Del Escitorio del Dr.
JORGE ROBERTO MARADIAGA M.

PROYECTO DE LEY SOBRE DELITOS INFORMÁTICOS

El presente proyecto de ley es sin dudas un tema pendiente, ya que la incorporación de las nuevas tecnologías de la información y de la comunicación como medios de comisión de distintos tipos previstos en nuestro Código Penal, es una necesidad impostergable.

El desarrollo tan amplio de las tecnologías de la información y de la comunicación, han signado un cambio significativo y cualitativo en el accionar en todos los campos del acontecer humano; pero igualmente ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

No cabe ninguna duda que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general. En todo caso es de destacar, que los delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido, el presente proyecto se dirige a la regulación penal de las posibles medidas preventivas de carácter penal que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de delitos, alcance en el país los niveles de peligrosidad que se han dado en otros países.

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.

2. El autor mexicano Julio Téllez Valdez 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)”

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.

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.

El Internet, avance tecnológico de enorme potencial en beneficio de la educación, que puede ser empleado con magníficos resultados, pero desafortunadamente es utilizado también para promocionar la pornografía infantil. El aumento vertiginoso de las computadoras y el uso de Internet, plantea el desafío de contar con normas que sancionen como delito, la transmisión de pornografía infantil a través de Internet o de cualquier otro medio de archivo de datos, reconociendo que el desarrollo de nuevas tecnologías para la producción y transmisión de la pornografía es muy rápido y que se podrán presentar otras formas más sofisticadas de

transmisión. Tipo penal que deberá sancionar el uso de un sistema de cómputo o de cualquier otro mecanismo de archivo de datos con la finalidad de exhibir a menores de edad realizando actos de exhibicionismo corporal, lascivos, agregándose el término pornográfico, por considerarse más aplicable.

La amenaza de este siglo que pende sobre los menores de edad va de la mano con la alta tecnología de un mundo glabalizado, así la explotación sexual comercial de niños es un fenómeno creciente que ocupa actualmente la atención de gobiernos, organizaciones sociales y de la comunidad en general. Los factores asociados a la explotación sexual comercial de la infancia son diversos. En general se citan la pobreza, la conducta sexual masculina irresponsable, la migración, el desempleo, la desintegración familiar, el creciente consumismo, violencia intrafamiliar y la desigualdad social como causas que facilitan las condiciones que la favorecen.

Dada la condición vulnerable de los niños y las niñas, principales víctimas de este tipo de explotación al ser utilizados por adultos para sacar ventaja o provecho de carácter sexual y/o económico sobre la base de una relación de poder/subordinación, considerándose explotador, tanto aquel que intermedia a un tercero, como el que mantiene la relación con el menor, no importando si ésta es frecuente, ocasional o permanente.

El daño producido en perjuicio de datos o programas, como agregado al art. 183 C.P. más conocido y receptado en la legislación comparada como "sabotaje informático". La cláusula se torna imprescindible ya que el código vigente sólo establece como delito el daño que recae sobre cosas tangibles, y los datos o programas de un sistema son bienes intangibles. También se introduce la figura de los "virus informáticos", al preverse la tipicidad de la distribución de programas destinados a causar cualquiera de los daños descriptos anteriormente.

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
5) Delitos contra el orden económico

“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: Se 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 modernas. 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.

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

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

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

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

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

FRAUDE.-

"inciso. 16: Será reprimido con prisión de un mes a seis años, el que con el fin de obtener un beneficio patrimonial para sí o para otros, provoque un perjuicio en el patrimonio de un tercero mediante la introducción de datos falsos, la alteración, obtención ilícita o supresión de los datos verdaderos, la incorporación de programas o la modificación de los programas contenidos en soportes informáticos, o la alteración del funcionamiento de cualquier proceso u operación o valiéndose de cualquier otra técnica de manipulación informática que altere el normal funcionamiento de un sistema informático, o la transmisión de los datos luego de su procesamiento."

DAÑO.-

"Se impondrá prisión de un mes a dos años, al que, por cualquier medio, destruyere en todo o en parte, borrare, alterare en forma temporal o permanente, o de cualquier manera impidiere la utilización de datos o programas, cualquiera sea el soporte en que estén contenidos durante un proceso de comunicación electrónica.

La misma pena se aplicará a quien vendiere, distribuyere o de cualquier manera hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños de los descriptos en el párrafo anterior, en los programas de computación o en los datos contenidos en cualquier tipo de sistema informático y de telecomunicaciones."

"Artículo 196 bis.-Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

"Artículo 217 bis.-Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

"Artículo 229 bis.-Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."