente basándose en la tradición del derecho civil. Conforme a dicho principio, quienes tienen la nacionalidad de un Estado están obligados a cumplir con

las leyes nacionales a pesar de encontrarse fuera de sus respectivos territorios. De esta manera, si una persona con una determinada nacionalidad comete un delito en el extranjero, la Parte está obligada a procesarlo, si la conducta constituye también un delito conforme a las leyes del Estado en el cual se cometió el delito o si la conducta tuvo lugar fuera de la jurisdicción territorial de un Estado.

En el caso de delitos cometidos mediante el uso de sistemas informáticos, podrán generarse situaciones de concurrencia, cuando más de una Parte tenga jurisdicción sobre algunos o todos los participantes en un delito. Por ejemplo, muchos ataques de virus, fraudes y violaciones a los derechos de autor cometidos mediante el uso de Internet están dirigidos a víctimas ubicadas en diversos estados. Con el fin de evitar la duplicación del esfuerzo, inconvenientes innecesarios para los testigos, o la competencia entre los funcionarios encargados de aplicar las leyes de los estados involucrados, o de lo contrario para facilitar la eficiencia o equidad de los procedimientos, las Partes afectadas han de desahogar consultas con el fin de determinar la jurisdicción apropiada para el proceso.

En algunos casos, será más eficaz para los estados involucrados elegir una jurisdicción única para el proceso; en otros, puede ser mejor que un Estado procese a algunos participantes y que uno o más estados se encarguen de procesar a los demás.

Cualquiera de ambas opciones están permitidas. Finalmente, la obligación de consultar no es absoluta, pero ha de tener lugar "cuando sea apropiada". Así, por ejemplo, si una de las Partes sabe que la consulta no es necesaria, por haber recibido la confirmación de que la otra Parte no está planeando iniciar una acción, o si una Parte considera que la consulta puede perjudicar su investigación o procedimiento, puede demorar o negarse a efectuar la misma.

Intentando una cobertura integral, el Convenio combina la regulación de aspectos sustantivos y adjetivos, en el último de ellos, se orientan los criterios de los Estados para determinar la competencia de sus autoridades, sin pasar por alto lo dispuesto en el derecho interno.

3.5. COOPERACIÓN INTERNACIONAL Y ASISTENCIA MUTUA CON RESPECTO A LOS DELITOS INFORMÁTICOS.

Entendida en el sentido más amplio posible, la cooperación que deben brindarse los Estados Partes en la lucha contra los delitos informáticos, habrá de eliminar los impedimentos para que la información y las pruebas fluyan de manera rápida e ininterrumpida a nivel internacional.

De acuerdo al Convenio, la cooperación ha de extenderse a todos los delitos penales relacionados con los sistemas y los datos informáticos, así como también, a la recopilación de pruebas en formato electrónico sobre un delito penal. Esto significa que, tanto el delito cometido mediante el uso de un sistema informático o un delito común no cometido mediante el uso de un sistema informático que involucra a pruebas electrónicas, quedan comprendidos en los términos del Capítulo III referido a la Cooperación Internacional.

Es de observarse que los artículos 24 referido a la extradición, 33 a la asistencia mutua con respecto a la recopilación de los datos de tráfico en tiempo real y 34 a la asistencia mutua con respecto a la interceptación de los datos de contenido, permiten que las Partes prevean diferentes alcances para la aplicación de estas medidas.

Se señala también que la cooperación ha de llevarse a cabo "conforme a las disposiciones del Capítulo III" como "mediante la aplicación de los convenios internacionales pertinentes sobre cooperación internacional en materia de asuntos penales, los acuerdos celebrados con base en una legislación uniforme y recíproca y las leyes nacionales." En consecuencia, se establece el principio general de que las disposiciones del Capítulo III no reemplazan las disposiciones de los convenios

internacionales sobre asistencia jurídica mutua y extradición, los acuerdos recíprocos celebrados entre las partes o las disposiciones pertinentes contenidas en las leyes de cada país con relación a la cooperación internacional. Este principio básico está explícitamente reforzado en los artículos 24 sobre extradición, 25 principios generales relacionados con la asistencia mutua, 26 información espontánea, 27 procedimientos que corresponde aplicar a los pedidos de asistencia mutua ante la ausencia de acuerdos internacionales pertinentes, 28 confidencialidad y limitaciones de uso, 31 asistencia mutua con respecto a acceder a datos informáticos almacenados, 33 asistencia mutua con respecto a la recopilación de datos de tráfico en tiempo real y 34 asistencia mutua con respecto a la interceptación de los datos de contenido.

En cuanto a la obligación de extraditar, se aplica sólo a los delitos establecidos conforme con los Artículos 2 a 11 del Convenio que sean punibles en virtud de las leyes de ambas Partes intervinientes, mediante la privación de la libertad por un período de al menos un año o por una pena más severa. Si una Parte no tiene un tratado de extradición con la Parte solicitante o los tratados existentes no abarcan un pedido efectuado respecto de los delitos establecidos de acuerdo con este Convenio, pueden utilizar el propio instrumento como base para efectuar la extradición de la persona requerida, si bien no está obligada a hacerlo.

Se aplica también el principio "aut dedere aut judicare" (extraditar o procesar), si la otra parte ha solicitado la extradición del acusado y la extradición ha sido rechazada fundándose en que el acusado tiene la nacionalidad de la Parte Requerida, a pedido de la Parte solicitante, la Requerida deberá presentar el caso ante sus autoridades para su procesamiento. Si la Parte Requirente no solicita la presentación del caso para que se lleve a cabo una investigación y un procesamiento a nivel local, no existe obligación para la Parte Requerida de iniciar las acciones.

Por otro lado, la asistencia mutua se rige bajo los mismos principios generales de la cooperación internacional, es decir, la asistencia mutua ha de ser en principio extensiva y los impedimentos a la misma estrictamente limitados, la obligación de cooperar se aplica en principio tanto a los delitos penales relacionados con sistemas y datos informáticos como a la recopilación de pruebas en formato electrónico de un delito penal.

Debido a la volatilidad de los datos informáticos, toda vez que apretando unas teclas o mediante la operación de programas automáticos estos pueden ser eliminados, haciendo imposible seguir la pista de un delito hasta su autor o destruyendo pruebas esenciales de su culpabilidad, la cooperación cobra significativa importancia. Algunas formas de datos informáticos están almacenadas sólo por cortos

períodos de tiempo antes de ser eliminadas. En otros casos, se puede causar un daño grave a personas o bienes si las pruebas no son reunidas rápidamente. En situaciones de urgencia, no sólo el pedido, sino también la respuesta deben efectuarse en forma expedita. El objetivo que persigue el Convenio es, por tanto, facilitar la aceleración del proceso de obtener la asistencia mutua de manera tal que la información o las pruebas esenciales no se pierdan debido a ser eliminadas antes de que el pedido de asistencia pudiera ser preparado, transmitido y respondido.

Se establece también, un tipo de información espontánea, una Parte, dentro de los límites de sus leyes nacionales, sin previa solicitud, puede enviar a otra Parte información obtenida dentro del marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte que la recibe, para iniciar o realizar investigaciones o procedimientos concernientes a los delitos penales establecidos conforme al Convenio. No obstante, antes de proveer dicha información, la Parte que la provee puede solicitar que sea mantenida en forma confidencial o utilizada de acuerdo a ciertas condiciones.

El Convenio obliga a las Partes a aplicar ciertos procedimientos y condiciones de asistencia mutua, cuando no existen tratados o acuerdos de asistencia mutua, con base en una legislación uniforme o recíproca vigente entre las Partes que

solicitan y a las que les solicitan un pedido de asistencia mutua. Se refuerza de esta forma el principio general de que la asistencia mutua debe llevarse a cabo mediante la aplicación de tratados pertinentes y acuerdos similares de asistencia mutua.

De esta forma, se establece una serie de normas para proveer la asistencia mutua ante la ausencia de un tratado de asistencia mutua o de un acuerdo apoyado en una legislación uniforme o recíproca, que incluyen el establecimiento de autoridades centrales, la imposición de condiciones, los motivos y procedimientos posibles en caso de postergación o denegación, la confidencialidad de los pedidos y comunicaciones directas. Con respecto a dichas cuestiones expresamente abarcadas, ante la ausencia de un convenio o acuerdo de asistencia mutua, con base en una legislación uniforme o recíproca, se aplican estas disposiciones en lugar de otras leyes nacionales aplicables sobre asistencia mutua.

En el Convenio se insiste, en la finalidad de proveer mecanismos específicos a fin de tomar medidas eficaces y concertadas a nivel internacional en los casos que involucren a delitos relacionados con el uso de computadoras y pruebas que estén en formato electrónico. De esta forma, se establece la pronta preservación de datos informáticos almacenados, autorizando a una Parte a solicitar la pronta preservación de los datos almacenados, a fin de que no sean alterados, removidos o

eliminados durante el período de tiempo requerido para preparar, transmitir y llevar a cabo un pedido de asistencia mutua para obtener los datos. La preservación es una medida limitada y provisional ideada para ser aplicada mucho más rápidamente que la ejecución de un pedido de asistencia mutua tradicional.

Si bien es mucho más rápida que la práctica convencional de asistencia mutua, esta medida es al mismo tiempo menos intrusiva. Este procedimiento tiene la ventaja de ser rápido y proteger la privacidad de la persona a quien corresponden los datos, ya que los datos no serán revelados ni revisados por ningún funcionario gubernamental hasta que se cumplan los criterios requeridos para permitir la revelación plena de los mismos conforme a los regímenes de asistencia mutua convencionales. Al mismo tiempo, la Parte a la que se le solicitó la asistencia puede usar otros procedimientos para asegurar la rápida preservación de los datos, incluyendo el pronto libramiento y ejecución de una orden de suministrar información o de una orden de allanamiento de los datos. El principal requerimiento es contar con un proceso extremadamente rápido para evitar que los datos se pierdan irreparablemente.

Cabe mencionar que la información suministrada será sumaria e incluirá sólo la información mínima requerida para permitir la preservación de los datos.

Además de especificar la autoridad que está solicitando la preservación y el delito por el cual se solicita la medida, el pedido debe suministrar una síntesis de los hechos, información suficiente para identificar los datos que han de preservarse y su ubicación y demostrar que los datos son relevantes para la investigación o el juicio relacionado con el delito en cuestión y que dicha preservación es necesaria. La Parte solicitante debe comprometerse a presentar posteriormente un pedido de asistencia mutua para poder obtener la producción de los datos.

Aspecto relevante, es que el principio de la doble criminalidad no puede ser requerido como condición para efectuar la preservación de los datos. Por consiguiente, la regla general es que las Partes no deben imponer ningún requerimiento respecto de la doble criminalidad a los fines de la preservación.

Si una Parte, para responder a un pedido de asistencia mutua relativo el suministro de los datos, tiene motivos para creer que, al momento de la revelación, no se cumplirá con el principio de la doble criminalidad, puede reservarse el derecho de requerir la doble criminalidad como una precondición para efectuar la preservación de los datos. Con respecto a los delitos establecidos en el Convenio, se presume que la condición de doble criminalidad se cumple automáticamente entre las Partes.

Una Parte, a la que se solicitó la asistencia, puede únicamente rechazar el pedido de preservación cuando su ejecución perjudique su soberanía, la seguridad, el orden público u otros intereses esenciales o cuando considere que el delito es un delito político o un delito relacionado con un delito político. Debido al carácter central de esta medida para una investigación o un juicio eficaz con relación a un delito informático o a un delito relacionado con el uso de computadoras, se acordó que se excluye la posibilidad de considerar cualquier otra base para rechazar un pedido de preservación.

Por otro lado, mientras se lleva a cabo un pedido para preservar datos de tráfico concernientes a una comunicación específica, si la Parte a la que se le efectuó el pedido descubre que un proveedor de servicios de otro Estado estuvo involucrado en la transmisión de la comunicación, deberá revelar con la mayor rapidez posible a la Parte solicitante, una cantidad suficiente de datos de tráfico con el fin de identificar a ese proveedor de servicios y el trayecto a través del cual se transmitió la comunicación.

Sin embargo, la Parte a la que se le solicitó la asistencia puede negarse a revelar los datos de tráfico sólo cuando sea probable que la revelación perjudique su

soberanía, la seguridad, el orden público u otros intereses esenciales o cuando considere que el delito es un delito político o un delito conectado con un delito político.

Por lo que se refiere a la Asistencia mutua con respecto a acceder a datos informáticos almacenados, se establece que cada Parte debe tener, para beneficio de la otra Parte, la capacidad de allanar o acceder de manera similar, secuestrar o conseguir de manera similar y revelar los datos almacenados por medio de un sistema informático ubicado dentro de su territorio.

El artículo 32, acceso transfronterizo a datos almacenados con consentimiento o cuando estén disponibles al público, por su parte, aborda dos situaciones: primero, cuando los datos a los que se ha de acceder están disponibles para el público y segundo, cuando una Parte ha accedido a datos o recibido datos ubicados fuera de su territorio a través de un sistema informático de su territorio y ha obtenido el consentimiento voluntario y legítimo de la persona que tiene facultades legítimas para revelar los datos a la Parte a través de ese sistema. En ambos casos, la Parte donde están ubicados los datos no puede tomar ninguna medida para impedir, castigar o reclamar las medidas unilaterales adoptadas por el Estado que accede a los datos.

Por último, las partes deberán proveerse asistencia mutua con respecto a la recopilación de datos de tráfico en tiempo real y a la recopilación o al registro en tiempo real de los datos de contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que las leyes nacionales y los tratados aplicables lo permitan.

Conforme al Título 3, denominado Red 24/7, cada Parte tiene la obligación de designar un punto de contacto que esté disponible las 24 horas, los 7 días de la semana a fin de asegurar la asistencia inmediata en las investigaciones y los procedimientos. Se acordó que el establecimiento de esta red, se encuentra entre los medios más importantes previstos por este Convenio, para asegurar que las Partes puedan responder eficazmente a los desafíos que plantea la aplicación de las leyes respecto de los delitos informáticos o los delitos relacionados con el uso de computadoras.

El punto de contacto 24/7 de cada Parte, es para facilitar o llevar a cabo directamente, entre otras cosas, la prestación de asesoramiento técnico, la preservación de los datos, la recopilación de pruebas, el brindar información legal y localizar a sospechosos.

Cada parte tiene la libertad de determinar dónde ubicar el punto de contacto dentro de su estructura de aplicación de las leyes. Algunas Partes pueden querer alojar el punto de contacto 24/7 dentro de la Autoridad Central encargada de la asistencia mutua, algunas pueden creer que la mejor ubicación es dentro de una unidad de la policía que se especialice en la lucha contra los delitos informáticos o los delitos relacionados con el uso de computadoras.

Como el punto de contacto 24/7 ha de proveer asesoramiento técnico para detener o rastrear un ataque y también ha de cumplir con las obligaciones de cooperación internacional, tales como localizar sospechosos, debe buscarse ofrecer respuestas correctas y que la estructura de la red evolucione con el correr del tiempo. Al designar el punto de contacto nacional, se debe dar especial consideración a la necesidad de comunicarse con puntos de contacto que utilizan otros idiomas.

De igual manera, se requiere que cada punto de contacto de la red cuente con los equipos apropiados. Contar con modernos equipos telefónicos, de fax y de computación, será esencial para que la red opere fluidamente, incorporando otras formas de comunicación de equipos analíticos como parte del sistema a medida que la tecnología avance. El personal que participa como parte del equipo de una Parte que

trabaja en la red, debe estar bien capacitado respecto de los delitos informáticos y de los delitos relacionados con el uso de computadoras y cómo responder a los mismos eficazmente.

Reproduciendo la experiencia de otros convenios alusivos al combate del crimen transnacional, el Convenio materia de análisis, insiste en las bondades de la cooperación. A lo largo de su texto, se destaca que la lucha contra el crimen electrónico no puede ganarse sola. Ningún país, por más avanzado que sea, debe permitirse el lujo de repudiar la cooperación y asistencia mutua.

CAPITULO IV

PANORAMA JURIDICO EN MEXICO SOBRE LOS DELITOS INFORMATICOS.

CAPITULO IV.- PANORAMA JURIDICO EN MEXICO SOBRE LOS DELITOS INFORMATICOS.

4.1. LA LIBERTAD INFORMATICA Y EL DERECHO MEXICANO.

En su forma más simple, la libertad de expresión, es la libertad de expresarse y comunicarse. Esta libertad es de naturaleza dual resumida de la siguiente forma: "toda persona tiene derecho de tener acceso a información e ideas difundidas por otros". El alcance de esta libertad es extremadamente amplio y abarca incluso información de contenido diverso, incluyendo al ofensivo, escandalizante o preocupante lo mismo que información comercial, cultural y científica, por nombrar algunas de ellas.

La aludida libertad de expresión conocida en el derecho positivo mexicano como la libre manifestación de las ideas, ha llegado a su esplendor en las últimas tres décadas a través de Internet, como se ha mencionado, cuenta con una amplia gama de servicios por los que cada persona ya sea física o moral, puede exteriorizar cualquier cosa en la red.

Prácticamente ilimitada es la posibilidad de colocar todo tipo de contenidos en Internet. Dentro de la red, se localizan enormes cantidades de material informativo, recreativo y didáctico, pero también, otros sitios destinados a promover actitudes de intolerancia, racismo, odio y numerosas páginas de pornografía.

Los principales y más frecuentes intentos para reglamentar Internet, buscan censurar los contenidos considerados obscenos. Se suele argumentar que la exposición abierta de materiales de esa índole, puede afectar a niños y jóvenes. Sin embargo la prohibición de que dichos materiales circulen por Internet representa para muchos usuarios una censura no sólo moral sino también ideológica y política, ya que cada quien puede juzgar, de acuerdo a sus propios parámetros, la obscenidad o lubricidad. En consecuencia esta censura resultaría anticonstitucional por atentar contra la libertad de expresión.

Al respecto podemos señalar que, si bien la libertad de expresión es un derecho inherente al hombre, también lo es, la obligación de no atacar derechos de terceros que redunden en un malestar o perjuicio a la sociedad. De ahí que nuestra legislación señale en que casos han de ser sancionados quienes se extralimiten sobre el ejercicio de dicha libertad.

Ante esta situación, es conveniente especificar si los medios informáticos de comunicación permiten evadir la obligación de respetar el derecho de los demás o, por el contrario, existe un marco jurídico efectivo para regular dichas conductas.

Sobre el particular, es oportuno destacar el comentario que hacen los juristas Gabriela Barrios Garrido, Marcia Muñoz de Alba Medrano y Camilo Pérez Bustillo en el libro titulado "Internet y Derecho en México"[15], en el que se considera que si Internet es un espacio caracterizado por la manifestación de las ideas entonces debe estar sujeto a las limitaciones constitucionales impuestas al ejercicio de la libertad de expresión. Internet no se ha tipificado en ley alguna, pero si se le conceptúa como un nuevo medio de comunicación masiva que, pese a todo, va más allá de la comunicación, y por tanto le son aplicadas por analogía las normas sobre libertad de expresión y derecho a la información contenidas en leyes señaladas, ya que la red conjuga, reconfigura y expande muchas de las características de los medios de comunicación tradicionales.

Sobre este comentario, es necesario destacar que en materias como la penal y administrativa, no esta permitido aplicar la analogía, ya que se rigen por el principio de aplicación estricta de la ley, de tal suerte que si la autoridad está

[15] BARRIOS-GARRIDO, Gabriela. **Internet y derecho en México.** Edit. Mc Graw Hill. 1ª. ed. 1998, México.

impedida para actuar más allá de lo preceptuado en la norma, habrá circunstancias en que pese a la flagrante violación de derechos de un tercero o de los intereses del propio Estado no podrá ser sancionado de un modo directo.

Ahora bien, el marco constitucional en nuestro país sobre la libertad de expresión se encuentra establecido en el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, que establece la libertad de expresión en forma general y en el 7°, establece la libertad de escribir y publicar obras sobre cualquier materia.

Art. 6°. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público;...

Art. 7. 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...

Interpretando los preceptos constitucionales, la Ley Reglamentaria[16] de los artículos 6° y 7°, desentrañando el sentido de las disposiciones, considera que se atenta contra:

a) La vida privada, cuando se cause odio, desprecio o demérito hacia una persona, o con tal actitud se le perjudique en sus intereses;
b) La moral, cuando se defiendan o aconsejen vicios, faltas o delitos, o se ofenda al pudor, decencia o buenas costumbres, y
c) La paz pública, cuando se desprestigien, ridiculicen o destruyan las instituciones fundamentales del país, se injurie a México, se lastime su buen crédito, o se incite al motín, a la rebelión o a la anarquía.

La idea anterior tiene su antecedente en la Declaración Francesa de los Derechos del Hombre y del Ciudadano, concretamente, en su artículo IV, mismo que especificaba que la libertad en su sentido lato, consiste en poder hacer todo lo que no dañe a otro sea este un individuo o el propio Estado. Sin embargo, de las cuatro limitantes que impone nuestra Constitución hacia la libre manifestación de las ideas, es menester señalar que para su fehaciente comprobación y valoración queda al

[16] Ley de Imprenta. Diario Oficial de la Federación. 12 de abril de 1917.

arbitrio y discrecionalidad de las autoridades judiciales y administrativas en sus respectivas instancias.

Asimismo, aunada a la libre manifestación de las ideas, y conforme a una adición al numeral 6 constitucional, en el sentido de que el derecho a la información será garantizado por el Estado, es preciso considerar que ésta adición se produjo con motivo de la iniciativa presidencial de 5 de octubre de 1977, para consagrar el derecho a la información que comprende:

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

En un trabajo reciente Jorge Carpizo[17] señala:

[17]CARPIZO, Jorge. **Constitución e Información**, en Carbonell, Miguel y Valadés, Diego, México, UNAM, Instituto de Investigaciones Jurídicas, 2000, pp. 161.

En 1948 con la Declaración Universal de los Derechos del Hombre nace la garantía fundamental del derecho a la información.

El derecho a la información es la garantía fundamental que toda persona posee a: atraerse información, a informar y a ser informada.

De la definición apuntada se desprenden los tres aspectos más importantes que comprende dicha garantía:

1. El derecho a atraerse información;
2. El derecho a informar, y
3. El derecho a ser informado.

A. El derecho a atraerse información incluye las facultades de a) acceso a los archivos, registros y documentos públicos, y b) la decisión de qué medio se lee, se escucha o se contempla.
B. El derecho a informar incluye las a) libertades de expresión y de imprenta y, b) la constitución de sociedades y empresas informativas.
C. El derecho a ser informado incluye las facultades de a) recibir información veraz y oportuna, b) la cual debe ser completa, es decir, el derecho a enterarse

de todas las noticias, y c) con carácter universal, o sea, que la información es para todas las personas sin ninguna exclusión.

El derecho a la información, fundamentado en la parte final del artículo 6° constitucional se considera un derecho social e individual, por medio del cual se garantiza que el gobernado esté debidamente enterado de los diversos procesos o factores de variada índole –social, política, o económica- que se realicen en la sociedad y que afecten o no a la misma.

De esta manera se considera que el derecho de acceso a Internet es una expresión del derecho a la información y a la comunicación, pero también, del derecho a la cultura y, de manera más amplia, al bienestar.

Lamentablemente, la promoción de Internet no ha formado parte de las prioridades de los gobiernos en países como el nuestro. Todavía, se mira con extrañeza, la promoción de una cultura informática que sea nacional tanto en calidad como en cobertura, en sociedades como la mexicana se suele considerar que esos asuntos no deben formar parte de las prioridades del Estado. Además, en el caso mexicano, se puede reconocer una notoria e incluso deliberada negligencia, en México el gobierno ha permanecido ausente del impulso a la instalación de redes de

cómputo y en el fomento para que el acceso a Internet forme parte de los recursos habituales de los ciudadanos. El resultado ha sido un crecimiento desigual del acceso de los mexicanos a Internet, por lo que sería preciso quitarle a Internet la imagen que tiene como medio que sólo puede interesar a las elites, o que únicamente sirve para el entretenimiento, ya que el derecho de todos a Internet es parte del derecho a la información.

Por otro lado, es frecuente encontramos ante la posibilidad de que nuestra información personal y más particular, tenga que ser almacenada o respaldada en fuentes o bienes informáticos. Este fenómeno que, a simple vista puede resultar cotidiano, es necesario vislumbrarlo o cuestionarlo como una posible o presumible intromisión en la esfera privada o íntima de las personas y, ante esto, es necesario también determinar si las normas jurídicas deben delimitar estos alcances.

Tarea fundamental de nuestros códigos Civil, Penal, y algunos artículos de la Ley Federal del Derecho de Autor, es asegurar el respeto de los derechos a la intimidad, cuando ciertas informaciones que le conciernen sean transmitidas por Internet a nivel nacional o mundial. En el caso de México, no contamos con disposiciones jurídicas que de manera general, ordenada, expresa y directa reconozca los mencionados derechos a la intimidad, o bien, de la vida privada, sobre todo con

especificaciones claras hacia el ámbito de aquella información de tal naturaleza que se automatiza.

Sin embargo, es importante señalar que la actual Ley Federal del Derecho de Autor[18], establece en sus artículos 107-110 algunas disposiciones respecto a los datos o informaciones contenidos en bancos de datos, tal es el caso del artículo 109 que a la letra dice:

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

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

[18] Ley Federal del Derecho de Autor. Diario Oficial de la Federación. Martes 24 de diciembre de 1996.

La redacción de este artículo permite la confidencialidad de los datos nominativos que circulen sobre Internet. Pero aunque sin lugar a dudas constituye un avance, en México falta aún concretar esta norma jurídica, poniendo a disposición de los quejosos una infraestructura que les permita resolver sus controversias en la materia.

A nivel internacional, el tratado de Libre Comercio de América del Norte[19], deja entrever una disposición sobre la protección de las personas.

Artículo 2105. Divulgación de información:

Ninguna disposición en este Tratado se interpretará en el sentido de obligar a ninguna de las Partes a proporcionar o dar acceso a información cuya divulgación pudiera impedir el cumplimiento de las leyes de la Parte o fuera contraria a sus leyes que protegen la privacía de las personas, los asuntos financieros y las cuentas bancarias de clientes individuales de las instituciones financieras.

Como se puede apreciar, estas disposiciones son de gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer

[19] Tratado de Libre Comercio de América del Norte (TLC). Diario Oficial de la Federación. Lunes 20 de diciembre de 1993.

con esta información. Así, al acceso no autorizado a una base de datos de carácter personal de un Hospital de enfermos de SIDA puede ser utilizado contra estas personas quienes a causa de su enfermedad, se encuentran marginados socialmente, en la mayoría de los casos.

De igual manera, es necesaria la protección a este tipo de bases de datos en virtud de que la información contenida en ellas, puede referirse a datos de carácter sensible, como son las creencias religiosas o la filiación política. Adicionalmente, pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de crédito que posean grandes sumas de dinero, en fin, la regulación de la protección a la intimidad personal es un aspecto de suma importancia que debe asegurarse y respetarse.

Si recurrimos a la dimensión normativa en el plano internacional sobre la libertad de expresión y los medios informáticos, apreciamos que en algunos países desarrollados, se ha adoptado el compromiso de no establecer un marco jurídico riguroso sobre dicha libertad. Desde esa perspectiva, aquellos sistemas jurídicos se abstendrán de regular con determinación la libertad de expresión, por considerar necesario brindarle espacios suficientemente amplios, ubicamos en este grupo a naciones europeas particularmente.

Otros estados, entre ellos México, aún no deciden en que tendencia se ubicarán. La ausencia de determinación respecto a si deben regular con rigor la expresión de ideas por medios informáticos, debe ser atendida. En el caso de adoptar una postura de control estricto, habrían de proceder a elaborar la normatividad específica, en caso contrario, sería necesario marcar las pautas para entender que se permite una expresión flexible de ideas.

Debido a las características de la red de redes, resulta sumamente complicado que la normatividad de un país, donde se decidió el control estricto en la expresión de ideas, resulte efectiva. Sobre todo, mientras no se consiga armonizar la tendencia en la regulación internacional de esa libertad de expresión.

4.2. PROTECCION JURIDICA DE LOS BIENES INFORMATICOS EN MEXICO.

En la actualidad es importante abordar el tema de la protección de los bienes informáticos, es decir, la regulación jurídica que existe en México sobre dichos bienes. En este entendido, es pertinente precisar que el marco jurídico de la propiedad intelectual es el que regula el status jurídico de los bienes informáticos. Entendemos a los bienes informáticos en un sentido amplio; es decir, la combinación

de los elementos de una computadora, a saber, el denominado hardware y software, también designados la parte física y la parte inteligente de la computadora.

Entonces, los derechos de la propiedad industrial son el marco jurídico que protege las creaciones de la parte física de la computadora; es decir, los derechos relacionados con las patentes, marcas, modelos de utilidad, diseños industriales, secretos industriales, avisos comerciales y signos distintivos; y los derechos de autor, protegen la parte inteligente de la computadora, precisamente, los programas de cómputo.

Con relación a la situación jurídica mexicana, los derechos de autor consisten en el reconocimiento del Estado a favor de todo creador de obras literarias y artísticas; donde se conceden derechos de naturaleza moral -unidos al autor, que son inalienables, imprescriptibles, irrenunciables e inembargables- y patrimonial, que implican el derecho del autor de explotar de manera exclusiva o de autorizar a otros la explotación. Estos derechos son reconocidos en Internet ya que contiene textos, imágenes, gráficos, software, el cual debe ser igualmente protegido.

La Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997[20], regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos.

Como ejemplo de las múltiples disposiciones que regulan el fenómeno Internet, tenemos el caso del artículo 13 del citado ordenamiento, en el que se reconoce la protección de programas de cómputo y de compilación, integrada por las colecciones de obras, tales como las enciclopedias, las antologías, y de obras u otros elementos como las bases de datos, siempre que dichas colecciones, por su selección o la disposición de su contenido o materias, constituyan una creación intelectual. De igual forma se reconoce en el artículo 16 la obra reproducida o almacenada, por

[20] Idem

medios electrónicos, que permitan al público leerla o conocerla visual, táctil o auditivamente.

Otra norma jurídica que protege la circulación de obras por medio de Internet, es el artículo 27 de la citada Ley, que regula los derechos patrimoniales de los titulares del derecho de autor y nos indica:

Art. 27. Los titulares de los derechos patrimoniales podrán autorizar o prohibir;

I. La reproducción, publicación, edición, fijación de su obra [...] por cualquier medio ya sea impreso, fonográfico, gráfico, plástico, audiovisual, electrónico u otro similar;
II. La comunicación pública de su obra;
    a) La representación, recitación y ejecución pública;
    b) La exhibición pública por cualquier medio o procedimiento;
    c) El acceso público por medio de la telecomunicación;
III. La transmisión pública o radiodifusión de sus obras, en cualquier modalidad, cable, fibra óptica, microondas, vía satélite o cualquier otro medio análogo...

Podemos observar en atención a este artículo, que hoy en día, todo tipo de información está disponible sobre Internet, pero que existe un límite para que toda reproducción de una obra circule sobre Internet, y este límite está constituido por los derechos patrimoniales y morales del autor de una obra. Así, vemos que este artículo 27 otorga la facultad a todo titular del derecho patrimonial de decidir acerca de la publicación, edición, representación, transmisión, acceso, ejecución o reproducción de su obra, trátese de una reproducción tradicional, como es el caso de una fotocopia o de una reproducción vía Internet o medio análogo.

Adicionalmente de que los autores conservan su derecho moral, encaminado a la protección de la originalidad, pueden oponerse a toda mutilación, deformación o cambio de su obra, situación que se presenta muy a menudo por medio de las redes, ya que algunos usuarios tienen tendencia a crear sus páginas Web con diseños o textos de otros autores, y en ocasiones lo adaptan a sus propios gustos, sin consultar al autor de la obra.

De la situación descrita, surge la necesidad de lograr el efectivo respeto de los derechos morales y patrimoniales en cada espacio del planeta; al no existir un organismo o autoridad competente en Internet que pueda rastrear copias ilegales,

cualquier trabajo en la red puede ser copiado y distribuido internacionalmente en segundos sin que se pueda evitar.

A nivel internacional, se han estipulado tradicionalmente dos requerimientos para la correcta protección de una creación autoral:

A. Debe ser creada en su totalidad por el ingenio del autor.
B. Debe estar de manera fija en un medio de expresión tangible; o el autor debe haber dejado una marca de su personalidad en la obra al distribuirlo en cierta forma.

En Internet se protegen las siguientes obras suponiendo que cumplen con los requerimientos tradicionales:

A. Trabajos escritos: como el correo electrónico y los archivos anexados a él, los artículos colocados en los servidores FTP o Web, y los que están integrados a una base de datos.
B. Trabajos musicales o audiovisuales.
C. Imágenes: pueden ser dos clases, las creadas por una computadora y las producidas por un medio de digitalización, la reproducción de éstas puede

constituir una vulneración al derecho de propiedad, aunque para el segundo caso si se ha puesto suficiente creatividad en el proceso de digitalización se creará un nuevo trabajo protegido por derechos de autor.

D. Software: está protegido por los derechos de propiedad intelectual.

E. Bases de datos: El autor tiene derechos económicos y en algunos casos morales y es necesaria su aprobación para modificar, reproducir o difundir su trabajo, sin embargo, en países como Estados Unidos no se necesita autorización para hacer un uso legal del trabajo.

Respecto al derecho de autor, habrá de tener presente que el objeto de protección es una obra del espíritu, la cual puede ser un sonido, música, imagen, texto o un conjunto de todos estos elementos. El derecho de autor protege, lo que concierne a una creación literaria y artística. No es la función de la obra lo que se protege, puesto que las ideas son de libre circulación, lo que se protege es la forma.

Con base en lo anterior, podemos observar que efectivamente el autor de un trabajo tiene derechos que protegen su obra, pero no solo el autor tiene derechos, los usuarios también, por lo tanto el derecho de la propiedad intelectual tiene ciertos límites, sobre todo si el trabajo es transmitido por Internet.

No tendría sentido que un derecho particular sea un obstáculo para la comunicación, la cultura, y en general, cualquier tipo de información que puede ser útil al público en general, siempre y cuando no cause un daño injustificado a los derechos legítimos del autor. Los derechos que se conceden a los usuarios, son todos los que puedan considerarse legales, pero deben tomar en cuenta los siguientes factores:

A. El fin y carácter del uso no deben ser comerciales o lucrativos.
B. La naturaleza del trabajo, la calidad y sustancia de la parte utilizada con relación al trabajo como un todo.
C. El efecto de su uso en el mercado o su valor.

Generalmente, se autoriza la reproducción de un trabajo para el uso privado del usuario. Por ejemplo, la ley permite a un estudiante universitario usar Internet para hacer copias de ciertos trabajos o a las bibliotecas, las cuales pueden reproducir y distribuir con fines pedagógicos y no comerciales aún sin la autorización de su autor. No obstante, se lo impide a una compañía privada que busque explotar la idea con fines lucrativos.

Sin abandonar la referencia a la protección de los derechos de autor, destacando en esta parte de la investigación, la evolución y desarrollo de la normatividad internacional, es conveniente señalar que existen disposiciones que contemplan la propiedad intelectual, citando el Tratado de Libre Comercio de América del Norte (TLC) firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993[21], contiene un apartado sobre propiedad intelectual, a saber la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado, se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas

[21] Tratado de Libre Comercio de América del Norte (TLC). Diario Oficial de la Federación. Lunes 20 de diciembre de 1993.

eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado, además en el párrafo 1 del artículo 1717 titulado Procedimientos y Sanciones Penales se contempla la figura de piratería de derechos de autor a escala comercial.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería de tres años a partir de la fecha de la firma del TLC, eso explica la entrada en vigor de nuestra Ley Federal de Derechos de Autor.

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información, se habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que estos consten en medios electrónicos o magnéticos.

Considerando las disposiciones normativas contenidas en las leyes específicas y aquellas que se derivan de los instrumentos jurídicos internacionales suscritos por nuestro país, estimamos que en México, el marco jurídico protector de los bienes informáticos es adecuado, ello no quiere decir que este exento de evolución.

4.3. RESPUESTA NORMATIVA NACIONAL SOBRE LOS DELITOS INFORMÁTICOS.

Para iniciar el estudio sobre la respuesta normativa de los delitos informáticos en México, es preciso retomar el tema de la Ley Federal del Derecho de Autor, ya que dicha ley regula, los programas de computación, las bases de datos, las infracciones derivadas de su uso ilícito y en su artículo 215 hace una remisión al Título Vigésimo Sexto, Artículo 424 Bis. Fracción II del Código Penal Federal[22] del que se infiere la sanción al uso de programas de virus.

Artículo 215.- Corresponde conocer a los tribunales de la federación de los delitos relacionados con el derecho de autor previstos en el titulo vigésimo sexto

[22] Código Penal Federal, De los Delitos en Materia de Derechos de Autor, Titulo Vigésimo sexto, Artículo 424 bis, fracción 2, Ediciones fiscales Isef, S.A., México 2002.

del Código Penal para el Distrito Federal en materia de fuero común y para toda la república en materia de fuero federal.

Por su parte, el título vigésimo sexto del Código Penal Federal, comprende los delitos en materia de derechos de autor, y en el mencionado artículo 424 Bis. Se establece:

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

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Si bien pudiera pensarse que la inclusión de las sanciones a la fabricación de programas de virus en el Código Penal lleva implícito el reconocimiento de un *delito informático,* debe tenerse presente que los delitos a regular en este título son en materia de derecho de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los *delitos informáticos* el bien jurídico a tutelar serían por ejemplo el de la intimidad, patrimonio, etcétera.

Igualmente, el artículo 231 de la Ley Federal del Derecho de Autor, fracción II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y "Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título Vigésimo Sexto del Código Penal citado. Sin embargo, la regulación existente no ha llegado a

contemplar, como ya lo mencionamos, el delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente.

Mantener en esas condiciones la normatividad específica, podría traer implicaciones desfavorables para México, entre las que podemos citar: la pérdida de prestigio a nivel internacional, por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional y la pérdida de credibilidad por las compañías proveedoras de programas informáticos, lo que se traduciría en un mercado poco atractivo para ellas que pondrían al país en una situación marginada del desarrollo tecnológico.

En este entendido, por la gravedad de la conducta ilícita en sí, y por las implicaciones que traería aparejadas, está totalmente justificada la regulación penal de los delitos informáticos.

En otro aspecto, es importante señalar la incidencia delictiva en los bienes informáticos. Como ya se explicó, las redes de telecomunicación pueden ser tanto objeto como instrumentos de una conducta delictiva. En términos generales, es cierto que pueden aplicarse los tipos clásicos del derecho penal, sin embargo, y por la

complejidad en el uso de los bienes informáticos, en muchos aspectos las conductas delictivas son difíciles de encuadrar en los tipos penales actualmente establecidos por el legislador.

Por ejemplo ¿cómo penalizar el robo de información?; ¿el acceso ilícito a un sistema o banco de datos?; ¿el manejo inadecuado de la información o su alteración? Recientemente el legislador mexicano, ha introducido nuevas figuras en este renglón, incorporando al Código Penal Federal el tipo de: "acceso ilícito a sistemas y equipos de informática".[23]

El marco jurídico penal federal se ha modificado para quedar de la siguiente manera: Título Noveno, "Revelación de secretos y acceso ilícito a sistemas y equipos de informática".

La reforma incorpora el artículo 211 bis 1-7, estableciendo tres nuevos tipos delictivos:

[23] Código Penal Federal, Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática, Título Noveno, Artículos 211bis1-211 bis 7, Ediciones fiscales Isef, S.A., México 2002.

a. acceso sin autorización a sistemas de información o equipos de informática que estén protegidos, modificando, destruyendo o provocando pérdida de información (artículo 211 bis-1);
b. acceso sin autorización a sistemas de información o equipos de informática del Estado que estén protegidos, modificando, destruyendo o provocando pérdida de información (artículo 211 bis-2), y
c. acceso sin autorización a sistemas de información o equipos de informática que integran el sistema financiero que estén protegidos, modificando, destruyendo o provocando pérdida de información (artículo 211 bis-4). Incrementándose las sanciones en cada caso que van desde seis meses a dos años de prisión y de tres meses a dos años de prisión y de cincuenta a trescientos días multa, para el caso del sistema financiero.

Pero cuando el acceso, la modificación o la destrucción son realizadas por algún sujeto que tenía autorización para introducirse en los sistemas de información o equipos de informática, evidentemente, un empleado, las sanciones aumentan. Éstas van desde los tres meses a un año de prisión y de cincuenta a ciento cincuenta días

multa; de seis meses a cuatro años de prisión y de cien a seiscientos días de multa para el caso del sistema financiero.

Si bien es cierto, que la reforma al marco jurídico penal mexicano sobre el acceso ilícito a sistemas de información y bancos de datos, constituyen un avance, también es cierto que existen todavía algunas lagunas de consideración, ya que debió modificarse, con la intención de proporcionar tanto al juzgador, al ministerio público, como a los abogados en general mayores elementos de juicio para la comprobación del delito. Es necesaria la creación de ministerios públicos especializados, así como peritos en la materia informática.

En conclusión, podemos decir que la Ley Federal del Derecho de Autor considera como bien jurídico tutelado la propiedad intelectual y que, el bien jurídico tutelado en los delitos informáticos es fundamentalmente el patrimonio, por lo que sería pertinente que en el Título Vigésimo Segundo sobre los "Delitos en contra de las personas en su patrimonio" del Código Penal Federal se añada un capítulo especial para los delitos informáticos.

Teniendo en cuenta también la gravedad que implican los delitos informáticos, es necesario que el Código Penal Federal incluya figuras delictivas que

contengan los delitos informáticos ya que de no hacerlo, la ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

Ahora bien, es preciso comentar que con respecto a la regulación jurídica de los delitos informáticos en México, en el estado de Sinaloa el Congreso Local ha legislado al respecto, incluyendo en el Código Penal Estatal, Título Décimo "Delitos contra el patrimonio", el Capítulo V titulado "Delito Informático"[24] en el que se establece:

Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:

I. Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o

[24] Código Penal y de Procedimientos Penales del Estado de Sinaloa. Editorial. Anaya 1996. México, D.F.

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 del delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Consideramos que se ubicó al delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

Por otra parte, es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste con base en las

facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, la jurisdicción federal y local de estos ilícitos.

4.4. EXPECTATIVAS DE LA NORMATIVIDAD MEXICANA SOBRE EL CIBERCRIMEN.

México no puede intentar regular Internet sin tomar en cuenta el contexto jurídico internacional. De hecho ningún país puede permitirse regular el fenómeno Internet aisladamente, puesto que la utilización masiva de Internet es sin fronteras; si se quiere regular eficazmente el mismo se tendrán que realizar más acuerdos internacionales que tiendan a armonizar las reglas aplicables a estos problemas.

No habría que olvidar que los valores de un país a otro cambian, se transforman y algunos prevalecen; lo que es importante resaltar es que los valores que siempre han orientado a la sociedad mexicana no deben ser influidos de manera negativa por otros, ajenos a nuestra idiosincrasia, sobre todo si es en perjuicio de los usuarios o de los creadores de una obra del espíritu intelectual.

Tal vez los problemas que México tendrá en el futuro con respecto a Internet serán problemas relacionados con la aplicación de leyes (conflicto de leyes en el tiempo y en el espacio), y la determinación del juez competente para resolver un conflicto dependerá de la cultura y de la sensibilidad del juez en la interpretación de las normas por aplicar. En cuanto al conflicto de leyes se tendrán que adoptar principios bien definidos, tal vez sea mejor la aplicación de la ley del lugar donde se constató la infracción, puesto que si la infracción se inicio fuera del territorio nacional, una sanción dada no será eficaz. Entonces hay que aplicar la ley en el territorio nacional, y este principio es el que por el momento parece, deberá aplicarse.

Otras dificultades deberán resolverse, como es el caso de los llamados sitios "espejo", o en materia de derecho procesal civil se presentarán los problemas de la prueba.

En cuanto a la protección de la propiedad intelectual en el mercado de la información, podemos decir que los productos y servicios no resultan efectivamente protegidos, es necesario el establecimiento de normas nacionales e internacionales claras, para la protección de la propiedad intelectual. Estas nuevas normas deberán estar equilibradas entre los intereses de los creadores y de los usuarios.

Deberá existir un compromiso con los creadores para proteger los frutos de su labor, y al mismo tiempo asegurar que el contenido de sus obras estará a disposición del público en general.

Se pide la creación de legislaciones nacionales e internacionales de efectiva aplicación para poder luchar eficazmente contra las actividades de piratería.

En cuanto al acceso abierto del mercado de la información, se dice que la protección de la propiedad intelectual y acceso abierto del mercado son las mejores maneras para estimular el desarrollo de productos locales y alcanzar las necesidades culturales e individuales. Hasta el momento Internet es más un lugar para intercambiar ideas y buscar información, que un lugar de transacciones comerciales. Lo que desean los grupos de interés es que la infraestructura de la información proporcione pleno acceso a la información económica y comercial para asistir a los esfuerzos de facilitación del comercio y alentar el apoyo para esas actividades.

CONCLUSIONES

Primera.- Resulta común que los avances tecnológicos representen un reto para el derecho, cada logro en la ciencia y la tecnología provocan una laguna en la normatividad existente y no es la excepción el campo de la informática, a menudo, el derecho responde con lentitud a los requerimientos tecnológicos.

Segunda.- Incuestionablemente, los medios informáticos o electrónicos traen enormes beneficios para la sociedad, pero también efectos negativos, en la medida que se han convertido en un terreno vasto para la delincuencia.

Tercera.- Debido a la naturaleza virtual de los delitos informáticos, su tipificación puede ser confusa. Es difícil la clasificación de estos actos, por ende, la creación de instrumentos legales podría no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de la normatividad relacionada con la informática.

Cuarta.- Catalogar a los denominados delitos informáticos, viene siendo uno de los puntos de mayor debate dentro del estudio de la criminalidad informática. La postura mayoritaria, se pronuncia diferenciando entre delitos computacionales, como nuevas formas comisivas de delitos tradicionales, y delitos informáticos que afectan un nuevo interés social, íntimamente ligado al tratamiento de la información.

Quinta.- Es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario para solucionar los problemas derivados del uso ilícito de la informática, desarrollar un régimen jurídico internacional que, mediante la cooperación, apoye la tipificación y persecución de los delitos informáticos.

Sexta.- Debido al carácter convencional del derecho internacional contemporáneo, con base en un instrumento jurídico obligatorio, como lo puede llegar a ser el Convenio Preliminar sobre Delitos Informáticos, se podría asegurar mayor eficacia en la lucha contra estos ilícitos.

Séptima.- En el marco del Convenio Preliminar sobre Delitos Informáticos, además de las medidas de cooperación internacional, se abordan cuestiones de derecho sustantivo y procesal, lo mismo que aquellas estrechamente conectadas con el uso de la tecnología de la información.

Octava.- Al igual que otros convenios, por la propia naturaleza de ellos, el Convenio Preliminar sobre Delitos Informáticos requiere la voluntad política de los estados interesados, no sólo para asegurar su entrada en vigor, sino la aplicación efectiva.

Novena.- Las normas jurídicas internacionales en vigor, están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, incluso, en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores.

Décima.- Sin duda, en materia de regulación de delitos informáticos, los europeos se han colocado a la vanguardia. Desde hace aproximadamente diez años, la mayoría de los países europeos han penalizado el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

Décima Primera.- En el derecho nacional, la reforma al marco jurídico penal sobre el acceso ilícito a sistemas de información y bancos de datos, constituye un avance, pero aún nos encontramos alejados de los logros obtenidos en otros sistemas jurídicos.

Décima Segunda.- El bien jurídico tutelado en los delitos informáticos es principalmente el patrimonio, sería pertinente que en el Título Vigésimo Segundo del Código Penal Federal, sobre los "Delitos en contra de las personas en su patrimonio", se añada un capítulo especial para los delitos informáticos.

BIBLIOGRAFÍA

LIBROS

BARRIOS-GARRIDO, Gabriela. **Internet y derecho en México.** Edit. Mc Graw Hill. 1ª ed. 1998, México.

BAZAINE GALLEGOS, Victoria Teresa, Legislar o no legislar: el dilema de Internet ignorado en México, México, UNAM, tesis de licenciatura en Ciencias de la Comunicación, Facultad de Ciencias Políticas y Sociales, p. 115.

BAZDRESCH, Luis. **Garantías Constitucionales.** Edit. Trillas. 4ª ed. México, 1992.

BURGOA-ORIHUELA, Ignacio. **Las garantías individuales.** Edit. Porrúa, 14ª ed. México, 1988.

CARPIZO, Jorge, **Constitución e Información,** en Carbonell, Miguel y Valadés, Diego, México, UNAM, Instituto de Investigaciones Jurídicas, 2000, pp. 161.

DEL PONT K., Luis Marco y NADELSTICHER Mitrania, Abraham, **Delitos de cuello blanco y reacción social,** Instituto Nacional de Ciencias Penales. México. 1981.

GUERREN M. F., **Penalización de la criminalidad informática**, Ediciones jurídicas Ibáñez, Colombia 1998.

HANCE, Olivier. **Leyes y Negocios en Internet.** Edit. Mc Graw Hill y Sociedad Internet. México. 1996.

MIR PUIG,S (Comp.) **Delincuencia Informática.** Promociones y Publicaciones Universitarias. Barcelona, 1992.

OLIVARES E., y PALACIOS J., **La informática en México.** Edit. Nuestro Tiempo, S.A., UAM Xochimilco, 1998.

TELLEZ Valdez, Julio. **Derecho Informático.** Edit. Mc Graw Hill. 2ª ed. México, 1996. Pp. 103-104.

TELLEZ Valdez, Julio. **La protección jurídica de los programas de computación.** Edit. UNAM, Instituto de Investigaciones Jurídicas. Serie 6: Estudios Doctrinales, núm. 124. 2ª ed. México. 1989.

VAZQUEZ PANDO, Fernando. **Aspectos Jurídicos del Tratado de Libre Comercio de América del Norte.** Edit. Themis, Primera Edición. México 1994.

ZAMORA SÁNCHEZ, Pedro, **Marco jurídico del lavado de dinero**, Colección Estudios Jurídicos, Editorial Oxford, México, D. F., 1999.p. 110.

ZAVALA, Antelmo. "El impacto social de la informática jurídica en México". Tesis. México. UNAM. 1996.

REVISTAS

ANIYAR DE CASTRO, Lolita. El delito de cuello blanco en América Latina: una investigación necesaria. ILANUD AL DÍA. Año 3 No.8 Agosto 1980. San José, Costa Rica.

ARTEGA S., Alberto. "El delito informático: algunas consideraciones jurídicas penales" Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela. 1987. Caracas, Venezuela. P. 125-133.

CALLEGARI, Lidia. "Delitos informáticos y legislación", Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985. P.115.

CEBALLOS DE LA MORA, C., El delito informático, Estudios Jurídicos, Universidad Intercontinental, Revista semestral, No.14/15, México 2001, p.p. 109-130.

DE LA CUADRA, Enrique. "Regulación jurídica de la informática computacional". Temas de Derecho. Año II No. 3, 1987. Universidad Gabriela Mistral. Santiago de Chile, p. 1-4.

FERNÁNDEZ Calvo, Rafael. El tratamiento del llamado delito informático en el proyecto de Ley Orgánica del Código Penal: reflexiones y propuestas de la Comisión de libertades e informática en Informática y Derecho. Pp.1150.

GARELLI, M., La ley Actualidad, La delincuencia informática, Año LXIII, No. 49, Buenos Aires 1999.

LIMA, Ma. de la Luz. "Delitos Electrónicos" Criminalia, México. Academia Mexicana de Ciencias Penales. Edit. Porrúa. No. 1-6. Año L. Enero-Junio 1984. Pp.100.

SARZANA, Carlos. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia. P.53.

TONIATTI, Roberto. "Libertad informática y derecho a la protección de los datos personales; principios de legislación comparada". Revista Vasca de Administración Pública. No. 29, Enero-Abril, 1991, España. p. 139-162.

DOCUMENTOS

CONSEJO DE EUROPA, Comité Europeo para los Problemas de la Delincuencia, **Convenio Preliminar sobre Delitos Informáticos**, Estrasburgo, 25 de Mayo de 2001.

NACIONES UNIDAS. **Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de delitos informáticos.**

Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. No.43 y 44. Naciones Unidas, Nueva York.1994.

NACIONES UNIDAS. **Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana. 27 de agosto a 7 de septiembre de 1990.** (A/CONF. 144/28/Rev.1) Nueva York, Naciones Unidas. 1991.

LEGISLACIÓN

Código Penal Federal, Ediciones fiscales Isef, S.A., México 2002.

Código Penal y de Procedimientos Penales del Estado de Sinaloa. Editorial. Anaya 1996. México, D.F.

Legislación sobre propiedad industrial e inversiones extranjeras. Colección Porrúa. Editorial Porrúa. 19 edición. México 1995.

Ley de Imprenta. Diario Oficial de la Federación. 12 de abril de 1917.

Ley Federal del Derecho de Autor. Diario Oficial de la Federación. Martes 24 de diciembre de 1996.

Tratado de Libre Comercio de América del Norte (TLC). Diario Oficial de la Federación. Lunes 20 de diciembre de 1993.