**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE DERECHO**

**SEMINARIO DE DERECHO PENAL**

# LOS DELITOS INFORMÁTICOS, SU DIFICULTAD PARA TIPIFICARLOS, PROBARLOS Y PROPUESTA DE REFORMA AL CÓDIGO PENAL FEDERAL.

**TESIS**
**QUE PARA OBTENER EL TÍTULO DE:**
**LICENCIADO EN DERECHO**
**PRESENTA**

**ROLANDO RAMÍREZ CARBAJAL**

**ASESOR**
**DR. PEDRO EMILIANO HERNÁNDEZ GAONA**

VNIVERSIDAD NACIONAL AVTNOMA DE MEXICO

U.N.A.M. FACULTAD DE DERECHO - LEX -

*A mis padres, cuyos desvelos, hoy se ven recompensados*

*Para Adriana, compañera eterna en la Facultad y en la vida*

*A la Universidad en cuyas aulas y pasillos forje mi destino*

**LOS DELITOS INFORMÁTICOS, SU DIFICULTAD PARA TIPIFICARLOS, PROBARLOS Y PROPUESTA DE REFORMA AL CÓDIGO PENAL FEDERAL.**

**ÍNDICE**

**INTRODUCCIÓN**……I

**Capítulo 1**

**Conceptos generales acerca de:**

1.1. Derecho Penal……..1
1.2. Informática……9
1.3. Computadora……..12
1.4. Internet……20
1.5. Derecho Penal y las nuevas tecnologías……...23

**Capítulo 2**

**Delito y Delito Informático**

2.1. Concepto de Delito……25
2.2. Elementos del Delito……26
2.3. Denominaciones para el Delito Informático……..33
2.4. Concepto de Delito Informático……...35
2.5. Clasificación del Delito Informático……37
2.6. Sujetos activos y pasivos……43
2.7. Bienes Jurídicos Tutelados……..45

**Capítulo 3**

**Legislación mexicana del Delito Informático y Derecho comparado**

3.1. México……48
3.2. España……57

3.3. Argentina……61
3.4. Estados Unidos……..64

**Capítulo 4.**

**Dificultad para tipificar y probar los Delitos Informáticos**

4.1. Problemas para tipificar los delitos informáticos……...68
4.2. La Computadora y las nuevas tecnologías como Medios Comisivos……...70
4.3. ¿Quién es responsable penalmente?.....71
4.4. ¿Pena proporcional a la gravedad del delito?.....83
4.5. Medios para probar los delitos informáticos, dificultad para su probanza……87
4.6. La Prueba en el Proceso Penal……..92
4.7. La Prueba o Evidencia Digital……103
4.8. Orden de suministrar Datos informáticos……111
4.9. Allanamiento y recolección de evidencia por orden de un juez……..114

**Capítulo 5.**

**Tipificación de los Delitos Informáticos en el Código Penal Federal**

5.1 Reproducción ilegal de Software……117
5.2 Daño provocado por Virus, Spyware y Códigos informáticos maliciosos……124
5.3 Delitos contra la privacidad y acceso ilegal a sistemas informáticos……..130
5.4 Fraude informático……138

Conclusiones……144

Propuesta……..147

Bibliografía……150

Legislación Nacional……..153

Legislación Internacional……154
Hemerografía……155
Otras fuentes……155

## *I. Introducción*

La presente investigación surge como respuesta a las preguntas ¿Qué sucede cuando se delinque a través de Internet?, ¿Existe un castigo para las personas que reproducen software de manera ilegal? ¿Cuáles son los medios de prueba para este tipo de ilícitos?, por lo que investigué acerca del tema, y pude observar que una gran parte de los compañeros, tratadistas y maestros no creen que estos delitos existan, o en algunos casos sostienen que estos no merecen una regulación especial en virtud de que ya existen tipos penales que se pueden aplicar análogamente, aunque recordemos que no se deben aplicar penas por analogía, por lo que es necesario que se regule expresamente sobre esta materia.

En la actualidad vivimos inmersos en la inseguridad, a diario en la ciudad de México se cometen alrededor de 4109 delitos, de los cuales 411 son denunciados, sin lugar a dudas esto trae una alta tasa de criminalidad y de impunidad ya que los delitos al no ser denunciados no pueden ser castigados, esta situación no es ajena al resto del país ya que aunque la mayor parte de delitos se registra en la Capital, las ciudades más importantes de la República también son asoladas por la delincuencia.

En este marco es donde surge un nuevo tipo de delincuente: el delincuente informático, este se vale tan solo de una computadora y sus conocimientos sobre la misma para cometer ilícitos que difícilmente pueden llegar a probarse, sin embargo estos ya tienen una fuerte repercusión en la sociedad, tan solo en 2009 se cometieron ¡más de 8000 fraudes bancarios por Internet!, a pesar de esto, nuestro país no tiene una legislación aplicable a este tipo de delincuente ya que sus conductas no se encuentran adecuadamente tipificadas aún en nuestros Códigos Penales, por lo que se ata de manos al Ministerio Público cuando trata de fincarle responsabilidad a un criminal de este tipo ya que no cuenta con las herramientas adecuadas para hacerle frente, y por lo regular tampoco tendrá los conocimientos necesarios para comprender a lo que se está enfrentando.

El Código Penal Federal y algunos estatales cuentan con un ligero esbozo de lo que son los delitos informáticos, pero este intento de regulación no es suficiente, falta mucho por hacer y resulta casi imposible legislar todas las conductas antijurídicas que pueden llegar a darse, por lo que es necesario entender y atender este creciente problema.

La Policía Cibernética adscrita a la Policía Federal Preventiva, al parecer sólo fue creada con el propósito de engañar a la población, puesto que en nuestro país no existen cifras exactas ni estimadas de los delitos informáticos esto es ilógico, puesto que si contamos con una unidad especializada ¿cómo es posible que esta no dé datos de los delitos se supone investiga?, por lo que se estima que en realidad esta no hace lo que debiera.

Al no tener un marco jurídico adecuado para perseguir y juzgar a los delincuentes informáticos, corremos el riesgo de que nuestra nación se convierta en un paraíso penal para este tipo de ilícitos, ya que países como Estados Unidos, España y Argentina entre otros ya cuentan con una regulación mucho más avanzada que la nuestra.

En estos momentos con la escalada de inseguridad y violencia de la que es víctima el país, se piensa en reformar leyes, implementar nuevas penalidades y con ello frenar estos males que azotan a México, debe saberse que la delincuencia que se pretende combatir, está a la vanguardia en lo que a tecnología se refiere por lo que es necesario implementar cambios en nuestra leyes que nos permitan castigar el uso ilícito que se le puede dar a estas nuevas tecnologías, es trabajo de los abogados y legisladores asimilar esta realidad y poner al día a nuestro Código Penal.

Nos hemos quedado rezagados en cuanto a legislación al respecto de los llamados Delitos Informáticos, nuestros legisladores no han entendido este

problema, ni se dan cuenta de que en gran parte de los llamados Delitos de alto impacto en su conformación existe un uso ilícito de las nuevas tecnologías, por medio de estas se allegan de datos personales, de familiares, estimaciones de los recursos con los que contamos, fotos, entre otras cosas, por lo cual nos pueden seguir la pista sin que nosotros estemos enterados, un ejemplo de esto son los llamados fraudes informáticos o Phishing, en los cuales el delincuente envía un correo electrónico haciéndose pasar por el ejecutivo de una institución bancaria y pide al usuario de la misma que ingrese a la página del banco que se cita en el cuerpo del mail, esta página es falsa pero aparenta ser la web de nuestro banco y se usa para robar la información del cuentahabiente, ya que se dice que hace falta corroborar datos para que su cuenta no sea cancelada, de esta forma el usuario cree en el engaño; accesa a la página y da sus datos, sin saber que alguien ahora tiene acceso a su cuenta y podrá conocer sus movimientos monetarios así como el monto del dinero que tiene en su cuenta.

Por lo cual el criminal podrá saber si su posible víctima cuenta con recursos suficientes para ser secuestrada o su casa asaltada, obviamente sin poner en riesgo su libertad puesto que las actividades en las que ha incurrido no son ilegales al menos en nuestro país, lo que trae consigo que muchas personas estén al servicio de la delincuencia organizada sin miedo a que los descubran, porque de cualquier forma sería muy difícil hacerles una imputación directa en el caso de que atraparan a los integrantes de la banda.

Otra forma de conocer la información antes mencionada, se da mediante la intrusión a las computadoras de las personas valiéndose de distintas técnicas de de intromisión tales como: virus, spyware, robos de contraseña, ingeniería social entre otras. Este tipo de seguimiento que se le puede dar a un ciudadano sin que él lo sepa, está al alcance de cualquier usuario de computadoras de nivel intermedio, por lo que es necesario que nuestras leyes se reformen con prontitud, para de alguna manera con el temor a ser castigado menos personas lleguen a las filas de la delincuencia organizada.

Las reformas se deben realizar a nivel Federal para que de esta manera, no importe desde que entidad de la República se den estas actividades ilícitas y no se aleguen problemas de competencias de los Ministerios Públicos y Jueces, ya que tal vez ante el desconocimiento de las tecnologías un juez, podría lavarse las manos diciendo que no entra en su jurisdicción por razones del territorio geográfico en el que se da la actividad delictiva, de esta forma considerando el Delito como Federal se evitan estos casos ya que cualquier Juez tiene la obligación de dar vista de inmediato al Ministerio Público Federal.

Considero que la solución a las conductas ilícitas no está siempre en elevar las penas corporales, también las penas alternativas pueden ayudar en la rehabilitación del delincuente, esto puede usarse para los casos en los que las personas utilizan programas de cómputo sin el respectivo pago de la licencia, ya que lejos de ayudar a nuestro país lo perjudicaríamos, porque muchas familias sólo utilizan estos productos para sus tareas escolares y lo hacen por necesidad y en muchos casos por falta de conocimiento ya que ni siquiera saben que el uso de esos programas se debe dar previo pago de un precio a la empresa creadora del software, distinto es el caso de las empresas que saben esto de antemano, aunque de igual manera se puede resolver con la imposición de multas o el pago del programa a la empresa.

Estas conductas aunque ilícitas, no laceran de manera muy grave el entramado social, lo importante de regular estas como delito, sería que la gente aprendiera que los programas tienen un valor y debe de pagarse por ellos, de igual manera al regular correctamente lo anteriormente comentado se pediría a las empresas que dieran facilidades para la compra y pago de sus programas para de esta manera atacar la falsificación de sus productos.

El Derecho, sin lugar a dudas como la vida misma está en constante evolución, tiene que ir de la mano de esta, ya que no ser así caemos en las conocidas lagunas legales que acarrean funestas consecuencias como lo son:

- Que los delincuentes no sean castigados
- Que si son castigados, no sea de la manera correcta
- Que los ciudadanos al ver que no se cumplen con las leyes pierdan el respeto por estas y por las autoridades
- Que las empresas no traigan sus inversiones en virtud de que no les ofrecemos un marco jurídico acorde al mundo actual.

El presente trabajo no pretende resolver el problema planteado, pero sí pretende hacer que se tome conciencia de este, y trata de aportar en la medida de lo posible al realizar una muy somera tipificación de los Delitos Informáticos con más alta incidencia e importancia desde mi punto de vista.

## *Capítulo 1.*

## *Conceptos generales acerca de:*

### *1.1 Derecho Penal*

El Derecho Penal es sin lugar a dudas la columna vertebral del presente trabajo, sin embargo el carácter del mismo obliga a realizar una breve referencia histórica haciendo un recorrido de manera muy general por la evolución de las distintas etapas penales.

Desde el principio de los tiempos cuando el hombre era poco más que un simio evolucionado, surgieron las primeras conductas que podemos llamar ilícitas puesto que todo entramado social contiene miembros que no guardan el comportamiento (deber ser) que todos esperamos, así tenemos que existían peleas (lesiones), apoderamientos ilegítimos de cosas ajenas (robos), por lo cual surgió la necesidad de castigar dichas conductas para que no afectaran a los miembros de una comunidad.

De esta forma surge el primer antecedente del Derecho Penal, la etapa de la Venganza, esta se caracteriza porque el daño que ocasionó la comisión de un delito se repara causando un daño igual o mayor al delincuente; cuando el daño infligido era mayor que el que originó el delito se tenían problemas ya que la pena no era proporcional al delito de ahí que derivara la aplicación de la llamada “Ley del Talión: ojo por ojo, diente por diente”.

En esta etapa tenemos cuatro tipos de venganzas:

- Venganza privada. Se caracteriza porque la persona que sufría el daño por el delito cometido tomaba la justicia en mano propia y causaba algún daño al infractor.

- Venganza familiar. En virtud de que un miembro de la familia era lastimado o menoscabado en su persona o bienes, algún consanguíneo propinaba el castigo al delincuente.

- Venganza divina. En este caso las personas no eran los que impartían justicia sino que se dejaba a las deidades del pueblo en cuestión el castigo que se le diera al criminal, en algunos casos se acudía a rituales religiosos o mágicos para que los dioses intervinieran de una manera más directa y efectiva.

- Venganza pública. El encargado de la impartición de justicia era un representante de la autoridad y la pena se aplicaba en una plaza pública, para que de esta manera el resto de la población pudiera escarmentar en cabeza ajena, dadas estas características las penas aplicadas de esta manera eran realmente crueles, ya que involucraban tortura y muerte dolorosa, algo a destacar era que casi siempre iban de la mano de la “Ley del Talión” y hasta cierto punto esta venganza es la más proporcional de todas ya que al impartirla un representante de la autoridad se tenía cierto control sobre los castigos.

Después de esta etapa tan cruenta y salvaje, el Derecho evolucionó dando origen a una fase Humanitaria, la cual se distingue por tratar de erradicar la crueldad de las penas y hacer que estas tengan un carácter más constructivo y ejemplar en la sociedad.

El máximo exponente de esta corriente lo encontramos en el Marqués De Beccaria; el cual en su tratado de los “Delitos y de las Penas” da las directrices que los castigos debían de contener para evitar la comisión de nuevos delitos, entre los que se encuentran:

- Las penas deben ser establecidas por las Leyes.

- Las penas deben ser públicas, proporcionales al delito y nunca crueles.

- Las penas deben tener carácter preventivo.

Es muy importante resaltar que Beccaria creía que las penas no debían ser crueles e inhumanas, sino pequeñas pero efectivas, lo que daría lugar a evitar que otras personas trataran de delinquir, puesto que lo que se buscaba con estas penas era acabar con la impunidad, para así crear en la población una percepción de que se cometiera cualquier delito por pequeño que fuera, este recibiría un castigo, por lo cual la población evitaría cometer delitos en virtud de que estos siempre eran sancionados, hoy en día esto podría ser tomado como una política de cero tolerancia.

La etapa humanitaria sentó los precedentes para el surgimiento de la etapa Científica, ésta al igual que la humanitaria se caracteriza por tratar de prevenir los delitos, además se introduce la idea de que no basta castigar al delincuente, sino que es necesario estudiar las razones del porqué delinque y más importante aún se buscan los medios necesarios para readaptar al sujeto, esto se pretende lograr estudiando su personalidad, y al medio social donde se desarrolló; ya que se cree que la persona cometió un delito por influencias tanto de orden externo como interno.

*Antecedentes del Derecho Penal en México.*

Los primeros esbozos del Derecho Penal en México los encontramos con nuestros pueblos originarios, entre los más importantes están las culturas Mayas y Aztecas.

*Los Mayas.*

Este pueblo se caracterizaba por su religiosidad, pero al igual que en otros sus castigos eran excesivamente violentos, los principales delitos eran, el adulterio, violación, estupro, homicidio, sodomía, traición a la patria, las penas eran; quemarlos vivos, el empalamiento, esclavitud y devoramiento por fieras entre otras.

Sus leyes fueron consuetudinarias y la prisión sólo se destinaba como medio de resguardo mientras eran ejecutadas las penas.

*Los aztecas.*

Este era el pueblo más importante y poderoso a la llegada de los conquistadores, de la misma forma su liderazgo no se limitaba a ser el pueblo más grande sino también el más avanzado.

"Ha quedado perfectamente demostrado que los aztecas conocieron la distinción entre delitos dolosos y culposos, las circunstancias atenuantes y agravantes de la pena, las excluyentes de responsabilidad, la acumulación de sanciones, la reincidencia, el indulto y la amnistía."[1]

A diferencia de los mayas los aztecas tenían un Derecho Penal escrito, ya que se han encontrado vestigios fidedignos de representaciones graficas de los delitos y de las sanciones que estos merecían, entre los principales podemos mencionar los siguientes: lesiones, homicidio, robo, fraude, daño en propiedad ajena, cuyas penas ameritaban: destierro, pérdida de la nobleza, esclavitud y pena de muerte que se ejecutaba por medio de estrangulación, machacamiento de la cabeza, incineración en vida, empalamiento descuartizamiento, etc; es de importancia señalar que el pueblo azteca también clasificó los delitos de acuerdo al bien jurídico protegido.

[1] Castellanos Tena, Fernando. Lineamientos elementales de Derecho Penal. Porrua.43 edición. México 2002. p. 42

Con la conquista, los pueblos fueron casi exterminados de manera que las leyes que se aplicaban eran las españolas; de las cuales es dable destacar a las leyes de Indias, a lo largo de la época Colonial existieron diversos ordenamientos todos de origen español con aplicación en nuestro país debido a que se consideraba el territorio mexicano como una extensión de España de ahí su nombre de Nueva España.

Podemos mencionar que durante muchos años del México Independiente las leyes españolas siguieron vigentes, fue hasta 1869 que se promulgó el primer Código Penal del Estado de Veracruz, dos años después se formuló el Código de Martínez Castro con aplicación Federal, fue en 1931 cuando se publicó el Código Penal vigente hasta nuestros días, este Código pese a tener bastantes años, hoy día con algunas reformas ha sido capaz de ser el modelo a seguir para elaborar las leyes penales de los Estados de la República, creo que como el mismo Derecho el Código debe evolucionar, por ello en este trabajo presento una propuesta de reforma al mismo para tratar de darle nuevos bríos y así ayudar a que nuestro México pueda combatir a la delincuencia de una mejor manera.

Siguiendo la línea del tiempo nos encontramos con el estudio de las escuelas penales que hasta el día de hoy influyen a nuestros Códigos.

*Escuelas Penales*

El análisis de estas nos brindaran las herramientas necesarias para entender al Derecho Penal hoy en día, concebir la evolución del mismo y así poder generar ideas que modernicen a nuestras instituciones.

*Escuela Clásica*

Entre sus representantes están Francisco Carrara quien se considera el fundador de esta corriente, Romagnosi, Hegel, Rossi, Carmignani entre otros.

Cada Escuela se encargaba de elaborar ideas que posteriormente fueron entendidos como postulados, en los cuales se resumen las posturas de cada grupo de pensadores.

Los postulados de la Escuela Clásica son:

- Libre albedrío. Se hace notar que si la persona delinque, lo hace por voluntad propia ya que no existe una predisposición a delinquir, el hombre es bueno por naturaleza.

- Igualdad de derechos. Ya que todos los hombres nacemos iguales, tenemos los mismos derechos, por ello la ley no tiene distinción alguna y se debe aplicar a todos por igual.

- Responsabilidad moral. Ya que el hombre puede elegir entre el bien y el mal, la responsabilidad que se tiene es de tipo moral.

- El delito como eje y como entidad jurídica. Lo que importa al mundo del Derecho Penal es el delito, lo que la ley califica como tal, se deja de lado el carácter subjetivo de la actividad delictiva.

- Método empleado. La Escuela Clásica empleó el método deductivo es decir de lo particular a lo general, en virtud de que el Derecho y las actuaciones del hombre se engloban dentro del mundo del deber ser, el método científico empleado en las ciencias naturales que tiene leyes perpetuas no es aplicable de ninguna manera al mundo jurídico, en virtud de que el hombre actúa de acuerdo a su libre albedrío.

- Pena proporcional al delito. Esto significa que la pena no debe ser excesiva en delitos menores, y de igual forma en delitos graves, la pena debe ser

dura pero humanizada, además si se pretende castigar una conducta esta debe encontrarse en las leyes penales calificadas como delitos.

*Escuela Positiva.*

Esta surge para contrarrestar las ideas de la escuela clásica, y sus concepciones se basan en el método científico aplicado a las ciencias naturales sus principales exponentes fueron: Enrico Ferri, Rafael Garófalo y César de Lombroso.

Como se dijo anteriormente los postulados de la escuela positiva son contrarios a los de la clásica, examinémoslos.

- No existencia del libre albedrío. La Escuela Positiva dice que el hombre no puede escoger libremente entre el bien y el mal, ya que la sociedad interviene en el desarrollo de la persona, también se cree que el hombre ya nace con cierta predisposición a delinquir esto gracias a los estudios de Lombroso sobre el criminal nato.

- Responsabilidad social. En virtud de que ya se sabe que algunas personas tienen predisposición a delinquir, la responsabilidad es social ya que la sociedad es la que debe de preocuparse por evitar la comisión de delitos y defenderse.

- El punto central es el delincuente. Este es el objeto de estudio de la Escuela Positiva, el Delito es consecuencia de la persona desviada.

- Método empleado. Se utiliza el método inductivo es decir de lo particular a lo general.

- Pena proporcional a la peligrosidad del delincuente. Se niega que la pena deba ser proporcional al delito cometido, esta deber ser proporcional a lo peligroso que es el sujeto no importando el delito que comete.

- Prevención, y medida de seguridad es más importante que la pena. En virtud de que se conoce la existencia de personas que tarde o temprano va a delinquir es necesario prevenir esta conducta, es decir no se debe esperar a que se cometan los delitos para castigar, más bien se trata de evitar la comisión de ilícitos, lo cual se hará estudiando a la sociedad en general.

- Clasificación de delincuentes. No se clasifican a los delitos sino a los delincuentes, ya que es necesario conocer su peligrosidad y predisposición a delinquir.

- Sustitutivos penales. Las penas deben ser evitadas ya que su aplicación crea más resentimientos en los delincuentes, por lo cual estas deben ser sustituidas, por terapias o trabajos.

Como podemos observar las ideas de la Escuela Clásica también son aportes fundamentales para la evolución del Derecho Penal, por lo cual no podríamos entender al mismo en la actualidad sin conocer estos postulados, haré un último recorrido histórico en la llamada Escuela Ecléctica.

Escuelas Eclécticas. Surgen como respuestas a las dos anteriores, aceptan y niegan postulados de las escuelas mencionadas, pero no se limitan a esto ya que aportan ideas de suma importancia, entre las cuales destacan: la tercera Escuela, la Escuela Sociológica y la Escuela Técnico Jurídica, entre los postulados más importantes podemos mencionar los siguientes:

- Adoptan la investigación científica del delincuente
- Se distingue entre imputables e inimputables
- La pena pretende preservar el orden jurídico
- Divide a los factores criminógenos en categorías
- Se reconoce el valor del Derecho positivo

Como se mencionó con anterioridad sería imposible entender el Derecho Penal actual sin el estudio de su historia, de la misma manera, sin conocer los postulados de las Escuelas nos sería imposible tratar de formular soluciones para los problemas que nos aquejan en el presente.

Al haber realizado un recorrido por la evolución de las ideas penales señalemos la definición actual de Derecho Penal según el maestro López Betancourt: "Conjunto de normas, cada una de ellas contiene un precepto (que prohíbe u ordena ciertas conductas) y una sanción (que puede ser una pena o una media de seguridad)".[2]

### *1.2 Informática.*

Desde el principio de los tiempos el hombre ha buscado facilitar su existencia de distinta manera, una de ellas fue con la creación de herramientas de esta manera inventó hachas, cuchillos, la rueda, vestimenta, conservación de los alimentos, la agricultura, los sistemas numéricos etc.

De esta forma con el paso del tiempo y la evolución de las sociedades fue necesario que inventara técnicas mediante las cuales tareas rutinarias fueran sustituidas o aminoradas por la utilización de estas herramientas, esto dio origen a

[2] LÓPEZ BETANCOURT, Eduardo. Introducción al Derecho Penal. Décima Edición, Editorial Porrúa, México, 2002. p. 8

la Automática “Ciencia que trata de la sustitución del operador humano por un operador artificial en la ejecución de una tarea física o mental previamente programada”[3]. Aplicada a los procesos industriales se busca que las fábricas sustituyan eslabones de hombres por eslabones de maquinas dando así origen a una automatización.

Debido a esto también se buscaba que la organización de los datos e información pudiera darse de forma automática dando origen a la Informática, este término se dio gracias a la fusión de dos palabras Información y Automática, entendiendo por información a todo conjunto de ideas, hechos o representaciones de interés humano en cualquier disciplina, debe señalarse que como se mencionó con anterioridad en la definición de la Automática debe mediar la intervención de una máquina para hablar de Informática en stricto sensu.

El primer antecedente de la informática y de la búsqueda de la organización automática de los datos o información en sentido estricto lo encontramos con el surgimiento del ábaco, instrumento con el que los comerciantes pretendían simplificar al máximo las operaciones aritméticas para de esta manera efectuar más ágilmente compraventas y así maximizar la ganancia del mercader al poder efectuar transacciones financieras rápidamente y en mayor volumen. Cabe señalar que la invención del ábaco se le atribuye a China y Roma sin embargo a la llegada de los conquistadores a América se observó que entre las culturas precolombinas de México y Perú ya se usaba este sistema con ligeras variaciones a los conocidos en Asia y Europa.

Hasta el momento hemos visto que la Informática trata de organizar de manera automática los datos que se deseen ordenar, por lo que entendemos a los datos como “Conjunto de símbolos que representan una información de una forma

[3] Prieto Espinoza Alberto, et al. Introducción a la informática. 3ra edición Mc Graw Hill. España. 2002, p. 647.

aceptable para ser procesada en alguna forma"[4] . Un dato puede ser la edad de una persona, la dirección de una página de Internet, el número de matrícula en la UNAM, etc. Pero estos datos por sí solos no tienen utilidad alguna se necesita de una persona que los interprete y les dé una función.

Se ha dicho que se necesita la mediación de una máquina para que la informática alcance su objetivo, en este caso la máquina de la cual hablamos es la computadora; en el siguiente subtema analizaré la historia de estas, su papel en la historia y su evolución hasta nuestros días por el momento sólo digamos que la computadora es:

Una maquina compuesta por elementos físicos (Hardware) y elementos lógicos (Software) que es capaz de recibir datos (entrada) , procesarlos y ordenarlos de manera que puede mostrarnos resultados (salidas) de acuerdo a las instrucciones que recibe, esto se percibe tangiblemente cuando escribimos un texto con Word, la computadora almacenara y ordenara los datos que le brindamos de acuerdo a las instrucciones que previamente fueron almacenadas en ella para el tratamiento de ese tipo de información y obtendremos como resultado un texto ordenado y procesado de manera que cualquier persona puede tener acceso a este y leerlo sin mediar que su autor explique el conjunto de ideas plasmadas en el texto.

Hoy en día cualquier actividad relacionada con las computadoras puede considerarse que tiene un carácter informático ya que siempre se estarán ordenando datos e información de manera automática en la que sin lugar a dudas intervendrá una máquina.

[4] Ureña A Luis; et al. Fundamentos de informática. Alfa Omega. México. 1999. p.2

### *1.3 Computadora*

Como se mencionó en el subtema anterior los primeros antecedentes de las computadoras fueron los ábacos, ya que con estos se realizaban cálculos de manera casi automática mecánicamente ya que como se sabe el operador tenía que acomodar las cuentas en cierto orden, este sistema como se sabe se usó por siglos en todo el mundo, pero en 1623 un visionario alemán Wilhelem Schickard diseñó una calculadora mecánica automática capaz de procesar hasta seis dígitos en sumas, su invento fracasó por su complejidad pero este dio pauta a que otros sabios innovaran en la materia, por lo cual en 1670 otro matemático alemán Gottfried Wilhelm inventó una maquina mecánica con la capacidad de realizar las cuatro operaciones básicas de la aritmética, su calculadora usaba el sistema binario (sistema en que solo se utilizan 0 y 1), el mismo sistema que utilizan las computadoras hoy en día por ello se le considera como el padre de este y como el primer hombre en concebir a nivel teórico la primera computadora.

Con el paso del tiempo y con el desarrollo del comercio, la educación y la industria en Europa; existió la necesidad de realizar complejos cálculos matemáticos, y como no existían maquinas que pudieran hacer el trabajo, en Inglaterra surgió una profesión muy particular, un grupo de trabajadores que se denominaban computers (del latín computare-Calcular) eran los encargados de calcular manualmente tablas numéricas que se utilizaban en estos ámbitos, pero usualmente estos cálculos contenían errores que algunas veces eran muy considerables, por lo que un matemático inglés Charles Babbage en 1822 se dio a la tarea de inventar una maquina que pudiera calcular de manera automática y sin errores esas tablas. Por lo cual empezó a construir su máquina diferencial, obtuvo la financiación del gobierno inglés para su proyecto, sin embargo nunca pudo ser terminado ya que la cantidad de piezas que pensaba utilizar era muy grande 25,000 y pesaba cerca de 15 toneladas por lo que su proyecto quedo trunco.

Pero con nuevos bríos desarrolló la maquina analítica, en la que se podían dar instrucciones manualmente o por medio de tarjetas perforadas, cabe señalar que algunos historiadores consideran a esta la primera computadora de la historia.
Como podemos observar estos fueron los primeros pasos de las computadoras en nuestro mundo, estas maquinas son consideradas como la primer generación de computadoras.
Dentro de esta categoría entran múltiples intentos realizados por diversos inventores pero estas computadoras eran casi iguales a las comentadas con anterioridad.

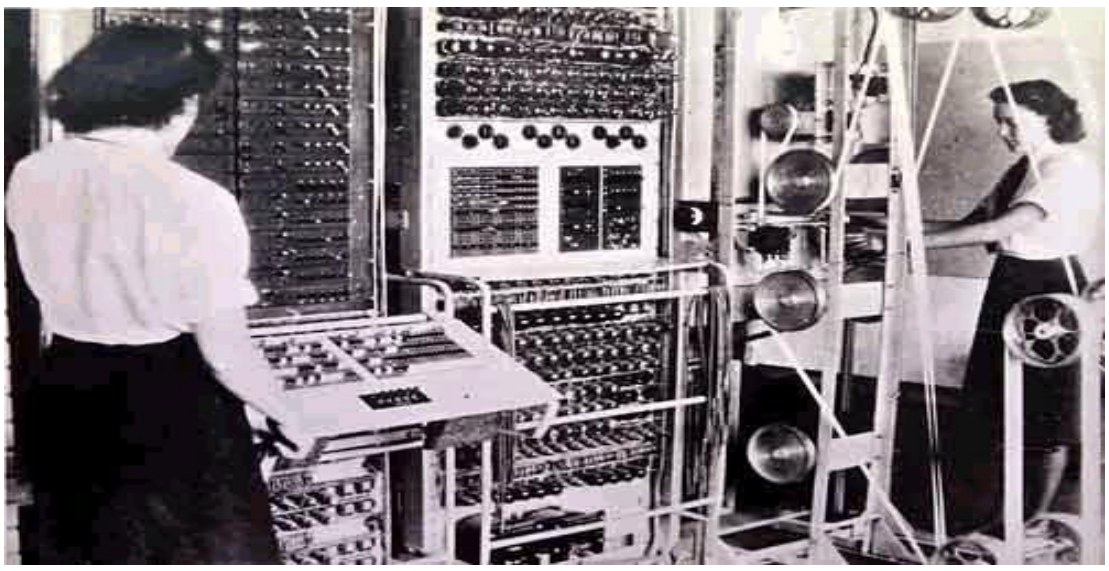
*La segunda generación de computadoras.*

Ya en pleno siglo XX en 1936 la Unión soviética crea el integrador de agua, un equipo que basaba su funcionamiento en cámaras con agua y su propósito era facilitar el diseño industrial. En 1937 Claude Shannon del Instituto Tecnológico de Masachusets publicó un artículo sobre cómo teóricamente se podían utilizar los circuitos electromecánicos para realizar operaciones de álgebra booleana, todo esto basado en las ideas del sistema binario creado por el ya mencionado Gottfried Leibniz. El alemán Konrad Zuse retoma estas ideas y crea una serie de calculadoras electromecánicas llamadas z1, z2 y z3 esta ultima la más avanzada ya que podía procesar palabras, pero fue destruida durante un bombardeo en Berlin durante la segunda guerra mundial, Zuse había intentado conseguir recursos para hacer otra z totalmente electrónica pero el gobierno alemán encontró su proyecto como no viable e inservible para el Estado.

Al mismo tiempo que Zuse pero en E.U John Vincent Atanasoff con la ayuda de Clifford Berry desarrollaba la primera computadora totalmente electrónica que denominaron como ABC Atanasoff-Berry Computer, era más rápida pero menos versátil que la Z; ya que al ser totalmente electrónica gastaba mucha energía y no se podía modificar fácilmente además de que funcionaba a base de bulbos, los cuales como sabemos eran de corta duración.

Sólo con la segunda guerra mundial, los involucrados se dieron cuenta de la necesidad de contar con equipos informáticos rápidos y poderosos. E.U e Inglaterra a diferencia de Alemania empezaron a construir computadoras monstruosamente poderosas sin precedentes hasta entonces: ENIAC y Colossus.

Colossus tenía como misión descifrar los mensaje criptográficos que transmitían los nazis, para lograrlo el primer diseño a cargo de Tommy Flowers poseía 1500 bulbos, en 1943 ya estaba funcionando, al no trabajar de la manera que se esperaba se creó una segunda versión con 2400 bulbos y cinco veces más veloz que su primera encarnación, todo este poder de procesamiento no era suficiente por lo que se decidió invertir en la construcción de más equipos para que funcionaran en paralelo y fueran más veloces, de esta forma se crea el procesamiento paralelo hoy día usado en los procesadores que promocionan como de doble núcleo.

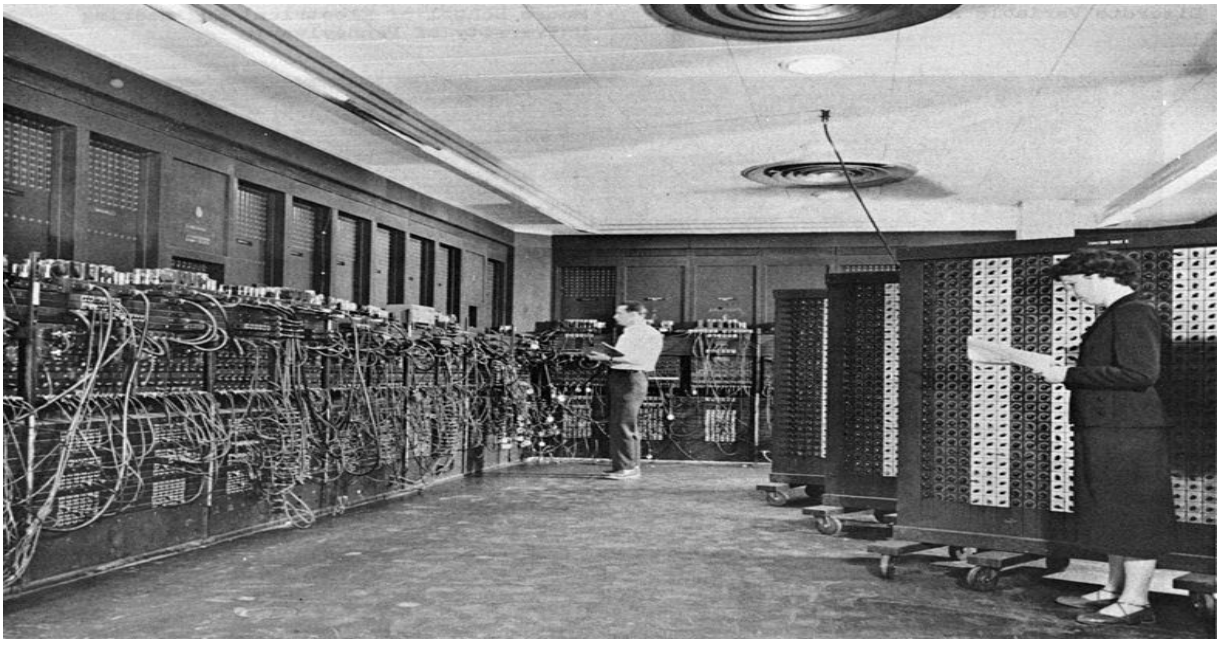


**Computadora Colossus 1943 Inglaterra**

Mientras tanto los E.U tenían la intención de que ENIAC (Electronic Numerical Integrator and Computer, integrador numeral electrónico y computadora), realizara cálculos matemáticos y ejercicios de balística, obviamente enfocadas al disparo de

armas de destrucción masiva, con la intención de obtener ventaja sobre sus rivales.

Estaba compuesta por 17,500 bulbos 15,100 bulbos más que Colossus, además pesaba más de 25 toneladas y contaba con más de 5 millones de puntos de soldadura realizados a mano y ocupaba más de 200 metros cuadrados, esta computadora fue construida por John Mauchly y J Presper Eckert.



**Computadora ENIAC E.U. 1944**

Como podemos observar el papel de las computadoras fue muy importante durante la segunda guerra mundial, de tal manera que Alemania al no hacer uso de ellas tuvo una gran desventaja en contra de sus adversarios, algunos estudiosos mencionan que tal vez la guerra no la hubieran ganado los aliados americanos de no ser porque contaban con computadoras.

Tony Sale, ingeniero que ayudó en la reconstrucción de Colossus reveló en una entrevista hace poco “Esa computadora fue muy importante para el Día D. Mostró

movimientos de tropas, el estado de las reservas, municiones y el número de soldados muertos, todo esto información vital para la segunda parte de la guerra"[5]

*Tercera generación de computadoras*

Como vimos hasta este momento las computadoras eran muy grandes y pesadas, pero en 1950 esto cambiaría gracias a William Shocley ingeniero de investigación de Bell Labs una división de la compañía telefónica Bell de E.U, este personaje basándose en estudios de Edgard Lilienfeld creó un implemento electrónico llamado transistor, este invento tenía por objeto reemplazar a los bulbos pero era infinitamente más pequeño, al principio no se obtuvo el éxito esperado ya que se consideraba caro, poco fiable y de corta duración, pero el producto se licenció a distintas empresas entre ellas a Sony, quien se encargó de crear la radio transistorizada de bolsillo, que en aquellos días era muy impresionante ya que los radios eran grandes muebles donde la familia se reunía alrededor de ellos.

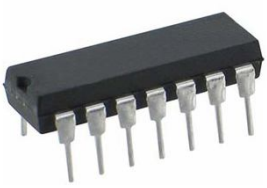

**Radio de Bulbos 1940**

[5]Los mensajes secretos de coloso. consulta en internet
http://news.bbc.co.uk/hi/spanish/science/newsid_7099000/7099362.stm Reino Unido 20-03- 2008

El radio lanzado en 1952 por Sony fue el que abrió las puertas hacia la miniaturización de los sistemas electrónicos ya que con él se confirmó que los transistores funcionaban y bastante bien y sustituían a los bulbos de una inmejorable manera.

**Primer Radio con Transistores Sony 1952**

Por esos mismo años en 1959 en los laboratorios de Texas Instruments compañía dedicada a la fabricación de calculadoras le había encargado a uno de sus ingenieros Jack Kilby que investigara acerca de un problema conocido como la tiranía de los números la cual especificaba que las computadoras necesitaban el doble de puntos de conexión en cada componente, haciendo que la detección de problemas fuera muy difícil. Por lo cual se avoco a buscar la manera de que todas esas conexiones desaparecieran junto con los bulbos, ya que estos eran los culpables de que existieran tantas conexiones en las computadoras, la solución que ideó fue: fabricar un implemento que concentrara un serie de componentes en una sola pieza de un material semiconductor (material que permite el paso de corriente parcialmente). Construyó un prototipo que presentó a sus jefes, no los convenció del todo, pero le pidieron que fabricara calculadoras con su invento, las calculadoras fueron todo un éxito, ya que eran muy rápidas y pequeñas, de esta forma se inventaron los circuitos integrados, un componente que permite al igual que el transistor sustituir muchas piezas por una sola en un aparato electrónico, por ello se dio la reducción de tamaño de todos los electrónicos.



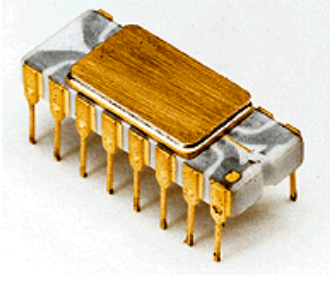
**Circuito Integrado**

Pasaron unos cuantos años hasta que las computadoras adoptaran a los circuitos integrados, las primeras en utilizarlos, fueron las computadoras de navegación del programa de la NASA Apoyo, que tiempo después llegarían a la Luna, esta primera generación con circuitos integrados y transistores también fueron utilizadas en sistemas de navegación de misiles.

*Cuarta Generación de computadoras*

Robert Noyce y Jack Kilby creadores de los circuitos integrado en 1968 funda la compañía Integrated Electronics, la muy célebre fabricante de microprocesadores conocida en la actualidad como Intel, al principio esta empresa se dedicaba a la producción y venta de circuitos integrado pero en 1971 dos empleados marcarían el rumbo a seguir.

Marcian Hoff y Federico Faggin crearon el primer C.P.U (Central Process Unit, Unidad Central de Proceso), llamado Itel 4004, lo cual trajo consigo otra revolución ya que este dispositivo con la unión de los transistores y los circuitos integrados permitían que las computadoras cada vez consumieran menos electricidad, fueran más pequeñas y más poderosas.



Intel 4004

Sin embargo, en el momento de su lanzamiento no fueron tan utilizados en las computadoras su destino fueron las calculadoras, hasta 1974 se usaron con la computadora que creó Jonathan Titus para la revista Radio Electronics, esta se vendía con la revista para que la armara uno mismo, se vendieron alrededor de 1000 piezas.

Poco después Popular Electronics, publicó los planos y vendió el kit, para que otra computadora pudiera armarse en casa la Altair 8800, tiempo después se empezaron a vender modelos que se podían conectar al televisor, lo que originó la necesidad de hacer más fácil, el uso de la computadora, por lo que Bill Gates fundador de Microsoft en ese entonces estudiante de Harvard, vendió un sistema operativo para esta máquina, dando lugar al nacimiento de Microsoft.


Fue durante la década de los 80´ que las computadoras empezaron a llegar a los hogares, ya que empezaron a bajar de precio gracias a que varias empresas empezaron a vender muchos modelos distintos, los monitores de ser monocromáticos cambiaron a ser de color, se inventó el mouse compañero

inseparable del teclado, fue durante estos años que se acuñó la frase Pc acrónimo de Personal Computer-Computadora Personal. Podríamos escribir páginas y páginas sobre la evolución de las computadoras hasta principios de los 90´, pero con lo visto hasta ahora nos damos cuenta del papel de la computadora en la historia y su evolución hasta nuestros días.

**Computadora Actual**

### *1.4 Internet*

Por principio de cuentas definamos lo que es Internet, se puede definir como la interconexión de varias redes de computadoras en una sola red, una red de computadoras es la conexión que existe entre una y otra y hace posible la comunicación de estas, después de observar la evolución de las computadoras hasta nuestros días ahora veamos ¿cómo es que surgió Internet?

Durante la guerra fría en 1957 la Unión Soviética lanza al espacio el primer satélite artificial sobre la tierra Sputnick, E.U no podía quedarse cruzado de brazos ya que ellos querían estar a la cabeza en lo que a tecnología militar se refería. Dada la preocupación existente por este suceso el Presidente de E.U encomienda al Departamento de Defensa (DoD) la creación de la Agencia de Proyectos de Investigación Avanzados (Advanced Research Projects Agency, ARPA), dentro de

esta nueva división se crea la Administración Nacional de Aeronáutica y del Espacio (National Aeronautics and Space Administration, NASA) con el objeto de ganar la carrera espacial a la Unión Soviética.

Dentro de estas divisiones existieron muchos proyectos militares, pero en 1969 con la creciente preocupación de que estallara la guerra nuclear y ante la fragilidad de la red telefónica, principal forma de comunicación hasta entonces; el DoD decidió que debían de buscar alternativas para que en caso del más mínimo ataque no se quedaran incomunicadas las agencias gubernamentales, por lo que se encargo a los empleados de ARPA Bolt, Beranek y Newman que desarrollaran una forma de comunicación, por lo cual se creó ARPANET una red experimental en la cual la tecnología utilizada permitía que la información que por ella transitara llegara a su destino a pesar de que parte de la red fuera destruida. Esta tecnología se llama conmutación de paquetes y dejando de lado los conceptos técnicos, su función se puede explicar de la siguiente manera:

Una computadora digamos del DoD generaba un mensaje el cual debía ser transmitido a todas las agencias gubernamentales, estas agencias reciben el mensaje ya que otra computadora estaba conectada por medio de la red a la computadora de DoD, esto permite que si la línea de comunicación que enlaza al DoD con el FBI era atacada y por tanto destruida, las otras agencias recibirían el mensaje y como a su vez estaban conectadas con la computadora del FBI estas sin problemas podrían reenviar el mensaje.

Ya en 1972 se crea el correo electrónico por lo cual se populariza más el uso de la red ya que permite a los investigadores comunicarse rápidamente, por ello el ejército tuvo que permitir que algunas instituciones como Universidades, centros de investigación y el gobierno de E.U se conectaran a ARPANET, pero bajo las reglas impuestas por ellos, una de ellas dictaba que los fines que se debían perseguir al conectarse a la red fueran científicos y con ánimo de apoyar al

gobierno de E.U. Por ello se empiezan a crear redes parecidas a ARPANET, pero eran privadas de distintos países y diferentes una de otra.

A principios de los 80´ el gobierno norteamericano por razones de seguridad decide dividir a ARPANET en dos redes: ARPANET Y MILNET, esta última con información militar clasificada. Esto con la intención de que las empresas, científicos y particulares siguieran colaborando con ellos, pero evitando así el riesgo de que información clasificada cayera en manos no deseadas. A estas redes interconectadas se les denomino INTERNET DARPA, pero con el paso del tiempo terminó llamándosele Internet.

Como se mencionó con anterioridad al ser restringido el acceso a ARPANET, los particulares, empresas y científicos crearon sus propias redes, todas con una arquitectura distinta ya que no existían estándares, las redes más importantes y conocidas eran: CSNET (Red de Ciencias de Computo), COMPUSERVE, BITNET, EARN entre otras. Todas estas redes tenían problemas de comunicación ya que no usaban los mismos protocolos para comunicarse por lo cual se crea la NSFNET (Red de la Fundación Científica Nacional), que conectaba a 5 grandes centros de cálculo en diferentes Estados de la unión americana, esta interconexión se fue expandiendo a otras redes, hasta que en 1989 se unifican todas las redes con el mismo protocolo de comunicación dando origen a Internet, por lo cual ARPANET se cierra definitivamente en 1990.

Mientras que en México "La primera conexión de una maquina con la red internet no fue sino hasta el año 1993 a través de un equipo de computo con base en el ITESM Campus Monterrey"[6]. Por ello puedo afirmar que nuestro país fue pionero en internet en Latinoamérica no así en la reforma de sus leyes.

[6] Molina Salgado, Jesús Antonio. Delitos y otros ilícitos informáticos en el Derecho Penal.Porrúa 2003. P. 10

### *1.5. Derecho Penal y Nuevas Tecnologías*

El Derecho desde su nacimiento ha tenido que adecuarse a la realidad de una sociedad, a sus costumbres, a su moral, a la forma de vida de la misma, así tenemos que durante algún tiempo fue legal la esclavitud, pasado un largo tiempo se luchó porque los esclavos pudieran comprar su libertad, ya durante la guerra de Independencia en nuestro país la abolió Don Miguel Hidalgo, por ende tenemos que el Derecho al igual que la sociedad no puede ser estático, tiene que cambiar, pero sobre todo evolucionar.

Entendemos por evolución en el Derecho, aquel cambio que permite que se adecue a una nueva realidad, ejemplo de esto es la despenalización del aborto antes de las 12 semanas de vida, el cambio en nuestra legislación se debe al reclamo que existe de la sociedad para que esta actividad no sea penada. De esta forma los legisladores observan, analizan y tratan de solucionar un problema que se plantea en la sociedad.

Así, la sociedad del siglo XXI ante los constantes desarrollos y adelantos tecnológicos, demanda una legislación que pueda hacer frente a los problemas que hoy vivimos. Por ello los productores y creadores de fonogramas y videogramas, piden que las leyes se actualicen y castiguen a quien lucran con sus creaciones indebidamente, sobre todo con las nuevas formas de comunicación que estas tienen, basta que la película más esperada del año sea estrenada en alguna parte del mundo para que esta ya pueda ser descargada de internet y posteriormente diseminada globalmente; pero surgen interrogantes ¿Quién es responsable penalmente de esta actividad? ¿Se incurre en algún delito con esta actividad? Este sólo es un vago ejemplo de las lagunas que tenemos en nuestro sistema legal, en este marco nuestras leyes se encuentran imposibilitadas para hacer frente a esta nueva ola de ilícitos que pueden darse con el uso de las nuevas tecnologías.

En México tenemos alrededor de 23 millones de usuarios de Internet, y esta cifra aumenta día con día, la cantidad de conductas indebidas que pueden darse también se incrementa, según cifras de Microsoft compañía creadora del sistema operativo Windows, el 40% de las computadoras que se comercializan en nuestro país contienen programas falsificados conocidos como piratas.

Por esta situación nuestro Derecho Penal tiene que tratar de regular estas nuevas conductas para de esta manera evolucionar y no quedarse rezagado en la materia.

## *Capítulo 2. Delito y Delito Informático*

### *2.1. Concepto de Delito*

Como en todos los ámbitos al querer elaborar un concepto, nos encontramos ante una encrucijada ante la cual no nos queda más que observar todas las aristas y posteriormente elaborar nuestro criterio.

"La palabra delito deriva del verbo latino delinquere, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley"[7]

Como podemos observar esta definición sin duda contiene los elementos necesarios para que cualquier persona entienda lo que es un Delito, sin embargo para nosotros los abogados es necesario analizar este concepto y definirlo de una manera más específica, por lo cual existen multitud de conceptos de la palabra delito aunque también suele usarse como sinónimo la palabra ilícito, que significa lo contrario o lo que se aleja del Derecho, de esta forma tenemos que todos los delitos son ilícitos pero no todos los ilícitos son delitos, ya que el pasarse un alto, o tomar bebidas alcohólicas en la en la vía pública, si bien son conductas contrarias a Derecho no son considerados delitos, puesto que no están tipificados como tales en el Código Penal.

El Código Penal Federal en el artículo 7 señala que delito es: el acto u omisión que sancionan las leyes penales, en stricto sensu esta definición sería suficiente, ya que para que una conducta pueda ser castigada por el Derecho Penal es necesario que esté señalada en el Código Penal.

Pero considero que la siguiente es una definición que abarca de manera completa lo que es el delito. "Conducta típica, antijurídica y culpable, cuya consecuencia

[7] CASTELLANOS TENA Fernando, Lineamientos elementales de Derecho Penal. Décimo Tercera Edición, Editorial Porrúa, México, 2002. p125.

generalmente es la pena"[8], al referirse a una conducta típica se sabe que la conducta ya se encuentra regulada en la Ley Penal y esta consigan una sanción para esa conducta, cuando se habla de que esta sea antijurídica se entiende por ello que la conducta sea contraria al Derecho vigente, por culpable entendemos que la persona que ejecuta la conducta es responsable de los daños causados por esta, y al decir que generalmente se tiene como consecuencia una pena se entiende que la conducta realizada con las características analizadas anteriormente es acreedora de una sanción que establecen las leyes penales.

### *2.2. Elementos del Delito*

Como es sabido existen muchas teorías acerca de cuantos elementos integran al delito, considero que la teoría hexatómica es la más idónea para su estudio por lo que haré un breve recorrido por sus conceptos, cabe señalar que cada uno de estos tiene un aspecto negativo que también analizaré brevemente.

*Conducta.*

Esta es el comportamiento humano voluntario que produce consecuencias, así, patear un balón es una conducta y la consecuencia será que este salga disparado según la fuerza que se le haya aplicado, aquí podemos observar a la conducta en su aspecto positivo, aunque aquí hablamos de que es un comportamiento voluntario, también el Derecho Penal también castiga a los comportamientos humanos involuntarios, como lo es que atropellemos a alguien por accidente, aquí se habla de delitos culposos.

Como se mencionó, la conducta es un comportamiento humano, por lo cual sólo las personas físicas pueden ser quienes cometen Delitos.

[8] AMUCHATEGUI REQUENA, VILLASANA DÍAZ Ignacio. Diccionario de Derecho Penal. Oxford México.2da edición, 2006. p.45.

*La acción*

La acción es hacer o algo, esto implica que el delincuente ejecuta movimientos físicos y/o con herramientas encaminadas a romper la ley, sus elementos son:

Voluntad. Es el deseo que tiene la persona de delinquir, es decir de querer las consecuencias.

Actividad. Son los movimientos físicos encaminados a cometer el delito.

Resultado. Son las consecuencias de la conducta, que castiga la ley penal.

Nexo de causalidad. Es lo que une a la conducta con la consecuencia, este deber ser material, es decir que con desear que alguien muera y si este muere, no es suficiente para hacerlo responsable penalmente, debe existir elementos materiales objetivos para que el hecho pueda ser castigado a la luz del Derecho Penal, por ello los autores intelectuales sí son castigados, ya que ellos son quienes realizan todo tipo de maquinaciones que instrumentan por medio de otros, pero exteriorizan esas maquinaciones no se quedan en su mente, esto da el carácter objetivo por el cual pueden ser objeto de castigos.

*Omisión*

Consiste en realizar la conducta típica por el hecho de no hacer algo que se debiera, o dejar de hacer algo a lo que se está obligado.

Omisión simple. Es un no hacer de lo que se debe hacer, por ejemplo pasarse un alto.

Comisión por omisión. Es un no hacer voluntario culposo, por ejemplo abandonar a un herido por creer que está fingiendo y este muere.

*Elementos de la omisión*

Son los mismos que los de la acción, por lo cual no es necesario repetir los conceptos sin embargo, cabe aclarar que en la omisión simple no existe el nexo causal y en la comisión por omisión sí, pero este debe ser comprobado.

*Ausencia de conducta*

Esto es el aspecto negativo de la conducta, es decir esta no existe y por tanto no existe delito, se habla de ausencia de conducta en los casos siguientes:

*Vis absoluta*

En esta una fuerza exterior humana invencible se ejerce contra la voluntad de alguien, y por ello ese alguien es quien comete el Delito. A la luz del Derecho Penal esto no es posible y nos encontramos ante ausencia de conducta ya que el sujeto es manejado por otro, pongamos el caso de una persona que apuñala a otra porque un tercero toma la mano del sujeto activo y empieza a tasajearlo, por lo cual el responsable es quien toma la mano, no el agente que fue usado como un instrumento.

*Vis maior*

Es la fuerza mayor y proviene de los elementos de la naturaleza, ejemplo sería el caso de que una persona en medio de un huracán empuja a otra y esta cae desde un segundo piso y muere.

*Actos reflejos*

Reflejo, ja**.** (Del lat. *reflexus*). Dicho del movimiento, de la secreción, del sentimiento, etc.: Que se producen involuntariamente como respuesta a un estímulo.

*Psicol.* Reacción automática y simple a un estímulo.

Como podemos observar los actos reflejos son reacciones a los estímulos externos involuntarios por lo cual cuando estos aparecen, no existe conducta que castigar ya que estos sólo aparecen como reacción a un estimulo.

*Sueño y sonambulismo*

En esos momentos el sujeto carece de voluntad por lo cual no es posible que se castigue a alguien que delinque en ese estado, aunque creemos difícil que esta situación se dé.

*Hipnosis*

Este al igual que en el caso anterior, se carece de voluntad ya que se está bajo las ordenes del hipnotista, que en todo caso sería el responsable si un delito se diera en estas circunstancias.

*Tipicidad*

El Maestro Lopez Betancourt menciona que “La tipicidad es la adecuación de la conducta al tipo penal”, y por tipo penal se entiende a la descripción que crea el Estado de la conducta antijurídica considerada Delito.

Para que un delito exista es necesario que la conducta de una persona se adecúe al supuesto normativo que creó el legislador, por ello es necesario crear tipos penales específicos para cada ilícito, ya que si la conducta ejecutada que puede llegar a considerarse delito no existe en el Código Penal esta no podrá ser castigada, de esta forma nace la atipicidad el lado negativo de la tipicidad, por lo regular se distingue entre la ausencia del tipo y la ausencia de la tipicidad, la primera se da cuando el Código Penal no contiene un tipo para aplicarse en el

hecho que se cree es un delito y la segunda se da cuando la conducta de las personas no se adecuan exactamente a la descrita en la ley.

*Antijuridicidad*

Para entender este concepto diré que todo lo contrario a Derecho se considera antijurídico, pero no por ello toda conducta que se adecue a los tipos penales existentes será antijurídica, ya que puede existir una causa de justificación por la cual la conducta no será considera delito. Esto es que si en un asalto se cometen lesiones en contra del agresor y estas tienen por objeto solo repeler el robo, operará la legítima defensa y por tanto la conducta no será considerada antijurídica.

Las causas de justificación son el lado negativo de la antijuridicidad ya que su existencia permite que las conductas realizadas bajo su amparo no sean antijurídicas, existen diversas causas de justificación pero no haré mención a estas puesto que escapa a los fines de este trabajo.

*Inimputablidad*

Es el aspecto negativo de la imputabilidad y a esta se le puede definir como la capacidad legal de ser castigado por los delitos contenidos en el Código Penal, la inimputabilidad se dará cuando por diversas circunstancias el sujeto activo no entienda las acciones que realiza, normalmente se considera como inimputables las personas que sufren trastornos mentales severos, pero para que la inimputabilidad pueda existir, es necesario que el estado mental trastornado no sea inducido por drogas, por ello para una persona sea considerada imputable debe estar en pleno goce de sus facultades mentales.

*Culpabilidad*

El análisis de este elemento del delito es muy amplio, por ello solo mencionaré sus principales elementos.

Sin la culpabilidad el delito no puede existir, y se puede entender como la relación que existe entre la conducta del sujeto y los resultados típicos de la misma, esto es si el sujeto decide pasarse un alto y con ello provoca un accidente, él será responsable de los perjuicios físicos y económicos que cause a los involucrados, puesto que el sabia que el pasarse el alto estaba mal (dolo) pero no le importo.

Por lo regular la culpabilidad tiene 2 formas de darse, la primera es cuando existe dolo y la segunda cuando existe culpa. En el dolo existen dos elementos uno intelectual y otro de acción, el primero consiste en querer realizar una conducta y el segundo en llevarla cabo, existen diversos tipos de dolo pero su estudio es muy amplio por lo cual escapa al objeto de la tesis, solo podemos decir que actúa con dolo quien de antemano sabe que cierta conducta se considera un delito y la lleva a cabo puesto que desea los resultados de la misma.

La culpa puede darse cuando por descuido de nuestras acciones cometemos un delito aun cuando no deseamos que esto ocurra, derivada de esta existen los delitos culposos, ejemplo de esto es cuando una persona conduce su auto y por cambiar de estación al radio atropella a una persona y esta muere, se dice que cometió un homicidio culposo, puesto que no deseaba arrollar a nadie ni mucho menos matarlo, sin embargo el delito se cometió y es culpable en virtud de que por su descuido atropello al transeúnte, por ello aunque el delito existe no se castiga de la misma manera que el delito doloso, puesto que el legislador entiende las distintas circunstancias en que se dio cada uno.

Mención aparte merece la preterintención, ya que es una mezcla entre la culpa y el dolo, ya que la persona si desea ejecutar cierta conducta pero no desea los resultados, el ejemplo perfecto es cuando una persona empuja a otra entre jugueteos, pero el empujado cae se golpea la cabeza y se lesiona, si bien se

deseaba empujar a la persona para jugar no se deseaba empujarla para lesionarla, el delito existe, sin embargo actualmente nuestro Código Penal solo acepta que los delitos son dolosos o culposos.

*Inculpabilidad*

Esta se presenta cuando alguno de los elementos del delito se encuentra ausente, o bien cuando opere una causa de justificación y por ende la culpabilidad como elemento del delito sea eliminada.

A continuación enumero las causas de inculpabilidad más importantes, legítima defensa, la no exigibilidad de otra conducta , temor fundado, estado de necesidad tratándose de bienes de la misma jerarquía, como ya mencioné estos son los más importantes, pero no los únicos.

*Punibilidad*

Se considera como punibilidad a la facultad que tiene el Estado de imponer una pena a las conductas de los individuos cuando estos trasgreden el Código Penal cometiendo un delito con todos los elementos que ya se mencionaron.

Existe discusión acerca de si la punibilidad es un elemento del delito o no, en mi opinión no es propiamente un elemento del delito sino una consecuencia de ejecutar el mismo, ya que si el delito no se comete no existirá la punibilidad, aunque es necesario mencionar que si el delito no se castiga es como si no existiera en el mundo del Derecho.

### *2.3. Denominaciones para el Delito Informático*

Entre la multitud de estudiosos del tema existen diversas denominaciones de lo que son los Delitos Informáticos, cada uno otorga cierto calificativo a estos, por lo cual analizaré las distintas denominaciones y diré él porque la mejor denominación es la de Delitos Informáticos.

*Delitos Computacionales*

Dentro de la doctrina chilena, se consideran como delitos computacionales a los delitos previamente tipificados en su Código, y que cuando se cometen existió el uso de una computadora o sistema informático calificando a estos como un medio comisivo.

Al seguir a esta corriente los delitos tipificados serían insuficientes, en virtud de las numerosas conductas delictivas que existen hoy en día con el uso de los sistemas informáticos. Como ejemplo pongamos las actividades que llevan a cabo los Hackers en E.U. es muy conocida la afición que existe por el futbol americano en ese país, también se sabe que el domingo que se juega el llamado SuperBowl se corren millones de apuestas en los casinos, tanto de forma física como vía internet, obviamente el valor de estas son de varios miles de millones de dólares, entonces al saber esto los Hackers entran a las computadoras donde los casinos almacenan toda la información de los clientes, números de tarjetas de crédito, a quien apostaron, qué cantidad, al tener esta información tan valiosa en sus manos, la secuestran y piden rescate por ella, los casinos no pueden darse el lujo de perder millones de dólares por perder esos datos y tampoco pueden poner en riesgo la información de los clientes, por lo cual pagan millones de rescate. Por lo cual un delito computacional pueda penar esta actividad, ya que el delito de secuestro castiga a quien priva ilegalmente de la libertad a una persona, no a quien priva ilegalmente a una cantidad de datos o información. Por lo que

considero que la doctrina de los delitos computacionales es insuficiente para castigar efectivamente la comisión de un Delito Informático.

*Delitos Telemáticos*

En España utilizan el término para englobar a los Delitos Informáticos y a los cometidos en contra de las telecomunicaciones o con uso de estas, pienso que la denominación es incorrecta en virtud de que la mayoría de los aparatos que hacen posible la comunicación son aparatos informáticos, por lo cual al referirnos a los Delitos Informáticos estaremos incluyendo a las telecomunicaciones dentro de estos.

*Delitos Cibernéticos*

Ninguna de las legislaciones que he investigado hacen referencia a estos, sin embargo en México la Secretaría de Seguridad Publica acogió esta denominación para darle nombre al cuerpo policiaco que se encarga de combatir estos delitos, la llamada Policía Cibernética es una unidad especial de la Policía Federal Preventiva, que se encarga de investigar a los Delitos Informáticos, aunque tengo dudas acerca de su eficacia en virtud de que no existen cifras oficiales en nuestro país, lo cual es realmente estúpido ya que al tener un grupo especializado para la investigación de estos delitos cómo es posible que no se tengan cifras al respecto de los mismos.

Considero esta denominación de Delitos Cibernéticos errónea en virtud de que esta ciencia estudia a:

> (Del fr. *cybernétique*, este del ingl. *cybernetics,* y este del gr. κυβερνητικ, arte de gobernar una nave).

1. f. Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas"[9]

Por lo cual no consideramos que estas características ayuden a saber lo que en realidad son los Delitos Informáticos, por lo cual en el siguiente subtema analizaré, estudiaré y trataré de dar la mejor definición de lo que son los Delitos Informáticos.

*Delitos de alta tecnología*

Según Debra Shinder, los Delitos de Alta Tecnología son: "casi todos los delitos tipificados en el Código Penal para cuya comisión emplean tecnología de la Información y Comunicación"[10]

### *2.4. Concepto de Delito Informático*

Por lo regular se ha tratado de encuadrar a estos Delitos en los tipos penales ya existentes en cada país lo cual es erróneo, ya que como se mencionó con anterioridad los tipos penales son insuficientes para atacar este problema.

Un compatriota Julio Téllez Valdés habla de dos tipos de Delitos Informáticos, el atípico y el típico veámoslos: en el concepto atípico se tiene que los Delitos Informáticos son "actitudes ilícitas que en que se tienen a las computadoras como instrumento o fin"[11] mientras que los Delitos Informáticos típicos son "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin".[12]

---

[9] Diccionario de la Real Academia Española consulta en internet. http://buscon.rae.es/draeI/SrvltGUIBusUsual?LEMA=cibern%C3%A9tica&origen=RAE España 23-10-2008

[10] SHINDER, Debra. Prevención y detección de Delitos Informáticos. Editorial Anaya Multimedia, Madrid, 2003.p. 35

[11] TELLEZ VALDEZ Julio, Derecho Informático. Mc Graw Hill. México 3ra edición, 2007. .p.105.

[12] TELLEZ VALDEZ Julio, Derecho Informático. Mc Graw Hill. México 3ra edición, 2007. .p.105.

Estos dos conceptos como un buen intento por explicar a los Delitos Informáticos, ya que engloban casi todos los elementos necesarios para su conformación, pero carecen de elementos precisos para abarcar a la totalidad de los mismos.

De la misma manera el concepto del tratadista Alberto Nava considera que los Delitos Informáticos son: "Toda conducta ilegal que involucra el procesamiento automático de datos y/o la transmisión de estos"[13].

Este concepto pienso es menos afortunado que las anteriores, ya que al decir "toda conducta ilegal" abarcaría a los ilícitos y estos por las razones que antes fueron expuestas no pueden ser considerados como Delitos, además deja sin mención exacta en donde se procesan automáticamente los datos, por lo cual su concepto no abarca a todos los equipos que pudieran utilizarse para tal fin, y por lo tanto deja de lado estos como medios comisivos.

Como ya se comentó con anterioridad compartimos el concepto de Delito de los maestros Amuchategui y Villasana por lo que los Delitos Informáticos son:

La conducta típica, antijurídica y culpable, que tenga por objeto vulnerar un sistema o red de sistemas informáticos, o los datos que este contenga, así como la transmisión de los mismos que puede ser por medios terrestres, aéreos o móviles.

A continuación desgloso este concepto, cuando se habla de sistema informático se refiere a cualquier maquina que procese datos automáticamente, es decir; computadoras, celulares, sistemas gps, tarjetas de memoria, cajeros automáticos, cámaras fotográficas, cámaras de video etc. Al decir red de sistemas informáticos incluimos tanto a Internet, como a las redes que pueden existir en empresas o domicilios particulares, cuando calificamos a medios móviles englobamos a;

[13]NAVA GARCÉS Alberto, Análisis de los Delitos informáticos. Editorial Porrúa, México, 2005. p.21

tarjetas de memoria, discos duros portátiles, reproductores mp3, o cualquier medio móvil que pueda transportar y transmitir información de esta forma se entiende que es necesario establecer al medio comisivo del delito.

### *2.5. Clasificación del Delito Informático*

Ya que se tiene una definición de los Delitos Informáticos plantearé su clasificación.

Algunos autores realizan una clasificación tomando como base a las computadoras como instrumento y medio o cuando estas son los fines u objetivos que se persiguen, creemos que esto es innecesario ya que como señalé en el subtema anterior no se pueden separar estos conceptos, ya que para cometer un Delito Informático desde nuestro punto de vista es necesario que exista un medio comisivo, entendiendo a este como el instrumento del que se vale el delincuente para cometer el ilícito y que siempre será un aparato informático, ya que sin este no puede darse ningún Delito que se califiqué como Informático.

La Organización de las Naciones Unidas se encargó de realizar una clasificación-descripción de los Delitos Informáticos, la cual es muy buena y que las conductas que ahí se analizan son un primer paso para lograr unificar la tipificación de estos Delitos en el mundo entero, la clasificación es esta.

| **Tipos de Delitos Informáticos Conocidos por Naciones Unidas** | |
|---|---|
| ***Delitos*** | ***Características*** |
| ***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 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 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 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 partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos 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 | Aprovecha las repeticiones automáticas de los procesos de computo. 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 transfieren a 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 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. |

| ***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, gusanos, bomba lógica o cronología, |
| Acceso no autorizado a Sistemas o Servicios | Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) 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. | 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. |

Como se puede observar la ONU tampoco hace una clasificación en base a que si los equipos informáticos son instrumentos o fines del delito, sólo al hablar de la falsificación de información hace alusión a esta situación ya que quiere establecer una clara diferencia entre lo que está siendo objeto de falsificación, no en cómo se clasifica al Delito en función de su objeto o fin.

El tratadista Argentino Pablo Palazzi hace una clasificación más acorde a los cánones del Derecho Penal que esta se basa en el bien jurídico que se protege: "Delitos contra el patrimonio, Delitos contra la intimidad, Delitos contra la seguridad pública y las comunicaciones, Falsificaciones informáticas, Contenidos ilegales en internet."[14]

Esta clasificación la es más acertada y aunque al ojo común puede parecer que estos delitos ya se encuentran tipificados en los Códigos Penales, la novedad que introduce este tratadista, es la variante de los medios que se utilizan para cometerlos.

La clasificación que a continuación presento la hago también basándome en el bien jurídico tutelado, ya que el Delito Informático no puede darse sin que exista un sistema informático por lo cual nuestra clasificación puede ser considerada también una pequeña descripción de los Delitos Informáticos.

- Delitos contra la Propiedad Intelectual

[14] PALAZZI, Pablo. Delitos Informáticos. Editorial Ad-hoc, Argentina, 2000.p 43-47

- Daño provocado por Virus, Spyware y códigos informáticos maliciosos

- Delitos contra la privacidad y acceso ilegal a sistemas informáticos

- Fraude informático

Esta clasificación como todo en el mundo del Derecho no es absoluta, pero tengo la convicción de que es suficiente para empezar a resolver el problema que se plantea, en los cuatro apartados se puede catalogar a la mayoría de Delitos Informáticos a la fecha, pongamos como ejemplo a los Delitos contra la Propiedad Intelectual, tanto el Código Penal Federal, como la Ley Federal de Derecho de Autor no regulan de manera adecuada al Software (programas de cómputo) ya que estos no prohíben ni castigan la utilización de otros programas para deshabilitar la protección de que son objeto para que se evite la ejecución no autorizada de estos, ya que prohíben el uso de aparatos cuyo fin sea desactivar la protección técnica de un programa de computo Art. 112 Ley de Derecho de Autor, pero por otro lado se contradice ya que cuando habla de las infracciones y sanciones en materia de Derecho de Autor, castiga a:

**Capítulo II De las Infracciones en Materia de Comercio**

**Artículo 231.-** Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto

V. Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación;

De esta forma la ley no es precisa y no castiga a quien permita la reproducción no autorizada de un programa de computo, ya que sanciona a quien tenga un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de

protección de un programa de computación, lo cual es una soberana tontería ya que los programas de computo no cuentan con algún dispositivo electrónico para evitar su reproducción, ya que un dispositivo es un aparato y salvo contadas excepciones los programas cuentan con una protección de este tipo, por lo que las personas que utilicen algún programa para desactivar la protección técnica de algún software quedan sin castigo ya que no lo utilizarán para desactivar ningún dispositivo electrónico.

### *2.6. Sujetos activos y pasivos*

*Sujeto activo*

El sujeto activo se puede definir como la "persona física que realiza la conducta típica descrita en la norma penal. También se le denomina agente, delincuente, criminal, etc."[15] En otras palabras es la persona que rompe la ley y que causa un daño a alguien o a algún objeto.

Desde este punto es interesante observar el perfil de las personas que pueden llegar a cometer delitos informáticos, como es obvio la persona tiene que tener conocimientos en informática, por lo que la mayoría de los sujetos activos son jóvenes o en el caso de personas mayores se trata de ingenieros o que cuentan con conocimientos técnicos para poder llevar a cabo conductas ilegales en este ámbito, ya que aunque casi todas las personas contamos con interacción de equipos informáticos la mayoría no alcanza lo conocimientos necesarios para delinquir.

También como característica de estos delincuentes tenemos que la mayoría persiguen un ánimo de lucro, ya sea vendiendo la información de las personas, defraudándolas o violando los derechos de propiedad intelectual.

[15] AMUCHATEGUI REQUENA, op. cit. p. 159

De igual manera podemos determinar que al hacer uso de equipos informáticos y el haber aprendido a usarlos tuvo que mediar que las familias de las que provienen no son de escasos recursos en virtud de que si así fuera difícilmente hubieran podido desarrollar los conocimientos técnicos necesarios para delinquir de esta forma.

Con ello el concepto de que las personas sólo cometen Delitos por carecer de educación y dinero, se viene abajo, ya que al igual que en los delitos de cuello blanco, los delincuentes son personas preparadas la mayoría de las veces movidos por la ambición.

*Sujeto Pasivo*

"Persona física o moral sobre la que recae el daño o peligro en un delito. También se le conoce como ofendido."[16]

Como podemos observar, cualquier persona o empresa puede ser objeto de estos Delitos, por lo regular al contrario que el sujeto activo, el pasivo será una persona que cuenta con conocimientos informáticos muy limitados, por ello los usuarios hogareños son blanco fácil de estos delincuentes.

Aquí se buscara averiguar el uso que la persona le da a la computadora, si usa cuenta de banco, sus datos personales, así como información que pueda ser vendida a empresas para que estas nos envíen publicidad, creo que nadie que use una cuenta de correo electrónico se ha salvado de recibir ofertas publicitarias de servicios que nunca solicitó y hasta de otros países, ello puede ser llevado a cabo porque alguien nos espió y vendió la información que recabó de nuestra computadora.

[16]AMUCHATEGUI REQUENA, VILLASANA DÍAZ Ignacio. Diccionario de Derecho Penal. Oxford México.2da edición, 2006 p. 159

En las empresas se invierten cantidades muy fuertes de dinero para resguardar la información que se encuentra alojada en sus redes y sus servidores, ya que en ella se encuentra información de impacto para los delincuentes, como lista de clientes, números telefónicos, números de tarjetas de crédito, compras hechas, con esto la delincuencia organizada puede darse cuenta de quién puede ser objeto de un secuestro o un robo a casa habitación.

A últimas fechas la mayoría de secuestradores hacen un seguimiento a sus víctimas, pero esto también incluye un espionaje bastante sofisticado en cual intervienen las llamadas telefónicas, celulares, correos electrónicos, computadoras y siguen todas las actividades de la posible víctima. Por ello El presidente del Consejo para la Ley y los Derechos Humanos Fernando Ruiz Canales en entrevista afirmó "se han detectado bandas que conocen con gran detalle programas de cómputo para manipular telecomunicaciones, por lo que echan mano de equipos GPS, micrófonos GSM, cámaras de video de largo alcance y aparatos para rastrear llamadas telefónicas".[17]

Con lo cual queda asentado que los Delitos Informáticos no sólo buscan vulnerar a las computadoras sino son un escalón para delitos de alto impacto que tanto afectan a nuestra sociedad en la actualidad.

### *2.7. Bienes Jurídicos Tutelados*

Empecemos por saber lo que es el bien jurídico tutelado, para ello tenemos que saber que las leyes penales, se crean en torno a las conductas que lastiman a una sociedad determinada, por ello después de una meticulosa observación el legislador trata de proteger por medio de leyes al o los elementos que sufren daños por el descuido de algunos o por el dolo de otros, esos elementos pueden

[17] Notimex. Actualizan secuestradores sus operaciones, afirma Fernando Ruiz Canales. Consulta en Internet http://www.zocalo.com.mx/seccion/articulo/cambian-secuestradores-sus-metodos-ruiz-canales México. 20-09-08

ser tanto físicos como etéreos, de esta forma surge el bien jurídico tutelado, y por ello podemos hablar de que se protege a la privacidad, al patrimonio o a la vida misma, el bien jurídico tutelado es aquello que el Estado pretende proteger, y lo protegerá en virtud de que es importante para el desarrollo de la sociedad que exista seguridad para las personas.

Como ya dijimos el bien jurídico tutelado es aquello que protege el Estado por medio de la creación de tipos penales, ya que cuando estos resulten afectados se castigará a la persona que provocó el o los daños.

A continuación detallo los bienes jurídicos que quiero proteger con la tipificación de los Delitos Informáticos:

- Patrimonio. Este se protegerá desde tres frentes, uno castigando a las personas que violen derechos de propiedad intelectual, otro evitando mediante el castigo, que vivales defrauden a las personas por medio de las computadoras valiéndose de la anonimidad y por ultimo regulando a los virus y códigos maliciosos que tienen por objeto dañar a las computadoras.

- Privacidad. Esto lo protegeremos sancionando las intromisiones no autorizadas a equipos informáticos definiendo que son estas, con ello podremos proteger información sensible de las personas que no debe llegar a manos de los delincuentes, pues pone en riesgo la seguridad de la sociedad, por ello también se salvaguardara la:

- Seguridad pública y seguridad de las personas.

Estos son los principales bienes jurídicos que creemos deben de protegerse en virtud de que ambos, dañan severamente el entramado social.

Por lo que protegiendo de una mejor manera la propiedad intelectual tendremos que las empresas tendrán a invertir más ya que sus creaciones se encuentran mejor reguladas, propondremos además de castigos a los infractores que se creen programas de descuentos para quien carece de recursos para comprar el software, para de esta manera no solo atacar a quien delinque por perseguir un lucro, sino quien lo hace por necesidad.

Sancionaremos a quien daña intencionalmente una computadora al introducir, virus, programas espías u otro tipo de códigos maliciosos, ya que esto la mayoría de las veces tiene como fin el robo de información para con ella delinquir, pues roban, mails, contraseñas, nips de bancos en línea, información personal e incluso fotos de las personas de quien obtienen la información. Otras veces pueden desear destruir información de una empresa ya que han sido despedidos o alguien más ha pagado a un delincuente para que este colapse a la empresa.

De igual forma atacaré los fraudes que hoy en día se están volviendo comunes, tales como pedir que depositen cierta cantidad de dinero en un banco extranjero y que le devolverán este con creces, o el pedir que ingresemos nuestras contraseñas en páginas creadas para robarlas, obviamente esto realizado con dolo, con ello no sólo evitaremos que la gente sea defraudada sino también que se sientan seguros al utilizar una computadora.

Como se puede observar, muy rara vez existirá un Delito Informático aislado, ya que quien introduce un virus intencionalmente, por lo regular persigue afectar el patrimonio de la persona, o tal vez vigilarla para saber cuándo es el momento oportuno para secuestrarla o robarla.

## Capítulo 3.

## *Legislación mexicana del Delito Informático y Derecho comparado.*

### *3.1. México*

En nuestro país los intentos por legislar los delitos informáticos, todavía son bastante infructuosos, la reforma hecha al Código Penal en esta materia en el artículo 211 es muy somera y errada, analizaré él porque.

**CODIGO PENAL FEDERAL**
**"LIBRO SEGUNDO**
**TÍTULO NOVENO. REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**
**CAPÍTULO II.**

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

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad,

se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

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

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

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

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

El artículo 211 bis I, castiga sólo a las personas que alteren, dañen o modifiquen información contenida en algún sistema de informática siempre y cuando esté protegido por un sistema de seguridad, esto es absurdo ya que la ley en principio de cuentas no define lo que es un mecanismo de seguridad, ¿se trata de un firewall físico, de un firewall de software, un programa anti espías, un programa antivirus, o se trata acaso de que el equipo atacado este resguardado bajo llave?, este intento de legislar sobre el tema se ve truncado de esta manera por esa desafortunada redacción que pide que el equipo esté protegido por un mecanismo de seguridad.

El mismo tratamiento se da a las personas que intercepten información, ya que sólo castiga al infractor si el equipo cuenta con un mecanismo de seguridad, además al no tener un solo Código Penal para toda la República algunos Estados han legislado sobre el tema pero como veremos estos cambios de igual manera no resuelven el problema y llenan de dudas a las personas encargadas de aplicar la ley.

Analizaré algunos intentos por legislar a los Delitos Informáticos en algunas de nuestras entidades, diré el porqué estas regulaciones no son efectivas y más que acertadas, son un pobre intento por modernizar las leyes.

*Código de defensa social del Estado libre y soberano de Puebla.*

**"Libro segundo Delitos en particular**
**Capitulo séptimo delitos contra la moral pública; contra hechos de menores, incapaces o personas que no pudieren resistir y contra la dignidad de la persona.**
**Sección segunda corrupción y pornografía de menores e incapaces o personas que no pudieren resistir.**

Articulo 219. Comete el delito de pornografía de menores e incapaces, quien con relación a una persona menor de dieciocho años de edad o de quien no tuviere capacidad de comprender el significado de los hechos o de quien por la razón que fuere no pudiere oponer resistencia, realice alguna de las siguientes conductas:

I.- produzca imágenes o representaciones de exhibicionismo sexual, mediante fotografías, filmes, videos, o cualquier otro medio impreso, electrónico o producido por el avance tecnológico;

II.- realice materialmente la toma de filmes, videos o cualquier otro medio de obtención de las imágenes a que se refiere la fracción anterior;

III.- emplee, dirija, administre, supervise o participe de algún modo en los actos a que se refiere este artículo a título de propietario, de director, empresario o cualquier otro que implique la participación en los actos mencionados en esta disposición, o

IV.- el que a sabiendas de que se trata de las personas a que se refiere este artículo reproduzca, venda, compre, rente, exponga, publicite, difunda o envié por cualquier medio las imágenes señaladas en esta disposición".

Como podemos observar los legisladores de Puebla al regular los delitos contra la moral pública y la dignidad de la persona, no quiere deja escapar la variante que representan los medios informáticos para la consumación de ilícitos, pero sólo esta pequeña inclusión que consideramos hasta cierto punto afortunada es insuficiente para atacar la problemática actual, ya que es la única mención que se hace en el Código de Defensa Social con respecto a los Delitos Informáticos.

Al analizar el artículo citado nos damos cuenta que la fracción IV es vaga e insuficiente para el objetivo que se persigue, ya que castiga a la persona que distribuya material pornográfico a sabiendas del tipo de personas que en ella participen, la citada fracción sería menos imperfecta si en ella no se hubiera incluido la palabra a sabiendas, ya que para que el delito se configure es necesario comprobar que la persona que difunde este material conocía de la incapacidad o minoría de edad de las personas que participan, esto en los tribunales es muy difícil de comprobar, ya que ¿cómo obligar al infractor a reconocer esta situación cuando no sea evidente?, por lo cual es necesario eliminar esta característica del tipo penal para aumentar la factibilidad de la comprobación, pongamos un ejemplo:

Juan recibe en su e-mail fotos de una mujer desnuda que dicen es mayor de edad, pero este no conoce al remitente por lo cual empieza a transmitir estas imágenes entre sus amigos, si por casualidad estas fotos llegaran a una persona que considera que la mujer es menor de edad y denuncia esta actividad a la autoridad, el tipo penal no podría ser aplicado en virtud de que las fotos que

recibió  decían que la mujer era mayor de edad y este lo creyó puesto que la minoría de edad para él no era evidente, también existe el problema de cómo comprobar que la mujer podía sufrir de algún trastorno mental, si este no es visible por las características físicas de la persona, creemos que en todo caso sería necesario suprimir en la redacción la palabra a sabiendas para que el tipo penal tenga un mayor alcance.

Como ya mencioné aunque novedosa la inclusión de las variantes informáticas en la leyes poblanas, estas son insuficientes para atacar al problema real, pero es un buen primer paso para modernizar nuestros Códigos.

Ahora analizaré Código Penal para el estado de Morelos que sigue la misma línea que el de Puebla.

*Código Penal de Morelos.*

**“Libro segundo**
**Parte especial Delitos contra el individuo**
**Título décimo primero delitos contra el desarrollo y la dignidad de la persona**
**Capítulo I de las personas menores de edad y de quienes no tienen la capacidad para comprender el significado del hecho**

Artículo 212.- Comete el delito de utilización de imágenes y/o voz de personas menores de edad y de personas que no tengan la capacidad para comprender el significado del hecho para la pornografía:

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

simuladas, con o sin fines lucrativos;

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

III. Quien posea o almacene intencionalmente para cualquier fin, imágenes, sonidos o la voz de personas menores de edad o de personas que no tengan la capacidad de comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas; y

IV. Quien produzca, facilite, incite, financie, distribuya, publique o divulgue, por sí o tercera persona, mediante sistemas informáticos y/o similares a los que se reproducen por vía de internet, imágenes pornográficas de personas menores de edad o de personas que no tienen la capacidad para comprender el significado del hecho, teniendo actividades sexuales explícitas, reales o simuladas o bien reproduzcan partes genitales de estos con fines primordialmente sexuales".

Este artículo sanciona la llamada pornografía infantil, al hacerlo incluye de manera novedosa como medios de comisión a los aparatos informáticos así como a Internet, ya que a decir de muchos este es el principal medio de difusión para este tipo de material, considero que la redacción está mejor realizada que la analizada en el Código de Defensa Social de Puebla que pretende regular la misma situación, creo que sólo cabe la crítica al hacer uso de las palabras virtual y sistemas informáticos, ya que la primera el Diccionario de la Real Academia la define como :

(Del lat. *virtus*, fuerza, virtud).

**1.** adj. Que tiene virtud para producir un efecto, aunque no lo produce de presente, frecuentemente en oposición a *efectivo* o *real*.

**2.** adj. Implícito, tácito.

**3.** adj. *Fís.* Que tiene existencia aparente y no real.[18]

Por lo cual se puede afirmar que virtual es sinónimo de irreal por tanto esta expresión debe ser eliminada para evitar malentendidos en la aplicación del citado artículo.

Cuando se habla de sistemas informáticos o similares que se reproducen por vía de internet, sólo existe una imprecisión de lenguaje ya que si se menciona como medio de distribución, difusión y reproducción a internet no es necesario mencionar a los sistemas informáticos o similares ya que se tiene implícito que es necesario que estos actúen para que la difusión pueda darse, por ello las palabras sistemas informáticos debe ser eliminada.

En el Código Penal de Tamaulipas a diferencia de los anteriores regula el daño e intercepción de comunicaciones con la variante informática.

*Código Penal Tamaulipas*

"TÍTULO OCTAVO
**DELITOS COMETIDOS POR SERVIDORES PÍBLICOS**
**CAPÍTULO II**
**ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**

**ARTICULO 207-Bis.-** Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos

[18] Diccionario de Real Academia Española. Consulta en internet. http://buscon.rae.es/draeI/SrvltGUIBusUsual España 10-01-09

por algún mecanismo de seguridad o que no tenga derecho de acceso a él, se le impondrá una sanción de uno a cuatro años de prisión y multa de cuarenta a ochenta días salario.

**ARTICULO 207-Ter.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a seis años de prisión y multa de doscientos a seiscientos días salario.

**ARTICULO 207-Quater.-** Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a cinco años de prisión y multa de cien a trescientos días salario.

**ARTICULO 207-Quinquies .-** Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente modifique, destruye o provoque pérdida de información que contengan se impondrá una sanción de tres a ocho años de prisión y multa de trescientos a ochocientos días salario.

**ARTICULO 207-Sexies.-** Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y multa de cien a trescientos días salario. Los delitos previstos en este título serán sancionados por querella de la parte ofendida".

El Código de Tamaulipas sigue la línea trazada por la legislación Federal por lo que tiene los mismos defectos de los cuales se pueden mencionar los siguientes:

- Al igual que el Código Penal Federal tipifica como delito el provocar la modificación o destrucción de información contenida en un equipo de cómputo siempre y cuando éste se encuentre protegido por un mecanismo de seguridad, pero no define que sé debe entender por éste, abundaré un poco más sobre el tema; cuando realicé mi servicio social en una dependencia de gobierno el equipo que utilizaba para desempeñar mis labores no tenía ningún tipo de mecanismo de seguridad, ni físico ni de software, en este caso si de manera deliberada hubiera provocado pérdida de información o alteración de la misma, no hubiera cometido ningún delito ya que el equipo de computo no tenía ningún mecanismo de seguridad, aunado a esto es muy difícil que se pueda comprobar que existió pérdida o modificación de información.

- En el artículo 207 Ter sólo habla de equipos protegidos por un mecanismo, por lo que volvemos a acotar ¿qué tipo de mecanismo es el que protege a un equipo de computo?, ¿el gabinete del mismo?

- Además en el afán de los legisladores por tratar de prever todas las posibles conductas que pueden darse en al artículo 207 quinquies , tipifican como delito el provocar pérdida o modificación de información entre otros, por una manipulación indebida, esto es una tontería ya que si el operador del equipo por un descuido lleva a cabo las conductas antes descritas es acreedor a merecer una pena de entre 3 y 8 años de prisión, lo cual lejos de ayudar a atacar el problema de los delitos informáticos crea desconfianza en los operadores lo cual traería consigo que pocas personas desearan manipular una computadora en dependencias públicas en virtud de que por un descuido pudieran ser merecedores de una pena privativa de libertad.

México tiene grandes rezagos en cuanto legislación para este tipo de Delito,s por lo cual es necesario observar lo realizado por otros países para de esta manera tratar de mejorar nuestras leyes.

### *3.2. España*

Es uno de los precursores del tema, desde 1995 reguló situaciones en sus leyes secundarias así como en el Código Penal para ajustarse a la realidad de esos días tan cambiantes. Como ya mencioné Internet entra de lleno al grueso de la población en 1990 a partir de este año se empieza a vivir una revolución informática en medio de esta vorágine se empiezan a dar conductas que pueden llegar a ser consideradas como ilícitas hasta ese momento tales conductas no las contemplaban las leyes vigentes por ello surgió la necesidad de adecuar las leyes. España es uno de los países que más apoyó el surgimiento y crecimiento de Internet, sus ciudadanos eran de las primeras personas que tenían acceso a la red de redes por ello se vieron en la necesidad de reformar su Código Penal.

Por ello se incluyeron las siguientes figuras en su legislación Penal:

1. De las amenazas, artículo 169 y artículo 171.
2. De los delitos de exhibicionismo y provocación sexual, 186.
3. De los delitos relativos a la prostitución y la corrupción de menores, artículo 187.1, 189.1, 2, 3,7 y 8.
4. Del descubrimiento y revelación de secretos, artículo 197, 199 y 200.
5. De la calumnia, artículo 205 y 206.
6. De la injuria, artículo 208 y 209.
7. De las estafas, artículo 248 y 249.
8. De las defraudaciones de fluido eléctrico, artículos 255 y 256.
9. De los daños, artículo 264.2.
10. De los delitos relativos a la propiedad intelectual, artículo 270.
11. De los delitos relativos a la propiedad industrial, artículo 273 y artículo 274.
12. De los delitos relativos al mercado y a los consumidores (descubrimiento de secreto de empresa), artículos 278 y 279.
13. De los delitos relativos a las falsedades documentales, artículos 390.1, 392, 395 y 400.

14. De los delitos contra la comunidad internacional (apología del racismo y la xenofobia), artículo 607.

Si bien los legisladores españoles no incluyeron un apartado de Delitos Informáticos propiamente, decidieron incluir en sus tipos penales la variante informática, de esta forma sin cambiar la estructura de su Código pudieron agregar lo necesario para atacar el problema que crecía rápidamente.

Son al menos 14 referencias a Delitos Informáticos que se hacen en el Código Penal Español, pero dado el objeto de este trabajo estudairé solamente los artículos 248 y 249 que tratan sobre las estafas:

**"Artículo 248.**

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

3. La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo.

**Artículo 249.**

Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excediere de 400 euros. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción".

CÓDIGO PENAL FEDERAL

LIBRO SEGUNDO
TÍTULO VIGÉSIMOSEGUNDO. DELITOS EN CONTRA DE LAS PERSONAS EN SU PATRIMONIO
**CAPÍTULO III. FRAUDE**

Artículo 386. Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

El delito de fraude se castigará con las penas siguientes:

I. Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario;

II. Con Prisión de 6 meses a 3 años y multa de 10 a 100 el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario.

III. Con prisión de tres a doce años y multas hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

Cabe mencionar que a pesar de que el tipo penal de fraude en México contiene muchas variantes y formas de comisión en ninguna se regula cuando este es realizado por medios informáticos.

En España la Guardia Civil, un grupo de investigación parecido a la Policía Judicial o Ministerial en México creó un grupo para atender las denuncias de Delitos Informáticos (GDI), desde su creación sus integrantes fueron debidamente capacitados en el ámbito informático de igual forma estos policías reciben entrenamiento para ser investigadores de campo para llevar a cabo operaciones en el mundo real, es decir cuando se trata de catear domicilios o atrapar al presunto responsable que rastrearon vía Internet.

Los primeros pasos del GDI se dieron en 1997 y sus principales investigaciones fueron las siguientes:

1. Operación TOCO: Detención en Tarragona de dos intrusos informáticos relacionados con el acceso ilegal a los ordenadores de la Universidad de Tarragona, Universidad de Valencia, Centro de Supercomputación de Cataluña y Registro Mercantil de Tarragona.
2. Operación HISPAHACK: Detención coordinada de cuatro intrusos informáticos relacionados directa o indirectamente con la sustracción de datos reservados de carácter personal de más de 2.500 usuarios de un proveedor de Internet de Girona, acceso ilegal a 16 ordenadores de la Universidad Politécnica de Cataluña, modificación de la Página Web del Congreso de los Diputados, e intentos de accesos no autorizados a ordenadores de la Universidad de Oxford y de la NASA.
3. Operación DIABLO Y BASURA: Detención, tras la reforma del Código Penal, de dos individuos en Palma de Mallorca y Madrid, por corrupción de menores y pornografía infantil a través de Internet.

Con el paso del tiempo la actuación del GDI se fue ampliando, ya que investigaba todo lo relacionado con los Delitos que involucraran nuevas tecnologías, por lo que se creó el Departamento de Delitos Telemáticos, este se enfocaba en investigar cuatro cuestiones pornografía infantil, fraudes y estafas, propiedad intelectual y delitos de hacking.

Para tratar de ampliar su campo de acción en 2003 se cambia el nombre nuevamente y se convierte en el Grupo de Delitos Telemáticos (GDT), pero al seguir creciendo la incidencia de Delitos Telemáticos como les llaman los españoles, se tiene la necesidad de capacitar a más personal para que se ataque al problema por ello se crean los Equipos de Investigación Tecnológica (EDITE,s) en cada provincia de España existe uno de estos con el propósito de resolver estos ilícitos con mayor capacidad y rapidez.

Como podemos observar México no ha modernizado sus instituciones ni sus leyes a comparación de otros países hermanos como España por lo que creemos que debemos tomar ejemplo de lo implementado en este y otros Estados para hacer frente a esta nueva era de delincuentes, ya que en los próximos años esta modalidad de delinquir dejará de ser novedosa y alcanzará al grueso de la población de una manera importante.

### *3.3. Argentina*

Este país ubicado en el cono sur del continente americano a pesar de lo alejado que se encuentra del principal actor en estas cuestiones E.U. es uno de los precursores en problemas y legislación informática.

Durante la década de los 90 Argentina al igual que la mayoría de países, sufrió una revolución Informática, pero la legislación vigente se empezaba a rezagar, por ello los tribunales enfrentaban problemas jurídicos nunca antes vistos y no sabían cómo resolverlos y actuar ante ellos. Durante muchos años estos casos se resolvían mediante jurisprudencia, por lo cual los juicios eran muy largos, después de todo ese tiempo los jueces decidían que no existían elementos para castigar al presunto delincuente puesto que las leyes no tipificaban la conducta como Delito, por ello el año pasado los legisladores Argentinos decidieron emitir una ley mediante la cual se adicionan Tipos Penales Informáticos a su Código Penal.

La Ley 26.388 promulgada el 4 de junio de 2008, no es un cuerpo normativo que regule de manera específica a los Delitos Informáticos de una manera especial aislándolos del Código Penal, sino es un Ley que se encarga de adicionar, suprimir o modificar algunos artículos del mismo Código para de esta manera tener un ordenamiento Penal puesto al día y con nuevos Tipos penales o variantes de tipos que ya existían.

Las conductas que ahora se regulan son las siguientes:

- ✓ Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP)

- ✓ Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP)

- ✓ Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP)

- ✓ Acceso a un sistema o dato informático (artículo 153 bis CP)

- ✓ Publicación de una comunicación electrónica (artículo 155 CP)

- ✓ Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP)

- ✓ Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP)

- ✓ Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP)

- ✓ Fraude informático (artículo 173, inciso 16 CP)

- ✓ Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP)

Dentro de este universo de conductas el acceso a un banco de datos personales llama nuestra atención en virtud de que con este artículo 157 se regula la intromisión de una persona a una computadora o al servidor de correo electrónico; explico el porqué:

*Código Penal Argentino*

“Artículo 157 bis : Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

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

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

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

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años”.

Este artículo protege de una manera eficiente y correcta a la computadora y sus archivos tanto dentro del disco duro de la misma como fuera de ella (servidores externos de internet como, correo, red de la empresa, etc.). Castiga a la persona que accede, revela o modifica archivos, ya que utilizando la hermenéutica podemos determinar que al referirse a banco de datos y datos personales se engloban a todos los archivos que alguien posee dentro de su computadora, ya que estos le pertenecen y por obvias razones son de carácter 100% personal.

Aquí lo difícil sería probar quién entró sin permiso, divulgó información o modificó datos, aunque en el caso de empresas por lo regular se tienen bitácoras de quien utiliza las computadoras y en algunos casos hasta videos, aunque el verdadero problema surge cuando el ilícito no se cometió en donde se ubica el computador sí no a través de Internet, porque se necesitará de mucha investigación y tiempo

para demostrar de manera fehaciente que alguien fue el infractor además de personal calificado que pueda certificar estos hechos.

La Ley que promulgó Argentina el año pasado aunque novedosa, tiene problemas de implementación dada la novedad de los ilícitos que regula, pero en los legisladores y en las autoridades está la responsabilidad de que esta ley aunque imperfecta como todas llene vacíos legales que ayuden a que se castigue a los infractores.

### *3.4. Estados Unidos*

Hablar de las Leyes que E.U ha promulgado en aras de regular a los Delitos Informáticos es hablar de historia, y entrar en la eterna discusión de hasta dónde el Estado debe respetar nuestra intimidad, ya que muchos estudiosos de estos temas en la Unión americana afirman que estas leyes trasgreden derechos fundamentales consignados en su carta magna.

E.U desde 1986 regula este tipo de Delitos con la Ley contra el Fraude y Abuso a través de computadoras (Federal Abuse and Fraud Act), obviamente esto se debe a que en ese país las computadoras empezaron a popularizarse a mediados de los años 70, y fue cuando se dieron en forma los primeros Ilícitos Informáticos, la mencionada ley sanciona en su articulado las siguientes conductas:

- Obtención de información de Seguridad Nacional, esto es que a través de las computadoras personas que no están autorizadas para conocer de esto obtengan y divulguen información reservada para el gobierno de los E.U.

- Obtención de información privilegiada propicia para defraudar, prohíbe el acceso a computadoras sin derecho o con derecho excediendo este, con el fin de obtener datos de instituciones financieras, o agencias de E.U que tenga carácter económico o comercial.

- Ingresar sin permiso a una computadora del gobierno, se castiga al infractor aunque su intención no sea sustraer información de seguridad nacional, obviamente la pena impuesta es menor a cuando la información que se recaba es sensible para el gobierno.

- Accesar a una computadora con la intención de defraudar, se sanciona a la persona que acceda a la computadora con el fin de defraudar a una persona o empresa o este acceso tenga por objeto instrumentar un fraude en contra de alguna persona sea física o moral.

- Daño a computadoras, este apartado prohíbe la transmisión de cualquier código, programa o instrucciones que tenga por objeto causar daño a una computadora, o entorpecer el flujo de datos de esta, o robar información, en pocas palabras regula a los virus de computadoras y sus variantes.

- Robo de contraseñas y métodos de acceso a computadoras no autorizados, por medio de este concepto se trata de castigar al hacking de sistemas (técnicas de intrusión ilegales para tener acceso a una computadora por medio de internet), en virtud de que a diario se generaban este tipo de ataques en contra del gobierno estadounidense.

Cabe señalar que todas estas conductas son investigadas por autoridades Federales, aunque en algunos Estados también se tienen leyes específicas en la materia, como podemos observar en esta Ley se tiene un amplio catalogo de los Delitos Informáticos, no obstante existen leyes que perfeccionan a esta y tratan de eliminar las lagunas existentes en la misma.

Estados Unidos cuenta con más leyes sobre el tema, una de las más importantes y comentadas se promulgó después de los atentados del 11 de septiembre de 2001, es la llamada USA Patriot Act (Ley Patriota) promulgada el 26 de octubre de

2001, con el fin de crear un país más seguro y poder atacar al terrorismo de una manera frontal, esto se logra eliminando algunos derechos fundamentales al menos de manera temporal, ya que si una autoridad tiene sospecha de que alguna persona es terrorista o brinda ayuda a estos, sin mediar orden judicial puede arrestar, catear o investigar sin prueba alguna al ciudadano que resulte sospechoso.

Estas prerrogativas de las autoridades no se limitan al domicilio del ciudadano, sino que se extienden a todas sus posesiones y comunicaciones, es por ello que la Ley Patriota también regula las comunicaciones vía internet, y de igual manera se investiga toda comunicación que resulte sospechosa, aunque la misma Ley contempla que si en el curso de la investigación de estas comunicaciones se descubren delitos que no tengan que ver con terrorismo, estos pueden ser perseguidos tomando como base la investigación aunque esta resulte violatoria del derecho a la privacidad que otorga la Constitución de E.U.

Es por ello lo controvertido de la Ley, que además cuenta con tintes de extraterritorialidad ya que autoriza a que se investigue toda comunicación vía internet siempre y cuando esta tenga como destino computadoras o servidores ubicados en territorio estadounidense, por ejemplo cuando nosotros utilizamos los servicios de correo de Hotmail o Yahoo estamos estableciendo una conexión con el servidor que se ubica en los E.U y por ende nuestras cuentas pueden ser investigadas aun sin ser ciudadanos estadounidenses, por esta situación esta Ley ha sido duramente criticada ya que como se menciono viola derechos fundamentales.

No se puede dejar de mencionar a La Digital Millennium Copyright Act (Ley del Milenio Digital sobre Derechos de Autor). Esta ley castiga, no sólo la infracción del derecho de autor en sí, sino también la producción y distribución de tecnología que permita eliminar las medidas de protección implementadas para proteger el

Derecho de Autor por otro lado incrementa las penas para las infracciones al Derecho de Autor que se cometan vía Internet.

Entre otras medida establece un proceso para evitar que se difundan contenidos protegidos por el Derecho de Autor llamado Notice and takedown cuyos alcances analizaré más adelante.

Esta Ley surge como respuesta a los problemas generados a finales de los 90 con el intercambio de archivos musicales vía Internet, y para que las leyes americanas estuvieran acordes al tratado firmado con el OMPI.

## *Capítulo 4.*
## *Dificultad para tipificar y probar los Delitos Informáticos*

### *4.1. Problemas para tipificar los Delitos Informáticos*

En la actualidad existe una fuerte discusión entre los estudiosos del Derecho Penal en virtud de que algunos piensan que los Delitos Informáticos son nuevos ilícitos y por ende deben de tipificarse en los códigos para que puedan ser castigados, y la otra parte menciona que no nos encontramos ante nuevos delitos que sólo se trata de nuevos medios comisivos de Delitos ya existentes.

Sin duda estas dos posturas son totalmente contradictorias, los que sostienen que son los mismos Delitos sólo con nuevos medios comisivos, dan como ejemplo que si se pretende tipificar nuevos Delitos sería tanto como tipificar al Homicidio en virtud del medio comisivo con que es realizado, es decir clasificar al Homicidio con piedras, Homicidio con arma de fuego, etc. Estos estudiosos no comprenden la realidad de lo que son los Delitos Informáticos, si bien casi todos son variantes de Tipos Penales ya existentes, por sus características es necesario tipificarlos de una manera específica puesto que su novedad y forma de ejecución hacen que la realidad jurídica tenga que ajustarse a la actualidad.

Si solamente fueran nuevos medios comisivos, ¿Cómo es posible que otros países hayan tipificado a los Delitos Informáticos en sus Leyes?, Pensamos que la Leyes sin reformas dentro del ámbito informático son inútiles ante el mundo virtual en el que vivimos, recordemos el principio *Nullum Crimen, Nullum poena sine lege*, por ello es necesario que las leyes capturen las nuevas conductas ilícitas, para que de esta forma no se trate de encuadrar conductas nuevas dentro de Tipos Penales no aptos para ello, ya que no se podrá castigar de manera correcta al infractor.

Aunado a esto, en el medio jurídico las computadoras no son bien vistas, de hecho la mayoría de los abogados no sabe utilizarlas correctamente, aunque esta sea una de sus principales herramientas de trabajo, la realidad es que no conocen lo suficiente acerca de ellas y algunos hasta miedo les tienen, esta situación no se limita al ámbito del abogado en ejercicio de su profesión de manera privada sino que desgraciadamente permea hasta a los servidores públicos encargados de impartir justicia, desgraciadamente tanto los Ministerios Públicos como el personal de apoyo de estos la mayoría de veces no están capacitados.

En países como Estados Unidos y España existen unidades especiales para perseguir la comisión de los llamados Delitos Informáticos, esto es posible gracias a que este tipo de ilícitos los contemplan sus leyes, por ello es posible que se les dé seguimiento. En México contamos con la Policía Cibernética adscrita a la Policía Federal Preventiva (PFP), desgraciadamente la ciudadanía ni siquiera sabe de su existencia ya que ni la propia PFP ni la Secretaría de Seguridad Publica Federal brinda información en sus páginas de internet de cómo se integra este cuerpo, cuales son sus funciones y si todavía existe en la actualidad puesto que no existe información al respecto de esta situación.

La Legislación en este materia como se ha comentado con anterioridad es casi inexistente, esto trae como consecuencia que los encargados de velar por la seguridad de los ciudadanos no tomen cartas en el asunto, puesto que no existe una obligación legal para capacitar y mantener a un cuerpo especializado para este tipo de Delitos, ya que no existen leyes que se tengan que hacer cumplir, por ello es necesario reformar los tipos penales existentes o crear nuevos para que con ello se creen cuerpos especializados en la persecución de los Delitos Informáticos.

### *4.2. La Computadora y las nuevas tecnologías como Medios Comisivos*

Sin lugar a dudas la computadora vino a cambiar la percepción del mundo entero, y también la del Derecho, ya que con su introducción a la vida cotidiana vino a revolucionar la forma en la que vivimos, no hay lugar en donde no estemos cerca de una computadora.

A raíz de esto también las computadoras y las nuevas tecnologías como los son los celulares, los gps, las cámaras de video y fotográficas por mencionar algunas se han convertido en instrumentos del Delito, puesto que estos son utilizados para cometer ilícitos.

La ley en algunos tipos penales exige determinados medios de ejecución o medios comisivos, que no son otra cosa que la circunstancia que necesariamente debe cumplirse para que el tipo penal pueda ser aplicado al caso concreto.

Ejemplo de esto es que nuestro Código Penal, exige que para que la violación sexual exista, debe cometerse por medio de violencia física o moral (medio comisivo), es decir si la relación sexual se da sin emplear la violencia física o moral, la violación no existe, ya que no existieron los medios comisivos que el Código exige para calificar de violación a una cópula.

Ahora pensamos que los Delitos Informáticos son medios comisivos, puesto que su existencia no puede darse sin el uso de las computadoras, es requisito indispensable que en cualquier Delito Informático se utilice una computadora, de no ser así, la conducta no se adecuará al tipo penal y por ende no podrá ser castigada.

En el mismo matiz se analiza a las nuevas tecnologías ya que sin el uso de estas los Delitos Informáticos no pueden existir, si se pretende legislar sobre internet

este también será considerado un medio comisivo, puesto que sin la existencia del mismo, no podrá tampoco calificarse a una conducta como Delito, si en el supuesto normativo se establece que el Ilícito se cometa a través de Internet.

### *4.3. ¿Quién es responsable penalmente?*

En la comisión de un Delito Informático en la mayoría de las veces no existe un solo responsable o delincuente sino varios, por ello analizaré a las partes que intervienen.

*Sujetos activos*

Cuando hablamos de violación a la propiedad intelectual, podemos establecer que al menos se involucran tres partes en la comisión del Delito y estas son:

*Uploaders*

Este término se refiere a cualquier persona que publica información, archivos o programas de cualquier tipo en una página de Internet, para que sea observado por otros, literalmente la palabra upload significa cargar o subir, al referirnos a uploader entendemos como tal a la persona física que se encarga de llevar a cabo la tarea antes descrita.

Con esto, la mayoría de personas somos uploaders, ya que todos o casi todos alguna vez hemos subido algún archivo a internet, ya sean fotos, o archivos de datos como tareas, demandas o documentos, esto no nos convierte en delincuentes, sino en personas que tenemos la necesidad de comunicar ciertos aspectos de nuestra vida o trabajo de una manera rápida y efectiva. Pero esto da lugar a que existan personas que no hacen un uso legitimo de este derecho, sino que abusan del mismo y violan la Propiedad Intelectual de empresas o personas,

publicando y difundiendo sin Derecho obras que gozan de la protección del Derecho de Autor y de la Propiedad Intelectual.

De esta forma publican en diversos sitios de Internet material protegido por Leyes y Tratados Internacionales en Derecho de Autor, con lo cual se convierten en delincuentes ya que su conducta crea daños patrimoniales a diversas personas que intervienen en el proceso de creación de una obra protegida por el Derecho, normalmente los encargados de subir este tipo de material son los Crackers.

El término cracker (del inglés *crack*, romper) tiene varias acepciones, entre las que se tienen las siguientes:

- Es una persona que mediante ingeniería inversa es decir violando la seguridad informática de afuera hacia dentro crea: números de serie válidos sin pagar por el software, keygens programas que se encargan de generar numero de series validos personalizados para cada usuario en particular y cracks, los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo, sino lo que pretende es activar al programa o equipo por completo sin que exista el pago a la empresa fabricante del software o hardware.

- Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño, normalmente este daño es patrimonial ya que por lo regular trata de hacer que los usuarios de internet obtengan programas gratis, evitando así que las empresas desarrolladoras obtengan beneficios económicos por las ventas del software.

El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker que se refiere a personas con alto grado de

conocimiento informático que utilizan el mismo para el bien, ya que se encargan de crear y mantener la seguridad en internet.

En ocasiones el *cracking* es la única manera de realizar cambios sobre software para el que su fabricante no presta soporte, especialmente cuando lo que se quiere es, o corregir defectos, o exportar datos a nuevas aplicaciones, en estos casos (sólo en estos casos) en la mayoría de legislaciones no se considera el *cracking* como actividad ilegal.

En muchos países existen crackers mercenarios que se ofrecen para romper la seguridad de cualquier programa informático que se le solicite y que contenga alguna protección para su instalación o ejecución.

Sin lugar a dudas los primeros en subir a internet software pirata son los crackers, pero una vez que esta disposición del grueso de los usuarios estos lo empiezan a compartir creándose así una gran red de delincuentes.

Este es un solo una parte del triángulo que se forma para la comisión de este tipo de delitos por ello es necesario estudiar a los:

*Downloaders*

Así se le nombra a toda persona que guarde en su computadora cualquier tipo de información, archivos o datos extraídos de internet, con o sin consentimiento del legítimo propietario o autor de dichos elementos, de manera coloquial se conoce esta acción como “bajar o descargar”, ya que el o los archivos obtenidos se encuentran de manera virtual “subidos” a Internet por algún *Uploader.*

Sin lugar a dudas esta acción no siempre es constitutiva de Delitos, ya que existen muchos elementos que podemos bajar sin necesidad de autorización del autor, entre ellos se encuentran: programas, música, videos, ensayos, etc. El problema surge cuando obtenemos estos elementos a pesar de que los legítimos

propietarios prohíben expresamente este tipo de distribución para sus materiales, o cuando sin pagar logramos conseguir alguno de ellos.

Aunque el maestro Cabanellas afirma que “Los Downloaders son el grupo mas numeroso de infractores en términos de piratería informática”[19]. Esto se entiende gracias a que este es el grupo más grande que puede involucrarse en estas actividades sea con conocimiento o no.

De esta forma el triángulo se cierra con los:

*Intermediarios e ISPs*

Se trata de las empresas que intervienen en el proceso de comunicación que es necesario para el funcionamiento de Internet, entre estas se encuentran a los ISPs por sus siglas en ingles Internet Service Provider Proveedor de Servicio de Internet es la compañía con la cual contratamos el servicio para nuestra casa u oficina, además de los intermediarios que entre otras cuestiones permiten la interconexión de computadoras, el alojamiento de información y programas así como la publicación de páginas de internet, por ello Jorge Navarro afirma que: “Los sujetos pasivos de los delitos en comento, cualquier usuario o prestador de servicio informaticos puede ser víctima de los mismos”[20]. Esto es verdad en virtud de que es prácticamente imposible investigar todas las actividades que realizan los usuarios o empleados.

Haciendo a un lado a los Delitos Informáticos en materia intelectual los sujetos activos son los navegantes de internet que forman parte de las llamadas ciber tribus a las cuales podemos definir como a la versión informática de las tribus sociales, sólo que en este caso se trata de personas que realizan actividades poco comunes en la computadora con tendencias normalmente a hacer daño o evitarlo,

[19] Cabanellas de las Cuevas, Guillermo. Derecho de Internet. Editorial Heliasta, Argentina, 2004. p.169

[20] Navarro Isla, Jorge. Tecnologías de la Información y de las Comunicaciones aspectos legales. Editorial Porrúa, México, 2005.p. 397

ya que para convertirse en delincuente informático es necesario contar con conocimientos avanzados en informática enlistemos y analicemos brevemente a algunas:

- Hacker:

Tal como comentamos los hackers son personas con un alto grado de conocimiento en informática, estas personas fueron las encargadas de crear y difundir a Internet en sus inicios, actualmente trabajan para el gobierno, universidades y empresas realizando pruebas de seguridad en sus redes o detectando ilícitos para el gobierno, así como desarrollando aplicaciones seguras para los bancos y entidades financieras, además de crear el software que usamos a diario, como Windows, office, videojuegos, las interfaces de los celulares, etc, con esto queremos establecer que hacker no es sinónimo de delincuente, y que este término siempre es mal utilizado ya que los delincuentes, normalmente son los crackers.

Pekka Himanen un Filosofo estudioso de la actualidad informática en su obra La ética del hacker y el espíritu de la era de la información señala que: "un *hacker* no es un delincuente, vándalo o pirata informático con altos conocimientos técnicos, sino que *hacker* es todo aquel que trabaja con gran pasión y entusiasmo por lo que hace"[21] de esta forma tenemos que cualquier persona puede ser hacker siempre y cuando ponga empeño en lo que hace, por ello más adelante señala que:

"En el centro de nuestra era tecnológica se hallan unas personas que se autodenominan hackers. Se definen a sí mismos como personas que se dedican a programar de manera apasionada y creen que es un deber para ellos compartir la información y elaborar software gratuito. No hay que confundirlos con los crackers, los usuarios destructivos cuyo objetivo es el de crear virus e introducirse en otros

[21] Himanen, Pekka; et al. La ética del hacker y el espíritu de la era de la información. Editorial Destino. España 2002. Pp264.

sistemas: En este sentido, la ética hacker es una nueva moral que desafía la ética protestante del trabajo, tal como la expuso hace casi un siglo Max Weber en su obra clásica La ética protestante y el espíritu del capitalismo, y que está fundada en la laboriosidad diligente, la aceptación de la rutina, el valor del dinero y la preocupación por la cuenta de resultados.Frente a la moral presentada por Weber, la ética del trabajo para el hacker se funda en el valor de la creatividad, y consiste en combinar la pasión con la libertad. El dinero deja de ser un valor en sí mismo y el beneficio se cifra en metas como el valor social y el libre acceso, la transparencia y la franqueza" [22].

De esta forma logramos entender de una mejor manera el significado de la palabra hacker y como en el lenguaje coloquial la empleamos de una manera equivocada, aunque después de todo estos individuos al gozar de conocimientos tan amplios en el campo informático pueden llegar a ser sujetos activos de este tipo de Delitos

- *Cracker:*

Ya estudié a esta tribu sin embargo es necesario decir que estas personas están debajo de los Hackers en cuanto a conocimientos debido a que estos destruyen, molestan y dañan. Mientras que los Hackers ayudan y construyen. La motivación de los Crackers varía desde el simple hecho de superar desafíos hasta obtener algún provecho económico ya que existen personas o empresas que contratan los servicios de los crackers para violar la seguridad de los programas y poder venderlos para obtener ganancias económicas, por ello si hablamos de violar la propiedad intelectual estos seres son los amos y señores.

Dentro de estas tribus podemos encontrar también a los:

- Ex-Lamer Hacker-WannaBe:
- Lamer Cracker-WannaBe:

[22] Himanen, Pekka; et al. La ética del hacker y el espíritu de la era de la información. Editorial Destino. España 2002. Pp264.

- Pro-User:
- Lamer:

Todos estos usuarios se caracterizan por contar con un grado de conocimientos avanzados en el ámbito informático, sin embargo los mismos no son suficientes para que puedan llegar a ser considerados hackers y crackers, por lo que en la búsqueda por llegar a ser reconocidos como parte de esas tribus de elite son muy propensos a delinquir para alcanzar los status ya mencionados.

Debemos hacer un clara distinción de que el triangulo mencionado con anterioridad es aplicable a los Delitos en materia de propiedad intelectual, pero estas mismas personas así como cualquier usuario que no sea cracker como tal, puede cometer otros ilícitos tales como Fraude Informático o Acceso ilegal a sistemas de computo, ya que para la realización de estas conductas no siempre es necesario contar con un alto grado de conocimiento informático, además de que casi siempre estos delincuentes actúan de manera solitaria.

Con este panorama podemos analizar y entender al:

*Sujeto pasivo*

Es la persona física o moral que gracias a la acción delictiva del sujeto activo se ve directamente afectada en su patrimonio o en sus Derechos morales, se puede señalar entre estos a los autores, productores, directores, actores, desarrolladores de software, etc, además de las personas comunes y corrientes que utilizamos internet como medio de comunicación.

La primera pregunta que surge es: ¿Quién es responsable penalmente? Como ya señalé existe un triángulo en los Delitos en materia de Propiedad Intelectual en la cual las tres partes involucradas pueden ser responsables, esto es en virtud de las actividades que desarrollan.

Los *uploaders* pueden ser sujetos activos en virtud de que ellos se encargan de subir material protegido por las leyes de Derecho de Autor como lo son: software es decir programas de computo, videojuegos, música, películas etc. y hacen de este una distribución del mismo sin tener el permiso que debería de otorgar el legitimo propietario de los Derechos de Autor.

En algunas ocasiones estos sujetos que normalmente son crackers, difunden el o los programas sin modificación alguna, ya que aprovechan la ventaja de que ciertas compañías permiten distribuir el material sin modificación siempre y cuando sea para fines de probar las funciones del mismo, sin embargo estas mismas personas suben otros archivos (cracks, llaves) por medio de los cuales se desactivan los medios de protección que el fabricante había puesto en sus programas, separan de esta manera estos archivos para así en teoría no contravenir a las disposiciones vigentes en propiedad intelectual, por estas situaciones podemos establecer que sin lugar a dudas los uploaders son sujetos activos en los Delitos informáticos siempre y cuando se cumplan con las conductas antes mencionadas.

Posteriormente ante esta difusión de los materiales los downloaders se encargan de bajarlo y muchas veces a redistribuirlo, por ello nuevamente se estarían violentado los preceptos jurídicos vigentes, el simple hecho bajar el material protegido por sí mismo no es actividad constitutiva de Delito, pero se convierte en esto cuando la persona decide instalarlo en su computadora o en la de alguien más con el fin de utilizarlo de manera ilimitada gracias al crack que viola la seguridad contenida en el programa para evitar el uso no autorizado, este es uno de los principales problemas que tienen las empresas a nivel mundial, ya que no sólo los usuarios finales u hogareños son los que utilizan software pirata, sino que existe un gran red de empresas o vendedores que obtienen grandes ganancias ilícitas a razón de vender software con derechos protegidos por la leyes en Derechos de autor y propiedad intelectual, por ello en el capítulo final diré porque es necesario tipificar este tipo de actividad en nuestro código.

Lo mismo pasa cuando el material difundido no se trata de programas o videojuegos, sino de películas, música o libros, ya que si bien se puede decir que las personas utilizan estos materiales para el sano esparcimiento o derecho a la información, no podemos dejar de lado que al poder observar o leer materiales por los cuales se debería de pagar cierto costo, obtienen un lucro indebido al no tener que ver disminuido su patrimonio por la obtención de dichos materiales, aunado a esto recordemos que existe una gran industria de piratería en México que se encarga de multiplicar y vender las películas y libros sin derecho a ello, afectando de manera seria a las empresas productoras y editoras.

Los proveedores de servicios de Internet (ISPs) también participan en este proceso, ya que ellos se encargan de enlazarnos con la información que busquemos en Internet por ello también pueden ser sujetos activos.

Explicaré el proceso que siguen los datos para involucrar a los ISPS, los uploaders suben archivos a Internet los cuales pueden estar protegidos por la ley o ser ilegales, pero para subir estos archivos necesariamente deben hacerlo a través del prestador del servicio de internet como lo puede ser Telmex, Cablevisión, Telcel, etc., por esta razón forzosamente los ISPS forman parte de los sujetos activos en los Delitos Informáticos, aunque lo hacen de manera involuntaria ya que es prácticamente imposible verificar todo el contenido que sus clientes pretenden subir a la red.

De la misma forma los servidores que utilizan Telmex y otras empresas para otorgar el servicio de Internet se ven afectados como ya observamos, ya que al subir archivos, estos necesariamente deben de ser almacenados en algún lugar por ello los servidores (empresas cuyo fin es almacenar información virtual) también forman parte en la comisión de los delitos analizados.

Por ello en Estados Unidos se creó un sistema llamado Notice and Takedown, el cual está resguardado en la Digital Millennium Copyright Act (DMCA) Ley en la

que se establece un procedimiento por medio del cual los Propietarios del Derecho de autor o Propiedad Industrial que está siendo compartida por internet sin derecho, pueden quejarse contra los servidores o ISPs que permiten esta transmisión, de esta forma los legítimos dueños de los archivos en cuestión pueden pedir que el contenido sea bloqueado o eliminado, para de esta manera evitar que sus derechos sean violentados, con esto el ISP al dar de baja el archivo se libra de responsabilidad penal, ya que al ser notificado de que en su servidor se encuentran archivos que violan la Propiedad Intelectual tiene la obligación legal de eliminar dicho contenido, esto tiene como fin no incluir como sujeto activo del Delito a las empresas que permiten estas violaciones, ya que es casi imposible evitar el mal uso de sus servidores.

Con este panorama general sobre quiénes y cómo participan en los Delitos Informáticos podemos determinar el grado de responsabilidad penal de los involucrados.

Entendamos que todos los sujetos activos mencionados con anterioridad son responsables de cometer Delitos Informáticos, pero establezcamos desde un punto de vista jurídico y de beneficio social a quién es mejor castigar.

Los principales delincuentes en los temas tratados sin lugar a duda son los crackers aquellas personas que se encargan de robar, manipular y romper protecciones de los sistemas, por ello están en primer lugar de lista de quien debe ser castigado en la comisión de estos ilícitos.

Desde este punto de vista tenemos que los posibles responsables son:

1- Crackers
2- ISPs
3- Usuarios Finales

Los crackers son las personas que buscan por lo regular lucrar con los contenidos protegidos, por ello para estas personas se debe implantar los métodos para poder castigar su accionar, ya que sin ellos la piratería de software, música y películas serían casi imposibles.

En las leyes vigentes se debe de regular la conducta de estas personas ya que esta daña de sobremanera a la industria del entretenimiento, según el último informe sobre piratería el problema pese a que es atacado alrededor del mundo crece de manera constante año con año, salvo la región de Norteamérica (no se incluye a México) y los países europeos están logrando detener su avance, no siendo así en nuestro país ya que el mismo informe no dice que el problema crece año con año irremediablemente.

Piracy Rate by Region

**Source:** Sixth Annual BSA-IDC Global Software Piracy Study, may 2009

2008

2007

61%

59%

Asia-Pacific

33%

33%

Western Europe

21%

21%

North America

59%

Middle East/Africa[23]

[23] Piracy Study. Business Software Alliance. 2008. p. 5

Tan solo el años pasado se confirmo que por cada 10 computadoras 6 tiene programas piratas [24] demostrándose de esta forma la magnitud del problema que tenemos en México.

Los ISPs, también son responsables ya que son los encargados de enlazar a la computadora personal con el mundo a través de internet y sus distintos servicios, pero la cantidad de información y conexiones es tan grande que tan solo en nuestro país contamos con 30 millones de usuarios de Internet[25] y en todo el mundo contamos con 1,802, 330,457[26] con lo cual de forma técnica es imposible controlar todo el tráfico de información que existe en el mundo a través de la carretera de la información.

Así nos encontramos ante el panorama de los usuarios finales personas que como nosotros sólo nos dedicamos a utilizar Internet como una herramienta para nuestras actividades diarias de comunicación, esparcimiento, académicas y laborales, pero en esta búsqueda de satisfacer estas necesidades normalmente delinquimos sin darnos cuenta, ya que en la mayoría de casos en nuestra computadora utilizamos programas sin licencias, o compartimos contenido que está protegido por Derechos de Autor.

Al empezar a legislar en la materia nos debemos de preocupar por empezar a crear un marco jurídico idóneo en donde se castigue con mayor severidad a quien daña más al entramado social, con esto queremos decir que las personas que se encargan de robar información valiosa sobre determinada empresa o individuos, crean el mismo daño o uno mayor que lo crackers que se encargan de quitar toda protección a los materiales protegidos para evitar una reproducción o copia no autorizada.

[24] Molina Gilberto. " Seis de cada 10 software son piratas en el país", El Universal, (México, D.F 11 de mayo, 2010).
[25]"Redacción." Conectados a Internet 30 millones, en México", El Universal,sección Tecno (México, D.F 17 de mayo, 2010).
[26]World Internet Users and Population Stats. Consulta en Internet http://www.internetworldstats.com/stats.htm 01-06-10

De la misma manera una persona que comparte música o películas sin afán de lucro, no puede ser comparada ni castigada con otra que usa estos archivos para venderlos sin derecho y obtener ganancias ilícitas.

También existen empresas creadas ex profeso para ayudar a los delincuentes a cubrir sus actividades en línea, desgraciadamente por lo regular estas empresas tienen su base de operaciones fuera de países con regulación en materia informática, por ello es importantes que nuestra legislación también persiga a los responsables de estas empresas para evitar la instalación de estas en México.

Las empresas que ven sus derechos intelectuales trasgredidos no tienen muchas armas para defenderse, ya que en la mayoría de los países no se enfrenta de manera frontal el problema de la piratería por medios electrónicos, dejado así a los empresarios luchar contra este flagelo.

Actualmente es muy difícil castigar con el peso de la ley a los delincuentes informáticos, ya que no existen las leyes ni los medios técnicos para poder probar sus actividades ilícitas en nuestro país, por ello se deben modificar nuestras leyes e instituciones para perseguir a estos delincuentes.

Con esto queremos lograr que los extranjeros no tengan miedo de invertir en el mercado mexicano por las pérdidas que pudieran tener por el problema de la piratería.

### *4.4. ¿Pena proporcional a la gravedad del delito?*

Desde las primeras civilizaciones la sociedad siempre buscó castigar a las personas que no seguían las normas sociales vigentes de su época, y como sabemos las penas eran realmente crueles, ya que buscaban castigar de manera ejemplar al delincuente para evitar que las malas conductas se repitieran en el entramado social.

Con el paso de los años esta situación fue evolucionando dando lugar a penas menos crueles y en teoría más justas para los delincuentes, por ello veamos la definición de pena desde el punto de vista de varios estudiosos.
Giuseppe Maggiore apunta: "la palabra pena denota el dolor físico y moral que se impone al transgresor de un ley. Esta noción puede precisarse más. Pero ya contiene lo necesario para definir la pena desde el punto de vista jurídico, es decir, el elemento de la sanción"[27]

Nuestro celebre maestro Fernando Castellano Tena señala "La pena es el castigo legalmente impuesto por el Estado al delincuente, para conservar el orden jurídico[28].

En su Diccionario de Derecho Rafael de Pina comenta que "La pena es el contenido de la sentencia de condena impuesta al responsable de una infracción penal por el órgano jurisdiccional competente, que puede afectar a su libertad, a su patrimonio o al ejercicio de sus derechos; en el primer caso, privándole de ella, en el segundo, infligiéndole una merma en sus bienes y en el tercero, restringiéndolos o suspendiéndolos[29].

Pienso que la pena es el castigo que se debe de imponer al delincuente por la comisión de un delito, atendiendo a la gravedad del mismo y las circunstancias en que este se dio. Considero que la severidad del castigo debe estar directamente ligada con el daño que cause el delincuente con su conducta antijurídica en la sociedad.

Por ello las penas no pueden ser iguales para un ladrón y para un homicida, ya que las conductas no dañan de igual manera a la sociedad.

---

[27] MAGGIORE, Giuseppe, Derecho Penal, vol. II, Temis, Bogotá, Colombia, 1989, p 223.
[28] CASTELLANOS TENA, Fernando, op. cit.p318
[29] DE PINA, Rafael. Diccionario de Derecho, 31ª ed. Porrúa. México 200. p 401

Ya en el siglo XVIII Cesare Bonesana, Marqués de Beccaria en su Tratado de los Delitos y de las Penas establecía su pensar con respecto de la proporcionalidad de la pena que a continuación acoto:

"No solamente es interés común que no se cometan delitos, sino que sean más raros en proporción con el mal que causan a la sociedad. Por consiguiente, los obstáculos que detengan a los hombres de los delitos, deben ser más fuertes a medida que sean contrarios al bien público y a medida de los impulsos que arrastren a ellos. Es decir, que debe haber proporción entre los delitos y las penas."[30]

Beccaria con gran razón aseguraba que se debía evitar que los delitos que más dañaran a la sociedad se reprodujeran por imitación, esto se lograría por medio de los castigos impuestos a los delincuentes, si la pena era muy dura las personas dudarían en realizar la conducta castigada, a contrario sensu si el castigo era muy débil para un delito muy grave entonces los delitos tenderían a reproducirse en la sociedad, por ello debe de existir una correspondencia directa entre el delito y el castigo que este tenga.

Por ello más adelante el Marqués señala:

"Todas las acciones opuestas al bien público llamadas *delitos*, todas las cuales, por grados insensibles, van decreciendo desde lo más elevado a lo más ínfimo. Si la geometría pudiese adaptarse a las infinitas y obscuras combinaciones de las acciones humanas debería haber una escala correspondiente de penas, que descendiesen desde la más fuerte a la más débil"[31].

Con esto establecía que el legislador tiene el encargo de crear un catálogo de ilícitos y a la par de este un cátalogo de castigos, para infringirlos a quien cometa

[30] BECCARIA CESAR. Tratado de los Delitos y de las Penas. 1ra ed. Cibernética Biblioteca Virtual Antorcha. 2003. p24. Consulta en internet http://www.antorcha.net/biblioteca_virtual/derecho/beccaria/24.html
[31] BECCARIA CESAR. Tratado de los Delitos y de las Penas. 1ra ed. Cibernética Biblioteca Virtual Antorcha. 2003. p25. Consulta en internet http://www.antorcha.net/biblioteca_virtual/derecho/beccaria/25.html

una conducta que este catalogada como delictiva, pero debe de cuidarse que esta relación sea lo más justa posible o en otras palabras la pena sea proporcional al delito cometido.

En este nuevo siglo al recordar este principio nos enfrentamos de nueva cuenta a un debate que se cree acabado, pero que; gracias a la realidad actual toma fuerza para redescubrir el significado del mismo en el presente.

Los Delitos Informáticos se perpetran por personas preparadas, o en su caso con un alto grado de conocimientos sobre computación, por ello hoy más que nunca, al crear nuevos tipos penales debemos crear penas que estén acordes al daño que causa este tipo de ilícitos. Ejemplo de esto es; que no puede castigarse de la misma manera al estudiante que con el afán de molestar o jugar una broma a un amigo, roba información de su computadora, que al delincuente que roba información personal del dueño de una empresa con el fin de lacerar sus bienes o su integridad física por medio de un secuestro o extorsión, de esta forma nos encontramos ante el reto de castigar de una manera adecuada a la conducta que en un principio pareciera ser la misma pero que en el fondo es totalmente distinta.

De la misma manera la persona que quema y vende programas o películas piratas de manera habitual, merece un castigo ejemplar, no así las personas que realizan estas actividades con el fin de esparcimiento personal o familiar, ya que esta conducta aunque ilícita, no daña de la misma manera a la economía, en comparación a la venta de discos piratas que de manera cotidiana realizan miles de personas.

Debo señalar con claridad que al igual que en los demás ilícitos en los Delitos Informáticos deben de existir agravantes, ya que aunque las conductas realizadas sean parecidas, no tiene que perderse de vista que son diferentes, especialmente cuando la frontera que divide a esta es tan delgada que puede confundirse una con otra.

Por lo cual creo que debe de existir una correspondencia de la pena con el Delito cometido, pero por encima de este debe atenderse al daño que causa la conducta ilícita para poder castigar correctamente, ya que aunque en el papel los Delios Informáticos pueden parecer inofensivos llegan a repercutir de distintas maneras en el ámbito social actual, desde afectaciones económicas hasta Delitos de alto impacto.

### *4.5. Medios para probar los delitos informáticos, dificultad para su probanza*

Sin lugar a dudas independientemente del caso que se trate es muy difícil probar situaciones o hechos que se dieron en un ámbito informático, por ello en la actualidad se discute cuál es el medio idóneo para poder demostrar la existencia de hechos jurídicos informáticos, entendiendo a estos como las acciones o actos informáticos que tienen relevancia para el mundo jurídico en específico para el Derecho Informático y en este caso para el Derecho Penal.

Por regla general tendríamos que aceptar como prueba informática a toda aquella que se acepte en el Derecho Penal, con los mismos limites y alcances que estas tienen conceptos que más adelante analizaré con detalle.

En un Homicidio existen pruebas materiales e irrefutables de que este sucedió, tenemos un cadáver, heridas y tal vez vestigios o rastros de quien pudo haber cometido el crimen, el tipo de arma con que se realizó y con suerte hasta testigos que a grandes rasgos contaran lo que observaron y percibieron con los sentidos, la diferencia es que en un Delito Informático carecemos de la mayoría de estas pistas, el primer problema será demostrar que el ilícito sobre el que se exige una investigación existió, si se llegara a probar la realización de este, el nuevo inconveniente sería perseguir al culpable puesto que seguramente es un desconocido y desgraciadamente carecemos de información de él.

Tal vez existan rastros pero difícilmente puede llegar a ser identificados por la victima y son difíciles de analizar hasta para el experto en la materia, ya que se enfrentara cara a cara con los obstáculos que el delincuente diseñó para evitar ser atrapado.

La persecución de estos ilícitos se vuelve muy complicada, ya que prácticamente no existe rastro de que estos se han cometido, ejemplo claro de esto se da cuando los delincuentes ocupan una técnica llamada Fishing (pescar en inglés), es un tipo de fraude que puede tener diversas modalidades, una de ellas trata de engañar a Juan Pérez por medio de un e-mail que le hace creer que el Sr. Miguel Pérez a fallecido en algún país del continente Africano y que tiene una cuantiosa fortuna depositada en el banco central de ese país, pero en su contrato de apertura de cuenta no nombro beneficiarios ni familiares vivos por lo cual el funcionario del banco que le hizo llegar el correo se dio a la tarea de buscar a una persona que tuviera los mismos apellidos y nacionalidad que el fallecido para hacerlo pasar como su familiar, el Sr. Juan Pérez es el afortunado que fue seleccionado, por lo cual lo único que necesita el funcionario bancario para iniciar con el proceso de reclamación de dinero es una carta firmada y algunos documentos para comenzar el tramite, pero este tiene un costo muy bajo de $1000 dólares ya que el Sr, Juan a cambio de ellos comenzará con la reclamación lo que traerá como resultado que le otorguen miles de dólares que tendrá que compartir con el empleado bancario, pero no importa ya que la cuenta tiene cientos de miles de dólares por lo cual se tiene un ganancia asegurada, ya que se haya tramitado la reclamación el Sr. Juan recibirá en la cuenta de su país de origen una cantidad muy fuerte de dinero, por lo cual no tendrá ya de que preocuparse. Una vez que se le otorga los $1000 dólares, el supuesto empleado bancario se supone comienza el tramite pero nunca se vuelve a saber de él, obviamente la estafa está consumada.

Este tipo de fraude tiene cerca de 10 años realizándose a través de internet, como se puede observar las personas que caen en este por lo regular son personas que carecen de educación y son blancos fáciles ya que necesitan dinero o piensan que

es una muy buena oportunidad de conseguir dinero extra fácil, este fraude continua dándose ya que en muchos países además del nuestro no puede perseguirse ya que no existen los convenios ni leyes que puedan aplicarse extraterritorialmente que castiguen esta actividad.

De esta forma entendemos la dificultad que representa probar este tipo de Delitos, de cualquier forma aunque se denunciara la situación esto sería inútil ya que no contamos con los medios técnicos ni procesales para tratar de castigar a los culpables.

Como este fraude existen muchos además de variantes de los mismos, esto sólo es la punta de iceberg ya que la dificultad para probar que los Delitos existen van más allá de saber quien los ejecuta, el principal problema que tenemos para la probanza de estos es contar con un cuerpo policiaco capacitado en la investigación de los mismos, ya que en casos muy sonados se pide que sean expertos extranjeros quienes hagan las periciales a los equipos de computo involucrados en algún ilícito, prueba de ello lo tenemos en el caso del secuestro de Fernando Martí y lo documenta el Diario Universal el día 12 de noviembre de 2008 de la siguiente forma "Especialistas en computación forense entrenados por la Oficina Federal de Investigaciones de Estados Unidos (FBI), analizaron los archivos de la computadora que usaba Sergio Humberto Ortiz Juárez, alias El Apá, y encontraron que con ella se hacía un monitoreo constante por internet del secuestro del joven Fernando Martí." Y continúan diciendo "En esta investigación sobre la banda La Flor a la que se atribuye el secuestro y muerte de Fernando, la PGJDF entregó primero la computadora de El Apá a especialistas de la Universidad Nacional Autónoma de México (UNAM), y un mes después la dio a peritos estadounidenses" [32]

Esto pone al descubierto la incompetencia de las autoridades locales, en lo que se refiere al análisis forense de computadoras, que pudieron ser herramientas para llevar a cabo alguna conducta delictiva, lo cual pone en entredicho al comandante

[32]"Icela Laguna." El Apá monitoreo caso Martí en red"", El Universal, sección D.F (México, D.F 12 de noviembre, 2008).

Gustavo Caballero Torres coordinador de la Unidad de Investigación Cibernética de la PGJDF quien el 23 de octubre de 2008 afirmó en entrevista para la agencia de noticias Notimex que "El día de hoy podemos decir que estamos en posibilidades de atender todos aquellos delitos que estén relacionados o tengan algún vínculo con la tecnología de la información, desde celulares hasta computadoras"[33], podemos sintetizar, que atender para el comandante se refiere a la acción de darle seguimiento a los Delitos en los que intervengan elementos tecnológicos, no así a realizar la investigación forense necesaria para tratar de encontrar pruebas que involucren a los usuarios de dichos equipos con la averiguación previa correspondiente.

Como podemos observar el coordinador de la Unidad de Investigación Cibernética de la PGJDF, aseveraba que los elementos a su cargo, estaban plenamente capacitados para investigar cualquier Delito en el que se utilizaran nuevas tecnologías, lo cual queda desmentido por el periódico el Universal días después al asegurar que la PGJDF no pudo realizar pruebas periciales a la computadora de Sergio Humberto Ramos Apá, "Por tratarse de una especialidad con un alto grado de dificultad técnica, ni el personal de la Procuraduría ni de la UNAM tuvieron las capacidades tecnológicas ni los especialistas calificados para una investigación de este tipo" y sigue La Procuraduría General de Justicia del Distrito Federal (PGJDF) pagó ese peritaje que le permitió saber que la computadora de El Apá era utilizada principalmente para ver pornografía, bestialismo y noticias relativas con policías corruptos y técnicas de secuestro. [34] Es importante destacar como la PGJDF no supo como manejar la situación ya que no pudieron extraer información alguna de la computadora del Apá, hecho que cuestionamos fuertemente, ya que parece imposible que si bien los expertos de la Procuraduría no pudieron hacer nada, tampoco lo hiciera el personal de la UNAM, pues la Universidad cuenta con un

---

**33** Policía Cibernética del DF en 700 casos de secuestros. Consulta en internet. http://www.terra.com.mx/noticias/articulo/749610/Policia+Cibernetica+del+DF+en+700+casos+de+secuestros.htm, México, 20-07-10

34 Icela Laguna." El Apá monitoreo caso Martí en red"", El Universal, sección D.F (México, D.F 12 de noviembre, 2008).

departamento completo para seguridad Informática conocido como CERT Equipo de Respuesta a Incidentes de Seguridad en Computo el cual entre sus servicios cuenta con un Análisis Forense "El UNAM-CERT proporciona el servicio de análisis forense informático para la investigación de incidentes de seguridad informática y de posibles delitos o faltas en los que está involucrado un sistema informático o de infraestructura.

Este servicio permite identificar huellas específicas de actividad en un sistema informático y determinar los eventos relevantes para una investigación. Los resultados obtenidos pueden ser útiles como elemento para deslindar responsabilidades y para mejorar la seguridad de la infraestructura informática de la organización"[35].

Por lo tanto dudamos mucho que los expertos de la UNAM no pudieran analizar la computadora del presunto responsable, pensamos que ante la inexperiencia e incapacidad en este tipo de asuntos por parte de las autoridades locales, estas decidieron lavarse las manos en la investigación al dar la computadora a expertos forenses del FBI. A pesar de esto la estructura de la Unidad Cibernética no ha cambiado y dudamos que puedan enfrentarse con los problemas que se suscitan a diario con el uso de nuevas tecnologías.

El problema para probar los Delitos Informáticos, no sólo se limita a capacitar a nuestra servidores públicos, también debemos crear un marco jurídico que permita atacar a estos ilícitos, además de proporcionar las herramientas procesales a las autoridades para que estas puedan realizar una verdadera investigación en los casos que presuma se cometen estos Delitos.

Para poder legislar en esta materia es necesario conocer las pruebas que el Derecho Penal acepta como válidas, además de reconocer la existencia de una prueba o evidencia digital, para que esta a su vez sea el principal medio de prueba en los Delitos Informáticos.

[35] Análisis Forense. Consulta en Internet. http://www.seguridad.unam.mx/servicios/. México 20-07-10

### *4.6. La Prueba en el Proceso Penal*

En la vida cotidiana de manera muy coloquial no referimos al concepto de prueba, hablamos de que podemos probar que realizamos cierto pago, que conocemos a cierta persona, que hicimos tal actividad, etcétera, pero en el ámbito jurídico y procesal penal, la prueba es el cimiento más importante para un juez, ya que este determinara con las pruebas que se le ofrezcan la culpabilidad o inocencia de los presuntos delincuentes.

Se cree que la palabra prueba tiene su origen etimológico "Es una derivación de la palabra probandum, vinculada al hecho mismo de experimentar patentizar o hacer fe"[36]

Por ello la palabra prueba ayuda en la actualidad a buscar la verdad histórica de un hecho que se considera antijurídico, ya que las pruebas nos permitirán posiblemente determinar la existencia de las actividades que fueron llevadas a cabo para realizar un Delito.

Ya en al ámbito del Derecho Procesal el jurista Guillermo Colín dice que la prueba "Es todo medio factible de ser utilizado para el conocimiento de la verdad histórica y personalidad del delincuente, para de esta manera estar en aptitud de definir la pretensión punitiva estatal"[37]

La definición citada, tiene todos los elementos necesarios para que en la actualidad el concepto de prueba pueda ser estudiado y analizado desde distintos ángulos. Lo que se pretende buscar en un proceso penal es conocer la verdad histórica, podemos entender por esta a la sucesión de actos que realmente pasaron y por tanto dieron origen a un Delito, con las pruebas el juez no pretende

[36] ORONOZ SANTANA, C arlos. Las pruebas en materia penal. 6ª ed. Ed Pac México. 2008 p. 2

[37] COLÍN SANCHEZ, Guillermo Derecho Mexicano de Procedimientos Penales, Porrúa México 1982 p. 300

descubrir los hechos que dicen que ocurrieron sino por medio de estas pretende conocer los que realmente existieron, además al hablar de conocer la personalidad del delincuente podemos determinar el nivel de malicia que este tiene y por ende conocer cómo es que maquinó los hechos, si fue un delincuente pasional o si este realizó toda una planeación para llevar a cabo el Delito, con esta información podremos tratar de entender el proceder del presunto delincuente y además estaremos en mejor posición de analizar su actividad para castigar en menor o mayor medida su proceder, esto cobra mayor importancia en el tema tratado ya que los delincuentes informáticos pueden no mancharse las manos de sangre, sin embargo las actividades desarrolladas por ellos merecerán un castigo de acuerdo al daño que causen así como al nivel de preparación que tuvieron que realizar para llevar a cabo estas.

Al haber establecido el concepto de prueba el siguiente punto es conocer a los medios de prueba, es una expresión ambigua, ya que por medios de prueba podemos entender al objeto material o personas que dan fe de un hecho determinado, pero esta acepción en el proceso penal es errónea, ya que por medio de prueba se entiende a la prueba en sí, pero ofrecida y admitida durante el proceso, es decir la prueba solo alcanza el nivel de medio de prueba cuando esta ha sido ofrecida y admitida por el juez de la causa, en el Derecho Penal mexicano tenemos los siguiente medios de prueba: la confesión; la testimonial; el dictamen de peritos; la inspección judicial; la reconstrucción de hechos; la documental; la confrontación; la circunstancial; los careos; y, las llamadas no especificadas.

Algunos tratadistas hablan de que los medios de prueba deben ser clasificados para su estudio, estas clasificaciones no tienen repercusión en el ámbito legal por lo cual pienso que es inútil mencionarlas en el presente trabajo puesto que escapan al objeto del mismo, sin embargo sí es necesario hablar de los principios que rigen a los medios de prueba puesto que estos han sido considerados por nuestras leyes penales en sus articulados, la doctrina habla de una gran variedad

de principios, pero las discusiones a lo largo del tiempo han tenido a bien identificar cuatro principios aceptados por los doctrinarios.

- *Principio de averiguación*

  Está ligado directamente a los involucrados en investigar al delito, tanto a los ministerios públicos como a los jueces, ya que las leyes les otorgan la libertad de allegarse de todas las pruebas que consideren necesarias siempre y cuando estas no sean contrarias a Derecho, por lo cual prácticamente cuentan con una facultad investigadora amplísima, este derecho se encuentra en nuestro Código Federal de Procedimientos Penales en el numeral 180.

- *Principio de inmediación*

  Este principio se refiere a la conducta que deba adoptar el juzgador ante los medios de prueba, en el aspecto formal el juez debe conocer e involucrarse con las pruebas por ello debe estar presente en su desahogo, y en el aspecto objetivo debe analizar las pruebas y dar preferencia a las que están más ligadas con la controversia, nuestro Código ubica esta facultad en el art. 16.

- *Principio de apreciación*

  Para el Jurista Niceto Alcalá Zamora y Castillo existen cuatro sistemas de apreciación de las pruebas : el ordálico, el legal, el libre, y el de sana crítica o apreciación razonada:

  *a*) Ordálico, es aquel sistema de apreciación de las pruebas que deriva de la divinidad, siendo ésta quien decide lo relativo al valor mismo de la prueba, ateniéndose el juez a los resultados físicos de la ordalía.

*b*) Legal, este sistema de apreciación se refiere a la situación de que la ley es la encargada de fijar el valor rigurosamente tasado de cada prueba

*c*) Prueba libre, en este sistema el juez aprecia, sin mayor vínculo, el valor que cada prueba le merece, sin cuidar de convencer en torno al porqué de tal determinación.

*d*) Sana crítica, en este sistema el juez resuelve sobre el valor de la prueba al margen de cualquier paradigma legal, pero fundado y motivando el porqué de su proceder.

En nuestro país encontramos la aplicación de los sistemas anteriores salvo el ordálico. La prueba tasada o legal es el sistema adoptado por la generalidad de los códigos procesales penales del país y el sistema de sana crítica al cual se acoge el Código Federal de Procedimientos Penales, tal como se desprende del texto del artículo 290 al expresamente mencionar que "los tribunales en sus resoluciones expondrán los razonamientos que hayan tenido para valorar jurídicamente la prueba", motivo por el cual, podemos deducir que los tribunales no están sujetos a reglas de valoración derivadas de una tasación legal, sino a valorar los medios de prueba a partir de razonamientos claramente expuestos.

- *Principio in dubio pro reo*

El objeto de este, es proteger al acusado en el sentido de que en caso de duda hay que fallar en su favor, se encuentra en el artículo 247 del Código de Procedimientos Penales del Distrito Federal, que menciona "en caso de duda deberá de absolverse". Este principio puede considerarse un símil de la figura anglosajona de la duda razonable.

Con lo que respecta al objeto de la prueba Rafael de Pina comenta que: “El objeto normal de la prueba son los hechos. No obstante las personas pueden serlo, como

vemos en aquellas legislaciones que autorizan directa o indirectamente la inspección o reconocimiento corporal"[38]

Como bien opina el célebre tratadista el objeto de la prueba son los hechos, ya que se busca patentizar que tales o cuales situaciones y actividades tuvieron lugar para que con ellos el juez pueda dilucidar qué fue lo que en realidad paso, es acertado decir que también las personas mismas pueden ser objeto de prueba puesto que estas bien pueden vestigios de que existió el delito o ciertas acciones.

Es necesario también analizar la siguiente opinión: "El objeto de la prueba es fundamentalmente la demostración del hecho mismo con sus circunstancias y modalidades y no necesariamente la demostración del ilícito, ya que esto se da en el proceso y, por tanto, este tiene la virtud de que mediante él podemos saber si ha existido o no delito, ya que se podrán hacer valer por las partes las excluyentes de responsabilidad o cualquier otra circunstancia que elimina la punibilidad del Delito" [39]. Disiento con estas afirmaciones, puesto que el objeto de la prueba es determinar que existieron o no ciertas actividades, y por ende la prueba trata de convencer al juez de que un Delito pudo o no haberse cometido, es decir la parte acusada tratará de probar que es inocente, mientras que el agraviado luchará porque sus pruebas demuestren la culpabilidad del acusado, por tanto las pruebas son las que causan un ánimo de convencimiento en el juez, y no el proceso en sí, ya que si las pruebas no se hubieran ofrecido el proceso seguiría y el mismo no podría determinar de una manera justa quién tiene la razón.

En el Derecho Penal los estudiosos debaten acerca de si en el proceso penal al igual que en el civil existe una carga de la prueba, esa "Necesidad que las partes tienen de probar en el proceso los hechos o actos en que fundan sus derechos para eludir el riesgo de una sentencia desfavorable, en el caso de que no lo hagan"[40],es que sí existe esta carga de la prueba, pues ya mencioné una parte

[38] DE PINA, Rafael. Diccionario de Derecho, 31ª ed. Porrúa. México 200. p. 385
[39] ORONOZ SANTANA, C arlos. Las pruebas en materia penal. 6ª ed. Ed Pac México. 2008 p.. 72
[40] DE PINA, Rafael. Diccionario de Derecho, 31ª ed. Porrúa. México 200 p. 144

quiere probar su inocencia y la otra la culpabilidad de su contrincante, además de que el Ministerio Publico tiene obligación de integrar la Averiguación Previa de la manera más completa, obviamente esto trae consigo que antes de consignar la averiguación al Juez se allegue de la mayor cantidad de pruebas posibles, por ello en realidad se preocupa por demostrar la existencia del Delito y como consecuencia tiene que demostrar mediante las pruebas la validez de su dicho.

De la misma manera el inculpado tiene la obligación de comprobar su inocencia mediante pruebas, y estas tienen que demostrar de la mejor manera que no es responsable del Delito que se le imputa por ello la carga de la prueba sí existe en el ámbito Penal.

Ahora analicemos los medios de prueba que son aceptados por nuestro Código de Procedimientos Penales, sólo señalaré los elementos más importantes, puesto que el tema es muy amplio y puede ser objeto de un extenso estudio.

*Confesión*

La llamada Reina de las pruebas, en la actualidad ha perdido esta categoría, gracias a los abusos que se cometían para obtener la confesión de los presuntos delincuentes, ahora ya no es suficiente tener la confesión del sujeto para hacerlo culpable y se toman en cuenta todos los medios de prueba que son ofrecidos durante el proceso, además de la forma en que es rendida la confesión.

El artículo 207 del Código Federal de Procedimientos Penales indica qué es la confesión y cómo debe ser rendida.

La declaración voluntaria hecha por persona no menor de 18 años, en pleno uso de facultades mentales, rendida ante el Ministerio Público, el Juez o tribunal de la causa, sobre hechos propios constitutivos del tipo delictivo materia de la imputación, emitida con las formalidades señaladas por el artículo 20 de la Constitución Política de los Estados Unidos Mexicanos, se admitirá en cualquier estado del procedimiento, hasta antes de dictar sentencia irrevocable.

Analizada la definición se pueden extraer elementos vitales para que la confesión sea válida.

a) Es una declaración voluntaria

b) Rendida por una persona no menor de 18 años

c) En pleno uso de facultades mentales

d) Ante el Ministerio Público, juez o Tribunal

e) Sobre hechos propios

f) Que los hechos sobre los que verse sean constitutivos del tipo delictivo materia de la imputación

g) Con las formalidades señaladas en el artículo 20 de la Constitución

h) Admisible en cualquier estado del procedimiento

La confesión para que sea válida tiene que rendirse ante el juez o el ministerio público, debe hacérsele conocer al indiciado quién lo acusa y de qué, además la confesión debe rendirse acompañado de un abogado o persona de su confianza, por lo cual tampoco debe existir coacción, violencia física o moral, por ello la confesión rendida ante autoridad no competente o policías no tendrá valor como tal y sólo se considerará lo dicho en esta como prueba testimonial de las personas que la escuchen.

*Inspección*

A través de la inspección, el Ministerio Público o el Juez, realiza una verificación directa de los acontecimientos, a través de sus propios sentidos, es decir visitando un lugar u observando objetos que puedan ayudar con el objetivo de apreciar la realidad de ciertos hechos, controvertidos.

La materia de la inspección acorde con el artículo 208 del Código Procesal Penal Federal, es todo aquello que pueda ser directamente apreciado por la autoridad que conozca del asunto. Siempre debe realizarse por el Ministerio Público, o, en su caso, del juez, dependiendo de la etapa en que se encuentre el proceso.

Para asentar todo lo que la autoridad pueda apreciar en la inspección, puede allegarse de todos los medios que crea convenientes para detallar circunstanciadamente todo lo que pudo observar, además podrá hacerse acompañar de peritos para recabara la mayor información posible de los vestigios que pueda encontrar

Además, es posible examinar a las personas presentes en la inspección, si pueden proporcionar un dato útil para la averiguación.

La inspección puede practicarse también como una reconstrucción de hechos, actividad que tiene por objeto reproducir en la medida de lo posible las actividades que dieron origen a la comisión del Delito; para que esta se lleve a cabo debe practicarse con todos los testigos del acto o con la mayoría de ellos, además si se amerita, la reconstrucción se realizara en el mismo lugar en que se cometió el ilícito; la diferencia sustancial entre la reconstrucción y la inspección radica en que la primera tiene valor de prueba plena mientras que la segunda sólo se considerara como un indicio.

*Peritos*

El Código de Procedimientos Penales Federal en su artículo 220 que en caso de que se requieran conocimientos especiales para examinar personas, hechos u objetos deberá recurrirse a un perito, el Juez en ocasiones analiza ciertos hechos, documentos o circunstancias que escapan a su conocimiento, por lo cual solicita el auxilio de ciertos expertos en alguna ciencia, arte u oficio.

La intervención del perito se da por solicitud de las partes o por instrucción del propio tribunal, aunque esta prueba no tiene un valor determinante ayuda a crear

convencimiento en el juzgador al entender cosas que escapaban a su entender. Esto trae como consecuencia que los peritos intervengan en la mayoría de los procesos, pues, cada parte tratará de probar su dicho por cualquier medio, el dictamen que da el perito es a su leal saber y entender, por lo que se presta a que exista corrupción en el análisis de los dictámenes por ello normalmente hay dos peritos en los procesos y el juez tomará en cuenta el dictamen que prefiera

*Testigos*

Son las personas que presenciaron los hechos por sus propios sentidos; por lo tanto su declaración es de suma relevancia ya que cada uno dará su versión sobre los hechos que observaron.

En lo relativo al valor de la declaración del testigo, el Juez debe tomar en consideración:

Que sea mayor de edad, su instrucción académica y su situación social y psicológica.

Que en la medida de lo posible, no tenga relación familiar o personal con los involucrados y por tanto tenga completa imparcialidad;

Que el testigo haya presenciado personalmente los hechos y su testimonio no sea de oídas o de lo que otros le contaron;

Que la declaración sea clara y precisa, sin dudas, que lo que declare tenga coherencia con los hechos

Que el testigo no haya sido coaccionado, ni impulsado por malicia, error o soborno. El apremio judicial no se reputará fuerza.

El valor de la prueba es de indicio, por tanto el juez necesitará conocer otros medios de prueba para acreditar los hechos de lo que sucedió.

*Confrontación*

Es un medio de identificación física, practicado durante el proceso penal, este tiene por objeto asegurar que los testigos no confundan al procesado con alguien más, de este modo podemos perfeccionar otros medios de prueba, sus reglas de de aplicación se encuentran en los numerales 258 a 264 del Código procesal de la materia.

*Careo*

Se considera que existe tres tipos de este, el constitucional, el procesal y el supletorio, el primero se encuentra regulado por el art. 20 fracción IV constitucional y consiste en carearse en presencia del juez con quien le acusan, esta diligencia sólo puede llevarse a cabo a petición del inculpado o de su defensa, esto con el objetivo de que el indiciado pueda defenderse de sus acusadores.

El careo procesal deriva de lo establecido por el Código Federal de Procedimientos Penales, esta diligencia se realizará cuando existan contradicciones en las declaraciones de dos personas, pudiendo repetirse cuando el tribunal lo estime oportuno o cuando surjan nuevos puntos de contradicción, es de suma importancia puesto que al tener frente a frente a las personas cualquier puede caer en sus propias contradicciones creando así una mayor certeza ante el juez de quién es la persona que miente respecto de los hechos.

El careo supletorio se practicara cuando las personas no pueden estar en el mismo tribunal por cualquier razón, y su fin es el mismo que en el careo procesal.

*Documental*

Es posible aportar en el proceso penal cualquier tipo de documento que aporten las partes, cumpliendo con el requisito de que sea idóneo para demostrar algo, por documento podemos entender cualquier representación material que demuestre la existencia de hechos o actos jurídicos.

Esta prueba distingue de los documentos públicos y privados, los primeros harán prueba plena y los segundos sólo serán considerados como indicios, actualmente no se consideran como documentos a las comunicaciones emitidas entre las computadoras o los celulares aunque estén fijados en un medio físico como lo es un disco duro, más adelante analizaré con cautela lo referente a este nuevo tipo de documento.

*Presuncional*

La doctrina procesal clasifica a las presunciones en dos rubros: la humana y la legal, se derivan del juez las primeras y las segundas de lo que la ley establece.

Este medio probatorio ha sido confundido constantemente como indicio; la palabra presunción tiene su raíz en el latín *presumtio, tionis*, que significa suposición que se basa en ciertos indicios, también significa la acción y efecto de presumir que a su vez proviene del latín *praesumere*, que significa sospecha o juzgar por inducción, o conjeturar una cosa por tener indicios o señales para ello.

*Medios de prueba no especificados*

En torno a estos medios de prueba no especificados, debo mencionar lo que señala el artículo 16 del Código Federal de Procedimientos Penales al referir: En las diligencias podrán emplearse, según el caso y a juicio del funcionario que las practique, la taquigrafía, el dictáfono y cualquier otro medio que tenga por objeto reproducir imágenes o sonidos, y el medio empleado se hará constar en el acta respectiva.

Cuando se redactó nuestro Código se buscaba que fuera lo más vanguardista posible, por ello, hacía referencia a medios de prueba no existentes en su época pero que pensaron pudieran existir en un futuro otros medios más idóneos para analizar nuevos Delitos lo que trae a colación la llamada, prueba digital que analizaré a continuación.

### *4.7. La Prueba o Evidencia Digital*

Después de estudiar los distintos medios de prueba que existen en nuestro Derecho Procesal Penal vigente, podemos observar que aunque nuestro Código trata de englobar hasta las pruebas no conocidas en los tiempos de su redacción, esto no es suficiente para los tiempos en los que vivimos.

El mundo hoy, más que nunca, avanza a pasos agigantados, la tecnología crece y se moderniza cada segundo, hace 21 años nace Iusacell , convirtiéndose en la primera compañía de telefonía celular en ofrecer el servicio en la Ciudad de México, en esos días era impensable que existiese un servicio con el cual podrían llamarnos a cualquier hora del día en cualquier lugar que nos encontráramos, hoy día pensar en aquellos celulares que eran grandes en costo y dimensiones nos produce risa, esa tecnología era tan cara que sólo las personas con un poder adquisitivo muy alto podían usar el servicio, hoy según el Portal Cnn: "Se estima que en México circulan 83 millones de celulares"[41],lo importante de esta cifra es que nos permite imaginar el crecimiento exponencial que tiene la tecnología, además del avance de la misma en su desarrollo, en sus inicios el teléfono celular no era más que un teléfono que podíamos utilizar en casi cualquier lugar, hoy son verdaderas computadoras que en su interior guardan gran parte de las actividades de una persona.

Toda esta serie de tecnologías son medios comisivos sin los cuales los Delitos Informáticos no podrían existir, por ello es necesario conocer cómo es que estos nos pueden dar las bases para entender la forma de ejecución de los mismos y esto se logra a través de la prueba o evidencia digital.

En un concepto amplio podemos aceptar como definición de prueba digital la ya mencionada del maestro Colín, ya que como él menciona *es todo medio factible de ser utilizado para el conocimiento de la verdad histórica,* por ello podemos

---

[41] Cofetel vigilará suspensión de celulares. Consulta en Internet http://www.cnnexpansion.com/tecnologia/2010/04/10/renaut-cofetel-celulares-cnnexpansion México 25-07-10

entender que cualquier vestigio sea del tipo que se trate puede ser utilizado como prueba en el juzgado, pero en un sentido estricto el concepto de prueba o evidencia digital no lo conocemos en nuestro Derecho es un concepto elaborado en el Derecho anglosajón específicamente en E.U y el investigador forense de computadoras Casey la define como "Digital Evidence, as any data that can establish that a crime has been comitted or can provide a link between a crime and its perpetrator"[42], esta se puede traducir como: cualquier dato que puede establecer una la existencia de un delito o la relación entre un delito y el responsable del mismo, como se puede observar es un concepto muy amplio, por ello analizo a continuación la definición más aceptada.

El Departamento de Justicia de E.U define a la evidencia digital como "Information of probative value stored or transmitted in digital form"[43], la cual podemos traducir de la siguiente manera: La evidencia Digital es aquella información con valor probatorio que está almacenada o ha sido transmitida en forma Digital.

Esta definición es mundialmente aceptada, ya que también la adopta la International Organization on Computer Evidence (organización Internacional en evidencia de computadoras) IOCE por sus siglas en inglés, organización que tiene como propósito proporcionar un foro Internacional donde las agencias de seguridad de todo el mundo, puedan intercambiar información concerniente a las computadoras y su análisis forense, la única variante que tiene la definición de la IOCE consiste en cambiar el término digital por binario y que esta debe ser presentada en un corte para su valoración: "*Digital Evidence* - Information stored or transmitted in binary form that may be relied upon in court"[44] la traducción sería:

---

[42] Eoghan, Casey et al. Digital Evidence and Computer Crime : forensic science, computers and the internet. Segunda Edición, Editorial Elsevier, Amsterdam, 2004.p 12

[43] Digital Evidence: Standards and Principles. Consulta en Internet. http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm Estados Unidos. 25-07-10

[44] General Definitions relating to digital evidence. Consulta en internet. http://www.ioce.org/core.php?ID=5 25-07-10

Evidencia Digital – Información almacenada o transmitida de manera binaria, que puede ser presentada en los Tribunales.

Como podemos observar las definiciones son prácticamente iguales, sin embargo difieren al mencionar la palabra digital y binario:

> Originalmente la palabra digital proviene del latín "(Del lat. *digitālis*).
>
> **1.** adj. Perteneciente o relativo a los dedos.
>
> **2.** adj. Referente a los números dígitos y en particular a los instrumentos de medida que la expresan con ellos. *Reloj digital."*[45]

Se entiende por digital todos los instrumentos que representen números con dígitos, o en su defecto que puede ser tocado por los dedos.

Mientras en los países de habla inglesa donde se originó el término de evidencia digital, usan el término digital para referirse a todo aparato que haga uso de la tecnología y que por medio de esta transforme el mundo real en un código binario de ceros y unos, es decir dígitos, que sólo puede ser entendido por estas maquinas, ya sean computadoras, cámaras fotográficas, celulares etc., de ahí el término de digital.

El idioma que utilizan las computadoras para almacenar la información no es más que un sistema de numeración llamado binario, en el cual todos los caracteres son representados con ceros y unos, creemos no es necesario explicar la complejidad del sistema puesto que he aclarado la confusión respecto de la palabra digital en el idioma inglés y en el nuestro.

Debido a lo anterior la IOCE cambió el término digital por binario, para asentar mejor el significado en todo el mundo.

---

[45] Diccionario de la Real Academia Española. Consulta en internet http://buscon.rae.es/draeI/SrvltConsulta?LEMA=digital 25-07-10

La diferencia que existe entre una prueba y evidencia en nuestro Derecho la primera ya la he definido, por lo cual veamos el concepto de evidencia "Certeza indudable"[46], por tanto afirmo que en nuestro Derecho la evidencia puede ser una consecuencia de la prueba, puesto que al desahogarse algún medio de prueba este puede desencadenar en el juzgador que la certeza de que un hecho sea indudable para él.

Coloquialmente los términos son sinónimos, y dado que el término evidencia puede generar confusión en nuestro Derecho, me referiré a esta como prueba digital, ya que en nuestro sistema legal nosotros ofrecemos pruebas, no evidencias.

En mi concepto la prueba digital es: Toda información que sea contenida o transmitida en un dispositivo informático, que pueda demostrar la existencia de una serie de hechos.

No pretendo que nuestra definición sea única y aceptada por todos, pero creo que es adecuada para englobar a todos los vestigios que pueden ser encontrados y analizados en una computadora para comprobar la existencia de un Delito Informático.

Por tanto al analizar nuestra definición y las aceptadas en la comunidad mundial podemos entender por información todo documento que existe dentro de un dispositivo informático, es decir e-mails, fotos, textos, historiales de mensajeros instantáneos, todo tipo de archivos, hojas de cálculo, historiales de búsqueda en internet, bases de datos, cds, dvds, discos duros, respaldos de datos, historiales de navegación de los ISPS, videos, audios, historial de llamadas en celulares, mensajes de texto celulares etc., como podemos observar son muchos los datos que pueden ser obtenidos y analizados, muchos tratadistas dirán que estos datos no son más que pruebas documentales, que de ser encontradas, pueden ser ofrecidas como cualquier otra, pero serán consideradas como documentos

[46] DE PINA, Rafael. Diccionario de Derecho, 31ª ed. Porrúa. México 200 p. 278

privados y sólo tendrán un valor de mero indicio, situación que se pretende evitar al regular jurídicamente a la prueba digital para de esta forma hacer que tenga un valor probatorio pleno, al ser encontrada y analizada bajo un proceso escrupuloso para que no pueda ser contaminada ni modificada. Al respecto Marc Goodman señala "hoy mucha información no está en papel, ni son hojas de papel, sino información existente en la computadora: En el mundo entero el setenta por ciento de documentos esta únicamente en las computadoras"[47]. Pardini al respecto señala que "Todo documento, cualquier que sea el soporte de la información que lleva consigo debe ser admitido como elemento de prueba"[48].

Este tipo de prueba puede aportar mucho a los procesos penales actuales y futuros, no importando si se juzgan Delitos Informáticos o no, ya que al especificar que puede ser un medio probatorio, su validez cambiará de ser un indicio a ser prueba plena, además de ello podré especificar cuándo, bajo que circunstancias y en qué casos, serán admisibles en un proceso, para que esto sea realidad se tiene que establecer un procedimiento para recolectar pruebas digitales, al igual que en cualquier otro tipo de prueba cuando la autoridad sea la involucrada en recolectar la prueba pues tendrá que seguir una cadena de custodia el cual es un sistema de seguridad para la preservación de las evidencias y o muestras, cuyo objetivo es garantizar la integridad, conservación e inalterabilidad de las mismas, desde el momento en que han sido colectadas, custodiadas, transportadas, procesadas y presentadas en los juzgados como medio de prueba, hasta su disposición final, este tipo de diligencias lo prevé nuestro Código Procesal, por lo cual sólo diré que debe agregarse al articulado, que aunque el Delito investigado no tenga relación con los Delitos informáticos, todo los dispositivos de este tipo encontrados deben ser recolectados y custodiados al igual que las demás pruebas.

Este procedimiento puede encontrarse viciado, puesto que los encargados de recolectar y custodiar las pruebas son personas que pudieron alterar las mismas,

[47] Goodman, Marc. Cibercriminalidad. Editorial Inacipe, México, 2003.p 19
[48] Pardini, Anibal. Derecho de internet. Editorial La Rocca, Buenos Aires, 2002.p 218

pero a diferencia de la mayoría de las otras pruebas este tipo de manipulación puede ser detectada, ya que todo dispositivo informático guarda un registro de todas las actividades que se dan en el mismo, y en el supuesto caso de que este fuera borrado, sería una presunción de que el dispositivo contenía información relacionada con los hechos investigados.

Llegado a este punto surge una pregunta ¿Cómo podemos saber si las pruebas digitales ofrecidas por las partes son reales? Supongamos que tratamos el caso de un fraude por internet como el ya comentado, en el cual el Sr X deposita cierta cantidad al Sr. Y con la promesa de que esta le multiplicará ese depósito; obviamente esto era mentira y el Sr. X perdió el dinero depositado, el afectado no tiene ninguna prueba de esta situación salvo el ticket que entrega el banco cuando se realiza un deposito, pero este por sí solo no prueba la existencia del fraude ya que el ticket sólo prueba que se hizo un deposito a favor de alguien, pero el Sr. X tiene los e-mails por medio de los cuales se le invitó a realizar la transacción, y presenta impresiones de los mismos como prueba de que fue defraudado, aqui aunque la autoridad tenga en su poder los correos no representaran más que meros indicios de los dichos del Sr. X, actualmente tal vez su denuncia no prosperaría ya que las pruebas que está entregando son endebles y tal el Ministerio Público piensa que se trata de un engaño; para resolver esta situación la autoridad tendría que pedir al Sr. X la contraseña de su correo y cerciorarse de que las impresiones que presenta son fieles a los mails que él recibió, posterior a esto tendría que analizar quién remite e investigar el rastro del correo para saber de qué lugar fue enviado, además de pedir la colaboración del banco que recibió el depósito para saber los datos de la persona defraudadora, y la presentación de los datos al ISP para que acredite que el mail fue enviado por alguien más en algún lugar de la República.

De esta forma podríamos comprobar que el correo es original y que la persona no miente, algunos tratadistas dirán que nos encontramos ante un caso de fraude genérico, y no un fraude informático, disiento de ellos ya que sin la utilización de la computadora (medio comisivo) esta persona no hubiera podido defraudar, además

de que las pruebas no hubieran sido plenas de no contar con la regulación necesaria para este tipo de casos, por ello ponemos especial atención a estos ya que muchas personas se valen del anonimato de internet para cometer fechorías.

Más allá de este ejemplo existe un sinfín de conductas que pueden ser comprobadas a través de las pruebas digitales, pueden demostrarse hechos que pueden ser considerados delitos, en un dispositivo informático, pueden encontrarse fotos, agendas, correos y otros vestigios que pueden indicar que los delincuentes hacen un estudio de sus posibles víctimas para extorsionarlos o secuestrarlos.

En el caso de que las autoridades hagan uso de su facultad de investigación, tanto el Departamento de Justicia de E.U y la IOCE, establece controles para el tratamiento de las pruebas encontradas, además de definiciones que creemos pertinentes retomar.

*Original Digital Evidence:* Physical items and the data objects associated with such items at the time of acquisition or seizure

Evidencia digital original. Equipos o cosas físicas que están asociadas a la información encontrada, en el momento del aseguramiento de los mismos.

*Duplicate Digital Evidence:* An accurate digital reproduction of all data objects contained on an original physical item.

Duplicado de Evidencia Digital. Copia fiel de todos los datos contenidos en un equipo o cosa asegurada.

*Copy*: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Copia. Copia fiel de cierta información que estaba contenida dentro de los equipos asegurados, pero esta copia es independiente de la que se encuentra en el equipo

Estas definiciones tienen por objeto inventariar la información encontrada en los equipos informáticos, además tratan de preservar el original íntegro sin ninguna manipulación para que este pueda ser ofrecido como prueba en un juicio.

Existe un manejo especial en las pruebas digitales, pero en principio cuando la autoridad busque a estas los procedimientos generales que se utilizan y se encuentran regulados en nuestro Código deben aplicarse; a continuación damos algunas recomendaciones de cómo recoger y resguardar las pruebas digitales.

- Los procedimientos que se conocen en el ámbito forense como cadena de custodia deben ser seguidos al pie de la letra.

- Las acciones llevadas a cabo para su recolección no deben alterar la prueba

- Cuando sea necesario analizar la prueba esto debe hacerlo un perito en la materia.

- Toda actividad involucrada en la obtención de la prueba, su acceso, almacenamiento o transferencia digital debe estar documentada y guardar el registro de la misma para garantizar la originalidad de la prueba

Estos son solamente lineamientos generales que propongo deben seguirse en la obtención de las pruebas digitales, pero sólo son aplicables cuando las autoridades se encuentran con estas en una investigación formal, esta obtención de pruebas no puede darse de una manera unilateral ni tampoco se darán cuando un particular las ofrezca en un proceso por ello los juristas alrededor del mundo se han dado a la tarea de buscar remedios procesales a los problemas ya

planteados, si no se ha encontrado una solución a estos por lo menos son propuestas que bien pueden ser benéficas para el desarrollo del Derecho.

### *4.8. Orden de suministrar Datos informáticos.*

Actualmente nuestro país forma parte de las discusiones que se han llevado a cabo en distintas partes del mundo, con el fin de celebrar un Tratado Internacional llamado Anti-Counterfeiting Trade Agreement ACTA "que en español de traduce como Acuerdo Comercial Anti -falsificación, es un pacto internacional para establecer reglas y estatutos sobre la propiedad intelectual, con el que se pretende regular el traspaso de datos en Internet, creando instituciones internacionales vigilantes de los derechos de autor" [49].

Con este tratado se pretende resolver la situación delictiva que existe en Internet en el mundo actual, ya que el ser aplicable de manera internacional los países firmantes tendrían que acatar las medidas que correspondan en sus países, cabe mencionar que el contenido de este tratado no versa únicamente en materia informática, sino en diversas áreas donde se falsifica mercancía que es comercializada como original y se ataca al Derecho de Autor, además que sólo algunos países son quienes lo negocian y promueven, ejemplo de ello es México que es el único País de América Latina que participa en las negociaciones.

El contenido del Tratado en negociación puesto que ataña totalmente al tema de la Tesis y del presente subtema, dentro del análisis del problema de la certeza y confiabilidad de las pruebas informáticas creo que es necesario establecer un proceso mediante el cual las autoridades puedan ordenar que los ISPs (Proveedores de Internet) les entreguen datos, que sirvan ya sea para verificar la autenticidad de las pruebas digitales ofrecidas por las partes, o en su labor investigadora la autoridad pueda allegarse estas pruebas que de no solicitarse no pudieran extraerse de otra manera.

[49] RUBIO, FRANCISCO. ACTA Te puede dejar sin internet. Consulta en internet. http://www.cnnexpansion.com/tecnologia/2010/08/11/telefonica-microsoft-web-cnnexpansion. México 15-08-10

Este nuevo tratado podría facilitar más todo este proceso, puesto que se piensa obligar a los ISPs a que monitoreen constantemente las actividades de los usuarios finales en la red, “El acuerdo contempla los "3 Strikes", con los que un proveedor de Internet verificará el contenido que sus suscriptores intercambian con otras personas y, a la tercera ocasión que se le sorprenda en dicho acto, se le suspenderá el acceso a Internet y, además, se le incluirá en una lista negra para que ningún otro proveedor le pueda otorgar el servicio hasta por un año”[50]. El Tratado pretende regular cosas que en las leyes de nuestro país todavía no se observan además de que estas acciones las considero contrarias a Derecho puesto que aludimos a nuestra garantía de privacidad, por la cual no podríamos ser objeto de tal diligencia.

Se debe regular la orden en comento siempre y cuando se funde y motive correctamente, es decir que exista una denuncia o averiguación previa que amerite pedir a un juez que otorgue esta orden, para que los ISPs puedan otorgar la información requerida.

Esta información que puede solicitarse en la orden será muy variada y acorde a lo que se pretende probar, podrán ser los historiales de acceso a internet, fechas y horas específicas sobre las páginas que visitó, en caso de tener un pagina web pedir los datos de acceso a la misma para saber qué actividades se desarrollaban en ella, si utilizaba servidores pedir acceso a los mismo para ver la información que guardaba, este en el caso de que el juez busque pruebas en contra de algún procesado.

Para el caso de que el inculpado sea quien ofrece las pruebas digitales, el juez podrá pedir información a los ISPs para verificar la autenticidad de las pruebas presentadas, supongamos que el sujeto pasivo reclama que alguien se ha introducido a su correo sin su autorización, aquí la autoridad debería de pedir el historial detallado de los accesos a esa cuenta, para verificar, desde dónde y

[50] RUBIO, FRANCISCO. ACTA Te puede dejar sin internet. Consulta en internet. http://www.cnnexpansion.com/tecnologia/2010/08/11/telefonica-microsoft-web-cnnexpansion. México 15-08-10

cuántas veces han accedido a la cuenta, ya que con la dirección ip (huella digital de las computadoras) podrán ubicar todos esos detalles.

Cabe señalar que toda actividad realizada por un equipo informático, por pequeña que sea deja un rastro que puede seguirse y analizar hasta donde lo permita el mismo, esta actividad se registra mediante archivos llamados logs, que sólo son historiales de todo lo que se realizó en un sesión de uso, estos logs se encuentran en todo dispositivo informático así como dentro de los servidores que usamos para navegar en internet, por lo cual estos archivos también pueden seguirse para aclarar las actividades de una persona en la red.

Si bien el Tratado ACTA ya se encuentra en su fase final de negociación, este no representa una solución como la ya propuesta, el ACTA pretende convertir a los ISPs no importando su nacionalidad en policías de internet con amplias facultadas para poder observar todo los que hagamos con nuestra computadora, la solución propuesta sólo se trata de un remedio procesal por medio del cual se pretende asegurar la originalidad de las pruebas digitales obtenidas, siempre y cuando medie un proceso judicial que justifique la investigación, ejemplo de ello sería que se ha puesto en conocimiento de la autoridad que cierta página distribuye contenido protegido por el Derecho de autor indebidamente, el Ministerio Público podrá por tanto perseguir de oficio esta situación y tendrá todas las facultades a su alcance para allegarse de medios de prueba que crea pertinentes, en este caso concreto podrá pedir la información al ISPs que aloja la página la actividad que ésta promueve así como el material que en ella se distribuye.

De hecho algunas empresas como Mercado Libre dentro de sus contratos de servicio con los usuarios ya incluyen una clausula en la cual declaran cooperar con las autoridades en caso de que estas requieran algún tipo de Información, “Mercado Libre podrá revelar la Información Personal de sus usuarios bajo requerimiento de la autoridades judiciales o gubernamentales competentes para efectos de investigaciones conducidas por ellas, aunque no exista una orden ni

una citación ejecutiva o judicial, o por ejemplo (y sin limitación a este supuesto) cuando se trate de investigaciones de carácter penal o de fraude o las relacionadas con piratería informática o la violación de derechos de autor. En tales situaciones, Mercado Libre colaborará con las autoridades competentes con el fin de salvaguardar la integridad y la seguridad de la Comunidad y la de sus usuarios"[51]

Por ello antes de que un Tratado Internacional nos imponga obligaciones contrarias a nuestro Derecho, nuestros legisladores pueden regular estos remedios procesales.

Rechazo la firma del ACTA puesto que no sólo ataca nuestras garantías individuales, sino la soberanía nacional al tratar de regular cuestiones que violan nuestra Constitución.

Ante ello además del remedio procesal comentado analizo otros que de igual manera ayudará a atacar los Delitos Informáticos.

### 4.9. Allanamiento y recolección de evidencia por orden de un juez

Además de legislar la prueba digital, necesitamos proveer de medios procesales a los jueces para que estos a su vez puedan valorar y encontrar las pruebas necesarias.

Por ello dentro de las facultades otorgadas al Poder Judicial, es necesario implementar una modalidad de visita domiciliaria y cateo, en la cual se buscarán dispositivos informáticos que se relacionen con la investigación de un posible Delito.

[51] Orden de autoridades competentes. Requerimientos Legales. Consulta en internet. http://www.mercadolibre.com.mx/jm/ml.faqs.portalFaqs.FaqsController?axn=verFaq&faqId=6171&categId=POLP2 México. 15-08-10

Mariliana Rico afirma que “Lo ideal es que la inspección se haga directamente sobre el sitio, pero en caso de no ser posible se podrá captar cualquier tipo de información archivada en diversos tipos de servidores y se puede considerar la captación y registro como indicio de la existencia de sitios o de su contenido”[52].

Es decir para que la visita o cateo pueda darse debe existir una investigación previa que así lo justifique, ejemplo de esto sería una pesquisa en la cual se buscan a secuestradores, por lo cual en la orden de cateo tendría que estipularse en los objetos que se buscan todo dispositivo informático, ya que cualquiera de ellos puede contener información vital para que el juez pueda probar la participación de un mayor número de personas en la ejecución del Delito,

Esta orden debe tener por intención allegarse de computadoras, cámaras, celulares, radios y cualquier equipo que pueda tener información que pueda relacionarse con el Delito que se investigue.

Como toda orden de cateo, la propuesta deberá cumplir con los mínimos necesarios que garantizan su legalidad a nivel constitucional.

- La Orden de cateo debe Constar por escrito.

- Debe ser emitida por autoridad competente (Juez).

- Se debe fundar y motivar el mandamiento.

- Debe expresarse la autoridad que la gira.

- Debe expresar el propósito de la Orden.

- Debe ostentar la firma del funcionario competente.

[52] Rico Carrillo, Mariliana. Derecho de las nueva tecnologías. La Roca. Buenos Aires Argentina 2007. p.572

- Expresar los objetos que se buscan, definir claramente que se busca cualquier dispositivo informático.

- El lugar o lugares donde que deba practicarse la visita.

- El nombre o nombre las persona o personas que deban efectuar la visita.

Con esta serie de medidas, este tipo de cateos pueden realizarse conforme a Derecho y por ende respetando todas las garantías individuales instituidas en nuestra Constitución.

Con las medidas procesales mencionadas, se puede tener un buen control sobre las pruebas informáticas, además de que las mismas tendrían un alto nivel de fiabilidad en lo que respecta a su discutida autenticidad, ya que siguiendo estas recomendaciones las autoridades podrán elaborar un manual de reglas a seguir en la obtención de las pruebas digitales, y con esto disminuir la posible alteración de las mismas.

## *Capítulo 5.*
## *Tipificación de los Delitos Informáticos en el Código Penal Federal.*

### *5.1 Reproducción ilegal de Software*

Este fenómeno ha crecido rampantemente, es bien sabido que la tecnología cada día se utiliza más, todas las oficinas cuentan con al menos una computadora para realizar las actividades propias del negocio, y esta debe operarse por medio de Software, pero la mayoría de las veces este no es original, ya que por economía las personas optan por comprar los programas piratas que se venden en la calle, con ello están atacando a los Derechos de Autor, ya que el uso de los programas de computo por lo regular tiene un costo a menos que el autor decida que sea gratis para quien quiera usarlo.

Entendamos qué es software ya que la palabra no tiene una traducción al español, pero la Real Academia lo define como "Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora."[53] Entonces podemos determinar que el software son programas, que a su vez contienen reglas e instrucciones por medio de las cuales la computadora puede funcionar, aquí debemos ser puntuales y por tanto recordar qué es lo que se entiende por computadora "Una computadora o un computador, (del inglés *computer*, y éste del latín *computare* -calcular-), también denominada ordenador (del francés *ordinateur*, y éste del latín *ordinator*), es una máquina electrónica que recibe y procesa datos para convertirlos en información útil."[54]

El concepto de computadora es más amplio de lo que imaginamos, no únicamente se refiere a las computadoras que diario utilizamos sino a cualquier dispositivo que reciba y procese datos para convertirlos en información por medio de un software (programas e instrucciones) especifico, así tenemos que en sentido amplio los

[53] Diccionario de la Real Academia Española. Consulta en internet. http://buscon.rae.es/draeI/SrvltConsulta?LEMA=software 17-08-10
[54] Computadora. Consulta en internet. http://es.wikipedia.org/wiki/Computadora . 17-08-10

aparatos reproductores de dvd, ipod, celular, y consolas de videojuegos son computadora, de hecho sus elementos internos están compuestos por las mismas partes que una computadora tiene, por tanto todas estas maquinas utilizan un software de por medio para realizar las funciones para las que fueron inventados.

De esta forma pienso regular la reproducción ilegal de software ya que es un ilícito que se comete cotidianamente "Durante 2009 la tasa de uso de software ilegal en México se ubicó en 60 por ciento, reveló el séptimo estudio Mundial de Piratería elaborado por el grupo Businnes Software Alliance (BSA)"[55] es decir que de cada 10 programas que se utilizan en una computadora 6 son ilegales, lo cual coloca a nuestra país en uno de los primeros lugares de piratería en de software en el mundo, por software debemos entender a todos los programas de computo, videojuegos y películas que se comercializan normalmente.

Cabe señalar que entendemos como reproducción ilegal de software, a la utilización del mismo, sin que medie el pago correspondiente de la licencia que da derecho al uso. En términos más coloquiales la reproducción ilegal de software es equiparable a la piratería de este, ya que en este caso tampoco se paga el derecho correspondiente por el uso del mismo.

Actualmente el Código Penal pretende regular a la piratería de software, en el art. 424 y siguientes:

Artículo 424. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa:

III. A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor.

[55] Molina Gilberto. "Seis de cada 10 software son piratas en el país", El Universal, (México, D.F 11 de mayo, 2010).

Existen muchas observaciones que se pueden hacer a la legislación vigente, la ley castiga a quien use sin autorización obras protegidas por el Derecho de Autor, por tanto debemos entender que por obras se engloban a todas las protegidas por Ley Federal del Derecho de Autor.

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.

Aunque el legislador quiso abarcar a toda las conductas que pueden ser consideradas como Delitos, la redacción es poco afortunada, en primer lugar en las obras que protege no menciona nada referente al software, ni específicamente ni de manera general, ya que quiso enfocar su esfuerzos en proteger a las películas y cd´s de música, dejando de lado a las demás obras, por lo cual se debe de tener un criterio uniforme en la redacción de los artículos, esto es decidir si se va a hablar de obras de manera general o se especificará a cuáles de ellas protege esta ley. Por otra parte algunos abogados creen que con este artículo queda ya regulado el intercambio de archivos vía internet, puesto que el artículo refiere y castiga la introducción del país de obras con fin de especulación comercial, así como el almacenamiento, transporte y distribución de los mismos, si

bien es cierto que el marco jurídico pudiera ser aplicable este se debe delimitar de mejor manera ya que de igual forma se cree que los usuarios de internet que bajan películas y música para uso personal, lo hacen con fines de lucro puesto que obtienen una ganancia indebida al no gastar su dinero en obtener una obra que de otra forma tendría costo.

Actualmente alrededor del mundo se piensa en soluciones para ésta, ya se comentó lo que se pretende hacer con el Tratado ACTA cosa que califico de inapropiada, la divulgación que actualmente tiene el contenido protegido, lejos de menoscabar las ganancias de los artistas y empresas, les da publicidad gratis permitiendo así que la cultura sea divulgada.

En la fracción II del artículo en comento la redacción es lo más inadecuada que el legislador pudo realizar, esta fracción sólo castiga a quien fabrique un sistema o dispositivo que elimina la seguridad de un programa de computo, hay que señalar en la mayoría de los casos en nuestro país no se fabrican los sistemas para desactivar la protección electrónica de los programas, ni mucho menos se desarrolla sistemas con este objetivo, por lo cual esta fracción no protege nada al software, ya que no pena a quien use estas herramientas para los fines ya citados cuestión clave que debería regular, ya que las herramientas para evadir la protección las instalan en los mercados de la ciudad, ejemplo de esto son los chips que se comercializan para poder jugar videojuegos piratas, o los programas que se venden en la calle con los programas necesarios para desactivar la protección del software, por ello esta fracción es poco menos que inútil dentro de nuestro Código.

Artículo 424 ter. Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, fonogramas, videogramas o libros, a que se refiere la fracción I del artículo anterior.

Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 Bis de este Código.

Esta fracción es totalmente cabal con la ilícita actividad que sanciona, puesto que castiga severamente a quien comercializa obras protegidas por el derecho de Autor.

Analizados ya los artículos correspondientes a la piratería de software, presento mi propuesta y las soluciones que planteo.

Hoy en día se busca regular a las descargas de material protegido por el Derecho de Autor, esto es benéfico puesto que de esta forma, los delincuentes que se dedican a la piratería de software tendrían menos herramientas para obtener las obras protegidas y posteriormente comercializarlas sin pagar los derechos correspondientes, pero también se atacaría el acceso a la cultura de muchos ciudadanos en aras de salvaguardar el Derecho de Autor, entonces ¿la regulación es necesaria o no?.

Sin lugar a dudas la postura es crear leyes que permitan evitar la violación de Derechos de autor, pero también que el acceso de internet no sea restringido por la protección de las obras, creemos que si las personas obtienen los contenidos protegido para su uso personal exclusivamente, no incurren en ninguna falta, ya que aunque no paguen por el contenido no piensan sacar provecho de el, solo piensan utilizarlo con fines de esparcimiento, y por tanto se debería:

- Castigar severamente a quien lucra ilícitamente con obras protegidas por el Derecho de Autor y a quien facilite su producción y reproducción.

- Imponer multas ejemplares a las empresas que usan software ilegal, además de pagar las licencias de los programas que utilizan indebidamente

- Creación de convenios con las empresas de software que permitan que las empresas y sobre todo los estudiantes obtengan sus productos a precios preferenciales.

Actualmente Microsoft ha firmado una serie de convenios con distintas instituciones educativas para que los estudiantes adquiera sus productos a precio de $399 c/u, esto es una muy buena oferta, que de expandirse la mayoría de las personas optaría por pagar esas licencias en lugar de comprar los programas en la calle puesto que las copias ilegales cuestan entre $50 y $150.

Así, estas medidas se promoverían con una adecuada reforma al Código Penal actual, para tipificar este Delito modificaríamos la redacción de los artículos ya analizados para quedar como sigue:

*Artículo 424. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa:*

*I. Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Pública;*

*II. Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos;*

*III. A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor.*

*En el caso de la fracción III, si el lucro se lleva a cabo de manera permanente, organizada o al público final la pena de prisión se aumentara hasta en 5 años.*

*Artículo 424 bis.*

*Comete el Delito de reproducción ilegal de software quien utiliza el mismo, sin que medie el pago correspondiente de la licencia que da derecho al uso. Por software*

*debemos entender a todos los programas de computo, videojuegos y películas que se comercializan normalmente. Se impondrá de cinco mil a treinta mil días multa, a las empresas que incurran en esta conducta, además del pago de la licencia de uso correspondiente. Los particulares estarán obligados a pagar el valor comercial del software y se impondrá de veinte a cien días multa.*

*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 por cualquier vía física o digital , almacene, transporte, distribuya, venda o arriende copias de obras protegidas 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, a que se refiere el párrafo anterior, o*

*II. A quien instale, modifique o venda, con fin de lucro un dispositivo, sistema o software cuya finalidad sea desactivar las medidas electrónicas de protección de un programa de computación o de un aparato, cuyo fin sea reproducir películas, videojuegos o ambos.*

*Artículo 424 ter. Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, a que se refiere la fracción I del artículo anterior.*
*Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se aumentará la pena hasta en 5 años*.

Tipifico el Delito de reproducción ilegal de software y proponemos castigar a las empresas puesto que son las más propensas a incurrir en estas conductas.

Se pena ejemplarmente la venta e instalación de dispositivos que permitan la reproducción ilegal de software, así al castigar esta actividad se disminuiría la compra de los usuarios finales y por ende se atacaría de manera frontal al problema.

Mi propuesta no es perfecta, pero representa un avance y una orientación en el tema para que nuestros legisladores puedan mejorar las leyes vigentes.

### *5.2 Daño provocado por Virus, Spyware y códigos informáticos maliciosos*

Algunos juristas creen que los Delitos Informáticos pueden englobarse en los tipos penales ya existentes, y aunque esto pudiera ser cierto haciendo una amplia interpretación, en la mayoría de los casos no sería suficiente esta para declarar culpable al posible delincuente, la particularidad de los Delitos en estudio es que existe un medio comisivo particular sin el cual el ilícito no puede existir por ello se deben reformar nuestra leyes.

El subtema pretende dar a conocer una nueva manera de daño que puede darse en la actualidad el cual no puede protegerse por el tipo penal de daño en propiedad ajena, aunque otros autores piensen lo contrario "Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. El delito anterior en nuestro concepto, no es sino una variante o modalidad del daño en propiedad ajena"[56]. Disentimos del citado autor al afirmar que el tipo penal existente no cubre al daño provocado por virus u otros programas maliciosos en las computadoras.

Daño significa:

**"daño.**

(Del lat. *damnum*).

[56] NAVA GARCÉS, Alberto. Análisis de los Delitos Informáticos. Porrúa México. 2005 p 92

**1.** m. Efecto de dañar.

**2.** m. *Am.* Maleficio, mal de ojo.

**3.** m. pl. *Der.* Delito consistente en causar **daños** de manera deliberada en la propiedad ajena."[57]

Para el objeto del presente estudio las definiciones que interesan son la uno y la tres, por ello se debe entender también que es dañar:

"**dañar.**

(Del lat. *damnāre*, condenar).

**1.** tr. Causar detrimento, perjuicio, menoscabo, dolor o molestia. U. t. c. prnl.

**2.** tr. Maltratar o echar a perder algo. U. t. c. prnl"[58]

Por tanto se determina que el daño, es maltratar alguna cosa, no importando si esta se vuelve inutilizable o no, el concepto de daño en sí abarca cualquier tipo de detrimento que sufra alguna cosa, en este punto es preciso analizar ¿cómo es posible que algún virus o software pueda dañar una computadora?

Para entender la pregunta anterior Leopoldo Parra afirma que: "Los virus informátciso son pequeños programas de cómputo que se auto-replican (de ahí el nombre que los caracteriza), especializados en llevara acabo diversas acciones que interfieren de alguna forma con el funcionamiento normal de una computadora"[59]. que un virus informático es un pequeño programas de software diseñado para propagarse de un equipo a otro y para interferir en el funcionamiento del equipo, estos pueden tener por objeto, eliminar datos y

[57] Diccionario de la Real Academia Española. Consulta en internet. http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=da%F1ar

[58] Diccionario de la Real Academia Española. Consulta en internet .http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=da%F1ar

[59] PARRA REYNADA, Leopoldo. La teoría y la práctica de la seguridad informática. Editorial México Digital Comunicación. p.7.

programas, entorpecer el funcionamiento de la computadora o borrar totalmente el disco duro.

Entonces los virus pueden causar daño a las computadoras, no desde un punto de vista físico, como sería golpearla o romperla, sino el daño que estos provocan lo hacen en la información que estas guardan, no dañan el disco duro, ni los elementos físicos de la computadora, sólo la información.

Existen otros programas los cuales dañan de la misma manera a las computadoras, es el llamado spyware y otros códigos maliciosos, en el primer caso se trata de programas que se dedican a espiar lo que hacemos con nuestra computadora, el atacante puede ver que programas usamos, que paginas visitamos, etc. y por tanto vende esa información a compañías de mercadeo que compran esa información para estadísticas. Existen muchas variantes de virus que he decidido sólo mencionar como software malicioso (malware), este tiene por objeto causar algún daño a la computadora, dentro de este podemos encontrar a los gusanos, caballos de troya, adware, rootkits, keyloggers, stealers, dialers, este tipo de software se le denomina así tomando en cuenta las intenciones para las que fue creado.

Todo estos programas maliciosos se distribuyen por internet, ya sea visitando paginas, bajando o intercambiando archivos, todo esto se hace sin la autorización del usuario, y en muchos casos nunca se entera puesto que tal vez no cuente con un antivirus, por lo cual estos se instalan contra la voluntad total del usuario de la computadora.

En el siguiente subtema analizaré más de cerca algunos de estos malware, pues su ejecución estas más ligada al acceso ilícito a los sistemas de computo y al fraude informático.

Como ya vimos el daño que causan este tipo de programas no es físico, sino se da en la información que reguarda una computadora, por tanto escapa al daño que tipifica nuestro Código Penal ya que este solo puede darse en las cosas.

**Daño en propiedad ajena**

**Artículo 397**.- Se impondrán de cinco a diez años de prisión y multa de cien a cinco mil pesos, a los que causen incendio, inundación o explosión con daño o peligro de:

**I.-** Un edificio, vivienda o cuarto donde se encuentre alguna persona;

**II.-** Ropas, muebles u objetos en tal forma que puedan causar graves daños personales;

**III.-** Archivos públicos o notariales;

**IV.-** Bibliotecas, museos, templos, escuelas o edificios y monumentos públicos, y

**V.-** Montes, bosques, selvas, pastos, mieses o cultivos de cualquier género.

**Artículo 398**.- Si además de los daños directos resulta consumado algún otro delito, se aplicarán las reglas de acumulación.

Los artículos 397 y 398 aportan nada al tema en estudio pero si lo hace el siguiente artículo.

**Artículo 399**.- Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple.

Aquí entra la discusión sobre si dentro del concepto de cosa puede considerarse cono tal, al la información que contiene la computadora, ya que el espíritu de la ley sanciona el deterioro de una cosa física o material que pueda palparse, veamos un criterio de la corte sobre la cosa.

**Registro No.** 191869

**Localización:**

Novena Época

Instancia: Tribunales Colegiados de Circuito

Fuente: Semanario Judicial de la Federación y su Gaceta

XI, Mayo de 2000
Página: 921
Tesis: VI.P.61 P
Tesis Aislada
Materia(s): Penal

**DAÑO EN PROPIEDAD AJENA. NO SE ACREDITA ESE DELITO CUANDO EL OBJETO MATERIAL RECAE SOBRE BIENES NO TANGIBLES, SINO FUTUROS.**

En atención a que el tipo penal de dicho injusto, tutela intereses patrimoniales, pues su esencia radica en la destrucción o deterioro de una cosa mueble o inmueble, implica entonces que debe colmarse, a plenitud, la existencia del objeto material sobre el que recayó el menoscabo pecuniario, de suerte tal que si la acción se hace consistir en la orden de no suministrar agua al pasivo, y éste argumenta que eso constituyó la causa eficiente para que perdiera una cosecha, ello desde luego no puede considerarse como una cosa tangible, sino futura, cuya existencia se supedita a cuestiones agrícolas y climatológicas.

TRIBUNAL COLEGIADO EN MATERIA PENAL DEL SEXTO CIRCUITO.

Amparo directo 419/99. 2 de marzo de 2000. Unanimidad de votos. Ponente: Diógenes Cruz Figueroa. Secretaria: Yolanda Leticia Escandón Carrillo

Con la Tesis aislada anterior podemos ver que la Suprema Corte considera que la destrucción o deterioro debe darse en una cosa mueble o inmueble, debido a esto razono que el Delito de daño en propiedad ajena tipificado actualmente no considera a la información como una cosa o bien mueble sobre la cual pueda recaer el daño. Entendemos perfectamente que si el perjuicio se da sobre el soporte físico de la computadora, ya sea por medio de golpes o destrucción del mismo, el tipo penal encaja a la perfección, pero dado que en el daño por virus no se lacera la integridad de ningún componente físico de la computadora podemos decir que el Delito de Daño en Propiedad Ajena no se configura.

Para que el Delito de daño pueda contemplar la información que guarda la computadora sólo hace falta una pequeña modificación al tipo penal vigente:

***Artículo 399**.- Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple.*

*Las mismas sanciones se aplicarán cuando por acción de un virus, un código malicioso informático o manipulación técnica de una persona, se dañen los programas, información o datos que contenga una computadora ajena o propia en perjuicio de tercero.*

De esta forma el Delito de Daño en Propiedad Ajena por acción de una persona o de Virus Informáticos quedaría regulado. Con ello no pretendo en sí que se resuelva la infección de equipos, sino que cuando se compruebe este daño en la investigación de un ilícito, se pueda castigar al culpable para de esta manera evitar que vuelva a delinquir.

Si bien en nuestro Código se pretendió tipificar a esta pérdida de información en él: TÍTULO NOVENO. REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA. **CAPÍTULO II. ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA,** esto no tiene sentido puesto lo que se pretende regular según el título del capítulo es el acceso ilícito a sistemas y equipos de informática, no el daño que este pueda causar a la información contenida en él.

Afortunadamente en nuestro país no se ha detectado, una distribución de un virus tan grande y masiva que afecte la seguridad de varias computadoras, caso contrario a E.U en donde se han contaminado hasta las computadoras de la NASA, estos sucedió en 1988 cuando " Robert Tappan Morris, estudiante de la Universidad de Cornell, introdujo un virus en la red Arpanet, esta red de

computadoras que actualmente forma parte de internet". [60] En México se han detectado algunos accesos ilegales así como hackeos a páginas del gobierno, tema que será analizado a continuación.

### *5.3 Delitos contra la privacidad y acceso ilegal a sistemas informáticos*

En este subtema analizo dos puntos, el derecho a la privacidad y el acceso ilegal a sistemas informáticos, ya en el punto anterior se habló del daño que puede ser causado en virtud de lo virus, pero ahora me enfocaré a hablar de porqué y cómo sancionar los ataques a la privacidad.

Este tipo de ilícitos ya fueron regulados en nuestro Código Penal, desafortunadamente no se hizo de la mejor manera y las reformas que se incluyeron se convirtieron en letra muerta debido a la inoperancia e inaplicabilidad de las mismas.

Podemos decir que los dos conceptos que analizo se complementan, puesto que si alguien accede a nuestra computadora, correos o archivos sin permiso está violando nuestra privacidad, es decir a ese ámbito de la vida que se tiene derecho a proteger de cualquier intromisión, este concepto sin duda es muy personal, pero así como tratamos de proteger a este, protegeremos la información que guardan las empresas así como a las dependencias del gobierno. Por ello Mariano Jiménez Huerta apunta "el secreto es el señorío o facultad que tiene el hombre y los demás ente jurídicos, de exigir que los hechos atinentes a su intimidad, tanto privada como negocial se mantengan ocultos o en reserva"[61]. Por ello es tan importante que el estado regule el derecho a la privacidad.

Los modos de ingresar a un sistema de cómputo son muchos y muy variados, desde la llamada ingeniería social hasta la infección de computadoras con malware para obtener los datos buscados, desgloso algunos.

---

[60] PALAZZI, Pablo. op. cit. p.155

[61] JIMÉNEZ HUERTA, Mariano. Derecho Penal Mexicano. Séptima Edición, Editorial Porrúa, México, 2003. Tomo III p. 206

- Ingeniería social. Esta técnica se caracteriza por tratar de conocer de la manera mas amplia información particular de la víctima, normalmente se mantiene una relación de amistad aunque no en todos los casos, se lleva a cabo de la siguiente manera:

  Se envía un correo electrónico con un cuestionario aparentemente inofensivo, el cual se supone tiene por objeto conocer más a fondo a nuestras amistades, se pregunta información muy Íntima y de carácter personal, datos como fecha de nacimiento, numero de hermanos, edad, comida favorita, escuelas a las que asististe, deporte y equipo favorito, entre otras, lo que la víctima no sabe es que al contestar y reenviar esta encuesta a sus amigos se hace y lo hacen víctima de robo de información personal, puesto que dentro todas las preguntas que respondió existe información vital para poder obtener contraseñas, ya que las preguntas se planean para que al ser contestadas se obtenga la respuesta a la pregunta secreta de nuestro correo o servicio de red social (páginas donde las personas se relacionan en línea, para que en su caso se accese a la cuenta aun cuando no se tenga la contraseña propiamente.

- Caballos de Troya. Estos son programas de cómputo que como su nombre lo indica se ocultan dentro de otros, normalmente se distribuyen dentro de programas útiles que los usuarios desean obtener sin el pago de la licencia respectiva. Su objeto es entrar a las computadoras de los usuarios sin que estos lo sepan para que el creador de estos obtenga información de cuentas bancarias, actividades que realiza en internet contraseñas, datos de carácter empresarial, comercial o industrial, su potencial criminal es muy alto ya que se obtiene información privilegiada.

- Spyware. Este tipo de software normalmente, sólo busca espiar las paginas que visitan los usuarios así como el tiempo que pasan en ellas, no roba

información personal ni contraseñas, casi siempre la información obtenida se usa para fines comerciales.

- Keyloggers y stealers. Son programas cuyo objetivo es robar contraseñas, en el primer caso se guardan todas las teclas que un usuario pulsa en su computadora de esta forma se pueden conocer conversaciones y contraseñas detalladas ya que se sabe con exactitud las letras que se utilizan, el programa atacante envía esta información a una cuenta de correo creada ex profeso para esta actividad, los stealers normalmente sólo se dedican a robar las contraseñas y nombres de usuarios de bancos, correos y cualquier formulario que llenemos de internet, usualmente la captura de la información se realiza en una página clonada de la original, creada de igual forma ex profeso, para que los usuarios crean que están en la pagina del banco o servidor de correo que utilizan con normalidad e ingresen sus datos.

- Deface . "es la modificación de una página web sin autorización del dueño de la misma. La mayoría de las veces logran defacear un sitio consiguiendo acceso mediante alguna vulnerabilidad que el programador haya dejado en el mismo. También por passwords débiles, problemas en el FTP, etc."[62]. El Objetivo de estas modificaciones normalmente es protestar en contra de los políticos o instituciones de un país.

Estas sólo son algunas de las técnicas que existen para ingresar a computadoras o de terceros sin autorización, de esta forma se viola la privacidad y se acceda a sistemas de forma ilícita.

[62] ¿Qué es un Deface/ Defacing/ Defacement?. Consulta en Internet. http://www.codenb.com/%C2%BFque-es-un-deface-defacing-defacement-14/ 01-09-10

En nuestro Código ya se sanciona  la violación de la correspondencia en los artículos 173 a 177, esta puede ser aplicada sin mayor problema en el caso de que un tercero lea correos que no están dirigidos a él ya que su artículo 177 dice a la letra:

A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Este precepto puede ser aplicado para quien viola la privacidad de un tercero leyendo correos ajenos, ya que sanciona a quien intervenga comunicaciones privadas sin orden judicial, con esto queda regulado al intruso que lee correos ajenos,  tal vez para perfeccionar la norma se podría reformar el artículo de la siguiente manera:

*A quien lea, escuche, modifique, o intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.*

Con este cambio, al mismo tiempo se sancionaría tanto a las personas que leen correos que no les pertenecen, como a las personas que realizan espionaje telefónico, ya que ambos tipo de comunicaciones son de carácter privado.

Por lo que hace propiamente al acceso ilegal a sistemas informáticos se opina que: consideramos un acceso ilegal cuando una persona sin derecho a realizarlo entra a alguna cuenta ajena de correo, cuenta bancaria, cuenta de red social, etc., no importando los fines que este tenga, de la misma manera quien hace uso de la tecnología para conocer información personal de un tercero sin que este lo sepa, por medio de programas nocivos incurre en el mismo Delito.

Mientras que  Simon Horsaman considera que “Para que se configure el acceso ilegitimo a sistemas de información debe darse una seria de presupuestos, como

la intención de quebrantar barreras de seguridad por parte del delincuente y que el titular del sistema no preste su consentimiento o voluntad para ingresar en él"[63]

Disiento de las consideraciones anteriores puesto que no es necesario forzar ninguna barrera de seguridad para que el delito se configure ya que puede darse el caso de que tengamos abierta una sesión de nuestro correo y por ende sin quebrantar ninguna seguridad tenemos accesos a información confidencial.

Esta actividad se trató de regular en nuestro Código en los artículos 211-bis1 a 211 bis 7, pero no fue de la mejor manera explico el porqué.

**Capitulo II**

**Acceso ilícito a sistemas y equipos de informática**

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

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

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

[63] Simon Horsman, Heriberto. Negocios en internet. Astrea. Buenos Aires Argentina 2005. p. 252

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

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

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

**Artículo 211 bis 4**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo

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

**Artículo 211 bis 5**.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

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

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

Después de leer la regulación del acceso ilícito a sistemas y equipos de informática, se destacan dos grandes errores, el primero es no sancionar el acceso ilícito, que se supone es lo que se busca, ya que en la redacción se aprecia claramente que sólo se castiga a la modificación, destrucción o pérdida de datos, pero nunca se castiga al acceso ilícito.

El segundo error es sancionar la modificación, destrucción o pérdida de datos, sólo si el sistema está protegido por algún mecanismo de seguridad, cuando ni siquiera define lo que se entiende por este, luego entonces el robo sólo debe ser sancionado si el sujeto pasivo cuenta con alguna medida de seguridad para evitar el mismo, es irrisorio este supuesto, ya que la redacción asume que si el equipo no cuenta con seguridad no puede ser objeto de ningún delito.

Posteriormente regula en muchos artículos lo mismo pero planteando diferentes situaciones, cosa que no debiera ser en virtud de que la actividad es la misma, por lo cual sólo se debe regular a la misma correctamente y no crear muchos supuestos ya que no tiene ningún caso, porque la ilicitud y gravedad de la conducta es la misma en cualquier caso, acceder a un sistema de la PGR es igual de grave que acceder a la computadora de un tercero.

Por lo cual la reforma que se propone es la siguiente:

***Artículo 211 bis 1***

*Al que acceda sin autorización, o por medio de software especial a un sistema informático o de cómputo y conozca, modifique, copie, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, se le impondrán de diez años a veinte años de prisión y de mil a dos mil días multa.*

***Artículo 211 bis 2***

*A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de instituciones seguridad pública, institución del sistema financiero, o dependencias de gobierno protegido, se le aplicarán las penas previstas en el articulo 211 bis 1. Si el responsable es o hubiera sido servidor público en una institución de las antes*

*citadas , se impondrá además, destitución e inhabilitación de veinte a veinticinco años para desempeñarse en otro empleo, puesto, cargo o comisión pública.*

***Artículo 211 bis 3**.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice para perpetrar otros delitos.*

La propuesta no es perfecta, pero tiene mejores intenciones que la que actualmente observamos, con esta reforma regularíamos tanto la intromisión a nuestras cuenta de correo, como a las bancarias, además de proteger los datos personales de los individuos y empresas ya que no sólo se legisla la obtención o copia de la información, puesto que la sanción prevé como delito el solo acceso a un sistema sin derecho.

Por otra parte se sanciona cualquier tipo de acceso sin autorización, ya que aunque un tercero pudiera identificarse en las páginas con nuestro usuario y contraseña, este acceso sería ilícito, aunque sería difícil identificar el mismo, existen los medios tecnológicos necesarios para poder comprobar el mismo.

Se ataca de manera especial a los funcionarios que valiéndose de su posición, entraran a sistemas sin autorización, por otra parte impone penas mas severas para quien acceda sin derecho a sistemas de computo, obtuvo información esencial y posteriormente esta se utiliza en la comisión de otros ilícitos.

### *5.4 Fraude informático*

La discusión en este ilícito es la misma que en los demás, el tipo penal de fraude ya existe, y tiene una amplia gama de posibilidades que se tipifican como tal, por ello opino que no está de más agregar una o dos fracciones extras para elevar al Código Penal lo que desde nuestro punto de vista puede ser considerado como fraude informático.

Para ese fin analizo el tipo penal del fraude en nuestro Código:
Artículo 386. Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

El tipo penal citado es muy amplio, y precisamente por esa amplitud una gran cantidad de actividades pueden ser consideradas como fraude, pero estas actividades tienen que cumplir con el requisito de inducir a un tercero al error, o aprovechándose de su ignorancia obtener un lucro.

Esto trae a colación el máximo exponente del fraude cibernético el Phishing (pescando): "El phishing es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera (o cualquier otro tipo de empresa de reconocido prestigio)"[64].

El objetivo del Phishing afirma Damian Fuentes es "Engañar a los clientes para conseguir sus datos confidenciales y ordenar operaciones no autorizadas por el usuario legitimo"[65]

El phishing funciona de la siguiente manera, se envía un correo al usuario de un banco indicando que por razones de seguridad debe ingresar a la pagina de la institución para corroborar una seria de datos, de no hacerlo su cuenta será cancelada hasta que acuda a una sucursal, ante el miedo de perder su cuenta y tiempo en acudir a una sucursal, el usuario da click en la liga que se supone el banco nos proporciona para completar el proceso, lo que el atacado no sabe es que la liga no lo llevara a la página de su banco, sino que lo dirigirá a una página

[64] ¿Qué es el phishing? Aspectos a tener en cuenta para evitar ser estafados. Consulta en internet. http://www.microsoft.com/business/smb/es-es/legal/plishing.mspx 01-09-10

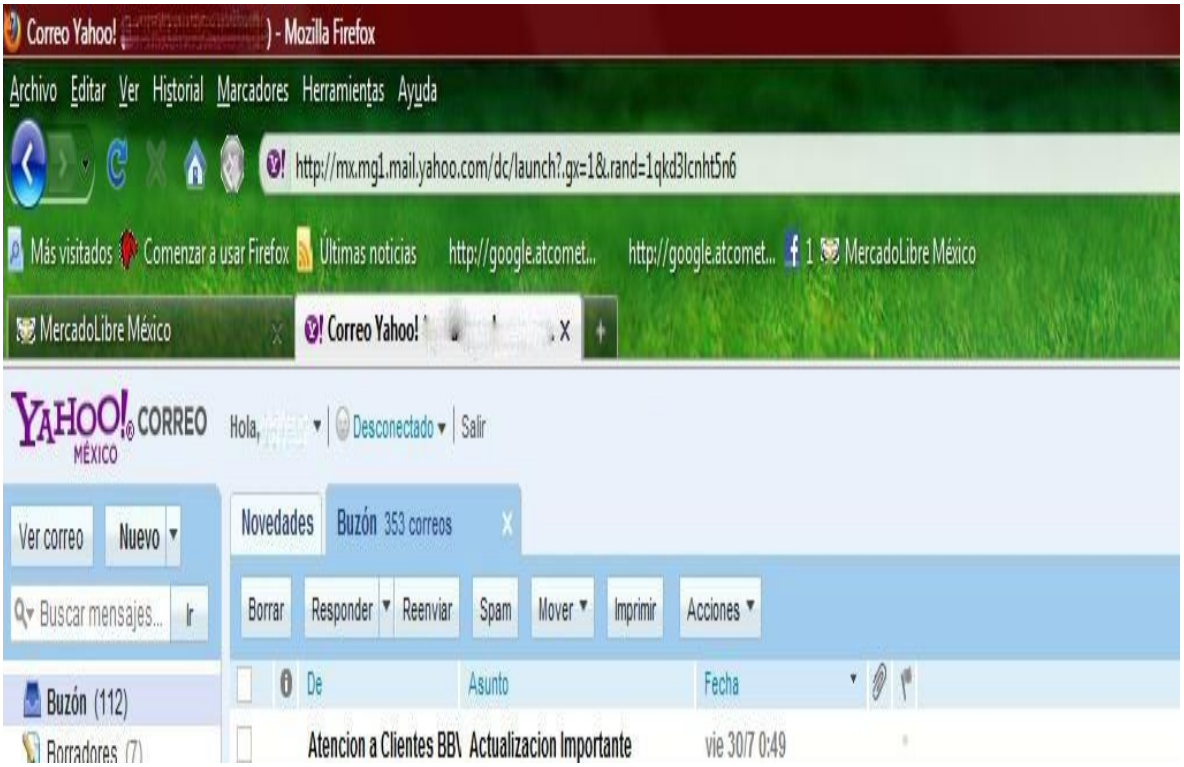
[65] Fuentes Sanchez, Damian. Cibercrimalidad. Inacipe México 2003. p37.

clonada en la cual sin saberlo ingresará todas sus claves de acceso y estas serán robadas, teniendo como resultado que los delincuentes tengan acceso a la misma con lo cual podrán transferir el dinero de esa cuenta a otras o pagar servicios, etc.

Este es el punto medular acerca del phishing, ya que por medio de la clonación de la apariencia de la pagina de nuestro banco, induce al error a los usuarios, ya que piensan están usando la pagina original del banco, por ello es que esta conducta puede considerarse un fraude ya que los usuarios de la banca introducen sus datos inducidos al error en una pagina clonada, pero este tipo de fraude exige un medio comisivo, el uso de las computadoras y paginas de internet, ya que sin la utilización de estas no sería posible concebir este ilícito.

Últimamente los bancos han mejorado sus medidas de seguridad para evitar esta situación, de hecho nos proporcionan un dispositivo llamado token el cual es necesario para poder realizar transferencias via internet, ya que este aparato nos da una clave de dígitos para confirmar las operaciones bancarias en línea, estos dígitos se obtiene en base a series numéricas programadas previamente por el banco, lo cual da como resultado que el banco reconozca las series que son validas para su institución y por tanto puede autorizar las operaciones, el problema es que este dispositivo pudiera no funcionar, ya que los delincuentes al obtener un gran cantidad de estas calves, pueden descifrar la serie numérica que el banco diseñó o introducir distintas series con distintos usuarios para poder obtener el acceso ilegal a las cuentas.

Este fraude no es ajeno a nuestro país, este año se ha atacado a los usuarios de Bancomer, el correo que llega contiene la información que ya comente, cabe señalar que la imagen que uso para describir el fraude no se trata de una extracción de alguna página de internet, sino que llegó al mail de un conocido que amablemente me lo proporcionó para los fines de esta investigación, el correo llega con el siguiente asunto:




Y el texto que contiene es el siguiente:

BBVA Bancomer

**Estimado Cliente De Bancomer**

Lamentamos informarle que usted no a realizado el proceso de sincronizacion de su Tarjeta Bancomer por lo tanto y como medida de seguridad su Tarjeta Codigos Bancomer fue Deshabilitada para evitar futuros problemas con ella al momento de que usted desee realizar sus transacciones en linea.
Para rehabilitar sus tarjeta codigos por favor realice el proceso que se le pide
Le rogamos que si usted usa este tipo de seguridad realice dicha sincronizacion de inmediato y de igual manera evitar que sus datos de acceso causen baja o deshabilitacion permanentes del nuestro sistema.
Esto le llevara solo un minuto de su tiempo Grupo Banco Bancomer Mexicano le ofrece una disculpa y le ruega atienda este comunicado.
Su tarjeta de claves digitales debe ser sincronizada y activada de acuerdo a su usuario de acceso.

Una vez emitido este correo electronico tendra un plazo de 24 horas para llevar acabo dicha accion de lo contrario y por medidas de seguridad su tarjeta de codigos sera descontinuada.
Luego terminado el proceso solicitado, presiona Continuar. A partir de aqui, podras seguir realizando sus transacciones de la manera acostumbrada.
De click en el enlace de abajo de Banca Por Internet Para Agilizar El Proceso
http://www.Bancomer.com/AccesoBancoEnLinea/

Sólo necesitas una cuenta o tarjeta con nosotros y un celular de cualquier compañía.

5226 2663 Cd. de México
8 157 9111 Monterrey 3 669 0229 Guadalajara
01 800 226 2663 Larga distancia sin costo

AMIPCI México IT SELLO DE CONFIANZA

**Click Aqui Para Realizar El Proceso**

http://www.Bancomer.com/Activacion

Innovación que te pone adelante.

Sera Automaticamente Redirigido a la pagina principal de bancomer al dar click en el enlace

Después se visitó la página que supuestamente era del banco.

La pagina clonada del banco tenía la siguiente dirección: http://www.mjbtaxi.co.uk/forms/use/config/files/000/Servicios_En_Linea/Ir/Activacion_Servicio.php por obvias razones sabemos que esa no es la dirección electrónica de Bancomer, la cual es www.bancomer.com.mx, pero al seguir la liga el usuario normalmente no se percata y sus datos quedan en manos de los delincuentes.
El phishing, sea utilizado contra instituciones bancarias o no, se trata un fraude, y aunque el tipo penal existente lo puede abrigar para su regulación es necesaria la reforma del Código Penal, para castigar severamente a los autores de estos delitos, puesto que su elaboración es hecha con un alto grado de sofisticación y malicia, y no sólo se afecta al patrimonio de los defraudados, sino a la reputación de los bancos y proveedores de internet.

La reforma que se propone es la siguiente:

*Artículo 389 bis 1. Se sancionará con prisión de diez a veinte años y multa de dos mil a tres mil días de salario, a quien valiéndose de sus conocimientos en informática haga uso de estos y cree programas y paginas de internet, cuyo objetivo sea obtener datos de los usuarios por medio de engaño o induzca al error, y con ello obtenga un lucro indebido.*

Con esta reforma, se regularía al phishing situación que día a día crece en todo el mundo, y nuestro país no es la excepción, los bancos y otras empresas han informado que son víctimas de este y por consecuente los usuarios de sus servicios también, las personas que cometen estos ilícitos, son personas altamente capacitadas en informática, seguramente cuentan con estudios universitarios, pero por ello deben de ser fuertemente sancionados, ya que los conocimientos obtenidos a través de las aulas no los usan a favor de la sociedad sino en contra de esta.

Esta es sólo una muestra de los fraudes informáticos, ya comente lo que sucede en torno a las cartas nigerianas, diré que los chinos cumplen su parte haciendo creer que venderán artículos a precios muy bajos enviándolos desde su nación, el problema es que cuando se les paga estos desaparecen y no se vuelve a saber del vendedor

Nuestras propuestas no son totalmente acertadas, tienen muchos defectos y deben ser comentadas, cambiadas y mejoradas, pero son los primeros pasos para una adecuada regulación en nuestro Código Penal,

## *Conclusiones*

Primera. El Derecho debe de cambiar según las necesidades de la sociedad, debe de ser versátil, dinámico, y en la medida de lo posible ser fácilmente actualizable.

Segunda. La realidad actual que cambia vertiginosamente, ha rebasado a las leyes penales vigentes, el cambio y adecuación de estas debe darse lo más pronto posible, para así evitar la comisión de Delitos Informáticos.

Tercera. No puede descartarse la existencia de los Delitos Informáticos, porque se cree que los tipos penales actuales ya los regulan, hay que estudiar el tema para entender la nueva realidad que vivimos.

Cuarta. Las reformas en la ley deben de darse a nivel federal de una manera inteligente e innovadora, se debe estudiar con detenimiento los tipos penales que existen en otros países como España y Estados Unidos, solo mediante el estudio y análisis de la sociedad, será posible impulsar reformas penales que sean aplicables y necesarias.

Quinta. Debe de capacitarse al personal, en todo el sistema judicial en el ámbito de los Delitos Informáticos, además de crear grupos especiales que persigan estos ilícitos.

Sexta. Debemos de valorar, desde un punto de vista actual a los llamados medios comisivos o de ejecución, puesto que la computadora es uno de ellos y sin su uso los Delitos Informáticos no pueden existir.

Séptima. Los medios de prueba existentes nos brindan la posibilidad de ofrecer pruebas digitales, se tiene que analizar a estas con la importancia que pueden

llegar a tener actualmente, de igual manera no sólo nuestro Código Penal debe cambiar sino también el procesal.

Octava. Los delincuentes informáticos son personas con una escolaridad avanzada, y conocen los alcances de sus conductas, por ello merecen ser sancionados con severidad, ya que explotan la ignorancia de las personas.

Novena. Antes de firmar Tratados Internacionales vinculantes, México tiene la obligación de regular en términos internos a los Delitos Informáticos, para después poder adaptar esta legislación a la Internacional.

Décima. El problema global que estos Delitos representan, no se resolverá con legislaciones nacionales, pero tampoco lo hará un Tratado ajeno a nuestra realidad como país.

Undécima. México cuenta con las herramientas necesarias para entender el mundo actual, sólo falta voluntad por legislar y dar un vistazo al futuro.

Décimo segunda. La regulación en materia informática es casi inexistente en nuestro país, algunos Estados de la República han tratado de legislar en la materia, pero estos esfuerzos no sirven de mucho en un mundo globalizado como en el que vivimos, interactuamos como nunca antes en la historia, con la rapidez de un parpadeo movemos cantidades de dinero exorbitantes sin la necesidad de ir al banco, la comunicación móvil hace posible que noticias que antes tardaran semanas en llegar, hoy lleguen en segundos, por ello legislar localmente sobre el problema en comento, no funciona, puesto que necesitamos leyes que se apliquen en todo el territorio nacional y en su caso en el internacional.

Décimo Tercera. Un reto totalmente nuevo es regular la llamada prueba digital, esta sin duda puede aportar muchísimos elementos en una investigación, desde las relaciones personales que tiene un delincuente hasta evidencias de los delitos

perpetrados por él o bajo su mando, por ello es necesario legislar sobre esta específicamente y crear peritos para analizar correctamente esta nueva prueba, la cual no sólo será aplicable en el ámbito penal o en los Delitos Informáticos, sino en todo el mundo jurídico.

## Propuesta

Mi propuesta va de la mano con mis conclusiones, desde que inicié este proyecto de investigación hace ya más de 2 años, creí necesario actualizar a nuestro Código Penal, ya que aunque se ha hecho reformas en materia de Delitos Informáticos estas no han sido del todo afortunadas, tal vez debido a que se tiene un profundo desconocimiento del tema en el medio jurídico.

La intención de este trabajo es acercar el medio informático al jurídico, lograr que los abogados entiendan las relaciones cotidianas que se dan en ese mundo virtual llamado Internet, este como todos los lugares en los que existe convivencia entre humanos, necesita una regulación adecuada que permita su desarrollo ordenadamente.

Por ello en el Capítulo final expuse con detalle algunos de los artículos que actualmente regulan al delito informático en el Código Penal, critiqué a los mismos y propuse de qué manera se deben reformar para que puedan ser utilizados en casos concretos en el mundo real, ya que actualmente aunque existen su aplicación es casi imposible, ya que tienen muchos vacíos que pueden ser utilizados por el defensor para impedir que el delincuente sea señalado como culpable.

Las reformas en el Código Penal deben darse a nivel Federal para que su aplicación pueda darse en todo el país, es inaceptable que solo algunos Estados regulen en sus Códigos Penales los delitos informáticos, ya que la realidad actual demanda que la protección que nos brindan las leyes se extienda a todo el país y no se limite sólo a algunos lugares de nuestra República, ya que el delincuente que vacía cuentas bancarias en Monterrey puede estar en Acapulco y delinquir desde ahí.

Los cambios propuestos son los mínimos necesarios que deben darse en nuestros códigos, existen más delitos informáticos que pueden darse, por ello de ser posible debe impulsarse la creación de un apartado especial para el tratamiento de estos ilícitos, si bien ya existe; como comente no se encuentra correctamente regulado, es por ello que los cambios deben darse lo más pronto posible.

Además de lo ya citado debemos regular la aceptación de la evidencia digital en todos los juicios, ya que la obtención de esta no se limita a probar delitos, sino también actos jurídicos como los contratos, por ello es muy importante que este nuevo tipo de prueba sea aceptado en todos los códigos procesales, además de regular la forma de validez de la misma y sus alcances.

Mención aparte merece la capacitación a todo el sistema judicial, jueces, ministerios públicos, policías, peritos, abogados, etc. Actualmente es bien sabido que la inexperiencia en estos menesteres no se limita a un funcionario, sino que permea en todos los niveles, por ello es necesario capacitar a todos los involucrados ya que la sociedad moderna así lo exige.

Por ello propongo crear un plan de modernización, en el cual se instruya a todo el Poder Judicial en el conocimiento de este tipo de delitos, sobre todo a los jueces y ministerios públicos que son las personas a las cuales encargamos la impartición de justicia.

La creación de un grupo especial para perseguir los Delitos Informáticos es necesaria. Por ejemplo en España cuentan con el Grupo de Delitos Telemáticos, en Estados Unidos el FBI está a cargo del grupo Cyber Investigations, si bien se habla de que la procuraduría del Distrito Federal, cuenta con un grupo especial es primordial que cuente con la capacitación técnica necesaria para investigar estos delitos, ya que como establecí en la tesis, al parecer no pudieron obtener información de la computadora de Sergio Humberto Ortiz alias el Apá involucrado en el secuestro del joven Fernando Martí. Tengo que dejar claro que este grupo no

sólo se debe encargar de investigar a los Delitos Informáticos, por lo que tiene que atender cualquier indicio de carácter informático que pueda aporta información a la investigación de otros delitos. Además la creación de este grupo no puede ser local sino debe ser federal con jurisdicciones locales en cada Estado, propongo la creación de una unidad especializada de investigación en la SIEDO que conozca de los delitos informáticos, esto con el fin de poder castigar a las personas que actualmente delinquen sin recibir sanción.

Se tiene que concientizar a la población del riesgo que corren con el uso de las nuevas tecnologías, si bien es cierto que sólo el uso no puede perjudicarnos, al igual que protegen sus datos personales en casa, deben de hacerlo en Internet, puesto que la publicación de estos supone un riesgo real del mal uso de los mismos.

México tiene una gran oportunidad ante sí, el crecimiento de Internet en nuestro país no es muy alto todavía, solo el 30% de la población tiene acceso a este, por lo cual propongo crear una política digital de Estado; la cual tenga por objeto regular desde el nacimiento esta nueva vida virtual de la cual formamos parte.

Por ello para resolver el problema de los Delitos Informáticos no basta con reformar las leyes, debemos de seguir un programa integral que haga que la mayoría de los ciudadanos entendamos los nuevos retos que el uso de las nuevas tecnologías representan, según los especialistas dentro de 25 años México tendrá una penetración de internet del 70%, por ello es el momento de crear una cultura digital de Estado.

## Bibliografía


1.- AMUCHATEGUI REQUENA, Irma Griselda. Derecho Penal. Tercera Edición, Editorial Oxford University, México, 2005.

2.- AMUCHATEGUI REQUENA, VILLASANA DÍAZ, Ignacio. Diccionario de Derecho Penal. Oxford México.2da edición, 2006.

3.- CABANELLAS DE LAS CUEVAS, Guillermo. Derecho de Internet. Editorial Heliasta, Argentina, 2004.

4.- CASTELLANOS TENA, Fernando. Lineamientos elementales de Derecho Penal. Décimo Tercera Edición, Editorial Porrúa, México, 2002.

5.- CASTILLO TAPIA, Fernando. Cibercriminalidad. Editorial Inacipe, México, 2005.

6.- COLÍN SÁNCHEZ, Guillermo Derecho Mexicano de Procedimientos Penales, Porrúa México 1982.

7.- DE PINA, Rafael. Diccionario de Derecho, 31ª ed. Porrúa. México 200. p 401

8.- EOGHAN, Casey et al. Digital Evidence and Computer Crime : forensic science, computers and the internet. Segunda Edición, Editorial Elsevier, Amsterdam, 2004.

9.- FUENTES SANCHEZ, Damián. Cibercrimalidad. EDITORIAL Inacipe México 2003.

10.- GOODMAN, Marc. Cibercriminalidad. Editorial Inacipe, México, 2003.

11.- HIMANEM, PEKKA; et al. La ética del hacker y el espíritu de la era de la información. Editorial Destino. España 2002.

12.- JIMÉNEZ HUERTA, Mariano. Derecho Penal Mexicano. Séptima Edición, Editorial Porrúa, México, 2003.

13.- LÓPEZ BETANCOURT, Eduardo. Introducción al Derecho Penal. Décima Edición, Editorial Porrúa, México, 2002.

14.- MAGGIORE, Giuseppe, Derecho Penal, vol. II, Temis, Bogotá, Colombia, 1989.

15.- MOLINA SALGADO, Jesús. Delitos y otros Ilícitos Informáticos en el Derecho de la Propiedad Industrial. Editorial Porrúa, México, 2003.

16.- NAVA GARCÉS, Alberto. Análisis de los Delitos Informáticos. Editorial Porrúa, México, 2005.

17..- NAVARRO ISLA, Jorge. Tecnologías de la Información y de las Comunicaciones aspectos legales. Editorial Porrúa, México, 2005.

18.- ORONOZ, Carlos. Las Pruebas en materia Penal. Editorial PACJ, México, 2005.

19.- PALAZZI, Pablo. Delitos Informáticos. Editorial Ad-hoc, Argentina, 2000.

20.- PARRA REYNADA, Leopoldo. La teoría y la práctica de la seguridad informática. Editorial México Digital Comunicación, México 2005.

21.- PARDINI, Anibal. Derecho de internet. Editorial La Rocca, Buenos Aires, 2002.

22.- PRIETO ESPINOZA, Alberto, et al. Introducción a la informática. 3ra edición Mc Graw Hill. España. 2002,

23.- RICO CARRILLO, Mariliana. Derecho de las nuevas tecnologías. Editorial La Rocca, Buenos Aires, 2007.

24.- SIMON HORSMAN, Heriberto. Negocios en internet. Astrea. Buenos Aires Argentina 2005.

25.- SHINDER, Debra. Prevención y detección de Delitos Informáticos. Editorial Anaya Multimedia, Madrid, 2003.

26.- TELLEZ VALDEZ, Julio. Derecho Informático. Mc Graw Hill. México 3ra edición, 2007.

27.- UREÑA A, Luis; et al. Fundamentos de informática. Alfa Omega. México. 1999.

## Legislación Nacional

Constitución Política de los Estados Unidos Mexicanos (Consulta en internet http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm). Ultima Reforma publicada DOF 13 de abril de 2011.

Ley Federal del Derecho de Autor (Consulta en internet http://www.diputados.gob.mx/LeyesBiblio/pdf/122.pdf) Ultima Reforma publicada DOF 23 de julio de 2003.

Código Penal Federal (Consulta en internet http://www.diputados.gob.mx/LeyesBiblio/ref/cpf.htm) Ultima Reforma publicada DOF 30 de noviembre de 2010.

Código Federal de Procedimientos Penales (Consulta en internet http://www.diputados.gob.mx/LeyesBiblio/ref/cfpp.htm) Ultima Reforma publicada DOF 30 de noviembre de 2010.

Código Penal para el Distrito Federal (Consulta en internet http://www.aldf.gob.mx/codigos-107-4.html). Ultima Reforma publicada Gaceta Oficial D.F 18 de marzo de 2011.

Código Penal del Estado de Morelos (Consulta en internet http://info4.juridicas.unam.mx/adprojus/leg/18/). Ultima Reforma publicada 29 de diciembre de 2010.

Código de Defensa Social del Estado Libre y Soberano de Puebla (Consulta en internethttp://www.congresopuebla.gob.mx/old_site/ficha_ley.php?CODIGO%20DE%20DEFENSA%20SOCIAL%20DEL%20ESTADO%20LIBRE%20Y%20SOBERANO%20DE%20PUEBLA.&clave=69). Ultima Reforma publicada 2 de marzo de 2011.

Código Penal del Estado de Tamaulipas (Consulta en internet http://po.tamaulipas.gob.mx/leyes/Codigos/Codigo_Penal.pdf). Ultima Reforma publicada 23 diciembre de 2010.

**Legislación Internacional**

Código Penal de la República de Argentina (Consulta en internet http://www.jusneuquen.gov.ar/share/legislacion/leyes/codigos_nacionales/CP_aindice.htm) Noviembre 2009.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Español, (Consulta en internet http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html) Marzo 2011.

Computer Fraud and Abuse Act (Consulta en internet http://www.law.cornell.edu/uscode/18/1030.html) Marzo 2011.

USA Patriot Act (Consulta en internet http://epic.org/privacy/terrorism/hr3162.html) Marzo 2011.

**Hemerografía**

Laguna Icela. ”El Apá monitoreo caso Martí en red””, El Universal, sección D.F (México, D.F 12 de noviembre, 2008).

Molina Gilberto. “ Seis de cada 10 software son piratas en el país”, El Universal, (México, D.F 11 de mayo, 2010).

Redacción.” Conectados a Internet 30 millones, en México”, El Universal, sección Tecno (México, D.F 17 de mayo, 2010).

Utilizan software *pirata* 40% de computadoras en México (Consulta en Internet http://www.eluniversal.com.mx/articulos/46593.html), El Universal versión electrónica, México, Martes 15 de abril de 2008.

**Otras Fuentes**

Análisis Forense. (Consulta en Internet. http://www.seguridad.unam.mx/servicios/) México 20-07-10

BECCARIA CESAR. Tratado de los Delitos y de las Penas. 1ra ed. Cibernética Biblioteca Virtual Antorcha. 2003. p24. (Consulta en internet http://www.antorcha.net/biblioteca_virtual/derecho/beccaria/24.html)

CAMPOLI, Gabriel Andrés. Pasos hacia la reforma penal en materia de delitos informáticos en México (Consulta en INTERNET http://www.alfa-redi.org/rdi-articulo.shtml?x=974), Revista de Derecho Informático: Alfa Redi, Febrero 2005.

CAMPOLI, Gabriel Andrés. Algunos delitos informáticos pueden ser combatidos por la IP o deben ser resarcidos por ella.(Consulta en Internet http://www.inacipe.gob.mx/htm/QuienEsQuien/Investigacion/Opiniones/Delitos.html ) Instituto Nacional de Ciencias Penales, México, 2008.

Cofetel vigilará suspensión de celulares. (Consulta en Internet http://www.cnnexpansion.com/tecnologia/2010/04/10/renaut-cofetel-celulares-cnnexpansion) México 25-07-10

Computadora. (Consulta en internet. http://es.wikipedia.org/wiki/Computadora) 17-08-10

Diccionario de la Real Academia Española (Consulta en internet. http://buscon.rae.es/draeI/SrvltGUIBusUsual?LEMA=cibern%C3%A9tica&origen=) RAE España 23-10-2008

Digital Evidence: Standards and Principles. (Consulta en Internet. http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm) Estados Unidos. 25-07-10

General Definitions relating to digital evidence. (Consulta en internet. http://www.ioce.org/core.php?ID=5) 25-07-10

Los mensajes secretos de coloso. (Consulta en internet http://news.bbc.co.uk/hi/spanish/science/newsid_7099000/7099362.stm) Reino Unido 20-03- 2008

Notimex. Actualizan secuestradores sus operaciones, afirma Fernando Ruiz Canales. (Consulta en Internet http://www.zocalo.com.mx/seccion/articulo/cambian-secuestradores-sus-metodos-ruiz-canales) México. 20-09-08

Orden de autoridades competentes. Requerimientos Legales. (Consulta en Internet http://www.mercadolibre.com.mx/jm/ml.faqs.portalFaqs.FaqsController?axn=verFaq&faqId=6171&categId=POLP2) México. 15-08-10

Policía Cibernética del DF en 700 casos de secuestros. (Consulta en internet. http://www.terra.com.mx/noticias/articulo/749610/Policia+Cibernetica+del+DF+en+700+casos+de+secuestros.htm) México, 20-07-10

Piracy Study. Business Software  Alliance. 2008. p. 5

Qué es el phishing? Aspectos a tener en cuenta para evitar ser estafados. (Consulta en internet. http://www.microsoft.com/business/smb/es-es/legal/plishing.mspx) 01-09-10

RUBIO, FRANCISCO. ACTA Te puede dejar sin internet. (Consulta en internet. http://www.cnnexpansion.com/tecnologia/2010/08/11/telefonica-microsoft-web-cnnexpansion) México 15-08-10

World Internet Users and Population Stats. (Consulta en Internet http://www.internetworldstats.com/stats.htm) 01-06-10