DELITOS INFORMATICOS

René De Sola Quintero[1]

1.INTRODUCCIÓN

El siglo XX y el comienzo del presente siglo han traído lo que sé de ha denominado la "revolución digital," caracterizada por el desarrollo de tecnología en todas sus formas y, por ello nos encontramos ante un complejo y laberíntico entramado de cables, satélites, redes, computadoras, fibra óptica, televisores e impulsos eléctricos que constituyen la infraestructura del cyberespacio[2]. Esta revolución, que encuentra en Internet su máxima expresión, es posible gracias al fenómeno de la convergencia, es decir, en el uso combinado de las computadoras y las redes de comunicación.

Los efectos de la revolución digital se hacen sentir en los distintos sectores de la sociedad como lo es en la economía, la política, la educación, el entretenimiento entre otras. Así pues, la sociedad encontró nuevas formas de interrelacionarse (compras on-line, chats, e-mail, educación a distancia, foros de discusión, etc.), y este fenómeno ha traído y traerá cambios profundos, por lo que es imprescindible estar preparados para enfrentar una evolución tecnológica acelerada, para que no se produzcan los efectos negativos como ocurrió en el salto de la era agrícola a la industrial.

Como hemos visto, los beneficios que ha traído esta revolución son de gran significación para la humanidad, pero como proceso también conlleva consecuencias negativas, como lo es que el ciberespacio ha sido concebido como un ámbito propicio para la realización de conductas antijurídicas. A partir de la existencia de nuevas formas de operar con la tecnología, aparecen delitos que no son nuevos, sino que existían desde mucho antes de la aparición de la informática, pero que presentan importantes particularidades que han planteado serios interrogantes que nuestro derecho positivo parece no saber cómo resolver.

Cualquiera de nosotros puede ser o ha sido víctima de tales delitos, que por su nueva forma de cometerse trae como consecuencia que por la falta de una tipificación y de no tener una legislación adecuada tanto nacional como internacional, esta nueva forma de delinquir quede impune.

Es por ello mi interés en el tema pues encuentro de vital importancia la investigación más profunda de estas nuevas formas antijurídicas y por lo tanto, la presente ponencia tiene como objeto fundamental explicar de una manera breve y concisa que son los delitos Infórmaticos, su caracterización, los sujetos que los realizan, la clasificación de las distintas formas en que se realizan, la legislación comparada que existe en esta materia, un breve sumario de la legislación que existe en la República Bolivariana de Venezuela que regula esta nueva forma de delinquir, y por último, su influencia en la propiedad intelectual. Todo esto a fin de que mis ilustres oyentes tengan una idea general de lo complejo que es la revolución digital y que nuestros gobernantes se adecuen a esta realidad legislando sobre esta materia coherentemente.

2. DEFINICIÓN DE DELITO INFORMÁTICO.

2.1 Comentario Inicial

Antes de establecer las definiciones más importantes sobre delitos informáticos es importante tener claro las definiciones de delito y fraude. Por delito en un plano sustancial tal y como lo señala el ilustre penalista venezolano Dr. Alberto Arteaga Sánchez3, se debe entender "*Como un hecho que, en sí mismo o por su forma, lesiona intereses fundamentales de la sociedad, intereses que se consideran básicos para la existencia, conservación y desarrollo del conglomerado social*." Por fraude se puede entender en general como "*engaño, abuso, maniobra inescrupulosa4.*"

Luego de haber dado una referencia de lo que es delito es importante resaltar cuales son los elementos integrantes del mismo según el ilustre penalista Cuello Calon5, los cuales son los siguientes:

- El delito es un acto humano, (acción u omisión).
- Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
- Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.
- El ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
- La ejecución u omisión del acto debe estar sancionada por una pena.

2.2 Definición de Delito Informático.

Después de haber definido que es delito, y sus elementos y haber dado una breve definición de lo que se entiende por fraude, pueden establecer las diferentes definiciones que se han dado por diferentes autores sobre el delito informático.

1. Se podría definir el delito informático como toda (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena[6].
2. El autor mexicano Julio Téllez Valdez[7] señala que los delitos informáticos son "actitudes ilícitas en que se 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)".
3. Por su parte, el tratadista penal italiano Carlos Sarzana[8], sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo."
4. El autor Davara Rodríguez[9] lo define como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software."
5. Finalmente, un grupo de expertos de la Organización para la Cooperación Económica (OCDE) en París en 1983, definió al delito informático como "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la trasmisión de datos[10]."

2.3. Algunas Consideraciones.

Luego de las definiciones anteriormente señaladas es importante hacer algunas consideraciones sobre las mismas. Cabe destacar sin establecer una regla genérica, se puede inferir que la computadora constituye un medio para cometer un delito o el objeto sobre el cual recae el mismo, es que se convierte en el primer supuesto de este tipo de conductas antijurídica. Es por eso, que debe entenderse que el aceptar el uso de la computadora como instrumento delictivo no significa aplicar analogía de ninguna especie, sino adaptar la figura penal a los avances de la técnica. Y ello resulta razonable pues el legislador no puede prever la infinidad de medios a través de los cuales es posible afectar un determinado bien jurídico penalmente protegido[11].

El límite a esta interpretación del tipo penal está dado por los supuestos en que el legislador puede prever un medio determinado, o en los casos en que la

estructura del delito no permita el empleo de ese medio. Pero sin perjuicio de que se enuncien genéricamente una serie de medios, dentro de los cuales tenga cabida el uso de ordenadores o se permita expresamente el uso de cualquier medio, ello no otorgará al delito el carácter de “informático”, lo cual lo que no necesariamente implica de que pueda hablarse de un delito relacionado con la informática12. Un ejemplo de ello, es la doble contabilidad llevada por un ordenador con fines de evasión fiscal, la creación de registros falsos con la finalidad de cobrar créditos inexistentes, jubilaciones, estafas etc.

El segundo supuesto que hay que mencionar es el caso en que la informática es el objeto del delito, aspecto de difícil determinación si tomamos en cuenta que se hace necesario diferenciar el hardware13 del software14, y acotar que al primero son generalmente aplicables las normas delictivas tradicionales pues no constituye una nueva forma de propiedad. Distinta situación es el software y de la información almacenada en una computadora, pues los mismos constituyen formas intangibles y su carácter novedoso hace que no siempre hallen cabida en las instituciones tradicionales del derecho15.

De esta manera, constituye delito informático cuando se perjudican a datos o programas informáticos, pero no cuando el objeto del daño es un ordenador cuyo resultado, la información que esta contenía queda malograda.

Por lo que se puede inferir que al tipificar un delito informático, lo que se está buscando es tutelar el contenido de la información de un sistema informático, y no el hardware en sí mismo.

Podemos también hablar de delito informático en el caso de reproducción ilícita de obras de software de bases de datos o de topografías de semiconductores16.

Por último encontramos, la situación en la que influyen ambos supuestos, es decir, el ordenador se usa como instrumento y es a la vez el objeto sobre el cual recae la acción delictiva. El caso más elocuente es la destrucción de datos mediante un programa o un virus informático17.

En síntesis, la informática puede constituir un medio o el objeto de una acción típica. En la medida en que se presenten alguno de estos elementos, o ambos, estaremos ante un “delito informático18”.

3. CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS.

Según el mexicano Julio Tellez Valdez19, los delitos informáticos presentan las siguientes características:

a) Son conductas criminales de cuello blanco (White collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios"de más de cinco cifras.
e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
h) Presentan grandes dificultades para su comprobación, ésto por su mismo carácter técnico.
i) En su mayoría son imprudencias y no necesariamente se cometen con intención.
j) Ofrecen facilidades para su comisión los menores de edad.
k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

4. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

Muchas son las clasificaciones que se han dado sobre delitos informáticos, por lo que considero que a objeto de la presente ponencia únicamente voy a dar a conocer la que según mi criterio es la completa, cuyo autor es el mexicano JULIO TÉLLEZ VALDEZ. Creo importante señalar adicionalmente los tipos de delitos informáticos reconocidos por las Naciones Unidas.

4.1 Clasificación por TÉLLEZ VALDEZ

El mexicano TÉLLEZ VALDEZ20 clasifica a estos delitos, de acuerdo a dos criterios:

1. Como Instrumento o medio.

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

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

2. Como fin u objetivo.

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

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

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

- Acceso no autorizado: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario. (Violación de la privacidad).
- 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 Internet.
- Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, la red Internet21 permite dar soporte para la comisión de otro tipo de delitos:

- Espionaje: Acceso no autorizado a sistemas de 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 la Internet los narcotraficantes puede 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.

4.2 Tipos de Delitos informáticos reconocidos por la Organización de Las Naciones Unidas.

Los tipos de delitos reconocidos por la Organización de las Naciones Unidades22 y que le han dado su carácter internacional, a fin de que los países los tomen en consideración para ser incorporados a sus distintas legislaciones penales correspondientes y los cuales cito textualmente son:

"Fraudes cometidos mediante manipulación de computadoras:

- Manipulación de los datos de entrada: Este tipo de fraude informático también conocido como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
- La manipulación de programas: Es muy difícil 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 tienen 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 equipo y programas de computadoras especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas crédito.
- Fraude efectuado por manipulación informática: Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfiere otra.

Falsificaciones informáticas:

- Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como Instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base rayos láser surgió una nueva generación de falsificaciones, o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, puede modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos falsos que producen son de tal calidad que sólo un experto puede diferenciarlo de los documentos auténticos.

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 proporciona 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: Sé fábrica de forma análoga al virus con miras en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus por que puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es tumor maligno. Ahora bien, las consecuencias del ataque de un gusano puede ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano subsiguiente se destruirá y puede dar instrucciones a un sistema informático de un banco que transfiera continuamente dinero a una cuenta ilícita.
- Bomba lógica 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 contrario 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 conocer el lugar en donde se halla la bomba.
- Acceso no autorizado a servicios y sistemas informáticos: Por motivos diversos: desde la simple curiosidad, como el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
- Piratas informáticos o hackers: El acceso se efectúa 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: Esta 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 moderna. Al respecto consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

5. CARACTERIZACIÓN DEL DELICUENTE INFORMÁTICO

Luego de haber examinado a lo largo de la presente ponencia la definición de delitos informáticos, su caracterización y clasificación, me parece muy importante señalar las particularidades del delincuente informático, debido a que

poseen ciertas características que no presentan el denominador común de los delincuentes, ésto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Las principales características que presentan los sujetos activos de esta conducta delictiva son las siguientes:23:

a) En general, son personas que no poseen antecedentes delictivos.
b) La mayoría de sexo masculino.
c) Actúan en forma individual.
d) Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos; actitud casi deportiva en vulnerar la seguridad de los sistemas, características que suelen ser comunes en aquellas personas que genéricamente se las difunde con la denominación “hackers”.
e) Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismo.
f) También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.
g) En el caso de los “hackers”, realizan sus actividades como una especie de deporte de aventura donde el desafío está allí y hay que vencerlo. Aprovechan la falta de rigor de las medidas de seguridad para obtener acceso o poder 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 sitio. Eso suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sitio.
h) Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras, muy motivadas (es el que siempre está de guardia, el primero en llegar y el último en irse).
i) Con respecto a los que se dedican a estafar, nos encontramos ante especialistas. Algunos estudiosos de la materia lo han catalogado como “delitos de cuello blanco”, (se debe a que el sujeto activo que los comete es poseedor de cierto status socio-económico.)

6. LEGISLACIÓN COMPARADA SOBRE DELITOS INFORMÁTICOS

Los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los delitos informáticos, debido a los daños y perjuicios que le han causado a la humanidad. Sin embargo, si bien es cierto existe un esfuerzo por parte de los países para tratar de evitarlos, no existe un criterio unificado de cómo deben ser atacados, es por eso que se hace imprescindible que

se siga trabajando para llegar a la unificación de los criterios y así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente.

Todo lo anteriormente señalado es corroborado por el brillante trabajo realizado en esta materia por la Organización de las Naciones Unidas titulado "<<El Manual de las Naciones Unidas par la Prevención y Control de Delitos Informáticos24>>", el cual señala que el problema se eleva a la escena internacional, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Sin embargo la misma 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 entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional."

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile.

Creo importante señalar a continuación algunos aspectos relacionados con la legislación y en los diferentes países, así como que tipo de delitos informáticos se persiguen.

Estados Unidos25.

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986, con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de troya y en que difieren de los virus. La nueva acta proscribe

la transmisión de un programa, información, códigos o comandos que causen daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. Por lo que constituye un adelanto porque está dirigido directamente contra los actos de transmisión de virus.

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

En el mes de julio del año 2000, el Senado y la Cámara de Representantes de este país tras un año largo de deliberaciones establece el "Acta de Firmas Electrónicas en el Comercio Global y Nacional". La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos, mensajes electrónicos y contratos establecidos mediante Internet – entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

Alemania26.

Este país sancionó en 1986 la ley contra la Criminalidad Económica, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

Austria27

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

Gran Bretaña[28]

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 específica la modificación de datos sin autorización.

Holanda[29].

El primero de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- 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).
- La distribución de virus.

Francia[30].

En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se considera aspectos como:

- Intromisión fraudulenta que suprima o modifique datos.
- Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la intromisión de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.
- Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

España[31].

En el Nuevo Código Penal de España, se establece que quien causare daños en propiedad ajena, se le aplicará pena de prisión o multa, en lo referente a: la realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en 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.

- En materia de estafas electrónicas, el nuevo Código Penal de España, 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[32].

Chile fue el primer país latinoamericano en sancionar una ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1983. Esta ley se refiere a los siguientes delitos:

- La destrucción o inutilización de los datos contenidos dentro de una computadora es castigado con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.
- 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.
- Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

7. LEGISLACIÓN EN VENEZUELA EN MATERIA DE DELITOS INFORMÁTICOS.

7.1. Antecedentes.

Como se puede observar en el punto anterior hice una breve mención de los países que legislan sobre la materia de delitos informáticos, así como, las organizaciones internacionales que han realizado esfuerzos dando sus recomendaciones para que se vaya adoptando una legislación uniforme en esta materia, particularmente la ONU. Ahora bien, dentro de este esfuerzo que se ha venido dando, tanto en el ámbito interno de cada país como a nivel internacional, para perseguir los delitos informáticos nos encontramos ante el caso de Venezuela que en los últimos cuatro años ha comenzado a legislar sobre este tema.

Dicho esfuerzo en Venezuela comenzó con la aprobación de la Constitución de la República Bolivariana de Venezuela[33], que establece en su artículo 110 lo siguiente:

> *Artículo 110. "El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de*

ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía".

El gobierno de Venezuela dando cumplimiento a la norma constitucional transcrita anteriormente, aprobó la Ley Orgánica de Ciencia, Tecnología e Innovación34, que tiene por objeto tal y como lo señala su artículo 1:

Articulo 1: "El presente Decreto-Ley tiene por objeto desarrollar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela, organizar el Sistema Nacional de Ciencia, Tecnología e Innovación, definir los lineamientos que orientarán las políticas y estrategias para la actividad científica, tecnológica y de innovación, con la implantación de mecanismos institucionales y operativos para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para generación, uso y circulación del conocimiento y de impulsar el desarrollo nacional".

Sin embargo para que este esfuerzo de incorporar a Venezuela en la era de la tecnología y de la información, alcance un nivel adecuado, se hace necesario la promulgación de un conjunto de instrumentos legales que proporcionen el marco institucional al desarrollo armonioso del sector y a su democratización y, que precisamente para lograr los objetivos tanto de la norma constitucional como de la Ley Orgánica de Ciencia, Tecnología e innovación, se hizo necesario promover al mismo tiempo las condiciones de seguridad que inspirarán suficiente confianza tanto a los administradores de las plataformas que brindan servicios tecnológicos como al usuario en general.

En este orden de ideas, nos encontramos con la aprobación de la Ley de Mensaje de Datos y Firmas Electrónicas35, cuyo contenido constituye un soporte jurídico fundamental para dotar de certeza a las transacciones electrónicas, conferir valor probatorio al documento digitalizado y así contribuir al desarrollo del comercio electrónico del país, tal y como lo señala su artículo 1, que transcribo a continuación:

Articulo 1: "El presente Decreto-Ley tiene por objeto otorgar y reconocer la eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o

privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.
El presente Decreto Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas.
La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos".

Todas las leyes anteriormente señaladas han contribuido fundamentalmente a la incorporación de Venezuela al desarrollo de la Ciencia y Tecnología de la información, y de esta manera adecuar su legislación en esta materia a las exigencias de la comunidad internacional. Pero así como se ha podido observar un gran desarrollo también hemos sido objeto de los daños y perjuicios que se producen a través de los delitos informáticos, es por eso que se tuvo que adoptar una ley en esta materia para que se facilitará perseguir este tipo de conductas antijurídicas.

7.2. Ley Especial Contra Delitos Informáticos[36].

Esta novísima Ley contra Delitos Informáticos, aprobada a finales del año 2001, significa un gran avance en materia penal para mi país, visto que nos permitirá la protección de la tecnología de la información, persiguiendo todas aquellas conductas antijurídicas que se realicen en este campo. Es por eso, que a continuación señalare los aspectos más importantes de la ley:

Objeto de la Ley.

El objeto de la Ley se encuentra consagrado en el artículo 1 el cual establece:

Artículo 1. "*La presente ley tiene por objeto la protección de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.*"

De la norma transcrita anteriormente se puede inferir que la ley tiene como objetivos principales, 1) la protección de los sistemas de tecnologías de

información; 2) prevención y sanción de los delitos cometidos contra tales sistema; Y 3) los delitos cometidos mediante el uso de dichas tecnologías.

Extraterritorialidad.

La previsión de la Extraterritorialidad se encuentra señalado en su artículo 3, y el cual es de gran importancia en razón de la dimensión transnacional del problema pues se trata de hechos que pueden cometerse de un país a otro,

Sanciones.

Para las sanciones se adopto simultáneamente el sistema binario, ésto es, pena privativa de libertad y pena pecuniaria. Con relación a esta última se fijan montos representativos calculados sobre la base de unidades tributarias por considerarse que la mayoría de estos delitos, no obstante la discriminación de bienes jurídicos que se hace en el proyecto, afecta la viabilidad del sistema económico, el cual se sustenta, fundamentalmente, en la confiabilidad de las operaciones. Cabe destacar que el legislador tomó en cuenta las deficiencias de otras leyes donde no se preveían las penas accesorias. Así, en la ley encontramos que las penas para los hechos punibles que se encuentran tipificados son principales y accesorias.

Se establece como penas accesorias las siguientes:

- El decomiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos.
- El trabajo comunitario.
- La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión industria, o para laborar en instituciones o empresas del ramo.
- La suspensión del permiso, registro o autorización para operar el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información.
- Divulgación de la sentencia condenatoria.
- Indemnización civil a la víctima por los daños causados.

Responsabilidad de las personas jurídicas.

Por cuanto algunos de los hechos punibles previstos en la ley pueden ser perpetrados por intermedio de una persona jurídica o con el fin que ésta reciba sus efectos o beneficios, se establece los supuestos que harían procedente su responsabilidad, es así que los gerentes, administradores, directores o

dependientes, actuando en su nombre o representación, responderán de acuerdo con su participación en el hecho punible.

Clasificación de los Delitos Informáticos.

La ley clasifica los delitos informáticos de acuerdo al siguiente criterio: 1) Delitos contra los sistemas que utilizan tecnologías de información; 2) Delitos contra la propiedad; 3) Delitos contra la privacidad de las personas y de las comunicaciones; 4) Delitos contra niños, niñas o adolescentes; y 4) Delitos contra el orden económico. Ahora bien, paso a nombrar cuales son los delitos que se encuentran tipificados dentro de cada una de estas categorías.

1) Delitos contra los sistemas que utilizan tecnologías de Información:
   - Acceso indebido. (Pena: Prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).
   - Sabotaje o daño a sistemas. (Pena: Prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).
   - Sabotaje o daño culposo. (Pena: se revisa el caso en concreto y se aplica una reducción entre la mitad y dos tercios).
   - Acceso indebido o sabotaje a sistemas protegidos. (Pena: las penas previstas anteriormente se aumentarán entre una tercera parte y la mitad cuando los hechos recaigan sobre un componente que utilice tecnología de información protegido con alguna medida de seguridad).
   - Posesión de equipos o prestación de servicios de sabotaje. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).
   - Espionaje informático. (Pena: prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).
   - Falsificación de documentos. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).

2) Delitos contra la propiedad.
   - Hurto. (Pena: prisión de 2 a 6 años y multa 200 a 600 Unidades Tributarias).
   - Fraude. (Pena: prisión de 3 a 7 años y multa de 300 a 700 Unidades Tributarias).
   - Obtención indebida de bienes y servicios. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
   - Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. (Pena: prisión 5 a 10 años y multa de 500 a 1000 Unidades Tributarias).
   - Apropiación de tarjetas inteligentes o instrumentos análogos. (Pena: prisión de 1 a 5 años y multa de 10 a 50 Unidades Tributarias).
   - Provisión indebida de bienes o servicios. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

- Posesión de equipo para falsificaciones. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).

3) Delitos contra la privacidad de las personas y de las comunicaciones.
   - Violación de la privacidad de la data o información de carácter personal. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
   - Violación de la privacidad de las comunicaciones. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
   - Revelación indebida de data o información de carácter personal. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

4) Delitos contra niños, niñas o adolescentes.
   - - Difusión o exhibición de material pornográfico. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).
   - Exhibición pornográfica de niños o adolescentes. (Pena: prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).

5) Delitos contra el orden económico.
   - - Apropiación de propiedad intelectual. (Pena: prisión de 1 a 5 años y multa de 100 a 500 Unidades Tributarias).
   - Oferta Engañosa. (Pena: prisión de 1 a 5 años y multa de 100 a 500 Unidades Tributarias).

Como puede apreciarse en Venezuela se ha dado un paso importante en la legislación penal que regula los delitos informáticos pero que debe continuar con su evolución para enfrentar la exigencias de un mundo en proceso de globalización.

8. LOS DELITOS INFORMÁTICOS Y LA PROPIEDAD INTELECTUAL.

Como se pude observar a lo largo de la presente ponencia, se puede inferir que los derechos de propiedad intelectual se ven frecuentemente vulnerados por los delitos informáticos. Es así como encontramos casos de confusión o imitación, como la creación de dominios similares a los de otros conocidos. Por ejemplo el dominio microsof.com buscaba el parecido con microsoft.com. Estos casos pueden resolverse desde el ámbito de marcas.

Otro caso es el plagio de páginas web, al que sería aplicable la legislación sobre derechos de autor e incluso l normas sobre patentes.

El traslado de información de otros web ajenos, pero que aparecen en la pantalla del usuario en una ventana previamente visitada, denominado como framing, es un claro ejemplo de conducta infractora de los derechos de autor y además puede constituir competencia desleal. No resultaría ilegal ni infractora si se cuenta con los permisos necesarios de los operadores o propietarios de otros web.

Y por último, el aprovechamiento de la reputación de otros, por el uso de dominios ajenos para crear confusión o para aprovecharse de marcas renombradas, también conocido como cyber-ocupación. Aunque es mucho más sencillo aplicar el derecho de marcas que el de competencia en el caso de usurpación de una marca o signo distintivo.

Finalmente, en síntesis podemos señalar que las conductas antijurídicas que vulneran la propiedad intelectual son:

- Creación de dominios similares.
- Plagio de páginas web.
- Traslado de información de otros webs ajenos (Framing).
- Aprovechamiento de la reputación de otros. (Competencia desleal).

9. CONCLUSIÓN.

Las nuevas realidades de la tecnología y la informática que se han venido desarrollando en este mundo globalizado debido a su acelerado desarrollo y su incidencia directa en varios ámbitos de la sociedad han alcanzado el rango de bienes jurídicos protegidos por el ordenamiento jurídico –particularmente por el Derecho Penal. Por lo que una vez más nos hace pensar que estamos en presencia de un proceso de transnacionalización del Derecho Penal, donde gracias a la globalización se ha logrado realizar esfuerzos para la creación de un sistema garantista capaz de proteger los derechos de la información.

Para que este sistema garantista del Derecho Penal de la Tecnología y la Información surta sus efectos, es necesario el compromiso de la comunidad internacional a fin de que regulen sus ordenamientos jurídicos de una manera uniforme siguiendo las recomendaciones y pautas señaladas por las diferentes organizaciones mundiales, y de esta manera se logre la armonización de sus legislaciones, para que los usuarios de la tecnología de la información se vean cada vez más protegidos y accedan al maravilloso mundo del ciberespacio.

Confío sinceramente que el tema tratado haya constituido una modesta contribución al mejor estudio por parte de mis ilustrados oyentes de la importante normativa que hoy se somete a su consideración.

10. Referencias.

Arteaga Sánchez, Alberto: **Derecho Penal Venezolano**, 7ª ed., Paredes Editores, Caracas, 1995, p.125.

Constitución de la República Bolivariana de Venezuela, Gaceta Oficial No. 5435 Extraordinaria, jueves 30 de diciembre de 1999.

Cousido González, M. Pilar: **Derecho De La Comunicación en Internet**, Editorial Colex, Madrid, 2001.

Delitos informáticos: Qué son y cómo se previenen. (Visitada 5 de junio de 2002). <http://www.estarinformado.com.ar/pag%20tecnologia/TECNOLOGIA-2.htm>.

Fernández Fernández, Fernando: **La Firma Electrónica y Los Delitos en la Red**, ponencia presentada en el seminario "Los Delitos Económicos y su Impacto en las Empresas", Auspiciado por la Asociación Venezolana de Derecho Financiero, Caracas, 2001.

Landaverte, Melvin; Soto, Joaquín; y Torres Jorge: **Delitos Informáticos**. (Octubre, 2000). Ver: <http://monografias.com/trabajos/legisdelinf/legisdelinf.shtml>

Ley N° 1.204 de Mensaje de Datos y Firmas Electrónicas. Gaceta Oficial Nro. 37.148, miércoles 28 de febrero de 2001.

Ley N°48. Ley Especial contra Delitos los Delitos Informáticos. Gaceta Oficial Nro.37.313, martes 30 de octubre de 2001.

Ley Orgánica de Ciencia, Tecnología e Innovación, Gaceta Oficial No.37.291, miércoles 26 de septiembre de 2001.

Manson, Marcelo: **Legislación sobre delitos informáticos**, pág.3 (visitada 25 de junio de 2002). Ver: <http://monografias.com/trabajos/legisdelinf/legisdelinf.shtml>.

Ossorio, Manuel: **Diccionario de Ciencias Jurídicas Políticas y Social**es, Editorial Heliasta, Buenos Aires, 1984, p.327.

Palazzi, Pablo A: **Delitos Informáticos**, AD-HOC, Buenos Aires, 2000, pág.37.

Tablante, Carlos: **Delitos Informáticos Delincuentes sin Rostro**, Encambio, Caracas, 2001.

Tipos de delitos informáticos reconocidos por Naciones Unidas. (Visitada el 5 de junio de 2002). <http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm>.

---

1 Abogado egresado de la Universidad Católica Andrés Bello, Caracas; Maestría en Negocios Internacionales, American University, Washington, D.C.; Especialista en Ciencias Penales y Criminologícas, Universidad Católica Andrés Bello, Caracas.

2 El ciberespacio se reduce a Internet, la red mundial más difundida y de mayor acceso, un espacio virtual donde la gente habla por medio de servicios de conversación o chats, transmite datos mediante el correo electrónico (e-mail), compra y realiza transacciones de todo tipo, accede a información, maneja y crea información.

3 Arteaga Sánchez, Alberto: Derecho Penal Venezolano, 7ª ed., Paredes Editores, Caracas, 1995, p.125.

4 Ossorio, Manuel: Diccionario de Ciencias Jurídicas Políticas y Sociales, Editorial Heliasta, Buenos Aires, 1984, p.327.

5 Landaverte, Melvin; Soto, Joaquín; y Torres Jorge: Delitos Informáticos. (Octubre, 2000). Ver: <http://monografias.com/trabajos/legisdelinf/legisdelinf.shtml>

6 Idem.

7 Manson, Marcelo. **Legislación sobre delitos informáticos**, pág.3 (visitada 25 de juniode 2002). Ver: <http://monografias.com/trabajos/legisdelinf/legisdelinf.shtml>.

8 Idem.

9 Palazzi, Pablo A: **Delitos Informáticos**, AD-HOC, Buenos Aires, 2000, pág.37.

10 Idem.

11 PALAZZI, Pablo, ob. cit. Pág.34.

12 PALAZZI, Pablo, ob.cit. Pág 35.

13 Hardware (fierros, maquinaria): Se trata de todos los componentes de una computadora, entre los cuales se pueden mencionar el disco duro, procesador, monitor, ect. Que en conjunto con el software hacen que funcione nuestra máquina.

14 Software: Término general que designa los diversos tipos de programas usados en computación.

15 PALAZZI, Pablo, ob. cit. Pág 36.

16 Idem.

17 Idem.

18 Idem.

19 MANZÓN, Marcelo, ob.cit. Págs. 3 – 4.

20 Idem.

21 Internet (La Red): Se denomina así a la red de telecomunicaciones que surgió en los Estados Unidos en 1969 por el Departamento de Defensa de los Estados Unidos, más precisamente. Se la llamó primero ARPAnet y fue pensada para cumplir funciones de carácter meramente militar, para convertirse en uno de los principales medios de comunicación que de manera global afecta la sociedad en diversos aspectos como son el social, cultural, económico, etc. Internet es además una red multiprotocolo capaz de soportar cualquier tecnología. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

22 Ver: **Tipos de delitos informáticos reconocidos por Naciones Unidas**. (Visitada el 5 de junio de 2002). <http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm>.

23 Ver. **Delitos informáticos: Qué son y cómo se previenen**. (visitada 5 de junio de 2002). <http://www.estarinformado.com.ar/pag%20tecnologia/TECNOLOGIA-2.htm>.

24 LADANVERDE,Melvin, ob.cit. Págs. 67 – 68.

25 Idem.

26 Idem

27 Idem.

28 Idem.

29 Idem.

30 Idem.

31 Idem.

32 Idem.

33 Constitución de la República Bolivariana de Venezuela, Gaceta Oficial No. 5435 Extraordinaria,, jueves 30 de diciembre de 1999.

34 Ley Orgánica de Ciencia, Tecnología e Innovación, Gaceta Oficial No.37.291, miércoles 26 de septiembre de 2001.

35 Ley N° 1.204 de Mensaje de Datos y Firmas Electrónicas. Gaceta Oficial Nro. 37.148, miércoles 28 de febrero de 2001.

36 Ley N°48. Ley Especial contra Delitos los Delitos Informáticos. Gaceta Oficial Nro.37.313, martes 30 de octubre de 2001.