Delitos Informáticos: Generalidades

DR. SANTIAGO ACURIO DEL PINO
Profesor de Derecho Informático de la PUCE

Introducción

"*Si Ud. piensa que la tecnología puede resolver sus problemas de seguridad, entonces Ud. no entiende los problemas de seguridad y tampoco entiende la tecnología*" SCHNEIER

Investigar el delito desde cualquier perspectiva es una tarea compleja; de eso no hay duda. Las dificultades que surgen al tratar de aplicar el método científico a la Delincuencia Transnacional y al Crimen Organizado en buena parte ya fueron establecidas en estudios anteriores, pero enfrentar este tipo de delincuencia a todo nivel es la tarea a la que se ve avocada le Ministerio Público por mandato constitucional y por disposición legal. Ahora bien el fenómeno descrito en los últimos tiempos ha tenido un avance significativo tomando en cuenta la manifestación de la globalización, la cual no solo ha tenido beneficios, sino también ha contribuido a la masificación de esta clase de delitos y tecnificado a otra clase de cómo son los llamados Delitos Informáticos.

Como escribe Albanese, citado por Carlos Resa[1], "*el crimen organizado no existe como tipo ideal, sino como un "grado" de actividad criminal o como un punto del 'espectro de legitimidad*". En este contexto es el crimen organizado que a través de los años se ha ido transnacionalizando su actividad y por ello se habla de Delincuencia Transnacional.

Dentro de esta definición de crimen organizado, la gama de actividades que puede ejecutar un determinado grupo de crimen organizado puede ser extensa, variando en cada caso según diversas variables internas y externas a la organización, y combinar uno o más mercados, expandiéndose asimismo por un

[1] **RESA NESTARES CARLOS:** Crimen Organizado Transnacional: Definición, Causas Y Consecuencias, Editorial Astrea, 2005.

número más o menos limitado de países, aunque en tiempos recientes existe una fuerte tendencia a la concentración empresarial en cada vez menos grupos de un mayor número de campos de la ilegalidad. Su repertorio de actividades incluye el delito de cuello blanco y el económico (en donde se encontrarían los Delitos Informàticos), pero supera a éste último en organización y control, aunque los nexos de unión entre ambos modelos de delincuencia tienden a fusionarse y el terrorismo y el ciberterrorismo pueden llegar a formar parte de sus acciones violentas en ciertas etapas o momentos. En un inventario amplio, las actividades principales de las organizaciones criminales, en suma, abarcan la provisión de bienes y servicios ilegales, ya sea la producción y el tráfico de drogas, armas, niños, órganos, inmigrantes ilegales, materiales nucleares, el juego, la usura, la falsificación, el asesinato a sueldo o la prostitución; la comercialización de bienes lícitos obtenidos por medio del hurto, el robo o el fraude, en especial vehículos de lujo, animales u obras de arte, el robo de identidad, clonación de tarjetas de crédito; la ayuda a las empresas legítimas en materias ilegales, como la vulneración de las normativas medioambientales o laborales; o la utilización de redes legales para actividades ilícitas, como la gestión de empresas de transporte para el tráfico de drogas o las inversiones inmobiliarias para el blanqueo de dinero. Entre aquellas organizaciones que pueden considerarse como típicamente propias del crimen organizado, practicando algunas de estas actividades, se encuentran, dentro de un listado más o menos extenso, las organizaciones dedicadas casi exclusivamente al tráfico de drogas a gran escala, ya sean propias de los países europeas o se generen en países latinoamericanos, del sudeste y el sudoeste asiático, la Mafia italiana en su proceso de expansión mundial que ya se inició hace décadas, las YAKUZA japonesas, las TRIADAS chinas y, en última instancia, ese magma que constituye el crimen organizado en Rusia y en otros países del Este europeo, y ahora existo otro grupo que a entrado a la escena del crimen organizado transnacional son los llamados CRAKERS, los verdaderos piratas informáticos, que a través del cometimiento de infracciones informáticas, han causado la perdida de varios millones de dólares, a empresas, personas y también a algunos estados.

Ahora en bien en el tema que nos interesa, en la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación. Según el diccionario de la Real Academia de la Lengua Española, informática es el "*conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales*".

La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información, para ejecutar tareas que en otros tiempos realizaban manualmente.

Vivimos en un mundo que cambia rápidamente. Antes, podíamos tener

la certeza de que nadie podía acceder a información sobre nuestras vidas privadas. La información era solo una forma de llevar registros. Ese tiempo ha pasado, y con él, lo que podemos llamar intimidad. La información sobre nuestra vida personal se está volviendo un bien muy cotizado por las compañías del mercado actual. La explosión de las industrias computacionales y de comunicaciones ha permitido la creación de un sistema, que puede guardar grandes cantidades de información de una persona y transmitirla en muy poco tiempo. Cada vez más y más personas tienen acceso a esta información, sin que las legislaciones sean capaces de regularlos.

Los progresos mundiales de las computadoras, el creciente aumento de la capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "**era de la información**"[2], a lo que con más propiedad, podríamos decir que más bien estamos frente a la "**ERA DE LA INFORMÁTICA**".

Por tanto, abordar el estudio de las implicaciones de la informática en el fenómeno delictivo resulta una cuestión apasionante para quien observa el impacto de las nuevas tecnologías en el ámbito social. Efectivamente, el desarrollo y masificación de las nuevas tecnologías de la información han dado lugar a cuestiones tales como el análisis de la suficiencia del sistema jurídico actual para regular las nuevas posiciones, los nuevos escenarios, en donde se debaten los problemas del uso y abuso de la actividad informática y su repercusión en el mundo contemporáneo

Es por esta razón, que paralelamente al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de **comportamientos disvaliosos** antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad.

La doctrina ha denominado a este grupo de comportamientos, de manera genérica, «**delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática**».

En efecto, tratándose del sistema punitivo, se ha suscitado una ingente discusión en cuanto a la vocación de los tipos existentes para regir las nuevas

[2] Algunos autores se han referido al proceso de desarrollo de la influencia la tecnología informática como la «segunda revolución industrial» que sus efectos pueden ser aún más transformadores que los de la industrial del siglo XIX. Referencia Ulrich Sieber, "Documentación Para Aproximación Al Delito Informático", publicado en Delincuencia, Editorial. PPU, Barcelona, España, 1992, Pág. 65.

situaciones, que el uso y abuso de los sistemas computacionales han logrado con los llamados delitos informáticos o también llamada criminalidad informática. Lo anterior tiene especial relevancia si consideramos los principios informadores del derecho penal, los que habrán de tenerse a la vista en todo momento. En efecto, no basta en este caso la "**intuición**" en cuanto a que se estima que una determinada conducta podría ser punible, el derecho penal exige una subsunción exacta de la conducta en la norma penal para que recién se esté en presencia de un "**hecho que reviste carácter de delito**"[3], que autoriza su investigación.

En nuestro país nos encontramos con que el ordenamiento jurídico en materia penal, no ha avanzado en estos últimos tiempos a diferencia de otras legislaciones, para darnos cuenta de esto simplemente debemos recordar que nuestro actual código penal es del año de 1938 y que de esa fecha a la actualidad han pasado más de 65 años, por tanto es necesario para enfrentar a la llamada criminalidad informática que los tipos penales tradicionales sean remozados, sean actualizados para así consolidar la seguridad jurídica en el Ecuador, ya que el avance de la informática y su uso en casi todas las áreas de la vida social, posibilita, cada vez más, el uso de la computación como medio para cometer delitos. Esta clase de conductas reprochables resultan en la mayoría de los casos impunes, debido a la falta de conocimiento y preparación de los organismos de administración de justicia y los cuerpos policiales que no poseen las herramientas adecuadas para investigar y perseguir esta clase de infracciones.

En este orden de ideas, y al verse la posibilidad, que por medio del uso indebido de los sistemas informáticos o telemáticos se dé paso a la manipulación de sistemas de hospitales, aeropuertos, parlamentos, sistemas de seguridad, sistemas de administración de justicia, etc. Nos permiten imaginar incontables posibilidades de comisión de conductas delictivas de distintas características, por eso es necesario que el Ministerio Público[4] en cumplimiento de su deber constitucional y legal instruya y facilite las herramientas necesarias a los Ministros Fiscales, Agentes Fiscales y personal de Apoyo a fin de combatir esta clase de comportamientos delictivos que afectan directamente a la sociedad ecuatoriana en su conjunto.

Esta dependencia de la *Sociedad de la Información* a las nuevas tecnologías de la información y de las comunicaciones (TIC), hace patente el grave daño que los llamados delitos informáticos o la delincuencia informática pueden causar a nuestro nuevo estilo de vida, la importancia que cobra la seguridad con la que han de contar los equipos informáticos y las redes telemáticas con el fin de poner obstáculos y luchar con dichas conductas

[3] **DONOSO ABARCA, Lorena,** Análisis del tratamiento de las figuras Relativas a la Informática tratadas en el título XIII del Código Penal Español de 1995.

[4] El Fiscal debe asimilar el uso de los nuevos sistemas de comunicación e información (Internet, correo electrónico), las bases de datos, las nuevas tecnologías de la información y las comunicaciones, y el documento electrónico.

delictivas, y la necesidad de tipificar y reformar determinadas conductas, a fin de que esta sean efectiva y positivamente perseguidas y castigadas en el ámbito penal.

Es en este orden de cosas que Augusto Bequai[5], en su intervención Computer Related Crimes en el Consejo de Europa señala que: "*Si prosigue el desorden político mundial, las redes de cómputo globales y los sistemas de telecomunicaciones atraerán seguramente la ira de terroristas y facinerosos. ... Las guerras del mañana serán ganadas o perdidas en nuestros centros de cómputo, más que en los campos de batalla. ¡La destrucción del sistema central de una nación desarrollada podría conducir a la edad del oscurantismo!. ... En 1984, de Orwell, los ciudadanos de Oceanía vivían bajo la mirada vigilante del Hermano Grande y su policía secreta. En el mundo moderno, todos nos encontramos bajo el ojo inquisidor de nuestros gigantes sistemas computacionales. En occidente, la diferencia entre el Hermano Grande y nuestra realidad es la delicada fibra política llamada democracia; de colapsarse ésta, el edificio electrónico para una implantación dictatorial ya existe. ... La revolución de la electrónica y la computación ha dado a un pequeño grupo de tecnócratas un monopolio sobre el flujo de información mundial. En la sociedad informatizada, el poder y la riqueza están convirtiéndose cada vez más en sinónimos de control sobre los bancos de datos. Somos ahora testigos del surgimiento de una elite informática*".

La reseña casi profética hecha por Bequai, es una visión aterradora que de lo que podría suceder y de hecho está sucediendo en estos momentos, por lo tanto si los países y las naciones no se preparan adecuadamente para contrarrestar a la criminalidad informática, podrían sucumbir ante el avance incontrolable de este fenómeno.

A este respecto el Profesor español Miguel Ángel Davara señala que: "*La intangibilidad de la información como valor fundamental de la nueva sociedad y bien jurídico a proteger; el desvanecimiento de teorías jurídicas tradicionales como la relación entre acción, tiempo y espacio; el anonimato que protege al delincuente informático; la dificultad de recolectar pruebas de los hechos delictivos de carácter universal del delito informático; las dificultades físicas, lógicas, y jurídicas del seguimiento, procesamiento y enjuiciamiento en estos hechos delictivos; la doble cara de la seguridad, como arma de prevención de la delincuencia informática y, a su vez, como posible barrera en la colaboración con la justicia. Todas ellas son cuestiones que caracterizan a este nuevo tipo de delitos y que requieren –entre otras- respuestas jurídicas. Firmes primeros pasos ya que se están dando a niveles nacionales, quedando pendiente una solución universal que, como todo producto farmacológico que se precie, se*

[5] **COMISION DE LAS COMUNIDADES EUROPEAS.** Delitos relativos a las Computadoras. Bruselas, 21.11.1996 COM (96) 607 final.

encuentra en su fase embrionaria de investigación y desarrollo"[6].

Nuestro país en este sentido no puede quedar a la saga de los otros países y debe empezar a tomar todas las acciones y todas las medidas necesarias, y prepararse para el futuro y así no quedar al margen de situaciones que podrían en forma definitiva terminar con la sociedad de la información ecuatoriana, en este sentido el presente trabajo pretende ser un aporte a la escasa o inexistente doctrina, que en el campo del Derecho Penal existe en nuestro país con respecto a los llamados Delitos Informáticos.

1.- Delimitación del Fenómeno de la Delincuencia Informática.

1.1.- Generalidades

El aspecto más importante de la informática radica en que la **información** ha pasado ha convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después[7].

Como señala Camacho Losa, "*En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia*[8]." Entonces el autor se pregunta ¿y por qué la informática habría de ser diferente?

Existe un consenso general entre los diversos estudiosos de la materia, en considerar que el nacimiento de esta clase de criminalidad se encuentra íntimamente asociada al desarrollo tecnológico informático. Las computadoras han sido utilizadas para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato. Los primeros casos fueron reportados en 1958. Para el profesor Manfred Mohrenschlager[9] este fenómeno ha obligado al surgimiento de medidas legislativo penales en los Estados Industriales donde hay conciencia de que en los últimos años, ha estado presente el fenómeno delictivo

---

[6] **DAVARA,** Miguel Ángel, Fact Book del Comercio Electrónico, Ediciones Arazandi, Segunda Edición. 2002.

[7] **MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena,** Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

[8] **CAMACHO LOSA Luis,** El Delito Informático, Madrid, España, 1987.

[9] **MOHRENSCHLAGER, Manfred.** El Nuevo Derecho Penal informático en Alemania" (Págs. 99 a 143). "Delincuencia Informática". (1992, Ed. P.P.U., Colección IU RA-7). Tendencias de Política Jurídica en la lucha contra la Delincuencia "(PÁGS. 47 a 64). "Delincuencia Informática". (1992, Ed. P.P.U., Colección IURA-7). Citado por Marcelo Huerta y Claudio Líbano, Los Delitos Informáticos. Editorial Cono Sur.

informático.

En nuestro país, el fenómeno de la criminalidad informática o de los llamados delitos informáticos, no han alcanzado todavía una importantacia mayor, esto por cuanto no se conoce en nuestro entorno mucho sobre esta clase de infracciones a pesar del efecto de aldea global que estamos viviendo, y la razón de que esta nueva forma de lesión a bienes jurídicos tutelados no sea tomada en cuenta, es por que se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual. (Problema que no solo es en el área Penal si no en todo el ordenamiento jurídico nacional). A continuación se intentará dar una delimitación de este fenómeno de la criminalidad informática

1.2.- Delimitación del Fenómeno

Un primer problema está en delimitar el campo de acción de la llamada criminalidad informática.

En primer lugar existe a decir de Claudio Magliona y Macarena López, una confusión terminológica y conceptual presente en todos los campos de la informática, especialmente en lo que dice relación con sus aspectos criminales, es por eso que es menester desenmarañar el intrincado debate doctrinario acerca del real contenido de lo que se ha dado en llamar los delitos informáticos. Desde esta perspectiva, debe reinar la claridad más absoluta respecto de las materias, acciones y omisiones sobre las que debe recaer la seguridad social que aporta el aparato punitivo del estado. La mayúscula trascendencia inherente a los delitos informáticos merece que toda persona que opere en el mundo del derecho se detenga a meditar sobre el lugar conceptual del espacio de lo jurídico-criminal en que tales agresiones se suceden[10].

En ese orden de ideas y siguiendo al profesor español Romeo Casabona el cual señala que "*En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al*

[10] **HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio,** Los Delitos Informáticos, Editorial Jurídica Cono Sur.

computador o a las tecnologías de la información[11]."

En este sentido el profesor español Davara Rodríguez, en concordancia con lo que manifiesta el profesor mexicano Julio Telles Valdés, menciona que no le parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. "*Ni el nuevo Código Penal español de 1995 introduce el delito informático, ni admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático*[12]".

De ahí que se hable más bien de criminalidad informática que de delitos informáticos propiamente tales. Es por eso que resulta extremadamente complejo buscar un concepto técnico que comprenda todas las conductas ilícitas vinculadas a los medios o procedimientos informáticos, tanto por la diversidad de supuestos, como de los bienes jurídicos afectados.

Ahora bien dicho lo anterior, es necesario decir que además dentro de este fenómeno existe una pluralidad de acepciones y conceptos sobre delincuencia informática, criminalidad informática, lo que ha constituido en un tema de debate también dentro de la doctrina, a continuación se expondrán brevemente algunas de estas acepciones o conceptos:

a) Delincuencia informática y Abuso Informático

La define Gómez Perals como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

Ruiz Vadillo recoge la definición que adopta el mercado de la OCDE en la Recomendación número R(81) 12 del Consejo de Europa indicando que abuso informático "*es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos*".

La misma definición aporta Correa incidiendo en la Recomendación (89) 9. Del Comité de Ministros del Consejo de Europa considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una

[11] **ROMEO CASABONA, Carlos María,** Poder Informático y Seguridad Jurídica, Fundesco, Madrid, España, 1987.
[12] **DAVARA RODRÍGUEZ, Miguel Angel,** Análisis de la Ley de Fraude Informático, Revista de Derecho de UNAM. 1990.

armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el computador.

b) Criminalidad informática

Baón Ramírez define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

Tiedemann[13] considera que con la expresión "criminalidad mediante computadoras", se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.

Como el mismo autor señala, el concepto abarca el problema de la amenaza a la esfera privada del ciudadano, y por otra parte, se refiere además a los daños patrimoniales producidos por el abuso de datos procesados automáticamente.

Para Carlos Sarzana, en su obra Criminalità e tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo"

1.3.- Definición y el concepto de Delitos Informáticos.

Nidia Callegari[14] define al delito informático como "*aquel que se da con la ayuda de la informática o de técnicas anexas*". Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también que lo informático puede ser el objeto de la infracción.

Davara Rodríguez[15] define al Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

[13] **TIEDEMANN, Klaus,** Poder informático y delito, Barcelona, España. 1985.
[14] **CALLEGARI, Nidia,** Citada por Julio Telles Valdés. Ob. Cita.
[15] **Ob. Cita 26**

Julio Téllez Valdés[16] conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin*".

Como ya se señalo anteriormente, determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los computadores, a este respecto el profesor Romeo Casabona señala que el término Delito Informático debe usarse en su forma plural, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general. Se hablará de delito informático cuando nos estemos refiriendo a una de estas modalidades en particular.

Parker define a los delitos informáticos como "*todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio*"[17], Parker además entrega una tabla en que la que se definen los delitos informáticos de acuerdo a los propósitos que se persiguen:

1. **Propósito de investigación de la seguridad:** abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (Parker, Nycum and Oura, 1973).

2. **Propósito de investigación y acusación:** delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática (Departamento de Justicia de Estados Unidos).

3. **Propósito legal:** delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica.

4. **Otros propósitos:** abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador.

[16] **TELLEZ VALDÉS, Julio.** "Los Delitos informáticos. Situación en México", Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.

[17] **PARKER, D.B,** Citado por Romeo Casabona Carlos M. Poder Informático y Seguridad Jurídica.

Con respecto a la definición entregada por Parker, y en concordancia con lo que piensan los autores chilenos Marcelo Huerta y Claudio Líbano considero que tales definiciones parten de una hipótesis equivocada, la cual es estimar que el propósito al cual se dirige la definición es relevante para los efectos de conceptuar los delitos informáticos. Pienso que los delitos informáticos siguen siendo tales, independientemente de los propósitos que se persigan al definirlos, y, por lo tanto, no se justifica la diversidad de definiciones para una sustancia de entidad única, además como dice Carlos María Casabona esta definición restringe a esta clase de delitos solamente al ámbito de lo patrimonial, lo que ofrece una visión parcial del problema, ya que debemos tomar en cuenta que con estas conductas no solo se puede afectar al patrimonio, sino que también pueden ser objeto de aflicción otros bienes jurídicos protegidos como lo son la intimidad personal hasta afectar bienes colectivos como es la seguridad nacional

María Cinta Castillo y Miguel Ramallo entienden que *"delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas"*[18].

Podemos decir además que a estas definiciones de una manera u otra son vagas en cuanto no entregan una concreta delimitación de las fronteras en la que pueden producirse los delitos informáticos, desde un punto de vista estrictamente jurídico, también no establecen con claridad los efectos susceptibles de punibilidad de los delitos informáticos, toda vez que se establecen conductas del agente sin referencia precisa a la necesidad o no de resultados y cuales serian éstos[19].

Antonio E. Pérez Luño señala que quienes se han preocupado del tema, atendiendo a la novedad de la cuestión y el vertiginoso avance de la tecnología, han debido hacer referencia no sólo *"a las conductas incriminadas de lege lata, sino a propuestas de lege ferenda, o sea, a programas de política criminal legislativa sobre aquellos comportamientos todavía impunes que se estima merecen la consiguiente tipificación penal"*[20].

Lo anterior, máxime si consideramos que parte importante de la doctrina estima que no necesariamente estamos frente a nuevos "*delitos*", sino más bien ante una nueva forma de llevar a cabo los delitos tradicionales, razón

[18] **CASTILLO JIMENEZ, María Cinta, RAMALLO ROMERO, Miguel.** El delito informático. Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático. 22-24 junio 1989.
[19] **HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio,** Los Delitos Informáticos, Editorial Jurídica Cono Sur.
[20] **PÉREZ LUÑO, Antonio Enrique.** "Manual de informática y derecho", Editorial Ariel S.A., Barcelona, 1996.

por la cual no cabe individualizarnos de una manera específica, correspondiendo al legislador introducir las modificaciones legales pertinentes a fin de permitir la adecuación de los tipos tradicionales a las nuevas circunstancias.

No obstante, a esta discusión doctrinaria para algunos tratadistas como el Ingeniero Alfredo Sneyers[21], siguiendo el pensamiento del español José María Romeo Casabona y manifiesta que el asumir el término delitos informáticos, en oposición a otros como abusos informáticos, fraudes, delitos de procesos de datos, etc., es el que ofrece la ventaja de su plasticidad al relacionarlo directamente con la tecnología en la que actúa. Asimismo, es un término omnicomprensivo de todas las figuras que habitualmente se utilizan, especialmente en los Estados Unidos, nación en la que los delitos informáticos han experimentado el desarrollo mayor.

Pero a quien le corresponde entregar la definición de los llamados Delitos Informáticos al respecto los autores chilenos Marcelo Huerta y Claudio Líbano en su libro titulado "Los Delitos Informáticos" señalan que "*Debido a que el concepto a definir es un concepto inmerso en el derecho, no nos cabe duda que son precisamente los expertos de este mundo-ciencia los llamados irrefutablemente a diseñar la definición de los delitos informáticos. El derecho es una ciencia llamada a regular todos los tópicos de la vida en sociedad y especialmente a salvaguardaría, sobre principios de justicia, de los atentados a la normal y pacífica convivencia. Desde esta perspectiva, el derecho debe entregar la definición del Derecho Informático y por ende de sus delitos, en relación de continente a contenido. Se podrá decir que el jurista no está capacitado para indagar en los fenómenos de la informática y que por lo tanto la definición debe provenir de aquellos que han abrazado ciencias relacionadas con ella. Sin ánimo de polemizar, decimos que el Derecho como expresión normativa de la Justicia regula todos los aspectos de la convivencia social, incluida la actividad informática que se aplica en toda actividad humana, con tanta trascendencia social y económica. Para tan alta empresa, el derecho, muchas veces se auxilia en los conocimientos propios de otras ciencias, a los cuales les aplica su sello distintivo constructor de normas y principios jurídicos. Pensar lo contrario, implicaría imposibilitar al mundo del derecho de normar sobre la medicina forense, las ingenierías, las ciencias que abarcan la expresión pública, etc. Aún más grave, se pondría al juez, que es un abogado, en la imposibilidad de administrar justicia en materias ajenas al derecho*[22]." De lo señalado por los tratadistas chilenos, coincido plenamente en el sentido, de que son los abogados y juristas quienes deberían conceptuar esta serie de conductas disvaliosas para la sociedad, por cuanto es misión de éstos contribuir al desarrollo y renovación constante del Derecho, además de ser uno de los pilares donde éste se asienta y fortalece, y que tendrá como fin último la realización de

[21] **SNEYERS, Alfredo.** El fraude y otros delitos informáticos. Ediciones T.G.P. Tecnologías de Gerencia y producción, 1990
[22] **Ob. Cita 17**

la justicia como valor intrínseco de las Ciencias Jurídicas y especialmente de las Penales.

En este panorama, los mismos autores chilenos Marcelo Huerta y Claudio Líbano definen los delitos informáticos como "*todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro*"[23].

Esta definición tiene la ventaja de ser omnicomprensiva de las distintas modalidades delictivas.

En conclusión, para poder delimitar el contenido de este fenómeno, optamos primero por una **DENOMINACIÓN GENÉRICA, FLEXIBLE**, acerca del mismo como sería delincuencia informática o criminalidad informática. Sin circunscribirnos así a términos rígidos, como sería por ejemplo delitos informáticos, en tal razón diremos que "**DELINCUENCIA INFORMÁTICA ES TODO ACTO O CONDUCTA ILÍCITA E ILEGAL QUE PUEDA SER CONSIDERADA COMO CRIMINAL, DIRIGIDA A ALTERAR, SOCAVAR, DESTRUIR, O MANIPULAR, CUALQUIER SISTEMA INFORMÁTICO O ALGUNA DE SUS PARTES COMPONENTES, QUE TENGA COMO FINALIDAD CAUSAR UNA LESIÓN O PONER EN PELIGRO UN BIEN JURÍDICO CUALQUIERA**".[24]

En segundo lugar debemos decir que la justificación y los detalles característicos de la criminalidad informática se encuentran precisamente en su carácter de informática es decir la **ESPECIFICIDAD**, cuyas notas características "*las aporta el computador junto con sus funciones propias más importantes: el procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales fines. Cualquier conducta que no opere sobre la base de estas funciones, aunque pueda resultar delictiva (o merecedora de sanción penal en su caso), no poseerá ya la especificidad (como sucede con la mayoría de agresiones al hardware) y debería ser, por tanto, apartada del estudio de la delincuencia vinculada a la informática o tecnologías de la información. En este sentido, es irrelevante que el computador sea instrumento u objetivo de la conducta, y que ésta esté criminalizada o merezca serlo por consideraciones político criminales*[25]."

---

[23] **Ob. Cita Anterior.**
[24] **El Autor.**
[25] **ROMEO CASABONA, Carlos María.** "Poder informático y Seguridad jurídica". Editorial Fundesco 1987

2. – Sujetos del Delito Informático

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo[26].

2.1.- Sujeto Activo

De acuerdo al profesor chileno Mario Garrido Montt[27], se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal.

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

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "*entra*" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que "*desvía fondos*" de las cuentas de sus clientes.

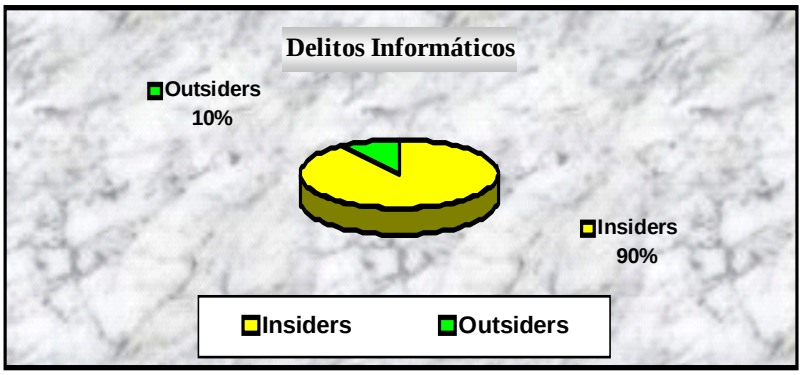
Al respecto, según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada (**Insiders**). Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa (**Outsiders**).

---

[26] **HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio,** Los Delitos Informáticos, Editorial Jurídica Cono Sur.

[27] **GARRIDO MONTT, MARIO.** Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile, 1992. Citado por Jijena Leiva Renato, Los Delitos Informáticos y la Protección Penal a la Intimidad, Editorial Jurídica de Chile, 1993

Cuadro 1: Porcentaje de los delitos informáticos cometidos en contra de empresas



El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "**delitos informáticos**", estudiosos en la materia los han catalogado como "**delitos de cuello blanco**" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "*violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros*".

Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no esta de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: "*el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.*"[28]

[28] **SUTHERLAND Edwin,** Citado por Tiedemann Klaus, Poder Económico y

Tiedemann, frente a esta definición nos dice "*De manera creciente, en la nueva literatura angloamericana sobre estos temas se emplea el termino* **"hecho penal profesional"** (O*ccupational Crime*). *Con esta referencia al papel profesional y a la actividad económica, la caracterización del delito económico se fundamenta ahora menos en la respetabilidad del autor y su pertenencia a la capa social alta y más en la peculiaridad del acto (modus operandi) y en el objetivo del comportamiento*"[29].

A este respecto Marcelo Huerta y Claudio Líbano dicen que "*en lo relativo a tratarse de "Ocupacional Crimes", es cierto que muchos de los delitos se cometen desde dentro del sistema por personas que habitualmente lo operan y que tienen autorizado los accesos* (**Insiders**). *Sin embargo, las tendencias modernas apuntan hacia el campo de la teleinformática a través del mal uso del ciberespacio y las supercarreteras de la información o redes de telecomunicaciones. Es decir, cada día gana más terreno el delito informático a distancia.* (**Outsiders**)."[30]

Es difícil elaborar estadísticas sobre ambos tipos de delitos (delitos de cuello blanco y delitos informáticos). La "**cifra negra**" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables". Esto en el caso de los delitos informáticos tiene relación con lo que se ha dado a llamar el síndrome de "**Robin Hood**" es decir a "*la creencia en cierto modo patológica de que mientras que robar a una persona física que tiene sus problemas y necesidades materiales como todo hijo de vecino es un hecho inmoral e imperdonable, robar a una institución como la banca que gana decenas de miles de millones al año es casi un acto social que contribuye a una más justa distribución de la riqueza*"[31].

Como sostiene Gutiérrez Francés, "*con carácter general, la delincuencia mediante computadoras se inscribe dentro de las formas de criminalidad de "Cuello Blanco", propias de la delincuencia económica, por lo cual desde el punto de vista criminológico, presentan las mismas peculiaridades que ésta, con las notas específicas que aporta lo informático*"[32].

Delito.

[29] **TIEDEMANN,** Klaus, Poder Económico y Delito

[30] **HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio,** Los Delitos Informáticos, Editorial Jurídica Cono Sur.

[31] **CAMACHO LOSA, Luis,** El Delito Informático.

[32] **GUTIÉRREZ FRANCÉS, María Luz,** Fraude Informático y estafa.

Por mi parte, considero que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, por tanto diremos que la cualificación del sujeto activo no es un elemento determinante en la delincuencia informática. Sólo algunos delitos, como los cometidos por los hackers propiamente dichos, podrán considerarse como realizados por un sujeto altamente calificado. Los más, no requieren, en cuanto al sujeto, calificación, ya que pueden cometerse por personas que recién se inician en la informática o por niños que están aprendiendo individualmente en sus hogares.

A este respecto el jurista mexicano Jorge Lara Rivera, en un artículo publicado en Internet[33] nos dice que "*Tradicionalmente se ha considerado que este tipo de delitos se encuadra dentro de los llamados "delitos de cuello blanco" debido a que se requiere que el sujeto activo tenga un conocimiento especializado en informática. Ahora bien, no podemos negar que la especialización informática facilita a los sujetos a incidir criminalmente por medio de las computadoras. Sin embargo, el mundo de la computación se va convirtiendo paulatinamente en un área común y corriente, gracias a la facilidad con la que los modernos sistemas y programas pueden ser controlados. Dentro de poco tiempo la operación de un sistema electrónico será tan fácil como manejar una televisión, por ejemplo. De esta manera, se puede ubicar como sujeto activo de un delito cibernético a un lego en la materia o a un empleado de un área no informática que tenga un mínimo conocimiento de computación. Por no hablar del problema que se plantea con los llamados "niños genio" que son capaces no sólo de dominar sistemas electrónicos básicos, sino que pueden incluso intervenir exitosamente en operaciones de alto grado de dificultad técnica, acarreando más problemas al tambaleante concepto de la impunidad para el caso de que algunos de estos menores logre cometer estragos importantes a través de los medios computacionales que maneje*".

2.2 - Sujeto Pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

En primer término tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones creditícias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos

[33] **LARA RIVERA, Jorge,** Los Delitos Informáticos. www.jusrismática.com.

conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; La falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que **para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento**.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los

delitos informáticos, sus posibilidades son limitadas, además de que en algunos países como el nuestro no existe legislación alguna sobre esta clase de conductas ilícitas lo que empeora más la situación de las víctimas de estas conductas ilícitas.

3. - Bien Jurídico Protegido

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir –ya que constituye la razón de ser del delito– y no suele estar expresamente señalado en los tipos penales.

3.1.- Los Bienes Jurídicos Protegidos en el Delito Informático.

Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

De otro lado otra vertiente doctrinaria supone que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la **INFORMACIÓN** misma como **bienes jurídicos de protección,** esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible. Esto por cuanto la información no puede a criterio de Pablo Palazzi ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual esta constitucionalmente protegida.

En fin la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de “dañosidad” o “lesividad”. Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada. Así inspira tanto a la criminalización como a descriminalización de conductas. Su origen directo es la teoría del contrato social, y su máxima expresión se encuentra en la obra de **BECCARIA “Los Delitos y las Penas”** (1738-1794). Se define como un bien vital, “**bona vitae**”, estado social valioso, perteneciente a la

comunidad o al individuo, que por su significación, es garantizada, a través del poder punitivo del Estado, a todos en igual forma.

En conclusión podemos decir que el bien jurídico protegido en general es la información, pero esta considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

- **EL PATRIMONIO**, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.
- **LA RESERVA, LA INTIMIDAD Y CONFIDENCIALIDAD DE LOS DATOS**, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.
- **LA SEGURIDAD O FIABILIDAD DEL TRÁFICO JURÍDICO Y PROBATORIO**, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.
- **EL DERECHO DE PROPIEDAD**, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "*que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo*"[34]. En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos.

Por tanto podemos decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos, en tal sentido de María Luz Gutiérrez Francés, respecto de la figura del fraude informático nos dice que: "*las conductas de fraude informático presentan indudablemente un carácter pluriofensivo. En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macrosocial), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macrosocial vinculado al funcionamiento de*

[34] **REYES ECHANDÍA, Alfonso,** La Tipicidad, Universidad de Externado de Colombia, 1981.

los sistemas informáticos"[35].

Por tanto diremos que el nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, *como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa*[36]. En tal razón considero que este tipo de conductas criminales son de carácter netamente pluriofensivo.

Un ejemplo que puede aclarar esta situación, es el de un hacker que ingresa a un sistema informático con el fin de vulnerar la seguridad éste y averiguar la información que más pueda sobre una determinada persona, esto en primer lugar podríamos decir que el bien jurídico lesionado o atacado es el derecho a **la intimidad** que posee esa persona al ver que su información personal es vista por un tercero extraño que sin autorización ha vulnerado el sistema informático donde dicha información está contenida. Pero detrás de ese bien jurídico encontramos otro un bien colectivo que conlleva a un ataque a la **confianza en el funcionamiento de los sistemas informáticos**. Es decir, de intereses socialmente valiosos que se ven afectados por estas nuevas figuras, y que no solo importan la afección de bienes jurídicos clásicos.

4. – Tipos de Delitos informáticos

Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es inimaginable, a decir de Camacho Losa, el único limite existente viene dado por la conjugación de tres factores: **la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas**, por tal razón y siguiendo la clasificación dada por el estadounidense Don B. Parker más la lista mínima de ilícitos informáticos señalados por las Naciones Unidas, he querido lograr una clasificación que desde el punto de vista objetivo sea lo más didáctica posible al momento de tratar esta clase de conductas delictivas, por lo expuesto anteriormente y sin pretender agotar la multiplicidad de conductas que componen a esta clase de delincuencia y como señala Gutiérrez Francés, es probable que al escribir estas líneas ya hayan quedado sobrepasada las listas de modalidades conocidas o imaginables, que ponemos a consideración del lector en forma breve en que consiste cada una de estas conductas delictivas:

[35] **GUTIÉRREZ FRANCÉS, María Luz,** Fraude Informático y estafa.
[36] **MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena,** Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

4.1. - Los fraudes

LOS DATOS FALSOS O ENGAÑOSOS (Data diddling), conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como ***manipulación de datos de entrada***, 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.

MANIPULACIÓN DE PROGRAMAS O LOS "CABALLOS DE TROYA" (Troya Horses), 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.

LA TÉCNICA DEL SALAMI (Salami Technique/Rounching Down), Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

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 basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones 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.

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 basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

PISHING.- Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

GRAFICO 1: SPEAR PISHING

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las victimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aun peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar.

En estos momentos también existe una nueva modalidad de Pishing

que es el llamado Spear Pishing o Pishing segmentado, que funciona como indica el GRÁFICO 1, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

4.2. - El 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:

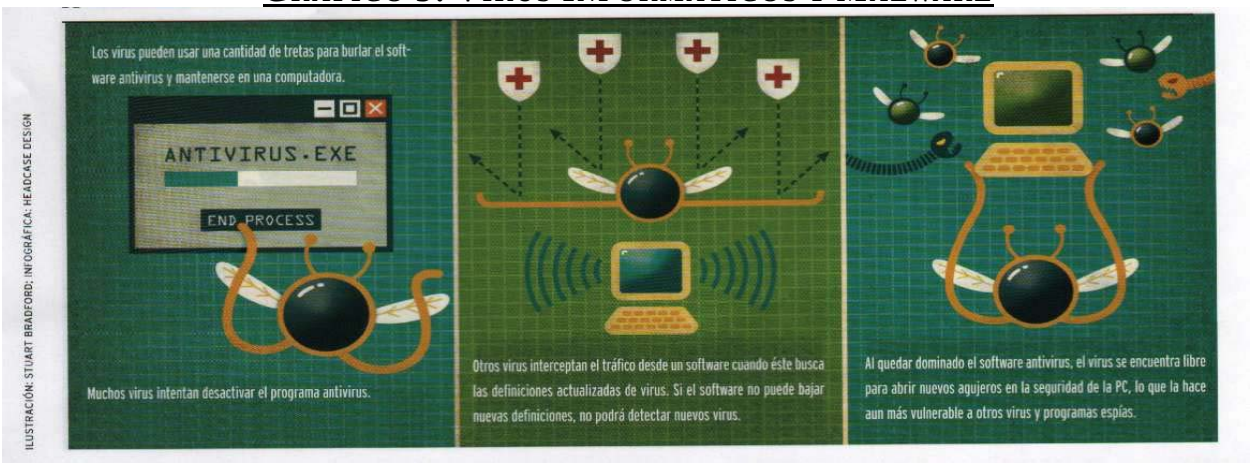
BOMBAS LÓGICAS (LOGIC BOMBS), es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas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

GUSANOS. Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita. (Gráfico 2)

GRAFICO 2: GUSANO INFORMÁTICO

VIRUS INFORMÁTICOS Y MALWARE, son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

GRAFICO 3: VIRUS INFORMÁTICOS Y MALWARE



Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. Han sido definidos como *"pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autorreporducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar"*[37].

[37] **GUIBOURG Ricardo A., ALENDE Jorge O., CAMPANELLA Elena M.,**

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y la debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos.

CIBERTERRORISMO: Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

ATAQUES DE DENEGACIÓN DE SERVICIO: Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

4.3. - El espionaje informático y el robo o hurto de software:

FUGA DE DATOS (DATA LEAKAGE), también conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, "*la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera*"[38].

La forma más sencilla de proteger la información confidencial es la criptografía.

Manual de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires, Argentina.

[38] **CAMACHO LOSA, Luis,** El Delito Informático, Madrid, España, 1987.

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, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

4.4. - El robo de servicios:

HURTO DEL TIEMPO DEL COMPUTADOR. Consiste en el hurto de el tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no esta autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

APROPIACIÓN DE INFORMACIONES RESIDUALES (SCAVENGING), es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. To scavenge, se traduce en recoger basura. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

PARASITISMO INFORMÁTICO (PIGGYBACKING) Y SUPLANTACIÓN DE PERSONALIDAD (IMPERSONATION), figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o

empresa determinada.

4.5. - El acceso no autorizado a servicios informáticos:

LAS PUERTAS FALSAS (TRAP DOORS), consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

LA LLAVE MAESTRA (SUPERZAPPING), es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.
Su nombre deriva de un programa utilitario llamado *superzap*, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador.
Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación

PINCHADO DE LÍNEAS (WIRETAPPING), consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

Como se señalo anteriormente el método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la que se envió en origen.

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.

5.- Situación Internacional

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

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

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que, los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadoras y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de

conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

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

Una vez desarrollado todo este proceso de elaboración de las normas en el ámbito continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "*recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales*". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

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

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

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la

delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal - hasta ese entonces - era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados.

Por todo ello, en vista de que, los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras, a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado a escala internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera de los delitos informáticos y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición.

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

Al respecto se debe considerar lo que dice el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos el cual señala que, cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos

constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para ello, como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la “lista facultativa”, especialmente la alteración de datos de computadora y el espionaje informático; así como en lo que se refiere al delito de acceso no autorizado precisar más al respecto, en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, se señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países como el Ecuador, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable, tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

En definitiva tanto los terroristas como las Organizaciones Delictivas Transnacionales se están aprovechando de los avances tecnológicos, para cometer sus fechorías a través del uso de las redes de telecomunicaciones en donde han encontrado un sitio propicio para expandir sus tentáculos situación que debe ser detenida por parte de los organismos a cargo del control de esta clase de conductas disvaliosas, pero la acción no debe ser aislada debe existir una cooperación interinstitucional e internacional en este campo.

5.1.- Tratamiento en otros países.

1. Alemania

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

- Espionaje de datos (202 a)
- Estafa informática (263 a)
- Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273)
- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, Inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b)

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, producción del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que, el perjuicio patrimonial que se comete consiste en influir en el resultado de

una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

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

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

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

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan solo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos.

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

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

2. Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987

Esta ley contempla los siguientes delitos:

- Destrucción de datos (126). En este artículo se regulan no solo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

3. Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

- Acceso fraudulento a un sistema de elaboración de datos (462-2). - En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje informático (462-3). - En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos (462-4). - En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados (462-5). - En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

4. Estados Unidos

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

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

El Acta de 1994 diferencia el tratamiento a aquellos que de manera

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

Nos llama la atención que el Acta de 1994 aclara que el creador de un virus no puede escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

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

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

Consideramos importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etcétera.

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

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a un grupo de instrucciones

informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

5. Chile[39]

En junio de 1993 entró en vigencia en Chile la Ley N°19.223, sobre delitos informáticos.

La Ley Nº 19.223 tiene como finalidad proteger a un nuevo bien jurídico como es: "*la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan*".

La Ley N°19.223, es una ley especial, extra código y consta de 4 artículos, que se enuncian a continuación.

> Artículo 1. "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
>
> Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".
>
> Artículo 2. "El que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".
>
> Artículo 3. "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".
>
> Artículo 4. "El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

En la Ley No. 19.223 se contemplaría los delitos informáticos de

[39] **HERRERA BRAVO, Rodolfo.** Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la ley chilena Nº 19.223, en http: derecho.org/, 1998

sabotaje y espionaje informáticos, aunque no de una forma clara. Así pues, en el artículo 1, el inciso primero alude a los daños que se puedan cometer contra el hardware, sea destruyéndolo o inutilizándolo, por lo que no se trataría de un delito informático sino mas bien de un delito de daños convencional. Es en el artículo 3° es en donde encontraríamos la figura del sabotaje informático al sancionar al que maliciosamente altere, dañe o destruya los datos contenidos en un sistema.

Por su parte, el espionaje informático se tipificaría en el artículo 2 y 4. En este último caso, el tipo es demasiado amplio y no otorga un valor determinado a los datos afectados, dando, a mi parecer, un tratamiento inadecuado.

En la Ley NO. 19.223, no se contemplan figuras como el hacking o el fraude informático.

En cuanto a la penalidad, esta ley establece según el artículo 1, por ejemplo, en el caso de que alguien destruya dolosamente un computador, puede recibir como castigo la pena de presidio menor en su grado medio a máximo, es decir, puede tener desde 541 días hasta 5 años de cárcel. En virtud del artículo 2, si un hacker, por ejemplo, ingresa indebidamente a un sistema para conocer información sin autorización, puede recibir desde 61 días hasta 3 años de presidio. De acuerdo al artículo 3, si alguien, por ejemplo, graba intencionalmente un virus en un sistema, puede ser castigado desde 541 días hasta 3 años de presidio. Finalmente, en virtud del artículo 4, podría recibir también presidio desde 541 días hasta 3 años, un operador que dé a conocer dolosamente el contenido de la información guardada en el sistema informático, e incluso podría alcanzar hasta 5 años si la persona es el responsable del sistema.

En conclusión podemos decir que son evidentes las falencias en las que incurre la ley chilena respecto a la regulación de la Delincuencia Informática, no obstante hay que señalar que la Ley N°19.223, es la pionera en la región al abordar expresamente el tema de los delitos informáticos.

6. España

En España el tratamiento dado a este tema es abordado en el nuevo Código Penal de 1995 aprobado por Ley-Orgánica 10/1995, de 23 de Noviembre y publicado en el BOE número 281, de 24 de Noviembre de 1.995.

El presente Código Penal incorporó a los tipos delictivos clásicos la realidad informática de manera global, no limitándose a regular solo los delitos informáticos de mayor conocimiento en la doctrina y otras legislaciones[40]. Pero

[40] **MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena,** Delincuencia y Fraude Informático, Editorial Jurídica de Chile.

a pesar de las críticas que se le pueden efectuar a este cuerpo normativo, es inobjetable su intento por lograr la armonía jurídica entre las figuras clásicas penales y el fenómeno informático, lo cual requiere de un gran esfuerzo, no tanto así la solución que han adoptado otros ordenamientos jurídicos, los cuales se han limitado a enfrentar el problema a través de leyes especiales, que consideran al fenómeno informático aislado del resto de la legislación, apartándose de la buena técnica jurídica, como en el caso de Chile.

A continuación se hará una breve reseña sobre el contenido del Nuevo Código Penal Español en referencia a la penalización de la delincuencia informática.

INTERCEPTACIÓN DEL CORREO ELECTRÓNICO	**USURPACIÓN Y CESIÓN DE DATOS RESERVADOS DE CARÁCTER PERSONAL**
En el apartado correspondiente a los delitos contra la intimidad se introduce la interceptación de correo electrónico, que queda asimilada a la violación de correspondencia. El artículo 197 extiende el ámbito de aplicación de este delito a las siguientes conductas: ▣ apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales. ▣ interceptación de las telecomunicaciones, en las mismas condiciones. ▣ utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos. Estas actividades deben producirse sin consentimiento del afectado y con la intención de descubrir sus secretos o vulnerar su intimidad. La pena que se establece es de prisión, de uno a cuatro años y multa de doce a	También quedan tipificados los actos consistentes en apoderarse, utilizar, modificar, revelar, difundir o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos. El art. 197.2 castiga con prisión de 1 a 4 años para el caso de acceso, utilización, etc. y de 2 a 5 años si los datos se difunden, revelan o ceden a terceros. Cuando dichos actos afectan a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior. Esta inclusión de los datos personales en el Código Penal (a partir de aquí CP) supone una importante innovación. Este apartado desarrolla el principio de la Protección a la Intimidad, contenido en el Art. 18.3 de la Constitución Española de 1978.

veinticuatro meses (Con el nuevo concepto de días-multa, un día equivale a un mínimo de 200 pesetas y un máximo de 50.000 pesetas)	
Fraude Informático	**Daños informáticos**
El nuevo CP introduce el concepto de fraude informático, consistente en la manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina. Los Arts. 248 y siguientes establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.	En el delito de daños se contemplan los supuestos de destrucción, alteración, inutilización, o cualquier otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes, o sistemas informáticos. El art. 264.2 establece una pena de prisión, de 1 a 3 años en el caso de daños informáticos. El valor que pueden alcanzar en la actualidad los datos o la información de una empresa o administración pública en formato digital, ha obligado a incluir la figura del delito de daños informáticos en el CP.
DIFUSIÓN DE MENSAJES INJURIOSOS O CALUMNIOSOS	**Falsedades documentales**
El artículo 211 establece que los delitos de calumnia e injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante. Puede incluirse perfectamente en este supuesto la difusión de mensajes injuriosos o calumniosos a través de Internet, en especial, en el entorno www que es el más similar a la prensa tradicional. Las penas establecidas pueden llegar a los 2 años de prisión en el caso de la calumnia, y multa de hasta 14 meses en el caso de la injuria.	Los artículos 390 y siguientes castigan con la pena de prisión de hasta seis años las alteraciones, simulaciones y demás falsedades cometidas en documentos públicos. Los artículos 395 y 396 se refieren a las falsedades cometidas en documentos privados, pudiendo alcanzar la pena de prisión hasta dos años. También se castiga la utilización de un documento falso para perjudicar a un tercero. El artículo 26 define como documento cualquier soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

El artículo 212 establece la responsabilidad solidaria del propietario del medio informativo a través del que se haya propagado la calumnia o injuria. En el caso de Internet, la responsabilidad civil solidaria alcanzaría al propietario del servidor en el que se publicó la información constitutiva de delito, aunque debería tenerse en cuenta, en este caso, si existió la posibilidad de conocer dicha situación, ya que el volumen de información contenida en un servidor no es comparable al de una revista, un periódico o un programa de TV o radio. En este sentido cabe recordar la tesis que asimila al propietario de un servidor al librero, en contraposición con los que lo asimilan a un editor. La primera teoría es partidaria de liberar de responsabilidad civil al propietario de un servidor, debido a la imposibilidad de controlar toda la información que es depositada en el mismo por los usuarios.	Entendemos que quedaría incluido en el concepto documento los mensajes estáticos, compuestos por información almacenada en un sistema informático después de haber sido remitida o recibida a través de la red, pero surgen dudas sobre la naturaleza documental del mensaje que está circulando. Finalmente, el artículo 400 introduce el delito consistente en la fabricación o tenencia de útiles, materiales, instrumentos, programas de ordenador o aparatos destinados específicamente a la comisión de estos delitos, se castigarán con las penas señaladas para los autores. Entrarían dentro de este tipo los programas copiadores, las utilidades empleadas por los hackers y cualquier otro dispositivo similar.
REVELACIÓN DE SECRETOS	**Robos**
El art. 278 establece una pena de 2 a 4 años para el que, con el fin de descubrir un secreto, se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo. Si los secretos descubiertos se revelasen, difundieren o cedieren a terceros, la pena llegará a los 5 años de prisión.	El artículo 239 – Considera llaves falsas las tarjetas magnéticas o perforadas así como los mandos o instrumentos de apertura a distancia, considerando por lo tanto delito de robo la utilización de estos elementos, el descubrimiento de claves y la inutilización de sistemas específicos de alarma o guarda con el fin de apoderarse de cosas muebles ajenas.

5.2.- Organización de Estados Americanos.

La Internet y las redes y tecnologías relacionadas se han convertido en instrumentos indispensables para los Estados Miembros de la OEA. La Internet

ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el Hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran la Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones. Asimismo, en la Tercera Cumbre de las Américas, en la ciudad de Québec, Canadá, en 2001, nuestros líderes se comprometieron a seguir aumento la conectividad en las Américas.

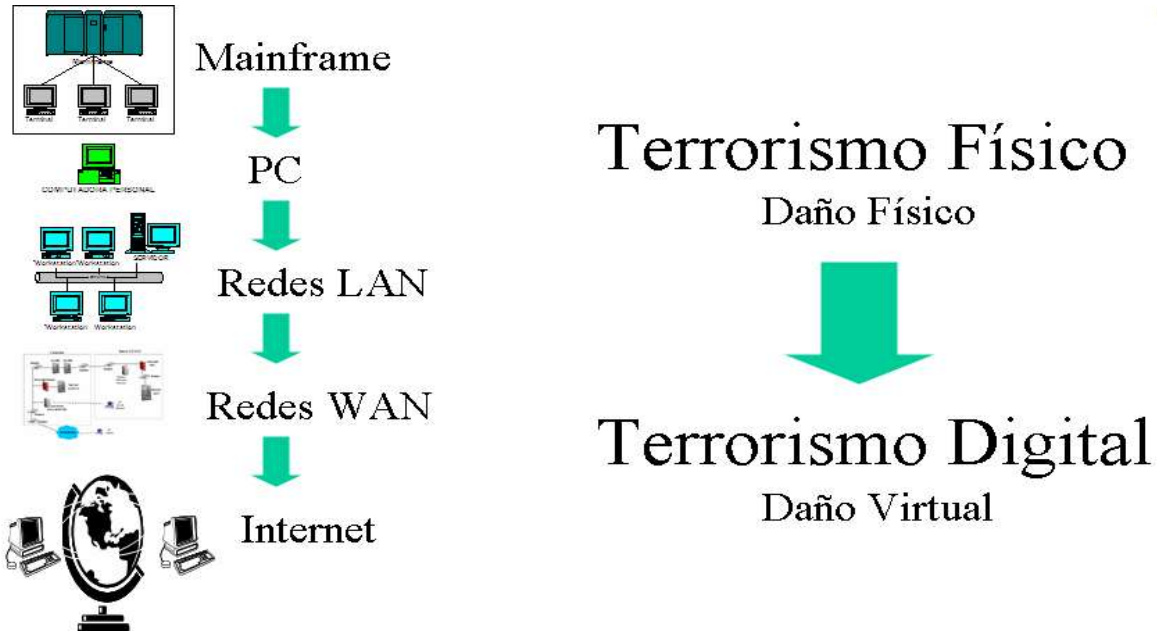
Lamentablemente, la Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet. La información que transita por Internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y defraudar a los negocios. La destrucción de los datos que residen en las computadoras conectadas por Internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas. Estas amenazas a nuestros ciudadanos, economías y servicios esenciales, tales como las redes de electricidad, aeropuertos o suministro de agua, no pueden ser abordadas por un solo gobierno ni tampoco pueden combatirse utilizando una sola disciplina o práctica. Como reconoce la Asamblea General en la resolución AG/RES. 1939 (XXXIII-O/03) (**Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética**), es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario. La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en respaldo a esto, celebró una Conferencia sobre Seguridad Cibernética (Buenos Aires, Argentina, del 28 al 29 de julio de 2003) que demostró la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, y que una acción eficaz para abordar este problema debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales.

La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética.

La Estrategia también reconoce que un marco eficaz para la protección de las redes y sistemas de información que integran la Internet y para responder a incidentes y recuperarse de los mismos dependerá en igual medida de que:

- Se proporcione información a los usuarios y operadores para ayudarles a asegurar sus computadoras y redes contra amenazas y vulnerabilidades, y a responder ante incidentes y a recuperarse de los mismos;
- Se fomenten asociaciones públicas y privadas con el objetivo de incrementar la educación y la concientización, y se trabaje con el sector privado –el cual posee y opera la mayoría de las infraestructuras de información de las que dependen las naciones—para asegurar esas infraestructuras;
- Se identifiquen y evalúen normas técnicas y prácticas óptimas para asegurar la seguridad de la información transmitida por Internet y otras redes de comunicaciones, y se promueva la adopción de las mismas; y
- Se promueva la adopción de políticas y legislación sobre delito cibernético que protejan a los usuarios de Internet y prevengan y disuadan el uso indebido e ilícito de computadoras y redes.

GRÁFICO 3: EVOLUCIÓN DE LA INFORMÁTICA Y EL TERRORISMO



En el gráfico 3, nos podemos dar cuenta del tipo de daño que puede causar el Ciberterrorismo, esto es decir que el bien jurídico afectado por este tipo de ataque pluriofensivo siempre será un daño digital, es por tanto que:

- Los sistemas informáticos son hoy en día el principal talón de Aquiles de los países desarrollados

- El terrorismo informático debe ser visto como un acto similar a

un acto de guerra.

- Desde el punto de vista militar, se debe comenzar a trabajar en un Plan para asegurar los sistemas críticos militares, del gobierno y de los servicios de infraestructura básica: agua, electricidad, gas y comunicaciones.

Se debe tomar en cuenta de igual forma lo manifestado en la AG/RES. 2137 (XXXV-O/05), aprobada en la cuarta sesión plenaria, celebrada el 7 de junio de 2005, en donde se reafirma que el terrorismo, cualquiera sea su origen o motivación, no tiene justificación alguna y que, de conformidad con la Declaración de Puerto España, adoptada por los Estados Miembros en el quinto período ordinario de sesiones del CICTE, el terrorismo constituye una grave amenaza a la paz y la seguridad internacionales, socava los esfuerzos continuos que fomentan la estabilidad, prosperidad y equidad en los países de la región, y viola los valores y principios democráticos consagrados en la Carta de la OEA, la Carta Democrática Interamericana y otros instrumentos regionales e internacionales, que dicha declaración está en concordancia con Declaración de Quito, en la cual se expresa por medio de sus miembros su más enérgico rechazo a toda forma de terrorismo y su respaldo al trabajo del CICTE, en el marco de la VI Conferencia de Ministros de Defensa de las Américas, celebrada en nuestro país en la ciudad de Quito del 16 al 21 de noviembre de 2004, donde se pone énfasis en la facilitación del dialogo de los países miembros de la OEA a fin de desarrollar y avanzar medidas preventivas que anticipen y enfrenten las amenazas terroristas emergentes, como son los **DELITOS CIBERNÉTICOS.**

5.2.- La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

El crimen organizado trata principalmente de la búsqueda de ganancias y se lo puede entender, en términos Clausewitzianos[41] como una continuación de los negocios por medios delictivos esto a decir de **PHIL WILLIAMS** Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh. Por consiguiente, igual que las compañías de ladrillos y argamasa trasladan sus empresas al World Wide Web en procura de nuevas oportunidades de ganancias, las empresas delictivas están haciendo lo mismo. Las organizaciones criminales no son los únicos participantes en los mercados ilícitos, pero muchas veces son los más importantes, no sólo debido a la "competitividad" adicional que provee la amenaza de la violencia organizada. Además, las organizaciones criminales tienden a ser excepcionalmente hábiles en identificar y aprovechar oportunidades para nuevas empresas y actividades ilegales. En este contexto, la Internet y el crecimiento continuo del comercio electrónico ofrecen nuevas y enormes

[41] Se refiere al filósofo alemán KARL VON CLAUSEWITZ, reconocido por la máxima "*La guerra es una continuación de la política por otros medios*"

perspectivas de ganancias ilícitas[42].

Es por tanto que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que entró en vigor en septiembre de 2003, es el principal instrumento internacional en la lucha contra la delincuencia organizada. La Convención tiene 147 Estados Signatarios y 100 Estados Parte y de la cual el Ecuador es parte, en dicha convención se pone de manifiesto las reglas básicas sobre la prosecución de Delincuencia Organizada Transnacional, dichas reglas hacen especial mención de los delitos relacionados con la legitimación de activos y los de corrupción. También se mencionan a los llamados "*delitos graves*" que son de acuerdo con el Art. 2 toda "*conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave*". En el caso de las llamadas infracciones informáticas todas ellas son delitos graves de acuerdo a la definición de la Convención, en tal razón se encuadran en su ámbito de aplicación de la convención de conformidad al Art. 3, siempre que dichos delitos sean de carácter transnacional y entrañen la participación de un grupo delictivo organizado.

De igual forma se debe tomar en cuenta que la Convención da la posibilidad de conseguir capacitación y asistencia de parte de los Estados signatarios en la prevención e investigación de esta clase de delitos e insta a contar con programas de capacitación y entrenamiento a las personas responsables del cumplimiento de la ley como Jueces, Fiscales y Policías. También insiste en el uso de Técnicas Especiales de Investigación como la vigilancia electrónica.

5.5.- Convenio de Cibercriminalidad de la Unión Europea

Este convenio firmado el 21 de noviembre del 2001 en Budapest, el cual fue impulsado por el Consejo de Europa y otros países como Estados Unidos y Japón.

El convenio se compone principalmente de varios puntos entre ellos se tratan definiciones de términos que necesariamente son necesarios para comprender el espíritu del convenio, esto se lo hace en su artículo primero, incluyendo los conceptos de sistema, datos de tráfico o proveedor de servicios. En su capítulo II se dedica a las medidas que deben ser tomadas a nivel nacional, distinguiendo las referentes a las leyes sustantivas penales, y entre éstas los tipos contra la confidencialidad, la integridad y el acceso a los datos y sistemas, los tipos relacionados con los equipos, con el contenido, con la infracción de los derechos de propiedad intelectual y derechos afines, y también las referidas a los aspectos de procedimiento, como las condiciones y garantías, o también reglas

[42] **PHIL WILLIAMS,** Crimen Organizado y Cibernético, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. **http://www.pitt.edu/~rcss/toc.html**

jurisdiccionales. Su capítulo III se refiere a la cooperación internacional, y se divide en principios generales y otros relativos a la extradición, la asistencia mutua, las reglas aplicables cuando no existan acuerdos internacionales, y también en disposiciones específicas, y en otras dedicadas a las redes de comunicaciones. Finalmente, el capítulo IV está dedicado a las Disposiciones Finales, que tienen la forma y utilidad de este tipo de disposiciones en los otros Convenios del Consejo de Europa, dedicadas, por ejemplo, a la entrada en vigor, al acceso de otros países, a la aplicación territorial, los efectos del Convenio y otras cláusulas de este tipo, reservas, declaraciones, enmiendas, etcétera.

Esta Convención busca como objetivos fundamentales los siguientes:

(1) Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático;
(2) Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y
(3) Establecer un régimen dinámico y efectivo de cooperación internacional.

La Convención se basa en el reconocimiento fundamental de que se necesita armonizar las leyes nacionales. Es decir contar a nivel de Latinoamérica con una herramienta común tanto sustantiva como adjetiva para procesar este tipo de manifestaciones delictivas, procurando con este elemento comunitario en la parte sustantiva el mejoramiento de la cooperación internacional de los países miembros, ya que solamente existiría en esta materia, la aplicación de una ley común de carácter supranacional que permita a los gobiernos intercambiar información y pruebas. Sin embargo, para que esto de resultados y exista una verdadera cooperación hemisférica y ayuda jurídica mutua debe entrar en vigor este tipo de convenios a fin de unificar los tipos penales existentes sobre la delincuencia informática y así lograr la correlación o correspondencia entre los tipos penales en las diferentes jurisdicciones nacionales.

De hecho, cuanto más alcance tengan las leyes, tanto menor será el número de refugios desde la delincuencia informática organizada puede operar con impunidad.

La armonización es necesaria tanto para las leyes substantivas como las procesales como lo manifestamos anteriormente. Es por tanto que todos los países deben reevaluar y revisar sus reglamentos acerca de las pruebas, el registro e incautación de los efectos de esta clase de infracciones, la vigilancia electrónica oculta y otras actividades similares, que abarquen la información digital, los sistemas modernos de computación y comunicación y la naturaleza mundial de la Internet y sus diferentes servicios. Ya que al igual que las leyes sustantivas, una mayor coordinación de las leyes procesales facilitaría, de hecho, la cooperación en las investigaciones que trasciendan jurisdicciones múltiples.

A decir de **Oliver Muñoz Esquivel, l**a Convención sobre Delitos Informáticos constituye sin duda el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos. La misma tiene lugar en momentos en que el Internet ha dejado de ser tan solo el vehículo más idóneo para la propagación y perfeccionamiento de actos criminales bajo condiciones de anonimato, sino que además representa el entorno más frecuentemente utilizado para la financiación de este tipo de actividades. Corresponde ahora a los países latinoamericanos la responsabilidad de reconocer la importancia de establecer sanciones y mecanismos de investigación adecuados, que sean lo suficientemente avanzados y dinámicos como para hacer frente a este tipo de actividades delincuenciales que afectan a la raíz misma de nuestra sociedad, una sociedad que ha llegado a ser denominada por algunos como "**sociedad de la información**".

En este punto cabe resaltar que en la Declaración de Principios de la Cumbre de la Sociedad de la Información realizada en Ginebra en año 2005 se menciona en el punto B5 sobre **Fomento de la confianza y seguridad en la utilización de las Tecnologías de la Información (TIC)** que:

- El fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. Se deberían respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura global de ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad, al mismo tiempo que se amplía el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, y respetar los aspectos de la Sociedad de la Información orientados al desarrollo".
- Si bien se reconocen los principios de acceso universal y sin discriminación a las TIC para todas las naciones, apoyamos las actividades de las Naciones Unidas encaminadas a impedir que se utilicen estas tecnologías con fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales, y que podrían menoscabar la integridad de las infraestructuras nacionales, en detrimento de su seguridad. Es necesario evitar que las tecnologías y los recursos de la información se utilicen para fines criminales o terroristas, respetando siempre los derechos humanos.
- El envío masivo de mensajes electrónicos no solicitados ("spam") es un problema considerable y creciente para los usuarios, las redes e Internet en general. Conviene abordar los problemas de la ciberseguridad y "spam" en los planos nacional e internacional, según proceda.

De otro lado la INTERPOL en la 6ª Conferencia Internacional Sobre Ciberdelincuencia realizada en el Cairo (Egipto), el 13 al 15 de abril de 2005, recomendó a todos sus países miembros que:

- Que se utilice el Convenio sobre Ciberdelincuencia del Consejo de Europa como referencia en materia de normas internacionales procedimentales y legales mínimas para la lucha contra la ciberdelincuencia. Se instará a los países a suscribirlo. Este Convenio se distribuirá a todos los países miembros de INTERPOL en los cuatro idiomas oficiales.
- Que INTERPOL aumente sus esfuerzos dentro de la iniciativa sobre formación y normas operativas con objeto de proporcionar unos estándares internacionales para la búsqueda, el decomiso y la investigación de pruebas electrónicas.
- Que la formación y la asistencia técnica sigan considerándose prioritarias en la lucha internacional contra la ciberdelincuencia, incluidas la preparación de los cursos adecuados y la creación de una red internacional de escuelas de formación y de instructores, lo que implica el uso óptimo de herramientas y programas tales como los cursos itinerantes INTERPOL y los módulos de enseñanza en línea. Las iniciativas de formación y asistencia técnica deben ser transversales, y en ellas deben participar los sectores públicos y privado, entre las que figuran las universidades.
- Que se inicie y desarrolle la esencial cooperación y comunicación con instituciones supranacionales, como pueden ser las Naciones Unidas, y con entidades nacionales dedicadas a la lucha contra la ciberdelincuencia, y se impulse una respuesta rápida.
- Que la información relativa a casos de ciberdelincuencia se recopile en la base de datos de INTERPOL y se transmita en forma de resultados analíticos, a fin de ayudar a los países miembros a adoptar las estrategias de prevención apropiadas.
- Que se creen grupos de trabajo de INTERPOL sobre delincuencia informática en las regiones donde actualmente aún no existen. Los conocimientos adquiridos por los grupos de trabajo ya constituidos deberán utilizarse para apoyar la creación de los nuevos.
- Que la Secretaría General de INTERPOL organice una conferencia en la que participen, entre otros, representantes de los distintos organismos que trabajan en el ámbito de la justicia penal, a fin de determinar un marco para la cooperación en matera de lucha contra la ciberdelincuencia.
- Que INTERPOL encabece la promoción de estas recomendaciones, que son esenciales para combatir eficazmente la delincuencia informática y proteger a los ciudadanos de todo

el mundo en el ciberespacio.

5.4.- Nuevos retos en materia de seguridad

Como resultado del proceso de globalización y la difusión de la tecnología, se están produciendo cambios significativos en la naturaleza y el alcance de la delincuencia organizada. Una tendencia clave es la diversificación de las actividades ilícitas que realizan los grupos delictivos organizados, así como un aumento del número de países afectados por la delincuencia organizada. También se ha producido una expansión rápida de tales actividades en esferas como la trata de personas, el tráfico ilícito de armas de fuego, vehículos robados, recursos naturales, objetos culturales, sustancias que agotan la capa de ozono, desechos peligrosos, especies amenazadas de fauna y flora silvestres e incluso órganos humanos, así como el secuestro para la obtención de un rescate.

Los adelantos en la tecnología de las comunicaciones han determinado que surgieran nuevas oportunidades para la comisión de delitos sumamente complejos, en particular un aumento significativo del fraude en la Internet, y esas oportunidades han sido explotadas por los grupos delictivos organizados. La tecnología de las comunicaciones también confiere más flexibilidad y dinamismo a las organizaciones delictivas; el correo electrónico se ha convertido en un instrumento de comunicación esencial independiente del tiempo y la distancia.

Las autoridades encargadas de hacer cumplir la ley suelen adaptarse con lentitud a las nuevas tendencias, mientras que los grupos delictivos organizados tienden a adaptarse rápidamente y a aprovechar los adelantos tecnológicos debido a los inmensos beneficios que producen sus actividades ilícitas.

La apertura de nuevos mercados y las nuevas tecnologías de las comunicaciones, junto con la diversidad de actividades en las que participan, también han alimentado el crecimiento de la delincuencia organizada en los países en desarrollo. Los países con economías en transición o en situaciones de conflicto son particularmente vulnerables al crecimiento de ese tipo de delincuencia. En tales casos, la delincuencia organizada plantea una amenaza real para el desarrollo de instituciones reformadas, como la policía, los servicios de aduana y el poder judicial, que pueden adoptar prácticas delictivas y corruptas, planteando un grave obstáculo al logro de sociedades estables y más prósperas.

La delincuencia organizada y las prácticas corruptas van de la mano: la corrupción facilita las actividades ilícitas y dificulta las intervenciones de los organismos encargados de hacer cumplir la ley. La lucha contra la corrupción es, por lo tanto, esencial para combatir la delincuencia organizada. Es más, se ha establecido un nexo entre la delincuencia organizada, la corrupción y el terrorismo. Algunos grupos terroristas, por ejemplo, han recurrido a la

delincuencia organizada para financiar sus actividades. Por consiguiente, la promulgación de legislación apropiada, el fomento de la capacidad de hacer cumplir la ley y la promoción de la cooperación internacional para luchar contra las actividades de la delincuencia organizada y las prácticas corruptas conexas también fortalecen la capacidad de combatir el terrorismo.

5.5.- Seguridad Informática y Normativa

A fin de evitar los ataques por parte de la Delincuencia Informática ya sea Nacional o Transnacional se debe contar con dos variables importantes que son:

LA SEGURIDAD INFORMÁTICA que es el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya sean estos individuales o conectados a una red frente a posibles ataques accidentales o intencionados[43].

La seguridad Informática a su vez está dividida en cinco componentes a saber:

- **SEGURIDAD FÍSICA:** Es aquella que tiene relación con la protección del computador mismo, vela por que las personas que lo manipulan tengan la autorización para ello, proporciona todas las indicaciones técnicas para evitar cualquier tipo de daños físicos a los equipos informáticos.
- **SEGURIDAD DE DATOS:** Es la que señala los procedimientos necesarios para evitar el acceso no autorizado, permite controlar el acceso remoto de la información, en suma protege la integridad de los sistemas de datos.
- **BACK UP Y RECUPERACIÓN DE DATOS:** Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back Up de los sistemas informáticos. Permite recuperar la información necesaria en caso de que esta sufra daños o se pierda.
- **DISPONIBILIDAD DE LOS RECURSOS:** Este cuarto componente procura que los recursos y los datos almacenados en el sistema puedan ser rápidamente accesados por la persona o personas que lo requieren. Permite evaluar constantemente los puntos críticos del sistema para así poderlos corregir de manera inmediata.
- **LA POLÍTICA DE SEGURIDAD:** Conjunto de normas y criterios básicos que determinan lo relativo al uso de los recursos de una organización cualquiera.
- **ANÁLISIS FORENSE:** El Análisis Forense surge como consecuencia de la necesidad de investigar los incidentes de

[43] **El Autor**

Seguridad Informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales.

SEGURIDAD NORMATIVA derivada de los principios de legalidad y seguridad jurídica, se refiere a las normas jurídicas necesarias para la prevención y sanción de las posibles conductas que puedan ir en contra de la integridad y seguridad de los sistemas informáticos.

En definitiva para que exista una adecuada protección a los sistemas informáticos y telemáticos se deben conjugar tanto la seguridad informática como la seguridad legal y así poder brindar una adecuada protección y tutela tanto técnica como normativa.

Esto se refleja en algunas compañías o entidades gubernamentales siguen creyendo o tiene la idea por decirlo errónea que sus sistemas y redes informáticos no son blancos idóneos de un ataque, por cuanto no mantienen ni genera ningún tipo de información relevante, es decir información que valga la pena realizar un acceso no autorizado a dichos sistemas de procesamiento y transmisión de datos. Esto a decir del Profesor Davara Rodríguez lo podríamos llamar el **"SINDROME DEL HOMBRE INVISIBLE**[44]" o como el lo llama "**la seguridad de pasar desapercibido**", es decir que dichas compañías se creen inmunes a cualquier ataque informático por que no tienen una presencia visible y preponderante en la red, situación que no es así, ya que si bien su información no podría ser el blanco de un delincuente informático, si lo podrían ser los recursos de dicho sistema informático posee, por ejemplo su capacidad de procesamiento, su capacidad de almacenamiento y de interconexión, en esta situación hace atractiva la idea de tomar dicho sistema como un medio por ejemplo para descifrar o romper claves de acceso utilizando sistemas zombis como alguna vez lo hizo uno de los primeros Hackers, KEVIN MITNICK alias **EL CONDOR,** quien a través de la ingeniería social y un troyano logro capturar toda la red de procesamiento de una Universidad Norteamericana para romper el código encriptado de un programa de Netcom On-Line Comunications desarrollado por **TSUTOMU SHIMOMURA** un especialista en seguridad informática. Por tanto el deseo del agresor puede meramente consistir en un lugar donde almacenar su compendio de números de tarjetas de crédito, o sus programas ilegalmente obtenidos, sus crackeadores, o pornografía.

Esto es el reflejo de la falta de conciencia en el uso de las TIC dentro de la Sociedad de la Información por parte de los usuarios, quienes no tienen un nivel de capacitación suficiente o directivas claras de lo que implica el manejo, creación y transmisión de información importante, no solo la personal, si no también la profesional y corporativa, y de sus posibles vulnerabilidades.

[44] **El Autor.**

En resumen la Seguridad Informática y Normativa debe usarse para impedir los ataques ya sean fuera del sistema (virus, syware, adware, etc) y dentro del mismo, exigiendo políticas claras y precisas sobre el nivel de acceso a cierta información de carácter confidencial y una debida protección a esta.

6.- El Delito Informático y su realidad procesal en el Ecuador

Desde que en 1999 en el Ecuador se puso en el tapete de la discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros. También se conformo comisiones para la discusión de la Ley y para que formulen observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven el Comercio Telemático una buena oportunidad de hacer negocios y de paso hacer que nuestro país entre en el boom de la llamada Nueva Economía.

Cuando la ley se presento en un principio, tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal de dicha ley, ya que las infracciones a la misma es decir los llamados Delitos Informáticos, como se los conoce, se sancionarían de conformidad a lo dispuesto en nuestro Código Penal, situación como comprenderán era un tanto forzada, esto si tomamos en cuenta los 65 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por decirlo menos, para dar seguridad al Comercio Telemático ante el posible asedio de la *criminalidad informática*.

Por fin en abril del 2002 y luego de largas discusiones los honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.

De acuerdo a la Constitución Política de la República, en su Título X, Capitulo 3ro al hablar del Ministerio Público, en su Art. 219 inciso primero señala que: "**El Ministerio Público prevendrá en el conocimiento de las causas**, **dirigirá y promoverá la investigación pre-procesal y procesal penal**. Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "**el ejercicio de la acción pública corresponde exclusivamente al fiscal**". De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto preprocesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá llevar como quien dice la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su

órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control Ministerio Público, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante del Ministerio Público a emitir su dictamen correspondiente.

Ahora bien el problema que se advierte por parte de las instituciones llamadas a perseguir las llamadas infracciones informáticas es la falta de preparación en el orden técnico tanto del Ministerio Público como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos, de igual manera falta la suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que lo auxiliara en dicha tarea, dado que no existe hasta ahora en nuestra policía una Unidad Especializada, como existe en otros países como en Estados Unidos donde el FBI cuenta con el Computer Crime Unit, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de infracciones. De otro lado también por parte de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados en tratándose de estos temas, ya que en algunas ocasiones por no decirlo en la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.

Por tanto es esencial que se formen unidades Investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos.

La cooperación multilateral de los grupos especiales multinacionales pueden resultar ser particularmente útiles - y ya hay casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales.

De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar. Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de

delincuentes que expone a los gobiernos, las empresas y los individuos a estos peligros.

Es por tanto como manifiesta **PHIL WILLIAMS** Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh[45], Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos transnacionales.

Es por estas razones que el Ministerio Público tiene la obligación Jurídica en cumplimiento de su mandato constitucional de poseer un cuerpo especializado para combatir esta clase de criminalidad a fin de precautelar los derechos de las víctimas y llevar a los responsables a juicio, terminando así con la cifra negra de esta clase de infracciones, ya que en la actualidad esta clase de conductas ilícitas no son tratadas en debida forma por los órganos llamados a su persecución e investigación, así por ejemplo un tipo de delito actualmente en boga en nuestro país es el llamado **CARDING (**utilización de tarjetas magnéticas, ya sean hurtadas o clonadas para defraudar mediante la técnica de manipulación de datos de salida) y, el cual que es una modalidad de Fraude Informático, mismo que es considerado por la Policía Judicial como una clase de estafa, lo que desde el punto de vista de la clasificación típica del delito es incorrecta ya que no es una estafa, tomando en cuenta los elementos típicos de este tipo de delitos, lo que si es una clase de defraudación, pero la solución doctrinaria y típica a dicha modalidad delictual es equipararla al robo calificado, en razón que la tarjeta magnética es considerada como una llave.

7.- Problemas de Persecución.

Este tipo de infracciones son difícilmente descubiertas o perseguidas ya que los sujetos activos actúan sigilosamente, y poseen herramientas capaces de borrar todo rastro de intrusión o la consumación del delito, pero a pesar de eso y de no contar ni con una policía entrenada para investigar dichos hechos, ni un Ministerio Público que pueda dar las directrices para la correcta indagación de dichos actos delictivos, por no contar entre otras con una Unidad Especial para la investigación y persecución de estas infracciones informáticas, existen dos problemas principales que a continuación se exponen:

[45] **WILLIAMS PHIL,** Crimen Organizado y Cibernético, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. **http://www.pitt.edu/~rcss/toc.html**

7.1.- Problemática con la concepción tradicional de tiempo y espacio.

Esta característica de transnacional de la delincuencia informática es otro de los problemas de perseguibilidad. Tradicionalmente se ha considerado que la ley penal solo se aplica en el territorio de la República, hecho que constituye el llamado "principio de territorialidad de la ley", el mismo que se encuentra tipificado como ya se menciono en el art. 5 del Código Penal. El principio de territorialidad sostiene que la ley penal de un país es aplicable cuando la infracción ha sido cometida dentro del territorio, en el momento actual esto puede haber cambiado teniendo en cuenta que el nuevo escenario en donde mayormente se da este tipo de delitos es el Ciberespacio, un lugar donde no existen fronteras territoriales, y que de acuerdo a **Jhon Perry Barlow**, quien publico lo que se llama **LA DECLARACIÓN DE INDEPENDENCIA DEL CIBERESPACIO**, en donde manifiesta: *"Gobiernos del mundo industrializado, gigantes obsoletos , de la nueva morada del espíritu (...) No os queremos entre nosotros, en el terreno donde nos reunimos no sois soberanos.. Vuestros conceptos jurídicos de propiedad, de expresión, de identidad, de movimiento y de contexto no se aplican a nosotros. Están basados en la materia"*[46]

Por lo dicho se puede constatar de prima facie que es difícil la persecución de estos delitos y su enjuiciamiento, ya que existe la posibilidad de preparar y cometer acciones delictivas informáticas en perjuicio de terceros en tiempo y espacio lejanos.

Debido a los adelantos de las telecomunicaciones y la telemática, hace que las distancias reales o fronteras entre países no existan como ya se ha dicho, ya que una persona puede realizar un acto delictivo en un lugar distinto del lugar de los hechos, como por ejemplo los creadores de MALWARE o de los VIRUS INFORMÁTICOS como el conocido: I LOVE YOU, el mismo que fue diseñado y creado en Filipinas y causo daños a nivel mundial en cuestión de días. Por otro lado, la posibilidad de realizar programas de efecto retardado como las llamadas bombas lógicas, las cuales no desatan su poder destructivo, hasta tiempo después de que el autor material de la infracción este a "buen recaudo"; o que con determinadas ordenes, rutinas y subrutinas de algunos programas se puede preparar el cometimiento de una infracción como la del fraude informático, y en el momento que esto sucede el hechor se encuentra realizando una tarea completamente incompatible con el acto delictivo cometido.

La territorialidad de la ley es considerada como un principio de soberanía del estado y se resume al decir que no se puede aplicar al ecuatoriano delincuente otra ley que no sea la ecuatoriana, aclarando que no importa el lugar donde se encuentre el delincuente, es decir, sin importar el país en donde se haya cometido el delito.

---

[46] **BARLOW, Jhon Perry,** Publicación hecha en el sitio Web: www.eff.org/pub/publications/Jhon_perry_barlow/barlow_0296

Este principio denota algunas características como las siguientes:

- La ley penal es aplicable a los hechos punibles cometidos dentro del territorio del Estado, sin consideración a la nacionalidad del actor.
- No se toma en cuenta la nacionalidad del autor.
- Se toma en cuenta el lugar de comisión del delito. Nuestra legislación se inclina por la teoría del resultado, es decir que la INFRACCIÓN se entiende cometida en el territorio del Estado cuando los *efectos de la acción u omisión* deban producirse en el Ecuador o en los lugares sometidos a su jurisdicción.
- Se aplica al concepto jurídico de territorio por el Derecho Internacional: los límites del Estado, mar territorial. Espacio aéreo.
- Se aplica también la teoría del **territorio flotante** o **Principio de la bandera**: Naves o aeronaves de bandera nacional ya sea que se encuentren en alta mar, en su espacio aéreo y en lugares en que por la existencia de un convenio internacional, ejerzan jurisdicción. Este principio no se aplica cuando las naves o aeronaves MERCANTES ESTÉN SUJETAS A UNA LEY PENAL EXTRANJERA.

El ámbito de aplicación de este principio esta en:

1.- Territorio Continental
2.- Espacio Aéreo
3.- Mar Territorial
4.- Naves y aeronaves ecuatorianas de guerra o mercantes.
5.- Infracciones cometidas en el recinto de una **Legación ecuatoriana en país extranjero.**

7.1.1.- Principios de extraterritorialidad

Tres son los principios que constituyen el principio de extraterritorialidad y son los siguientes: el principio de la nacionalidad o personalidad, el principio de la defensa y el principio de la universalidad y justicia mundial.

A.- Principio de la nacionalidad o personalidad.

Según este, se debe aplicar al delincuente únicamente la ley que corresponde a su nacionalidad, es decir, la ley del país de su origen, sea el país que sea en el que haya cometido el delito. Este principio tiene dos divisiones:

A.- PRINCIPIO DE LA NACIONALIDAD ACTIVA.- Se funda en la obediencia que se exige al súbdito ecuatoriano con respecto a su legislación. Se toma en cuenta la nacionalidad del autor del delito.

B.- PRINCIPIO DE LA NACIONALIDAD PASIVA.- El alcance espacial de la ley se extiende en función *del ofendido o titular del bien jurídico*

protegido. Se aplicaría cuando está en juego la protección de los bienes jurídicos individuales

B.- Principio de la defensa.-

Este nos dice que es aplicable la ley del país donde los principios son atacados por el delito, sin tomar en cuenta la nacionalidad de los realizadores. Se toma en cuenta la nacionalidad del bien jurídico protegido, es decir se aplica este principio cuando se afecta la integridad territorial. Quedando en juego la protección de los bienes nacionales. Ha sido tomado por algunos países, como por ejemplo el nuestro el cual puede pedir la extradición de una delincuente informático que haya vulnerado bienes jurídicos protegidos en nuestro país como resultado de su acción delictiva. Claro que esta norma no puede ser aplicada en todos los países ya que algunos de ellos como el nuestro prohíbe la extradición de ecuatorianos que hayan cometido una infracción en otro país, en este caso se aplica un principio de equivalencia, es decir si el delito cometido en el otro país se encuentra tipificado en el nuestro también puede seguirse el proceso penal por el cometimiento de dicho delito, pero en nuestro país.

C.- Principio de la universalidad y justicia mundial.

Este principio se refiere a que es aplicable la ley del país que primero aprese al delincuente, sin considerar otro aspecto.

Este principio tiene una finalidad práctica para reprimir los delitos contra la humanidad, aquellos que han sido catalogados como tales en virtud de ser considerados como ofensores de toda la humanidad. Para ello es necesario firmar convenios internacionales y unilaterales con el fin de que cada país pueda sancionar al delincuente con su propia ley, sin importar el lugar donde el individuo haya cometido el acto ni tampoco la nacionalidad del mismo.

Se prescinde tanto de la nacionalidad del autor como del lugar de comisión del delito, se fundamenta en el principio de **solidaridad de los estados en la lucha contra el delito.**

En doctrina penal se concede en virtud de este principio eficacia extraterritorial a la ley penal; pero en el Derecho Internacional condiciona esta eficacia extraterritorial tomando en cuenta:

- La calidad del bien jurídico protegido, como bienes culturales supranacionales.
- Cuando los autores del delito sean peligrosos para todos los estados.

En cuanto a los delitos informáticos de carácter transnacional, en especial el Ciberterrorismo es necesario aplicar este principio por cuanto la peligrosidad de este tipo de ataques puede causar más daño que el terrorismo convencional.

7.2. Anonimato del Sujeto Activo.

El sujeto activo de esta clase de infracciones puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que este no necesariamente puede usar su propio sistema informático, sino que se puede valer de un tercero, como por ejemplo en el caso del envión de correo no deseado o SPAM, en el cual se puede usar a una máquina *zombi,* es decir una computadora que está bajo el control del SPAMER y que le permite usarla como una estación de trabajo de su propia red de máquinas zombis, las cuales pertenecen a usuarios desaprensivos que no tienen al día sus medidas de seguridad y que son fácil presa de los hackers y crakers para cometer este tipo de infracciones. También existen programas de enmascaramiento o que no permiten ver la verdadera dirección ya sea de correo electrónico o del numero IP.

8.- Glosario de Términos

- **ACTIVO PATRIMONIAL:** Conjunto de bienes y derechos que integran el haber de una persona física o jurídica.
- **BASE DE DATOS:** Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.
- **BROWSER (BUSCADOR):** El software para buscar y conseguir información de la red WWW. Los más comúnmente usados son Microsoft Explorer, Firefox y Opera.
- **COOKIE**: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que esta haciendo. Hay una variedad de "anti-cookie" software que automáticamente borra esa información entre visitas a su sitio.
- **DIALUP (MARCAR)**: El método de conectarse con Internet vía la línea de teléfono normal mediante un modem, en vez de mediante una LAN (Red Local) o de una línea de teléfono alquilada permanentemente. Esta es la manera mas común de conectarse a Internet desde casa si no ha hecho ningún arreglo con su compagina de teléfono o con un ISP. Para conexiones alternativas consulte con su ISP primero.
- **DIGITAL SIGNATURE (FIRMA DIGITAL)**: El equivalente digital de una firma autentica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma escribió o autorizo el Archivo.
- **DOCUMENTO ELECTRÓNICO:** Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles de

ser presentados en una forma humanamente comprensible[47].

- **DOMAIN NAME (NOMBRE DE DOMINIO)**: Un nombre de dominio es su propiedad en el mundo cibernético. Esta propiedad, tal y como su homologo tangible, tiene valor dependiendo de su dirección y de su contenido. Usted puede cobrar a sus invitados o darles un tour gratis, o llevar un negocio paralelo como parte de la propiedad. Igual que una dirección de la 5 Avenida que es limitada y también más valorada que la inmensa mayoría de las demás direcciones, el valor de su dominio puede variar de unos cuantos dólares por ejemplo, algunos están en el millón de dólares. No le podemos decir que muebles, obras de arte, o negocio paralelo debe tener en su propiedad en el mundo cibernético, pero su dirección es bien segura que realzara el valor de su contenido, o igual lo eliminara si ese nombre no atrae clientes. Técnicamente, es un concepto creado para identificar y localizar computadoras en Internet. Los nombres de dominio son un sistema de direcciones de Internet fácil de recordar, que pueden ser traducidos por el Sistema de Nombres de Dominio a las direcciones numéricas usadas en la red. Un nombre de dominio es jerárquico y usualmente acarrea información sobre el tipo de entidad que usa ese nombre de dominio. Un nombre de dominio es simplemente una etiqueta que representa un dominio, que a su vez es un subgrupo del total del espacio de nombres del dominio. Nombres de dominio en el mismo nivel jerárquico tienen que ser únicos: solo puede haber un .com al nivel más alto de la jerarquía, y solo un DomainMart.com en el siguiente nivel.
- **FTP O FILE TRANSFER PROTOCOL (PROTOCOLO DE TRANSFERENCIA DE FICHERO)** Un estándar de Internet para transferir ficheros entre ordenadores. La mayoría de las transferencias FTP requieren que usted se meta en el sistema proveyendo la información mediante un nombre autorizado de uso y una contraseña. Sin embargo, una variación conocida como "FTP anónimo" le permite meterse como anónimo: no necesita contraseña o nombre.
- **HTML (HYPER TEXT MARKUP LANGUAGE)**: El lenguaje de computador usado para crear paginas de red para Internet. Aunque estándares "oficiales" de Internet existen, en la práctica son extensiones del lenguaje que compañías como Netscape o Microsoft usan en sus buscadores (browsers).
- **HTTP (HYPER TEXT TRANSPORT PROTOCOL)**: El conjunto de reglas que se usa en Internet para pedir y ofrecer paginas de la red y demás información. Es lo que pone al comienzo de una dirección, tal como "http:/," para indicarle al buscador que use

[47] Definición dada por EDIFORUM.(Foro de Intercambio Electrónico de Datos)

ese protocolo para buscar información en la pagina.

- **INTERNET PROTOCOL (IP) NUMBERS O IP ADRESSES (PROTOCOLO DE INTERNET, NÚMEROS)**: Un identificador numérico único usado para especificar anfitriones y redes. Los números IP son parte de un plan global y estandarizado para identificar computadores que estén conectados a Internet. Se expresa como cuatro números del 0 al 255, separado por puntos: 188.41.20.11. La asignación de estos números en el Caribe, las Américas, y África la hace la American Registry for Internet Numbers.
- **INTERNET SERVICE PROVIDER (ISP) (PROVEEDOR DE SERVICIO DE INTERNET)** Una persona, organización o compagina que provee acceso a Internet. Además del acceso a Internet, muchos ISP proveen otros servicios tales como anfitrión de Red, servicio de nombre, y otros servicios informáticos.
- **MENSAJE DE DATOS:** Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.
- **MODEM**: Un aparato que cambia datos del computador a formatos que se puedan transmitir mas fácilmente por línea telefónica o por otro tipo de medio.
- **SISTEMA TELEMÁTICO.** Conjunto organizado de redes de telecomunicaciones que sirven para trasmitir, enviar, y recibir información tratada de forma automatizada.
- **SISTEMA DE INFORMACIÓN:** Se entenderá como sistema de información, a todo sistema utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma de mensajes de datos[48].
- **SISTEMA INFORMÁTICO:** Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.
- **SOCIEDAD DE LA INFORMACIÓN:** La revolución digital en las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de información, ideas y conocimientos en todo el planeta. Ha causado una impresión profunda en la forma en que funciona el mundo. La Internet se ha convertido en un recurso mundial importante, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial, como para el mundo en desarrollo por su función de pasaporte para la participación equitativa y para el desarrollo económico, social y educativo.
- **SOPORTE LÓGICO:** Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que

[48] Definición entregada por La Ley Modelo de Comercio Electrónico de la UNCITRAL

pueden ser empleados para registrar información en un sistema informático.

- **SOPORTE MATERIAL:** Es cualquier elemento corporal que se utilice para registrar toda clase de información.
- **TELEMÁTICA:** neologismo que hace referencia a la comunicación informática, es decir la transmisión por medio de las redes de telecomunicaciones de información automatizada.
- **TCP/IP: TRANSMISIÓN CONTROL PROTOCOL/INTERNET PROTOCOL:** Conjunto de protocolos que hacen posible la interconexión y tráfico de la Red Internet

9.- Bibliografía

ALESTUEY DOBÓN, María del Carmen. "Apuntes sobre la perspectiva criminológica de los delitos informáticos", Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi.

ÁLVAREZ DE LOS RÍOS, José Luis. "Delitos Informáticos". Ponencia en las Jornadas sobre Marco Legal y Deontológico de la Informática, Mérida 17 de septiembre de 1997.

ANDRADE SANTANDER, Diana. El Derecho a la Intimidad, Centro Editorial Andino, Quito – Ecuador, 1998.

BAÓN RAMÍREZ, Rogelio. "Visión general de la informática en el nuevo Código Penal", en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996.

BARATTA Alessandro: Derecho Penal Mínimo, Editorial Temis S.A. Santa Fe de Bogotá, Colombia, 1999.

BARBIERI Pablo, Contratos de Empresa, Editorial Universidad, Buenos Aires, Argentina, 1998.

BARRIUSO RUIZ, Carlos. "Interacción del Derecho y la informática", Dykinson, Madrid, 1996, pág. 245 a 252.

BECCARIA Alessandro, De los Delitos y las Penas, Editorial Temis S.A. Santa Fe de Bogotá, Colombia, 1997.

BERDUGO GOMEZ DE LA TORRE, Ignacio: Honor y libertad de expresión. Tecnos. Madrid, 1.987.

BETTIOL Giusseppe, Derecho Penal, Editorial Temis, Bogotá, Colombia, 1990

BUENO ARÚS, Francisco. "El delito informático", Actualidad Informática Aranzadi Nº 11, abril de 1994.

CABANELLAS, Guillermo, Diccionario de Derecho Usual, Tomo 1, Editorial Heliasta. 1990.

CANO JEIMY, Inseguridad Informática: Un concepto dual de la Seguridad Informática. Universidad UNIANDES 1994

CASTILLO JIMENEZ, María Cinta, RAMALLO ROMERO, Miguel. El delito informático. Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático. 22-24 junio 1989.

CHOCLAN MONTALVO, José Antonio. "Estafa por computación y criminalidad económica vinculada a la informática", Actualidad Penal Nº 47, 22-28 diciembre 1997

CORREA Carlos María, El Derecho Informático en América Latina, Publicado en Derecho y Tecnología Informática, Edit. Temis, Bogotá, Mayo de 1990.

CREUS Carlos, Derecho Penal Parte Especial, Edit. Astrea, Buenos Aires, 1998, Tomo 2.

CUERVO José, Delitos Informáticos y Protección Penal a la Intimidad, Publicación hecha en Internet URL: www.derecho.org

DALLAGLIO Edgardo Jorge, "La Responsabilidad Derivada de la Introducción y

Propagación del Virus de las Computadoras", publicado en El Derecho, año 1990.

DAVARA RODRÍGUEZ, Miguel Angel, Análisis de la Ley de Fraude Informático, Revista de Derecho de UNAM. 1990.

DAVARA RODRÍGUEZ, Miguel Ángel. "De las Autopistas de la Información a la Sociedad Virtual", Editorial Aranzadi, 1996.

DAVARA RODRÍGUEZ, Miguel Ángel. "Manual de Derecho Informático", Editorial Aranzadi, Pamplona, 1997.

DONOSO ABARCA, Lorena, Análisis del tratamiento de las figuras Relativas a la Informática tratadas en el título XIII del Código Penal Español de 1995.

FERNÁNDEZ CALVO, Rafael. "El Tratamiento del llamado "Delito Informático" en el proyecto de Ley Orgánica de Código Penal: Reflexiones y propuestas de la CLI (Comisión de Libertades e Informática), Informática y Derecho Nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996.

FERREYROS SOTO, Carlos. "Aspectos Metodológicos del Delito Informático", Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996

FÍGOLI PACHECO, Andrés. El Acceso No Autorizado a Sistemas Informáticos, Uruguay 1998, Publicación hecha en Internet, www.derecho.org.

FROSINI Vitorio, Informática y Derecho, Editorial Temis, Bogotá, Colombia, 1988.

FUMIS Federico, Informática y Derecho de Daños, Boletín Hispanoamericano de Informática y Derecho, 1998, Buenos Aires, Argentina. URL: Http//ww.ulpiano.com

GARCÍA GIL, F. Javier. "Código Penal y su Jurisprudencia. Adaptada a la Ley Orgánica 10/1995, de 23 de noviembre", Editorial Edijus, Zaragoza, 1996.

GARCÍA VITORIA, Aurora. El Derecho a la Intimidad en el Derecho Penal y en la Constitución de 1978. Editorial Aranzadi, Pamplona – España, 1983.

GÓMEZ PERALS, Miguel. "Los Delitos Informáticos en el Derecho Español", Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi.

GUASTAVINO, Elías P., Responsabilidad Civil y otros problemas jurídicos en computación, Ediciones La Rocca, Buenos Aires, 1987.

GUIBOURG Ricardo A., ALENDE Jorge O., CAMPANELLA Elena M., Manual de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires, Argentina.

GUTIÉRREZ FRANCÉS, María Luz, Fraude Informático y estafa.

GUTIÉRREZ FRANCÉS, Mª Luz. "Fraude informático y estafa", Centro Publicaciones del Ministerio de Justicia, Madrid, 1991.

HANCE OLIVIER. Leyes y Negocios en Internet. México. De. Mc Graw Hill Sociedad Internet. México. 1996.

HANSSENER Winfried, "Derecho Penal", Editorial Azalea, 1998.

HEREDERO HIGUERAS, Manuel. "Los Delitos Informáticos en el proyecto de

Código Penal de 1994", Informática y Derecho Nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996.

HERNÁNDEZ GUERRERO, Francisco. "Delitos Informáticos", Ponencia Jornadas sobre el Marco Legal y Deontológico de la Informática, Mérida, 17 de septiembre de 1997.

HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur.

HULSMANN Louk, Derecho Penal, 1982

JIJENA LEIVA, Renato, Chile: Protección Penal a la Intimidad y los Delitos Informáticos, Editorial Jurídica de Chile, 1993.

JOVER PADRÓ, Joseph. "El Código Penal de la informática", X Años de Encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi Editorial, Pamplona, 1997.

LARREA HOLGUÍN, Juan, Derecho Civil del Ecuador, Los bienes y la posesión, Tercera Edición, Corporación de Estudios y Publicaciones.

LIMA DE LA LUZ, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. . No. 1-6. Año L. Enero - Junio 1984.

MADRID-MALO GARIZABAL Mario, Derechos Fundamentales, Escuela Superior de Administración Pública, Santa Fe de Bogotá – Colombia, 1992.

MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

MANZANARES, José Luis y CREMADES, Javier. "Comentarios al Código Penal"; La Ley- Actualidad, Las Rozas (Madrid), 1996.

MERLAT, Máximo, Seguridad Informática: Los Hackers, Buenos Aires Argentina, 1999, Publicación hecha en Internet. www.monografías.com

MIR PUIG Santiago, Función de la Pena y la Teoría del Delito en el Estado Social y Democrático de Derecho, Bosch, 1979

MORAL TORRES, Anselmo del. "Aspectos sociales y legales de la seguridad informática", Ponencia 1ª Jornadas sobre "Seguridad en Entornos Informáticos", Instituto Universitario "General Gutiérrez Mellado", Madrid 12 de marzo de 1998.

MORALES PRATS, Fermín. "El Código Penal de 1995 y la protección de los datos personales", Jornadas sobre el Derecho español de la protección de datos personales, Madrid, 28 al 30 octubre de 1996, Agencia de Protección de Datos, Madrid, 1996, pág. 211 a 250.

NOVOA MONREAL EDUARDO, Curso de Derecho Penal, 1966, Universidad de Chile.

PALAZZI Pablo Andrés, Virus Informáticos y Responsabilidad Penal, sección doctrina del diario La Ley, 16 de diciembre de 1992. Http://ulpiano.com

PARELLADA, Carlos Alberto, Daños en la actividad judicial e informática desde la responsabilidad profesional, Ed. Astrea, Buenos Aires, 1990.

PÉREZ LUÑO, Antonio Enrique. "Ensayos de informática jurídica", Biblioteca de Ética, Filosofía del Derecho y Política, México, 1996.

PÉREZ LUÑO, Antonio Enrique. “Manual de informática y derecho”, Editorial Ariel S.A., Barcelona, 1996.

PIERINI Alicia, LORENCES Valentín, TORNABENE María Inés, Hábeas Data, Derecho a la Intimidad, Editorial Universidad, Buenos Aires – Argentina, 1998.

RADBRUCH Gustav, Teoría General del Derecho, 1990

REYNA ALFARO Luis Miguel, Fundamentos para la protección penal de la información como valor económico de la empresa. Publicación hecha en internet en www.dercho.org.pe.

RESA NESTARES CARLOS: Crimen Organizado Transnacional: Definición, Causas Y Consecuencias, Editorial Astrea, 2005.

RIVERA LLANO, Abelardo, Dimensiones de la Informática en el Derecho, Ediciones Jurídicas Radar, Bogotá, Colombia. 1995.

ROMEO CASABONA, Carlos María. “Delitos informáticos de carácter patrimonial”, Informática y Derecho Nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.

ROMEO CASABONA, Carlos María. “Los llamados delitos informáticos”, Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995.

ROMEO CASABONA, Carlos María. “Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información”, FUNDESCO, Colección impactos, Madrid, 1987.

RUIZ VADILLO, Enrique. “Responsabilidad penal en materia de informática”, Informática y Derecho Nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.

RUIZ VADILLO, Enrique. “Tratamiento de la delincuencia informática como una de las expresiones de criminalidad económica”, Poder Judicial número especial IX, 1989.

SALT G. Marcos, Informática y Delito, Publicación en Internet, URL: http://www.derecho.org.ar

SANTOS Jaime Eduardo y GUERRERO M María Fernanda. Fraude Informático en el Banca, Ed. Jesma, Bogotá, 1993

SERRANO GÓMEZ, Alfonso. “Derecho Penal. Parte Especial I. Delitos contra las personas”, Dykinson, Madrid, 1996.

SOLANO BÁRCENAS, Orlando, Manual de Informática Jurídica, Editorial Jurídica Gustavo Ibáñez, Santa Fe de Bogotá D.C. Colombia 1997.

TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Editorial Temis 1999.

TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Situación en México”, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, pág. 461 474.

TIEDEMANN, Klauss. “Poder económico y delito”, Barcelona, 1985.

TORTRAS Y BOSCH, Carlos. “El delito informático”, número 17 monográfico de ICADE, Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales.

VELÚ, Jacques. Convención Europea de Derechos Humanos: El respeto a la Intimidad en el hogar y las comunicaciones. Publicación hecha en

Internet www.google.com

WILLIAMS PHIL, Crimen Organizado y Cibernético, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. http://www.pitt.edu/~rcss/toc.html

ZABALA BAQUERIZO Jorge, Delitos contra la Propiedad, Tomo 2, Editorial Edino, Guayaquil, Ecuador, 1988.

ZANONI Leandro. Los Hackers, la nueva cara de los piratas de Fin de siglo, Revista de Informática y Derecho. De Palma, Buenos Aires Argentina 1998.