UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

CARRERA DE DERECHO

TESIS DE GRADO

TEMA: **LOS DELITOS INFORMÁTICOS**

AUTOR: **AB. FABIÁN ALTAMIRANO DÁVILA**

QUITO – ECUADOR

2001 - 2002

CONTENIDO

DEDICATORIA

A Dios y al Sagrada Virgen Dolorosa, por ser mi guía espiritual
A mis padres Carlos y Marcela, por su ejemplo y apoyo incondicional
A mis hermanas Francia y Sylvita, por estar siempre a mi lado
A mis sobrinos Carlos, Macarena y Mauricio y a mi primo Roberto, para que este esfuerzo sirva de ejemplo en su vida estudiantil

AGRADECIMIENTO

A la Universidad Internacional "SEK"
Al claustro académico
Al Dr. José Luis Barzallo, por sus concejos y ayuda, durante este proceso de investigación

INTRODUCCIÓN

El mundo en el que vivimos ha experimentado una gran variedad de cambios, el hombre por su parte se adapta y modifica su accionar de acuerdo a sus necesidades y, a los instrumentos que según cada época podía crear, utilizar o adquirir. Estos cambios sin duda adecuan la conducta humana, cada creación o cada invento tiene como finalidad la utilización por parte de los hombres, sea como fin social o económico.

Es innegable que en nuestros días nos encontramos en una nueva era, para muchos tecnológica o electrónica pero generalmente denominada ***"ERA INFORMATICA"***, este proceso de transformación si bien trajo consigo una serie de beneficios, especialmente a las grandes empresas, ha sido también el impulsador de una forma de conductas criminales antes desconocidas, que han revolucionado las tradicionales teorías tanto del delito, como de los autores del mismo.

Esta revolución informática alcanza su mayor expresión en lo que muchos han llamado *La sociedad de la información,* entendiendo como tal, a ese grupo extenso al que abarca y acoge la nueva era informática, en la que los sistemas computacionales alcanzan un desarrollo incalculable, siendo la sociedad el pilar fundamental que sustenta esta nueva época, es una etapa de transición de la era industrial a la era informática, esta nueva sociedad en la que nos encontramos encierra en su círculo, no solo formas de expresión y comunicación, sino también sistemas de educación y evaluación, cooperación internacional y desarrollo tecnológico de los diversos estados.

El hablar de la sociedad de la información, es remontarnos a los antecedentes norteamericanos del Plan Gore de 1993, y al europeo del Plan Delors, que se referían al crecimiento de la sociedad en lo que denominaron "mundo multimedia", surgiendo para 1994 el Informe Bangemann que definió a la sociedad de la información bajo los siguientes términos "Es una revolución basada en la información, la cual es en sí misma expresión del conocimiento humano. Esta revolución dota a la inteligencia humana de nuevas e ingentes capacidades, y constituye un recurso que alerta el modo en que trabajamos y vivimos. La educación, la información y la promoción desempeñarán necesariamente un papel fundamental".[1]

Las nuevas formas de comunicación vienen acompañadas de varios términos propios de esta nueva etapa, tales como alfabetización electrónica, ciberespacio, firma digital, certificado electrónico, comercio electrónico o delito informático, es decir hablamos de un mundo digitalizado en el que todo lo que al hombre le es intrínseco va adjunta una connotación jurídica, el nacer, morir, o contratar tiene necesariamente que ver con el mundo del Derecho y sus normas, y esta nueva época no puede estar al margen de leyes que regulen su normal desenvolvimiento.

La creación de un computador, no solo vino ha ser el eje propulsor de esta nueva época, el afán inventivo del hombre, llevo a perfeccionar cada vez más estos aparatos, que de una u otra forma llegaron para alivianar el trabajo diario del ser humano, reemplazó a las máquinas de escribir manuales y electrónicas o a las calculadoras, y se convirtieron en instrumentos necesarios de trabajo, desde la oficina

[1] **FERNÁNDEZ ALLER,** Cecilia, y otro, Informática para Abogados, Pág. 34 - 35

más simple, hasta los estudios cinematográficos más grandes del mundo los convirtieron en su arma principal de labores.

Sin embargo, no todo lo que el hombre crea tiene solo beneficios y bondades, estos aparatos, se fueron convirtiendo de a poco, ya no solo en instrumentos de trabajo, sino en verdaderas armas, que de algún modo podrían llevar a la destrucción total de la humanidad, pero sin tratar de ser extremistas, la verdad es que el hombre, si a creado una forma de beneficiarse de manera negativa de los mismos, así como dijimos adapta su conducta una nueva forma de expresión delictiva.

Los sistemas computacionales, se han convertido en el mejor método de comunicación, ya no solo escrita sino incluso visual, la constante investigación y creación humana, ha llegado a límites insospechados quizá hasta hace apenas diez o quince años atrás, hoy en día, el sistema de comunicaciones es tan amplio en todo el planeta, que casi nadie esta exento o ha quedado rezagado de esta nueva forma de expresión.

El Internet, es la muestra más grande de lo que la imaginación humana puede llegar a realizar, si bien sus inicios fueron puramente militares, la necesidad de comunicación, llevo a desarrollar de manera efectiva esta idea, que en nuestros días se ha convertido en la mejor manera de información, comunicación y expresión.

Pero como todo conlleva un riesgo, estos aparatos denominados computadoras junto con la red de información, se han convertido en el mejor medio de cometer ilícitos, que por su naturaleza misma, no pudieron ser legislados con anterioridad.

Ni al mas modernista de los legisladores de todo el mundo, y peor aún, a los tratadistas de la ciencia penal, se les pudo haber ocurrido que algún tiempo después, se creen máquinas mediante las cuales se pueda llegar a cometer delitos, la tecnología avanza y el Derecho se va quedando en el tiempo, la necesidad de modernizar una sociedad, empieza en la nueva estructura que deben adquirir sus normas y leyes, adaptándose a las nuevas formas de delinquir.

Estas nuevas conductas, que vienen desarrollándose, justamente a partir de la creación de estos fenómenos revolucionarios llamados computadoras e Internet, los expertos o estudiosos del tema las han denominado, ***"DELITOS INFORMATICOS"***, dándole así vida a una forma de cometer ilícitos aprovechándose del uso de estas nuevas tecnologías, pero por sobre todo, beneficiándose de que al no existir una norma penal que reprima sus conductas, estaban exentos de pena alguna, nullum crimen, nulla pena, sine lege.

La necesidad de contar en todo el mundo con una efectiva legislación punitiva en materia de delitos informáticos, trajo una seria discusión sobre el tema, si se trataba de una nueva forma de delitos o de una simple adaptación de los ya existentes, sin duda que la figura es la misma, lo que cambia es la medio o la forma de cometerlos, y además cambia el sujeto activo de la infracción, ya que todos podríamos cometer un robo a mano armada, pero no todos estaríamos en las condiciones o capacidad de cometer un delito informático, es decir estamos frente a delincuentes altamente capacitados, que de alguna forma le dan una característica diferente a estas conductas delictivas.

Hoy en día, la mayoría de países especialmente los del primer mundo o desarrollados, se han preocupado de estas nuevas formas de delinquir y han

establecido dentro de su ordenamiento jurídico, las normas necesarias que permitan una efectiva sanción a quines comenten estos actos, dando el primer paso, de lo que llamaríamos la modernización del Derecho.

Para referirnos a la modernización del Derecho deberíamos partir analizando si las actuales condiciones de la sociedad se adaptan a las normas legales vigentes, y al hacernos esta pregunta, la respuesta es muy simple NO, en nuestro país las leyes están desactualizadas, lo que implica que trasladar el derecho a la nueva era en la que nos encontramos conlleva una ardua tarea de transformación de todas y cada una de las normas tanto en lo civil, lo penal, laboral, etc., y más aún si intentamos establecer normas que sancionen conductas penales informáticas, es decir que la Modernización del Derecho empieza con una retrospectiva de las leyes vigentes y trasladarlas a los días actuales, es una aplicación del método comparatista de encuadrar lo bueno con lo actual, el legislador debe tomar la posta de lo que implicaría modernizar las leyes.

Las normas de conducta que el Derecho pretende establecer en una sociedad, no bastan sino se adaptan al mundo informático en el que vivimos, la ventana abierta para la consumación de estas infracciones, nos pone en desventaja frente a los delincuentes, el Ecuador, ha sido presa fácil de la delincuencia informática, sin embargo podemos estar tranquilos, porque los legisladores han comprendido las graves consecuencias que significaba el no contar con una ley efectiva, las reformas a nuestro ordenamiento penal, facultarán a las autoridades, a reprimir de manera eficaz a los infractores informáticos.

Esta nueva era en la que nos encontramos, nos presenta nuevos retos, los que debemos afrontarlos y asumirlos de manera responsable, por tal razón, el

presente trabajo de investigación, no es más, que una muestra de la preocupación que significa en las nuevas generaciones de abogados la creciente ola delictiva que tiene que afrontar la sociedad en la que vivimos, por tal motivo, pretendemos dar una óptica real de lo que actualmente tenemos que enfrentar.

La posibilidad de analizar en este estudio los delitos informáticos, es sin duda un reto, que lo hemos asumido con la responsabilidad que la temática lo amerita, por lo que, pese a ser la doctrina un poco limitada por lo novísimo del tema, aportaremos con lo que a nuestro criterio resulte lo más importante y significativo.

CAPITULO 1

1.1. CONCEPTO DE DELITO INFORMATICO

Al intentar dar un concepto de lo que significan los delitos informáticos, necesariamente, debemos remitirnos a las fuentes penales fundamentales y trascendentales, para poder comprender este tema.

DELITO. – Concepto. –

No existe un concepto o criterio mundialmente aceptado sobre lo que significan o lo que son los delitos informáticos, muchos incluso han llegado ha establecer que no es necesario conceptualizarlos, ya que son los mismos delitos previamente existentes en las legislaciones nacionales, y lo que cambia es la herramienta utilizada, pero sin duda, el creciente número de infracciones informática, ha hecho que este criterio varíe y se modernice, haciendo que sean las legislaciones penales, las que de una u otra forma tengan que adecuarse a esta nueva realidad.

Debemos desmenuzar la frase "Delito Informático", y podremos entender su significado, la palabra Delito, tiene muchísimas acepciones, según los tratadistas, son actos ilícitos, no permitidos por las leyes, la moral, las buenas costumbres, que de una u otra manera alteran el orden social, así lo podemos entender en su manera más común, Cabanellas, dice que la etimología latina lo relaciona con *"delictum"*, como la calificación de un acto antijurídico sancionado con una pena, dice además "delito es culpa, crimen, quebrantamiento de una ley imperativa"[2]

Para el italiano Ranieri, "Delito es un hecho humano previsto de modo típico por una norma jurídica sancionada con pena en sentido estricto, lesivo o peligroso para los bienes o intereses creados por el legislador como merecedores de la más enérgica defensa, y expresión reprobable...."[3], este concepto mas amplio, nos permite determinar, si duda, que hay una intervención humana en la consumación del delito, acompañado de ánimo dañoso y destructivo.

Jiménez de Asua en su obra "La Ley y el Delito", incorpora varios conceptos de otros autores, como el de Mayer que dice sobre le tema: "acontecimiento típico, antijurídico e imputable"[4], definición simple pero a la vez completa, el delito necesariamente debe ser imputable, y en concordancia con lo anotado anteriormente, esa conducta es imputable a un ser humano, el mismo que adapta su acción o comportamiento a una norma establecida con anterioridad al acto, porque no hay pena sin ley previa, se habla de una adecuación de la conducta humana a la norma establecida, debido ha que el legislador advierte con la norma, la sanción aplicable.

---

[2] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo III, Pág. 58-59
[3] **RANIERI,** Silvio, Manual de Derecho Penal, Tomo I, Pág. 141
[4] **MAYER,** Citado por Luis Jiménez de Asua, en su obra La Ley y el Delito, Pág.255

Siguiendo la estructura previa, el mismo Jiménez de Asua, dice sobre el delito: "acto típicamente antijurídico, imputable a un hombre y sometido a una sanción penal"[5], refiriéndose al acto como acción u omisión, como manifestaciones básicas de la voluntad que concatenan con ese accionar imputable a un hombre, el mismo que por su conducta esta sometido a una sanción penal, previamente establecida en un código sustantivo penal.

De igual forma lo entiende nuestro Código Penal, al considerar al delito como una infracción sancionada con una pena, la característica fundamental del delito en general, es la irrogación de un acto, el cual de manera general es repudiado por la sociedad, cometido por personas, a las cuales según la normativa vigente, se los denomina sujeto activo de la infracción, y sobre los que recae una sanción punitiva, generalmente privativa de la libertad, como medio efectivo de precautelar los bienes jurídicos sometidos.

El Manual del Régimen Penal Ecuatoriano, lo describe en su definición formal, como "un acto legalmente punible"[6], y materialmente lo define como "aquel acto que ofende gravemente el orden ético-cultural de una sociedad determinada en un momento determinado y que, por tanto, merece una sanción"[7], como se advierte, el cometer un delito, es un acto que faculta, al aparato represor de un Estado, a sancionarlo de manera efectiva, y amparado bajo una norma legal previa.

Pero con más precisión, se ha dicho que el delito como tal, posee ciertos rasgos típicos, al respecto el mismo Régimen Penal señala que el delito es "acto típico, antijurídico y culpable"[8], determinando que, si cumple estos requisitos se

---

[5] **JIMÉNEZ DE ASUA,** Luis, La Ley y el Delito, Pág. 256
[6] **Régimen Penal Ecuatoriano,** Manual Práctico, Pág. 71
[7] **Ibid Op. Cit.** Pág. 72
[8] **Ibid Op. Cit.** Pág. 74

convierte en punible, al desmenuzar este concepto, el texto nos sugiere algunos criterios sobre el mismo, como acto típico, al referirse a la conducta humana previamente establecida por la normativa penal vigente, como antijurídico, por ser contrario a las normas del Derecho, y como culpable, por ser imputable al autor.

INFORMATICA. – Concepto. –

El término informático/a, por su parte tiene también varias concepciones, lo relacionamos directamente con el término automática y con la información, como una especie de fuente etimológica, así Guibourg dice: "Es el tratamiento de la información por medio de las computadoras"[9], de algún modo nos refiere este concepto, a que por medio de un computador, podemos de una manera adecuada y óptima, ingresar en el mismo una serie de información, la cual, gracias a los sistemas integrados de circuitos, se convierten o conforman archivos, fáciles de utilización por parte del hombre.

Sobre la palabra automática, podría resultar no necesariamente de un procedimiento electrónico, pero para definir el tema de nuestro estudio, lo entenderemos en tal sentido, dicho de otro modo, la informática, esa mezcla de información y automatización, es un conjunto perfecto que nos permite acceder a los datos creados por nosotros mismos, de manera rápida, efectiva y por sobre todo fácil, es más sencillo manejar cien archivos contables dentro de un programa computacional, a manejar veinte libros contables tradicionales.

Para Solano, la información "es la transmisión de un mensaje hecha de un emisor a un receptor utilizando un código de señales que el primero codifica y emite y el segundo recibe e intercepta"[10], concepto apegado mucho a nuestro estudio, por

[9] **GUIBOURG,** Ricardo, Manual de Informática Jurídica, Pág. 19
[10] **SOLANO,** Orlando, Manual de Informática Jurídica, Pág. 31

lo que entendemos a la información como ese conjunto de datos sean palabras, números o imágenes que las podemos convertir en un mensaje y trasladarlo de un lugar a otro.

Para el mismo autor la informática como tal, es "una teoría de la información, que la aborda desde un punto de vista racional y automático, a fin de transformar la información en símbolos y, mediante una serie de mecanismos electrónicos para aplicarla a la mayor cantidad posible de actividades"[11], como vemos entonces, la informática, es aquella que nos permite procesar la información de manera automática..

Para el autor ecuatoriano Ignacio Carvajal la informática es "El conjunto de conocimientos y técnicas en las que se basan los procesos de tratamiento automático de la información mediante computadores"[12], sin ahondar mucho sobre los diversos conceptos sobre el tema, la informática de manera general, es la que nos permite manejar de manera automatizada la información por nosotros creada, dándole un tratamiento adecuado, para facilitar su uso, mediante la utilización de las computadoras.

Delito Informático. – Concepto. -

Con estos antecedentes podemos referirnos de manera más precisa a los delitos informáticos, de igual forma, la teoría es muy diversa, varios han sido los autores que hasta la actualidad los han tratado, sobre este tema en concreto ampliaremos los diversos conceptos sobre él vertidos.

Julio Téllez, dice que atípicamente son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin", y típicamente dice que son "conductas

[11] **Ibid Op. Cit.** Pág.31
[12] **CARVAJAL,** Ignacio, Jurismatica, Pág. 137

típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin"[13]

Claudio Magliona, en su obra, extrae algunos conceptos muy diversos, así para el Departamento de Justicia norteamericano es "cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática sea esencial para su investigación o persecución".[14]

Para Parker es "cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor obtuvo o pudo haber obtenido intencionalmente un beneficio"[15], recogemos de lo expuesto que el delito informático es una conducta antijurídica, realizada por un acto humano voluntario, utilizando como medio o como fin un sistema integrado de circuitos, denominado comúnmente computadora.

Correa, por su parte, cita la definición de la Organización para la Cooperación Económica y el Desarrollo (OECD), la cual dice "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos"[16], cabe destacar que, la mayoría de tratadistas incluyen este concepto dentro de sus obras, como es lógico suponer, todas las definiciones sobre delitos informáticos, los relacionan directamente, con actos ilícitos, antijurídicos, anti éticos, inmorales, que buscan un beneficio a favor del que lo comete, y un perjuicio en contra del agredido, mediante la utilización de un computador.

---

[13] **TÉLLEZ**, Julio, Derecho Informático, Pág. 103
[14] **MAGLIONA**, Claudio, Delincuencia y Fraude Informático , Pág. 38
[15] **Ibid. Op. Cit,** Pág. 38
[16] **CORREA – BATTO – CZAR – NAZAR**, Derecho Informático, Pág. 295

Durante esta investigación sobre el concepto de los delitos informáticos, he precisado remitirme a otro tipo de fuente como el Internet, dentro del cual se indican los siguientes conceptos:

- Carlos Sarzana: "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".[17]
- Nidia Callegari: "aquel que se da con la ayuda de la informática o de técnicas anexas".[18]
- Silvia Palazuelos: "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".[19]

Pretender encontrar una unidad de conceptos sobre los delitos informáticos, resultaría utópico, como se dijo, existen criterios muy convergentes y parejos, que a manera de conclusión nos llevan a suponer que este tipo de conductas, tienen como finalidad o como medio la utilización de sistemas computacionales, para cometer una infracción, sin duda existente con anterioridad, por la doctrina y por la ley, pero que su modo peculiar de cometerlo es lo que obliga a la adaptación de esas normas.

Sin intentar ser repetitivo sobre lo anotado, como una opinión personal diré que, a mi criterio los delitos informáticos no son una nueva forma de cometer infracciones, sino que son los mismos delitos existentes ya en la normativa penal y lo que los diferencia de los tradicionales es su forma de realizarlos, es una adaptación de la conducta delictiva a una forma moderna de consumarlos, mediante la

[17] www.stj-sin.gob.mx/Delitos_Informáticos2.htm
[18] **Ibid Op. Cit.**

utilización de una o más computadoras, sean estas como medio o como fin de concretar el daño a un tercer perjudicado, que se ve gravemente afectado en su patrimonio o en su integridad.

De lo establecido se desprende que por el hecho mismo de ser conductas existentes, adaptadas a su nueva forma de cometerlos, suponemos ya, que son actos típicos, punibles, antijurídicos y culpables, en los cuales de manera determinante, actúa la voluntad humana, como elemento sustancial que permite reprochar el acto a un individuo que valiéndose de su capacidad y conocimiento, procede a la adaptación de su conducta al modelo penal existente.

Estructura del delito informático. -

Toda conducta antijurídica considerada como delito, conlleva en su estructura una serie de elementos que no les son ajenos a los delitos informáticos, según la base explicativa del Manual del Régimen Penal Ecuatoriano, podríamos decir que estos tipos de conductas pueden encuadrar en la siguiente clasificación:

- Por la gravedad y según lo indica el Art. 10 del Código Penal, estas conductas son delitos, sancionados generalmente con penas privativas de la libertad.
- Por su naturaleza en el ejercicio de la acción penal cabe, la pública de instancia oficial y la pública de instancia particular, por contemplar ciertos delitos como el Hurto, la Estafa, y el Robo, Art. 34 del Código de Procedimiento Penal.
- Por el momento de su descubrimiento, entendemos que son delitos no flagrantes.

[19] http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm

- Por su estructura, pueden ser simples, por que un solo hecho puede lesionar un solo bien, o complejos, por que ese mismo hecho puede lesionar más de un bien.
- Por el resultado que produce, son materiales, ya que ese acto humano produce efectos posteriores.
- Por su duración pueden ser instantáneos, permanentes o continuados. Instantáneos, por que se puede consumar en un solo momento; permanentes, por que la consumación puede durar un lapso de tiempo largo, según el daño causado al bien protegido (información, software, hardware); continuado, por que se los puede realizar con diversos actos ilícitos que poco a poco procuren un daño mayor.
- Por sus efectos, pueden ser de daño, por la afectación del bien jurídico tutelado, y de peligro, por que su consumación conlleva una situación de riesgo a más de un individuo, (virus).
- Por el bien jurídico protegido, sin duda son delitos económicos, por el autor que logra cometerlos, denominados por el Régimen como "delincuentes de cuello blanco"[20], para los cuales valiéndose de su condición académica, intelectual o profesional, les resulta más simple consumar sus acciones, que de una u otra forma buscan perjudicar o dañar a un tercero.

1.2. SUJETO ACTIVO

Al referirnos al sujeto activo de la infracción o del delito, advertimos que se trata de un individuo al cual, se le imputa la conducta delictiva, el que actuó con voluntad y conciencia de que ese acto implicaba una violación de la normativa penal.

[20] **Régimen Penal Ecuatoriano**, Manual Práctico Pág. 88

Para muchos tratadistas es el autor mismo del delito, no obstante la doctrina suele diferenciar entre autor, cómplice y encubridor, pero pese a esta diferenciación, el sujeto activo del delito, es el ser humano que comete por si o por intermedio de otro el hecho repudiable por la sociedad.

Cabanellas, dice "El autor cómplice o encubridor; el delincuente en general. Tiene que ser una persona física forzosamente; pues, aun en casos de asociaciones para delinquir, las penas recaen sobre sus miembros integrantes.."[21], para trasladar este concepto al tema de nuestro estudio, bien se ha dicho que el sujeto activo necesariamente tiene que ser una persona física, como expresábamos en la definición de los delitos informáticos, dijimos que, es un medio de cometer infracciones utilizando un computador como medio o como fin, pero esa conducta es obligatoriamente efectuada por una persona, y en este caso capacitada eficientemente.

Algunos escépticos sobre la materia han manifestado, que no necesariamente es el hombre el que comete el delito, sino la máquina, ya que recibe una serie de órdenes que se limita a cumplir, pero cabe destacar que esa máquina sino esta previamente programada por un experto difícilmente llegaría a funcionar y peor aún a cometer el delito. Bien se ha dicho que el computador es el medio o es el fin, no se engaña a la máquina, se engaña a la persona, sobre la que recae la conducta delictiva. Mal podríamos decir entonces que un computador se pueda convertir en sujeto activo de la infracción, ya que ésta es solo el producto de la creación humana, y responde a sus necesidades, en base a su sistema de programación, el sujeto activo

[21] **CABANELLAS,** Guillermo, Enciclopedia de Derecho Usual, Tomo VII, Pág. 566

es el que realiza la acción u omisión dolosa que pretende perjudicar o engañar a otro sujeto de su misma condición, la máquina es el medio de engaño, no la engañada.

Muchos tratadistas consideran como sujeto activo, ya directamente al autor, así tenemos "Autor es quien ejecuta la acción que forma el núcleo de cada delito *in specie.*"[22], coincidimos sin embargo en la teoría penal tradicional, que sobre el autor existen muchas acepciones, y el mismo puede dividirse en intelectual y material, sin tomar en consideración a los diversos grados de complicidad, pero de manera general el sujeto activo de la infracción es el que irroga el daño.

Otros como Maggiore lo asimilan directamente al término de reo o de culpable, "Culpable es el trasgresor, imputable, de una ley penal"[23], sin duda que el sujeto activo es el culpable y más aún el imputable de la conducta delictiva, "Reo es todo el que puede ser sujeto del derecho penal"[24], no obstante es muy vano hablar de que el reo es sujeto de derecho penal, ya que dentro de la materia existen generalmente dos sujetos el activo como causante del delito y el pasivo que ve afectado sus derechos y ambos son sujetos del derecho penal, reo a nuestra concepción es el individuo al que tras la imputación de una infracción, y la comprobación de su autoría en el mismo, se le impone una sanción punitiva privativa de la libertad, y que debe purgar su pena en un centro creado para el efecto.

El Código de Procedimiento Penal, en su Art. 70 inc. 1ro, dice: "Se denomina imputado la persona a quien el fiscal atribuya participación en un acto punible como actor, cómplice o encubridor; y, acusado, la persona contra la cual se ha dictado auto de llamamiento a juicio o en contra del cual se ha presentado una

---

[22] **JIMÉNEZ DE ASUA,** Luis, La Ley y el Delito, Pág. 629
[23] **MAGGIORE,** Guiseppe, Derecho Penal, Tomo I, Pág. 463
[24] **Ibid. Op. Cit.** Pág. 469

querella"[25], precisamos esta diferencia, para determinar que, al imputado o al acusado, según nuestra legislación vigente, es al que podríamos denominar como el sujeto activo del delito.

Antiguamente se consideraba como autores de los delitos a los animales e incluso a las cosas, modernamente y con absoluta razón se habla de que solo las personas son susceptible de cometerlos, y al hablar de personas nos referimos al ser humano, a la persona física, sin embargo, en los últimos tiempos y muy acorde con este tema, se ha llegado ha establecer que también las personas jurídicas podrían convertirse en potenciales sujetos activos de una infracción, pero como atribuirle a ente ficticio un hecho delictivo penal, si tan solo puede adquirir derechos y obligaciones civiles, y, además los actos de esos entes jurídicos, son de exclusiva responsabilidad de sus representantes.

La persona jurídica, criterio introducido por Savigny, nuestro ordenamiento civil en su Artículo 583 la entiende como "..una persona ficticia, capaz de ejercer derechos y contraer obligaciones civiles, y de ser representada judicial y extrajudicialmente"[26], claramente se indica que puede contraer obligaciones ***civiles,*** pero en el tema de los delitos informáticos, y como se dijo, se intenta asimilarlos a estos entes jurídicos ficticios como sujetos activos de una infracción, pero de que responsabilidad penal hablaríamos, o acaso nos imaginamos a un empresa farmacéutica tras las rejas, o a una comercializadora multinacional frente a un juez rindiendo cuentas de sus actos, más aún, el articulado al respecto es muy claro, e indica además que puede ser representada judicial o extrajudicialmente, precisando así, que este ente requiere necesariamente de una persona natural que la represente, y

[25] **Código de Procedimiento Penal Ecuatoriano**
[26] **Código Civil Ecuatoriano,** Art. 583

como los sujetos activos de la infracción (delito), solo pueden ser personas naturales, físicas, entonces serían solo a ellos a los que podríamos imputar la comisión de un delito, bien se ha dicho que la computadora es un medio o fin para cometer la infracción, claro está, que la persona jurídica podría ser el medio efectivo para cometer la infracción mas que nada en busca de impunidad, pero quien responderá por sus actos será la persona natural que actuó como sujeto activo.

En concordancia con lo anotado, como entonces podemos atribuirle a un computador la consumación de un delito, si es su operador, o dueño, el que lo usa para cometer la infracción, coincidiendo una vez más que la máquina solo es un medio o un fin.

Encontrar las razones por las que un delincuente actúa, sería introducirnos en un tema social, ético y moral, situaciones económicas y culturales, que dependen exclusivamente del entorno social sobre el cual se desenvuelve o desarrolla el individuo, en materia de delitos informáticos, los antecedentes son mucho más modernos, por lo que a este tipo de individuos se los ha denominado generalmente delincuentes informáticos, los cuales actúan de manera extraña o diferente a un delincuente común.

Magliona explica, que este fenómeno surge de una corriente norteamericana, de jóvenes estudiantes, altamente capacitados, con un coeficiente intelectual muy alto, considerados incluso como inofensivos, que iniciaron esta actividad sin tratar de causar ningún daño, especialmente al común de las personas, influenciados por lo "Síndrome de Robin Hood", que es "la creencia en cierto modo patológica de que mientras que robar a una personan 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"[27], sin pretender justificar esta teoría, ya que todo hecho delictivo conlleva una responsabilidad, y el no conocer una norma legal, no excluye de responsabilidad al autor, sin duda que nos encontramos frente a delincuentes, que de ninguna manera aceptan su responsabilidad en tales actos, ya que se amparan en el fundamento ilógico de actuar motivados por su profesión o por su actividad tal es el caso de programadores en sistemas, ingenieros informáticos o técnicos entendidos en la rama tecnológica de la computación.

Se presume que estos hechos son cometidos especialmente por individuos cuya edad fluctúa entre 18 y 35 años, generalmente varones, solteros, estudiosos de la ciencia informática, pero cabe destacar, que estas actuaciones serían de un modo técnico las que menos perjuicios causan, sin duda que los hechos delictivos más preocupantes y más crecientes, son efectuados por personas ajenas a estos parámetros, que incluso no necesariamente deben tener tal capacitación, sino que simplemente abusan de su condición interna dentro de una empresa.

La doctrina los define como, empleados de confianza, que tienen acceso a cierto tipo de información, y que se valen de su posición para cometer tales infracciones, denominados *insiders,* generalmente actúan en instituciones bancarias, para transferir información (fondos), de una cuenta a otra, mediante la utilización de un computador, en este caso como medio, claro está, que a estos sujetos activos se suma el ataque que sufren de sujetos exteriores, denominados delincuentes

[27] **MAGLIONA,** Claudio, Delincuencia y Fraude Informático, Págs. 68-69

informáticos a distancia, que pueden ser clientes de la institución bancaria, que pretenden causar una defraudación.

Como anotamos, estas conductas, por el autor que las comete, se los ha llamado de cuello blanco, encuadrados en la categoría de delitos económicos, y que además están dentro de la cifra negra de la criminalidad, ya que las instituciones que lo sufren, por temor a perder credibilidad, no los denuncian.

El sujeto activo en los delitos informáticos, poseen ciertas características o rasgos diferentes a los delincuentes comunes, ya que "tiene 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 sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales.."[28], pero hay que diferenciar entre el sujeto activo que ingresa al sistema informático, bien dentro de una institución o bien fuera de ella, e incluso diferenciar si ingresa con el fin de causar un daño, o con el objetivo de simplemente poner a prueba sus habilidades de vulnerar la seguridad del sistema.

Características del sujeto activo informático. -

El delincuente informático tiene ciertos rasgos fundamentales:

- Tiene alta capacitación en materia informática
- Generalmente se encuentra en una posición laboral privilegiada para el manejo de la información
- Su condición económica es moderadamente buena
- Su desarrollo intelectual, se considera en parámetro altos

[28] www.stj-sin.gob.mx/Delios_Infomáticos2.htm

- Actúa por motivación personal y raras veces por agentes externos a su voluntad
- Algunos no pretenden causar daños a terceros, sino demostrar sus habilidades
- Otros buscan un perjuicio, no solo a instituciones sino a personas naturales
- Su herramienta de trabajo es un computador y la red de información denominada Internet
- No se consideran delincuentes
- Su accionar los hace sentir orgullosos y respetables
- Incluso han llegado a formar comunidades de apoyo entre ellos
- Reciben varias denominaciones como Hacker, Cracker, según su actividad
- Por su actividad secreta y en muchos casos por la inexistencia de leyes en la materia, sus actos son impunes

El sujeto activo de la infracción informática, si bien en su definición como tal no difiere mucho del establecido por la doctrina penal, como vemos sus rasgos característicos, nos demuestran que estamos frente a personas que consideran su actividad como un don, pero gracias a las normas penales, podríamos establecer que tales conductas, por más justificativo que estos pretendan, son hechos dañosos que alteran el orden social, que van en contra de las buenas costumbres y de la ética, constantemente defendidos dentro de una sociedad organizada, la misma que en la actualidad se encuentra sometida a esta nueva forma de situaciones antijurídicas y delictivas.

1.3. SUJETO PASIVO

Como en todo orden de cosas, si existe un agente que realiza el acto, al cual se lo denomina sujeto pasivo, debe necesariamente existir un agente que recibe ese acto dañoso, al que se lo llama sujeto pasivo de la infracción.

El sujeto pasivo, es la víctima, es el que sufre el accionar malicioso y doloso del agente activo, a diferencia de lo que normalmente la doctrina penal lo entiende, pese a no ser generalizada en su concepto, el sujeto pasivo al contrario que el activo, no siempre resulta ser una persona natural, sino que además pueden ser las personas jurídicas, sean públicas o privadas, incluyendo dentro de esta categoría todas y cada una de las diversas instituciones que pueden formar parte de una sociedad, sean de gobierno, sean bancarias o empresariales.

El Código de Procedimiento Penal, en su Art. 68, y concordante con lo expresado se refiere al ofendido (sujeto pasivo), así el numeral 1ro considera como tal "Al directamente afectado por el delito y, a falta de este a su cónyuge o conviviente en unión libre, a sus ascendientes o descendientes y a los demás parientes dentro del cuarto grado de consaguinidad o segundo de afinidad", y el numeral 3ro "A las personas jurídicas, en aquellos delitos que afecten a sus intereses"[29], como vemos, el sujeto pasivo, puede ser tanto personas naturales como personas jurídicas, según sea el perjuicio por cada uno declarado.

Dentro del margen del bien jurídico tutelado, muchos pueden ser derechos que se afecten con la consumación de un delito informático, bien en el patrimonio, en la propiedad, en la honra, en la privacidad; o en el caso de entidades gubernamentales incluso en la seguridad misma del Estado.

---

[29] **Código de Procedimiento Penal Ecuatoriano**

Cabanellas sobre el sujeto pasivo del delito, afirma que es "La víctima del mismo; quien en su persona, derechos o bienes, o en los de los suyos, ha padecido ofensa penada en la ley y punible por el sujeto activo."[30], la doctrina sobre este tema, pese a ser muy extensa es al mismo tiempo muy reiterativa, sin duda que el sujeto pasivo, sea persona natural o jurídica, es el que sufre para sí el delito, el que ve afectado su patrimonio, como ese conjunto de obligaciones y derechos que posee una persona, y que es susceptible de transmitirse por causa de muerte, ese patrimonio afectado, por el accionar delictivo del sujeto activo, es el que convierte en víctima al ente receptor.

Pese a todos los derechos consagrados por las leyes penales y constitucionales para precautelar los derechos del sujeto pasivo, en materia de delitos informáticos, los mismos no suelen ser reclamados por los perjudicados, ya sea por falta de ley expresa sobre el tema, o bien porque consideran una labor infructuosa el denunciar los mismos, o porque en el caso de las instituciones especialmente financieras, consideran que, al hacer público el daño causado, sufrirían más perdidas por falta de credibilidad y seriedad, que por el daño mismo.

Estos han sido los parámetros fundamentales que han impedido lograr, una efectiva sanción a los infractores, y de la cual sin duda los únicos beneficiados resultan ser los sujetos activos del delito.

---

[30] **CABANELLAS,** Guillermo, Diccionario del Derecho Usual, Tomo VII, Pág. 567

1.4.- BIEN JURÍDICO PROTEGIDO

Al referirnos al bien jurídico protegido, estamos hablando del objeto o persona sobre le cual recae la protección penal, como dice Welsel, "es un bien vital de la comunidad o del individuo que por su significado social es protegido jurídicamente"[31].

En el ámbito jurídico informático, varios han sido los criterios que han considerado exclusivamente al computador como el bien a proteger, lo que a su vez a traído como consecuencia el determinar si el computador es un medio para engañar o es el engañado, el desenlace de un delito es el causar un daño a otra persona, sea un su integridad (física, intelectual o psicológica), o en su patrimonio, y lo que pretende la norma penal es limitar y advertir que esa acción dañosa conlleva una sanción, es decir el afectar un bien ajeno significa afrontar una pena, sin embargo dentro de los delitos informáticos la doctrina considera que no sollo se afecta un bien jurídico sino que por el contrario tiene un carácter pluriofensivo.

Todos los proyectos de ley y las diversas legislaciones en materia de infracciones informáticas tuvieron como fundamento esencial el considerar como único bien protegido a la información contenida en soportes informáticos, computacionales o automatizados, capaces de procesar la misma de manera rápida y efectiva, sin embargo este criterio se ha vista en la actualidad muy limitado, por las diversas formas modos y medios de cometer delitos informáticos, ya que no solo se esta protegiendo la información, sino también la propiedad sobre la misma, los soportes en los que reposa, el patrimonio, la integridad personal, la intimidad, entre otros, por lo que se puede considerar dentro de las legislaciones qua han incorporado

[31] **Welsel**, citado por Claudio Magliona en su libro Delincuencia y Fraude Informático, Pág. 63

en su normativa penal estas infracciones, dándoles a los delitos clásicos el carácter de informáticos, que el bien jurídico es típicamente aceptado con las adecuaciones informáticas y electrónicas, que los podrían afectar.

Podríamos concluir diciendo que no solo se afecta un bien, como en el caso de un delitos clásico, sino que en esta nueva forma de cometer infracciones penales, pueden ser varios los bienes jurídicos protegidos, ya que una sola conducta afecta varios bienes, la sola intromisión no autorizada a un sistema informático podría afectar la intimidad, el patrimonio, la confianza en el sistema, la pureza de la información, sin considerar claro esta, la alarma social que podría traer consigo una conducta de tal magnitud, si se afectaran bienes nacionales.

1.5. CLASIFICACION DE LOS DELITOS INFORMATICOS

Las diversas formas de cometer delitos informáticos, hace que su clasificación sea muy variada y extensa, conforme a trascurrido el tiempo, en el que se fueron convirtiendo en verdaderas conductas antijurídicas, han aumentado y cambiado las distintas maneras de perpetrarlos.

La clasificación ha sido extensa y se la realiza según el tipo de delito, ya que cada uno conlleva más de un accionar doloso para consumar la infracción, al igual que en el concepto, no existe una clasificación mundial o generalmente aceptada, muchas han sido las categorías en las que se los encuadra.

Existen varias formas de clasificarlos, en efecto la Organización de las Naciones Unidas, ha presentado la siguiente clasificación:

Fraudes cometidos mediante manipulación de computadoras	Estos pueden suceder al interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede acceder a este tipo de registros y programas.
La manipulación de programas	Mediante el uso de programas auxiliares que permitan estar manejando los distintos programas que se tiene en los departamentos de cualquier organización.
Manipulación de los datos de salida	Cuando se alteran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de computo.
Fraude efectuado por manipulación informática	Accesando a los programas establecidos en un sistema de información, y manipulándolos para obtener una ganancia monetaria.
Falsificaciones Informáticas	Manipulando información arrojada por una operación de consulta en una base de datos.
Sabotaje informático	Cuando se establece una operación tanto de programas de computo, como un suministro de electricidad o cortar líneas telefónicas intencionalmente.
Virus	Programas contenidos en programas que afectan directamente a la maquina que se infecta y causan daños muy graves.
Gusanos	Se fabrican 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.
Bomba lógica o cronológica	Su funcionamiento es muy simple, es una especie de virus que se programa para que explote en un día determinado causando daños al equipo de computo afectado.
Piratas Informáticos	Hackers y Crackers dispuestos a conseguir todo lo que se les ofrezca en la red, tienen gran conocimiento de las técnicas de computo y pueden causar graves daños a las empresas.

Acceso no autorizado a Sistemas o Servicios	Penetrar indiscriminadamente en todo lugar sin tener acceso a ese sitio.
Reproducción no autorizada de programas informáticos de protección Legal	Es la copia indiscriminada de programas con licencias de uso para copias de una sola persona, se le conoce también como piratería.[32]

De manera algo escueta, la ONU, ha pretendido expandir esta clasificación, pero por lo complejo del tema, es mucho más amplia la clasificación, por otro lado, varios también han sido los autores que han intentado dar una clasificación de delitos informáticos, trataremos entonces, de precisar la mayor cantidad posible, de los delitos hasta ahora descubiertos y perpetrados.

Una de las teorías más difundidas, por ser uno de los primeros en Latinoamérica en tratar sobre el tema, es la del autor mexicano Julio Téllez, el cual los clasifica según el uso que se de a la computadora, sea como método, medio fin, de la siguiente manera:

"Como Instrumento o medio:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
b) Variación de los activos y pasivos en la situación contable de las empresas
c) Planeación y simulación de delitos convencionales (robo, homicidio, fraude, etc)
d) "Robo" de tiempo de computadora
e) Lectura, sustracción o copiado de información confidencial

f) Modificación de datos tanto de entrada como de salida

g) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (Caballo de Troya)

h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa "técnica del salami"

i) Uso no autorizado de programas de computo

j) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, tales como "consulta a su distribuidor"

k) Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles "virus informáticos"

l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos

m) Acceso a áreas informatizadas en forma no autorizada

n) Intervención en las líneas de comunicación de datos o teleproceso"[33]

Este mismo autor en su otra clasificación usando la máquina como fin u objetivo presenta los siguientes delitos:

"a) Programación de instrucciones que producen un bloqueo total al sistema

b) Destrucción de programas por cualquier medio

c) Daño a la memoria

d) Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etc)

---

[32] http://tiny.uasnet.mx/prof/cln/der/silvuia/tipos.htm
[33] **TÉLLEZ** Julio, Derecho Informático, Págs. 105-106

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados

f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate, etc.)"[34]

Con esta clasificación pretende el autor, encasillar las conductas delictivas informáticas, si bien la misma es algo extensa, existen otros tipos de accionar incluso más peligrosos y controversiales no contemplados en la misma, por lo que, mas adelante indicaremos y explicaremos la mayor cantidad posible de delitos informáticos tratados por los diversos tratadistas.

De lo anotado, desprendemos que hay dos tipos de clasificación, aquella en la que usa a la computadora, como medio para la consumación del delito, procurando un daño y aquella que en la que el computador es su objetivo o finalidad, y se va contra el computador, bien en su parte física, o bien, en los programas en ella introducidos.

Para María de la Luz Lima, los delitos informáticos están dentro de tres categorías:

- "Los que usan la tecnología electrónica como método
- Los que usan la tecnología electrónica como medio
- Los que usan la tecnología electrónica como fin"[35]

Diferenciando el método del medio, porque en el primero se usan métodos electrónicos para consumar el delito, y el medio, en concordancia con lo expuesto anteriormente, en el que se usa la computadora como medio para cometer el delito.

---

[34] **Ibid. Op. Cit** Pág. 106
[35] tiny.uasnet.mx/prof/cln/der/silvia/clases.htm

Otra clasificación es la de Jorge Pacheco Klein, el cual los distingue de la siguiente manera:

- "Delitos informáticos internos, Eje. Sabotaje de programas
- Delitos a través de las telecomunicaciones, Eje. Hacking
- Manipulación de computadoras, Eje. Apropiación indebida (cuello blanco)
- Utilización de computadoras en apoyo a empresas criminales, Eje. Lavado de dinero
- Robos de software, Eje. Piratería"[36]

María Viega, sobre la clasificación dice que se debe considerar ciertos aspectos, según los cuales se los podría llegar a clasificar al respecto dice, y deberían ser por:

- "El perjuicio causado
- El papel que el computador desempeñe en la realización del mismo
- El modo de actuar
- El tipo penal en el que se encuadren
- Clase de actividad que implique según los datos involucrados"[37]

Advertimos con anterioridad que los delitos informáticos, por su naturaleza, poseían características típicas de todo delito (ver Pág. 10), pero como se ha venido diciendo, por esa misma naturaleza sui generis de estas conductas, existen varios tipos de delitos, que se los mira de diferente óptica, generalmente como medio o como fin.

Creemos que solo se los podría encuadrar en las categoría en las que se utiliza al computador como efectivo medio conducente para adaptar la conducta al

---

[36] **VIEGA,** María José, Un nuevo desafío jurídico, Pág. 4
[37] **Ibid Op. Cit** Págs. 3-4

tipo penal existente, es decir aquellos delitos, mediante los cuales, gracias a los diversos medios de comunicación, en los que utilizando estos aparatos, se puede llegar a cometer la infracción punible.

Y la otra categoría, en los que el computador es el objetivo o finalidad de la acción criminal, en este caso, nos encontramos a conductas, que pretenden ocasionar el hecho lesivo, destruyendo, sustrayéndose, desapareciendo u ocultando el computador, dentro del cual se puede contener información calificada como altamente delicada, privada o confidencial, para retardar o cuasar un daño inmediato o posterior, o simplemente para disminuir el patrimonio de una persona natural o jurídica.

Cabe destacar, que tal clasificación dependerá del tratamiento legislativo que se le dé, y de las normativas penales vigentes, indicando además, como ya se ha dicho, que no son una nueva clase de delitos, son las ya existentes, adaptados una nueva modalidad de cometerlos, no previstos con anterioridad.

1.6. TIPOS DE DELITOS INFORMATICOS

Sobre los diversos tipos de delitos informáticos, ha sido muy extensa su determinación, la doctrina los ha catalogado de manera general, según la forma de cometerlos, según el daño causado, según el sujeto activo y pasivo de la infracción, según el bien jurídico tutelado o la peligrosidad de los mismos.

Previo a dar un concepto de lo que significan los diversos delitos informáticos presentaremos una clasificación personal según la categoría a la que

podrían pertenecer por su modo y forma de cometerlos, para posteriormente proceder a dar un concepto y una explicación de los mismos.

Según la actividad realizada utilizando a la computadora como medio o como fin se pueden distinguir los siguientes por la forma de cometerlos:

1. - Mediante el uso de la máquina para dañar el funcionamiento de esa máquina o engañar al usuario, como medio y fin, varias formas de defraudaciones

- Introducción de datos falsos
- Manipulación de datos de salida
- Caballo de Troya
- Fraude Informático
- Técnica del salami

2. - Mediante daños al sistema, como fin

- Sabotaje Informático
- Virus
- Gusanos
- Rutinas Cáncer
- Bomba lógica
- Espionaje
- Superzapping
- Pinchado de líneas
- Puertas falsas
- Hacker
- Cracker

3. - Uso de la máquina para cometer otros daños, como medio

- Piratería
- Falsificación
- Homicidio
- Hurto de Tiempo
- Hurto Informático
- Violación de la intimidad

1. - Mediante el uso de la máquina para dañar el funcionamiento de esa máquina o engañar al usuario, como medio y fin, varias formas de defraudaciones:

Introducción de datos falsos (datta diddling). –

Método sencillo, que consiste en ingresar en un computador, datos falsos o ilegítimos, para eliminar información verdadera o bien para cambiarlas. Es una especie de defraudación, usando la máquina como medio o como fin, en la que se puede introducir los diversos datos, para obtener beneficios inmediatos o posteriores. No se requieren mayores conocimientos de informática para cometerlos, al que realiza esta actividad suele denominársele insiders, debido a que generalmente los cometen empleados de confianza de una empresa.

Los sujetos pasivo de la infracción pueden ser de variada característica, aunque la preferencia de los delincuentes recae en el ámbito privado sobre, instituciones bancarias, financieras o de seguros, y, en el sector público,

especialmente en instituciones que por sus razón pueden manejar bases de datos muy grandes, como las telefónicas o recaudadoras de impuestos.

Los datos de entrada pueden alterar el sistema de tal forma, que los resultados si bien pueden ser exactos, en realidad son la consecuencia de los ingresados al inicio, por lo que el mismo resulta fraudulento e ilegal.

Ejemplo. - Magliona, cita el siguiente caso real: Varios empleados de un banco suizo, se pusieron de acuerdo para cometer una defraudación a la entidad, tanto el operador del sistema, como los que tenían a su cargo la obligación de enviar el dinero, de tal modo que, el operador intercepto varias ordenes de transferencias dadas por sus coautores, y multiplico cada una de esas cantidades por mil, así, los que debían recibir el dinero, en vez de cien francos, recibían cien mil; como bien se dijo en esta forma de delito es muy difícil de descubrir a sus autores, solo después de varias averiguaciones se dio con los mismos, se los apresó y juzgo.[38]

Manipulación de datos de salida. –

Forma de cometer fraude, mediante la codificación de la información, usado generalmente en tarjetas de crédito falsificando sus bandas magnéticas, para que emitan información inexistente. A los autores de este tipo de infracción se los denomina outsiders.

Romeo Casabona, dice que es "el resultado del procesamiento de aquellos que en principio es también correcto, pero finalmente no se corresponde con los mismos a causa de una manipulación posterior, bien sea cuando son reflejados por escrito a través de la impresora del ordenador – manipulando aquella o la consola de este último - , bien se registre en una banda magnética cuando van a ser trasmitidos a

[38] **MAGLIONA,** Claudio, Delincuencia y Fraude Informático Pág. 192

otro ordenador. Por lo general no se requieren especiales conocimientos técnicos por parte del autor.[39]

De esta manera si bien el programa no es el alterado en su estructura inicial, si lo es en su resultado final, bien por el que arroja directamente en una pantalla, como en el caso de un cajero que indica un saldo inexistente partiendo de datos falsos, como el que se puede encontrar en una impresión, que no es más que el resultado escrito de los procesos informáticos alterados.

Ejemplo. – Utilizando una tarjeta de crédito robada se procede a cambiar su banda magnética por otra falsificada y realizar compras no autorizadas o retiros bancarios falsos a través del uso de un cajero automático.[40]

Caballo de Troya. –

Se introduce en un programa de continuo uso , una serie de órdenes diversas, que hacen actuar a ese programa de manera diferente, sin que los demás se vean afectados. Para Romeo Casabona, "consiste este tipo de manipulaciones en que partiendo de una correcta entrada de los datos se consigue que su procesamiento conduzca a resultados falsos por interferir en el programa que contiene las ordenes precisas para el tratamiento adecuado de los datos, de acuerdo con los objetivos perseguidos por la entidad o usuario que adquirió o confecciono dicho programa. Tales instrucciones del programa son alteradas por el autor por diversos procedimientos: modificando o eliminando algunos pasos del programa, o introduciendo partes nuevas en el mismo".[41]

---

[39] **ROMEO CASABONA,** Carlos, citado por Claudio Magliona en su obra Delincuencia y Fraude Informático Pág. 194

[40] **COBA,** Santiago, Los delitos informáticos en la legislación ecuatoriana, Pág. 78

[41] **ROMEO CASABONA,** Carlos, citado por Santiago Coba en su tesis Los delitos informáticos en la legislación ecuatoriana, Pág. 74

Solano, sobre el mismo tema dice que "es otro método de sabotaje muy utilizado, mediante el cual se introduce una serie de órdenes en la codificación de un programa con el propósito de que este realice funciones no autorizadas"[42], pese a que la definición del delito en su estructura concuerda con las otras ya mencionadas, discrepamos con el mismo al considerarlo como un sabotaje, ya que como se ha venido tratando esta iniciales formas de delitos informáticos, están dentro de una categoría a la cual la hemos definido como varias formas de defraudaciones, estando a nuestro criterio la figura del Caballo de Troya, dentro de la mencionada categoría y no como una especie de sabotaje, al cual le dedicamos un tratamiento individual mas adelante.

Ejemplo. - Introducir en el programa de una entidad bancaria un programa que, cada vez que se consulta el saldo de una cuenta, este se multiplique por mil, diez mil, etc, para autorizar pagos superiores inexistentes.[43]

Fraude Informático. –

Para Ranieri, la figura penal del fraude se enmarca en "el interés del Estado por la defensa de los bienes patrimoniales contra los engaños efectuados con el fin de obtener un provecho injusto"[44]

Considerada por muchos autores, como el más común de los delitos informáticos, Magliona en su obra recoge varios conceptos de esta modalidad como el de Romeo Casabona que dice "La incorrecta modificación del resultado de un procedimiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su

---

[42] **SOLANO,** Orlando, Manual de Informática Jurídica, Pág. 284
[43] **MAGLIONA,** Claudio, Delincuencia y Fraude Informático, Pág. 46
[44] **RANIERI,** Silvio, Manual de Derecho Penal, Tomo VI, Pág. 118

procesamiento o tratamiento informático, con ánimo de lucro o en perjuicio de tercero"[45]

Camacho Losa, "en los que el uso indebido o la manipulación fraudulenta de elementos informáticos de cualquier tipo (hardware, software, líneas de comunicación, etc.), posibilitan un beneficio ilícito"[46]

Para Solano, es el "uso indebido o por manipulación dolosa de documentos informáticos de cualquier clase que posibilite un beneficio ilícito"[47]

Muchos autores lo asimilan de manera directa con la "técnica del salami", es decir, el envío paulatino de dinero en pequeñas cantidades a otra cuenta que de a poco acumula sumas grandes, El fraude, es un modus operandi, es decir son actuaciones reiterativas de una conducta intelectual, que de una o otra manera evidencian que el procedimiento utilizado es más o menos similar, la cual unida al ánimo de cuasar un perjuicio económico a un tercero, más el uso de sistemas informáticos, se constituye en lo que se denomina fraude informático.

Se lo considera como el que suelen cometer los empleados de una empresa de manera directa, y además adquiere una particularidad que, mediante el uso de una terminal remota o por acceso telefónico, se puede acceder al sistema computacional, para llegar a cometer estas infracciones, adecuándose los sujetos activos a los que mencionamos con insiders y outsiders, el fraude informático, lo asemejamos a una apropiación ilícita de la información o de los productos que esta pueda arrojar como resultado de aquel proceso para el que el programa ha sido

---

[45] **ROMEO CASABONA,** Carlos, citado por Claudio Magliona, en su obra Delincuencia y Fraude Informático, Pág. 47

[46] **CAMACHO LOSA,** Luis, citado por Claudio Magliona, en su obra Delincuencia y Fraude Informático, Pág. 185

[47] **SOLANO,** Orlando, Manual de Informática Jurídica, Pág. 282

fabricado, bien por introducir datos que alteren el sistema, o bien por hacer aparecer datos falsos.

El fraude es el resultado de una conducta, sea por acción u omisión, depende mucho además del conocimiento del autor, si es en menor o mayor grado el daño causado, se podrá verificar la capacitación del que lo comete, por tal razón y conforme a lo que indica Solano, serán muchas las formas de fraude, ya sea por la manipulación de datos de entrada o salida, o por diversas técnicas como la del salami, o bien por los bienes que son mayormente apetecidos, así tenemos:

- "Sustracción de dinero o documentos que los sustituyan (cheques auténticos o ficticios)
- Sustracción de mercancías (Por manipular inventarios de entrada o de salida)
- Sustracción de valores negociables (acciones)
- Sustracción de servicios (agua, luz)
- Sustracción de software
- Sustracción de información (lista de clientes, planes de lanzamiento)"[48]

Desde nuestro análisis, entendemos que si bien muchas de las modalidades mencionadas ingresan en nuestra clasificación de los diversos modos de fraude, otros como la sustracción de software, encuadrarían más en la piratería, que la hemos considerado en otra forma de delincuencia informática.

El sujeto pasivo de este delito, al igual que en casi todas las infracciones informáticas que tratamos, son de manera preferente las instituciones financieras, pero ya en el ámbito de la protección que se pretende brindar a la información, podrían estar incluidas empresas que por su naturaleza poseen grandes bases de datos

[48] **Ibid Op. Cit.** Pág. 287

de personas naturales, tal es el caso de las empresas prestadoras de diversos servicios, como telefonía celular, cadenas de restaurantes con servicio a domicilio, agencias de empleo, etc.

Dentro del Internet muchos se han preguntado como se puede llegar a cometer una infracción de tal naturaleza, como se ha dicho en sentido penal, el fraude es una forma de engaño en cualquier tipo de actividad, sea comercial, industrial, social, se comete fraude induciendo sin duda al error ya sea en la persona o en la cosa, a nivel del Internet, se puede cometerlo, vendiendo una mercadería por otra ofertada, siendo el perjudicado el comprador, el cual no tuvo acceso directo al producto previo a la compra, y basado en su buena fe, lo adquiere sufriendo un perjuicio posterior generalmente irreparable.

El delito de fraude como tal, dentro de nuestro ordenamiento penal no existe, pero se incluye esta figura como "Otras Defraudaciones", en el que se hace hincapié, que es una conducta de aquel que pretende favorecer de ciertas acciones para las que fue encomendado, por lo que asumimos que dentro de la figura del fraude informático, éste se comete, ya que aprovechándose de ciertas calidad los autores manipulan información, para beneficio personal o de un comitente.

Dentro de esta figura, considero que el bien jurídico a proteger es la información, ya sea esta inicial, final o de resultado; inicial, por que se pueden introducir datos falsos; final, por que se puede alterar la información que en inicio era real y obtener un resultado diverso.

Técnica del Salami. –

Su nombre se dice que procede, más en razón de forma de cometerlos, ya que se lo va realizando en pocas cantidades o tajadas. Se lo usa en instituciones bancarias o financieras, consistente en el traslado de pequeñas cantidades de dinero de una cuenta a otra inexistente, gracias a una especie de redondeo de los pocos centavos que puede poseer esa cuenta, poco descubierto y muy utilizado, ya que las otras cuentas siguen manteniendo su saldo cuadrado.

Solano sobre esta técnica señala que "Es muy utilizada en las instituciones en que hay continuo movimiento de dinero y consiste en la sustracción de pequeñas cantidades activas de diferentes procedencias, logrando a través de él un redondeo en las cuentas"[49], como vemos este criterio no dista mucho del ya planteado, sin embargo cabe destacar, que el beneficio puede resultar en la persona del sujeto activo mismo de la infracción o en el de un tercero para el que actúa.

Para cometer este tipo de infracción mas que un experto en informática se requiere ser un experto contable, ya que la cualidad que posee el delito, esta en que es muy difícil de descubrirlo por que las cuentas siempre cuadran, ya que como dicen los españoles Ramallo Romero y Castillo Jiménez, esto se logra gracias al "redondeo de los intereses de las cuentas bancarias, aproximando las cantidades centesimales, a la unidad, produciéndose con ello la cuadratura de los balances.."[50], claro esta que este experto contable debe manejar de manera correcta el programa informático.

Los sujetos activos de esta modalidad pueden ser empleados de las instituciones, como el caso de los insiders, o externos como el caso de un cracker. Los sujetos pasivos de la infracción son de manera casi generalizada las instituciones

---

[49] **Ibid Op. Cit.** Pág. 284

del sistema financiero, y por excepción aquellas públicas o privadas en las que se manejen significativas cantidades de dinero.

Ejemplo. – Citado por Santiago Coba, en el que hace referencia a las planillas de cobro que por servicio telefónico realizaba la antigua empresa EMETEL, y que nunca se llego a determinar para donde se dirigió ese dinero, que pese en algunos casos ser muy pequeño, pero ya sumados podían dar cantidades significativas.[51]

2. - Mediante daños al sistema, como fin

Sabotaje Informático. –

Para Romeo Casabona, es "la destrucción o inutilización del soporte lógico, esto es de programas, así como de los datos contenidos en un ordenador o del soporte físico del sistema informático"[52]

El Diccionario de la Real Academia de la Lengua Española, define al Sabotaje como "Daño o deterioro en la maquinaria, productos, etc., se hacen como procedimiento de lucha contra los patronos, el Estado o contra las fuerzas de ocupación en conflictos sociales o políticos".[53]

En términos jurídicos, es según Ranieri "El daño voluntario a edificios destinados a establecimiento agrícolas o industriales ajenos, o de maquinarias, herramientas, aparatos o instrumentos destinados a la producción agrícola o industrial."[54]

De lo anotado podemos definir al sabotaje en general como un daño que se procura en bien ajeno, con el fin de que con tal acto se produzca un daño aún más

---

[50] **RAMALLO – CASTILLO,** citado por Santiago Coba en su tesis Los delitos informáticos en la legislación ecuatoriana Pág. 76

[51] **COBA,** Santiago, Los delitos informáticos en la legislación ecuatoriana, Pág. 76

[52] **ROMEO CASABONA,** Carlos, citado por Claudio Magliona en su obra Delincuencia y Fraude Informático, Pág. 175

[53] **Diccionario de la Real Academia de la Lengua Española**

grande y grave. Así esta conducta aplicada a la informática, sería el mal funcionamiento del sistema por existir otros problemas que lo producen de manera premeditada.

Para Guillermo Cabanellas, el sabotaje proviene del término francés "sabots", que son "las almedrañas que los primeros trabajadores que recurrieron a este sistema violento arrojaban a las máquinas para producir su brusca detención y su rotura incluso", además dice "ir u obrar en contra de los intereses que están encomendados"[55], en fin, es un modo de causar daño a instrumentos que pueden facilitar el trabajo, dándole una estructura penal a dicha figura, que atenta contra los intereses económicos de una institución sea pública o privada.

Nuestro Código Penal, lo clasifica en tres categorías: Sabotaje en casos de incendio, inundación, naufragio u otra calamidad; Sabotaje a servicios públicos o privados; y, Sabotaje a la producción"[56], pero en las tres categoría se hace referencia a la conducta maliciosa que pretende el sujeto activo de paralizar de cualquier modo una actividad, causando alarma social en unos casos, y pérdidas económicas en otras.

Si bien la doctrina jurídica sobre el sabotaje, no coincide con el concepto trasladado al estudio informático de los delitos, se ha considerado, que el acto de sabotaje atenta de alguna manera contra un bien intangible como es la información contenida dentro de un sistema computacional, dándole ese carácter de bien a la información, es que se puede considerar como una conducta penal antijurídica al sabotaje informático.

La polémica se produce tras la marcada intención en la actualidad de considerar a la información como un bien, como lo han venido haciendo

---

[54] **RANIERI,** Silvio, Manual de Derecho Penal, Tomo V, Pág. 40
[55] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo VII, Pág. 265

especialmente los países donde esta normado este tipo de conductas, la información como tal, es un conjunto de datos "sean en forma de números, imágenes o palabras"[57] que organizados de manera automática por el computador se presentan de manera clara a los ojos del usuario, pero estos datos pueden contener caracteres referentes a la vida privada de las personas, a los secretos comerciales de las empresas, al sigilo profesional, en fin, pueden ser altamente peligrosos en manos ajenas a las de su propietario o usuario.

Por eso es necesario considerar a la información como un bien intangible, pero apreciable en dinero, como dice León "el bien jurídico informático es la información"[58], puede ser tan o más valiosa que el mismo derecho a la vida de la persona, la información es un bien, para unos más preciado que para otros, pero que requiere tener ese carácter de protección penal, para evitar su mala utilización.

Se lo puede asumir como dice Solano, a una especie de "vandalismo contra la integridad de los elementos informáticos"[59], ya que se busca la destrucción o paralización de un sistema.

El sabotaje informático, acoplándose al criterio penal, es aquel mediante el cual se puede borrar, sustraer, suprimir, ocultar, modificar o inutilizar, sin autorización los datos, programas o diversas funciones de una computadora, con el objetivo de impedir su normal funcionamiento, ya sea para causar un daño momentáneo o permanente, que inutilice de forma parcial o total, el desempeño de la máquina, introduciendo en el sistema un programa que realice tales funciones.

---

[56] **Código Penal Ecuatoriano,**
[57] **Diccionario de Términos de Computación**, Pág. 251
[58] **LEON,** Fernando, De la comunicación a la informática jurídica penal, Pág. 57
[59] **SOLANO,** Orlando, Manual de Informática Jurídica, Pág. 282

Existen algunas formas de cometer este tipo de delitos: virus, gusanos, bombas lógicas, rutinas cáncer, etc.

El sujeto activo, sin duda es una persona altamente capacitada especialmente en la destrucción de las seguridades de un sistema, recibe el nombre de Cracker, sin embargo discrepamos de tal denominación, ya que como se explicará más tarde el cracker realiza otro tipo de funciones, y se lo podría incluir si lo hace desde funciones remotes y con la ayuda de un acceso de conexión telefónica, para nosotros el sujeto activo, puede ser un individuo que por razones de su empleo o por tener cierto acceso a los sistemas, puede realizar estas acciones, incluso sin ser un experto, ya que el que posee leves nociones sobre el manejo de un sistema puede borrar intencionalmente un programa o alterarlo y así producir un daño, el sujeto pasivo, pueden ser personas naturales por la información que estos posean o personas jurídicas públicas o privadas, estas últimas dependiendo de su actividad.

El sabotaje de manera general es una como dice Maggiore "una forma de daño calificado"[60], es decir que en el ámbito del tema, altera, modifica, omite o aumenta datos, para provocar daños al sistema o a determinados programas previamente seleccionados por el sujeto activo. Una empresa podría verse perjudicada, ya que mediante un sabotaje informático se puede destruir totalmente la información, o ciertos datos clasificados, o bien se puede destruir un programa, mediante la introducción de "Programas Borradores"[61], que complicarían el normal funcionamiento de la misma, provocando, como función misma del sabotaje, una parálisis total o parcial. Dentro de la categoría de las empresas, en su calidad de

[60] **MAGGIORE,** Giuseppe, Derecho Penal, Tomo IV, Pág. 25
[61] **SOLANO,** Orlando, Manual de Informática Jurídica, Pág. 296

sujetos pasivos, pueden ingresar las de producción, que serían blanco fácil especialmente de su competencia.

Muchos tratadistas actuales, que mantienen una posición indeclinable respecto de la antigua doctrina penal, no conciben esta actual tendencia, de considerar estas nuevas formas de delincuencia, y peor aun considerar como bien jurídico protegido a la información, cabe señalar que la los diversos convenios internacionales y las legislaciones mundiales, han considerado este tema por los graves perjuicios que han causado, y más aún consideran a la información, como un bien intangible, incluso apreciable en dinero, bien para su poseedor como para el que desea apoderarse de la misma, y además dentro de casi todas las legislaciones del mundo se ha protegido al software, como una creación humana, pero esta creación incluye como es lógico información, la cual si no fuera debidamente protegida contra ataques como el sabotaje, podría ser objeto de apropiación o destrucción indiscriminada por parte de terceros interesados en la misma, ya sea para obtener lucro, o por que simplemente no les interesa que la misma se divulgue por cualquier medio.

Existen muchas formas de atentar contra un computador como fin de la infracción, así tenemos que dentro de esta conducta podemos hallar las siguientes formas de sabotaje informático: virus, gusanos, rutinas cáncer, bombas lógicas.

Virus. –

Es un programa creado por expertos en el área informática, que pretenden la destrucción total o parcial del sistema, causando graves daños al mismo, muchas veces irreparables, suelen introducirse por cualquier medio de acceso de la información, como un disquete, la instalación o descarga de un programa a través del

Internet, la recepción y apertura de un mensaje electrónico, se reproduce con mucha facilidad, y actúan en el momento preciso de su programación, se los puede transmitir de un sistema a otro con mucha facilidad, pueden ser combatidos con los denominados antivirus.

Se los conoce también con el nombre de Bichos, a decir de Solano, actúan llevando una serie de instrucciones, las cuales permiten su desarrollo a manera de copias o clones, que se introducen en los lugares y programas sanos del sistema conforme se vaya trabajando o utilizando los mismos, según Solano, hoy en día existen más de cien virus, al menos conocidos.

Según su programación pueden ser simples molestias al sistemas como el *ping – pong,* denominado así, ya que una vez desarrollado, se lo puede apreciar en la pantalla como una pelotita que esta rebota en los bordes, o pueden ser constantes como el virus del viernes 13, que tenía como fin la destrucción de programas y memorias militares israelitas, el 13 de mayo de 1983[62], y que suele activarse cada vez que llega esta fecha, y hay otros muy temidos y peligrosos que han alcanzado fama mundial como el Michelangelo, Surivo 3, Alabama, Form, Sunday[63], Pakistán o Brian, Scores, Jerusalén, Typos, Viena, Madona, etc.[64] que ha afectado a muchísimos ordenadores en todo el planeta.

Los virus se pueden clasificar de varias formas, así tenemos:

Según su tipo:

Benignos. – Son simples mensajes que no causan problemas, aparecen como meras informaciones, sin destruir o modificar la programación o los archivos del sistema.

---

[62] **VIEGA,** María José, Un nuevo desafío jurídico, Pág. 9
[63] **GUIBOURG,** Ricardo, Manual de Informática Jurídica, Pág. 278
[64] **SOLANO,** Orlando, Manual de Informática Jurídica, Pág. 289

Malignos. – Son todo lo contrario, su nombre lo indica, provocan terribles problemas, incluso al soporte físico del sistema (hardware), pueden destruir desde simples archivos, carpetas, programas y hasta todo el disco duro, impidiendo de forma total o parcial el normal funcionamiento de la máquina.

Según el grado de infección, para Solano son de arranque, del sistema o genérica[65]

De arranque. – El virus infecta el programa del sector de arranque de carga del sistema, el cual forma parte del disco duro.

Del sistema. – Ataca al sistema adhiriéndose a la memoria principal, y actúa dentro del margen de una fecha determinada por el agresor.

Genérica. – Se aloja dentro de los archivo ejecutables y se desarrolla cuando una vez que se ejecuta dicho archivo, luego se traslada a la memoria principal y contagia a los demás.

Según su accionar:

Rápida o inmediata. – Una vez introducidos en el sistema, comienzan a contaminar el mismo, sin esperar ninguna ejecución de programas o archivos.

Lenta o posterior. – Luego de ser introducidos, pueden demorarse algún lapso de tiempo, establecido por su autos, para que, cumplido el mismo se desarrolla y actúa, o bien se aloja dentro de un programa o parte del sistema sin causar daños, pero actúa conforme se vaya ejecutando un determinado programa, mientras más se usa el mismo, más daños causa el virus.

No se ha podido determinar las causas por las que se suelen fabricar estos programas, se cree que de alguna manera sus autores los realizan con fines militares y comerciales, no obstante, existe un elemento fundamental casi no tomado en

[65] **Ibid. Op. Cit.** Pág. 289-290

cuenta, que es el considerar a más del intelecto del autor su condición anímica que lo lleva a fabricar los mismos.

El problema de los virus es que su fabricación, se la debemos a los mismos individuos relacionados con la ciencia informática, llegándose a creer incluso, que son los mismos fabricantes de antivirus, los creadores de los virus, con fines netamente comerciales.

A nivel de los antivirus, se ha desarrollado varios programas tendientes a detectar, eliminar y proteger de las diversas clases virus, como es lógico suponer aún no se ha creado un verdadero antivirus que proteja de todos los conocidos, pero existen muchos que al menos prestan defensas de la mayoría o los más peligrosos, dentro de estos antivirus encontramos los siguientes:

- Norton Antivirus V 2000
- Univirus V 7.0
- Map-ram
- Scan Virus

Gusanos. –

Son fabricados de manera similar a un virus, y que incluso pueden causar los mismos daños, pero la diferencia es que no tiene la posibilidad de reproducirse, es decir una vez infiltrados solo pueden causar el daño para el que fueron introducidos y nada más, es decir causaran el problema al programa o archivo para el que fueron creados.

"En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno"[66], si bien un tumor benigno no causa

[66] www.stj-sin.gob.mx/Delitos_Informáticos2.htm

daño, no podemos considerar al gusano bajo tal parámetro, ya que si bien no causan los mismos daños que un virus, es innegable que son productores de muchas fallas del sistema, provocando graves daños al mismo.

Rutinas cáncer. –

"Distorsionan el funcionamiento del programa y se autorreproducen al estilo de las células orgánicas alcanzadas por un tumor maligno"[67]

Para Sieber son "instrucciones que consumen poco tiempo de programa y en una serie de comandos que producen una reproducción del programa cáncer en otras partes del programa de aplicación, arbitrariamente escogida, durante cada uso"[68], al igual que todo tipo de cáncer médico, si no se lo extrae se sigue reproduciendo, por lo que son una especie de virus, aunque no cause daños tan graves, pero si una vez descubiertos no se lo elimina en su totalidad, basta que solo uno se haya quedado para que los problemas de reproducción persistan.

* Tanto en los virus, gusanos y rutinas cáncer, el creador posee un alto grado de conocimiento sobre los sistemas informáticos, conoce a fondo los mismos, y sabe que clase de accesos vulnerables poseen.

Bombas Lógicas. –

Introducción de ordenes no permitidas, dentro de un sistema, para que en un momento determinado, o tras la ejecución de ciertos procedimientos, realice la destrucción de cierta información deseada, produciendo constantes y posteriores interferencias dentro del sistema afectado, siendo además muy difíciles de detectarlas.

---

[67] **GUIBOURG**, Ricardo, Manual de Informática Jurídica, Pág. 280

[68] **SIEBER,** Uhlrich, citado por Santiago Coba, en su tesis Los delitos informáticos en la legislación ecuatoriana, Pág. 93

La diferencia fundamental, incluso con el mismo virus, es que posee el "máximo potencial de daño"[69], por lo que sus consecuencias pueden ser mucho más graves, precisamente por ese sistema que le permite al autor introducir el programa bomba, para que este funcione o se active, en un determinado período de tiempo, ya sea corto o largo, o para que se active y estalle tras la ejecución de un determinada orden o programa.

Espionaje Informático. –

Forma de un enriquecimiento económico ilícito, mediante la obtención no autorizada de datos introducidos en un sistema computacional ajeno, sin embargo la figura pude variar, ya que en sí, es la vulneración de la seguridad, para acceder a información privilegiada, incluso con fines políticos, militares, industriales o como se dijo generalmente para fines económicos personales o de terceros.

Es aquel mediante el cual se puede obtener información a través de medios informáticos, usando un computador y una línea telefónica, para violentar las seguridades incluso muy avanzadas del sistema, para acceder a información y beneficiarse de la misma a favor personal o de terceros, o bien para demostrar sus habilidades de penetrar en sistemas inseguros.

Según lo indica Cabanellas, "Comprende una fase informativa y otra de comunicar los datos a la fuente que ha de explotarlos"[70], figura explicativa de lo que se conoce como competencia desleal, aquel que accede a información privilegiada con fines lucrativos, para perjudicar a los propietarios de la misma.

---

[69] www.stj-sin.gob.mx/Delitos_Informáticos2.htm

[70] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo III, Pág. 553

Dentro de la rama informática del derecho, se la puede asemejar a aquel individuo, que con ayuda de un computador accede a información de empresas o personas naturales, para aprovecharse de la misma, con fines generalmente ilícitos.

Guibourg denomina al sujeto activo como Hacker, el que actúa para "su regocijo deportivo"[71], pero este sería una conducta sancionada tan solo como una contravención, y que hasta cierto punto no causaría graves daños, pero para considerar al espionaje informático como delito mismo, sería necesario establecer que el sujeto activo en este caso es efectivamente el cracker, ya que es el que vulnera la seguridad para obtener beneficios, contrario al accionar de un hacker.

Realmente que en este delito, el sujeto activo, si tiene profundos conocimientos de informática y sabe como trasladar esos conocimientos, para cometer la infracción penal, por su parte el sujeto pasivo, al igual que en casi todos los casos de delitos informáticos pueden ser tanto personas naturales como jurídicas. Hay muchas formas de cometer espionaje informático, entre las más destacadas están el Superzapping, el pinchado de líneas, las puertas falsas, y los delitos de Hacker y Cracker.

Superzapping. –

Es la forma de cambiar, alterar, borrar o insertar datos diferente a los guardados en los archivos de un sistema, mediante el ingreso no autorizado del mismo.

Como dice Magliona es una "especie de llave que abre cualquier rincón del ordenador"[72], esta denominación se la debe al programa Superzap, el cual tiene

[71] **GUIBOURG,** Ricardo, Manual de Informática Jurídica, Pág. 277
[72] **MAGLIONA,** Claudio, Delincuencia y Fraude Informático, Pág. 47

como característica poseer un acceso universal, el cual le faculta a ingresar dentro de un sistema, pese a las seguridades que éste pueda tener.

Comúnmente se lo conoce como llave no autorizada, que abre archivos protegidos con sistemas de seguridad, para modificarlos de cualquier forma, que permitan la inutilización de los mismos, o para que estos arrojen datos diferentes o inexistentes dentro del sistema.

Pinchado de líneas. –

"Pinchar líneas de transmisión de datos y recuperar la información que circula en ellas"[73], método muy común, que permite interceptar la información enviada de una lado a otro, con la simple utilización de un módem que convierte la información análoga en digital, la que luego se la puede trasladar a una hoja de papel, gracias a una impresora.

Es lo que comúnmente se conoce como interferencia de líneas de comunicación, para acceder a la información por ellas trasmitidas, para aprovecharse de la misma y manipular los datos enviados, este tipo de delito es tan frecuente, e incluso tan antiguo como el mismo sistema de comunicación telefónica, sin embargo en la actualidad, por los métodos digitales es mucho más fácil de cometerlos, ya que la información puede ser interceptada por sistemas computacionales, que facilitan esta figura delictiva.

El método más sencillo de evitarla, es mediante el uso de la criptografía, que permite codificar la información mediante el uso de claves que transforman la misma en ilegible e incomprensible, y la cual solo podrá ser interpretada por el

[73] **CAMACHO LOSA,** citado por Claudio Magliona en su obra Delincuencia y Fraude Informático, Pág. 59

receptor de dicho mensaje, claro que esto implica un acuerdo previo entre el que el envía el mensaje y el que lo recepta.

Se entiende por Criptología "el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor", mientras que la criptografía es "la parte de la Criptología que estudia como cifrar efectivamente los mensajes"[74], sin embargo pese a presentarse como una solución, este tema a traído mucha controversia, existen países como Francia y China en donde esta expresamente prohibido el uso de mensajes encriptados o cifrados, en otros como los Estados Unidos esta muy controlado, hoy en día incluso, tras las amenazas terroristas no se permite la importación de programas encriptadores, por ser considerados como una especie de armamento, mediante el cual se pueden comunicar los agresores sin que sus mensajes corran el riesgo de ser descubiertos.

Sin embargo este tipo de controles contrasta especialmente con la libertad de expresión y el derecho a la intimidad que tenemos todos los seres humanos, con el agravante de que por ejemplo cuando la información viaja por el Internet, esta puede quedarse en el ciberespacio por un tiempo indeterminado, sin que nosotros podamos suponer quien la puede estar copiando o almacenando. Pero lo importante del caso es impedir que nuestros mensajes sean interceptados, pero si así resulta, lo que se busca es que dichos mensajes no puedan ser descifrados por quien los intercepta, y esto se lo consigue únicamente gracias a la criptología.

[74] www.ctv.es/USERS/mpq/criptologia.htm#enlaces

Puertas falsas. –

Introducción al sistema, valiéndose de accesos no establecidos en las instrucciones generales, que permiten revisar o recuperar información cuando se produce un error en el sistema de programación.

Generalmente al autor de este delito, puede ser el programador del sistema, o el que mantiene íntimo contacto con el ordenador, es decir el operador de la máquina, se puede aprovechar ciertos errores producidos durante el normal funcionamiento de la computadora, ciertos datos por dichas fallas, aparentemente no pueden ser recuperados, por lo que se suele indicar que la información se ha perdido, pero existen accesos no conocidos por el usuario, que permiten acceder y aprovecharse de esta información.

Como dice Ricardo Guibourg, son las "que permiten a los programadores producir rupturas en el código y posibilitar así accesos futuros"[75], en consecuencia, el sujeto activo de la infracción es sin duda un individuo que posee gran conocimiento del área informática, ya que descubre en el sistema o programa los ingresos que le permiten acceder a la información mas tarde.

El mismo autor nos presenta el ejemplo llamado "caso Rifkin", en el cual, el perjudicado fue un banco de los Estados Unidos en Los Ángeles, el mismo que registraba usualmente un movimiento diario de decenas de millones de dólares mediante trasferencias electrónicas, Stanley Rifkin, especialista en informática fue contratado por el banco para realizar una copia del programa que efectuaba dichas transferencias, pero descubrió que el sistema poseía algunas fallas que facilitaban realizar transferencias ilegales, una vez que término su trabajo, se guardo para sí una

[75] **GUIBOURG,** Ricardo, Manual de Informática Jurídica, Pág. 276

tarjeta plástica que facultaba el ingreso al sistema. El 25 de octubre de 1978, regreso al banco e indico a los empleados que debía verificar el normal funcionamiento del programa, y descubrió que éste seguía siendo el mismo del que instalo, anoto el código de ese momento, ya que éste se lo cambiaba diariamente y se lo publicaba en una cartelera, se retiro del banco, y, luego se conecto con el sistema usando un pequeño computador y transfirió a su cuenta bancaria en Nueva York diez millones doscientos mil dólares, y luego los trasfirió a un banco en Suiza, a su retorno de Europa fue descubierto, detenido y condenado.[76]

Hacker. –

Delito mediante el cual, se accede a sistemas no autorizados, violando sus seguridades, generalmente realizado por jóvenes que disfrutan de esta actividad, no pretenden causar daños, sino demostrar sus habilidades.

Se considera al hacker como un fanático de la informática, que son capaces con un "modem de acceder a redes de transmisión de datos saltándose las medidas de seguridad y leer información confidencial, sustraerla, alterarla, destruirla o cometer fraude sobre ella"[77], sobre esta característica podemos decir, que si bien esta es la función primordial de un hacker, según como ellos se definen, no suelen causar ilícitos, es decir, solo acceden a la información, más no se aprovechan de la misma, por lo que a criterio nuestro esta figura encuadra más en la del cracker, pero como se dijo, el hecho mismo de acceder a redes de sistemas que contienen datos privilegiados, ya significa cometer una infracción.

---

[76] **Ibid. Op. Cit.** Pág. 276
[77] **SOLANO,** Orlando, Manual de Informática Jurídica, Pág. 288

Se considera al hacker como un "programador hábil"[78], pero otros los consideran como simples allanadores de sistemas computacionales, Eric Raymond, compilador de The New Hacker's Dictionary, indica que un "buen hack" es "una solución astuta a un problema de programación" y "hacking" es "el acto de lograrla".[79], el hacker, sin duda que se lo puede considerar como un genio informático, lo que de ninguna manera justifica su accionar, pero si algún beneficio a reportado esta actividad, es el de poner alerta a las diversas empresas que han visto vulnerado sus sistemas, para tomar medidas de seguridad que limiten dichas acciones.

Se suele decir que las acciones de los hackers son conductas anti éticas, si bien el hecho de acceder a sistemas de información sin autorización se puede considerar como actos ilícitos, también es cierto que estos sujetos son consecuencia de la misma informática, que ha sido la que de una u otra forma ha permitido tales conductas, los programas informáticos son creados por el ser humano en base a sus necesidades, siendo ellos mismos los que han facilitado la consumación de tales actos.

Concatenando lo expresado Ripper, dice que "El hacker, no puede ser considerado antiético por el hecho de que tiene su propia ética, hay que ver si esta ética coincide con la de las demás personas que tienen un pensamiento muy distinto al de los hackers, que buscan la verdad y no el conformismo como el resto de las personas."[80], no obstante a tener un código de ética, cada persona es responsable por sus actos, y el acceso no autorizado a la información, desde la óptica de un hacker no es delito, cualquier persona puede ver vulnerada su privacidad, y con todo derecho

---

[78] **YAMMENI,** citado en la Página www.dva.com.ar
[79] **RAYMOND,** Eric, citado por Yammeni, en la página www.dva.com.ar

puede exigir sanciones penales sobre el autor de tal violación, pero desde otras perspectiva, el hacker es un individuo investigador, que cree firmemente en la libertad de expresión, contrario a las limitaciones que la propiedad intelectual y los derechos de autor imponen, considera especialmente que, la información debe ser pública a todo nivel, son contrarios además a las políticas de restricción que muchos estados imponen, pero lamentablemente si bien su labor puede ser desde su visión muy altruista, las normas dentro de una sociedad son para respetarlas, sino viviríamos en una anarquía, contraria a la época de globalización que se forja en el mundo, toda creación intelectual debe ser protegida, ese bien intangible llamado intelecto se vería gravemente afectado por estas conductas.

Existen muchos defensores de los hacker, que consideran que sus actuaciones deben ser valoradas y aplaudidas, pero es una figura delictiva, que puede ser utilizada por curiosidad, pero que sucedería y si tales actos se trasladarían a un sistema integrado de espionaje, sería fatal, todas las personas tenemos derecho a que ciertos datos no sean divulgados, la religión, filiación política, profesión, preferencia sexual o condición de salud, pueden ser datos altamente peligrosos en manos ajenas, y ni hablar de una persona jurídica, su situación financiera, su cartera de clientes, y en el caso del Estado, información confidencial como la militar, pueden caer en manos de personas que pueden jactarse de ser solo hacker, y que ingresaron al sistema por curiosidad, esa información pierde el carácter de privilegiada y puede ser utilizada con fines ilícitos.

Camacho Losa indica que son tres los procedimientos a seguir por un hacker para acceder a un sistema:

---

[80] **RIPPER,** citado en la Página www.delitos_informaticos.com

1. – "Encontrar el número de teléfono que le permita conectar con el ordenador
2. – Descubrir el identificativo que le permita abrir la sesión de trabajo
3. – Averiguar la clave de acceso (password) que le autorice a entrar en las áreas o ficheros reservados".[81]

Pero quien mejor que un hacker puede definir lo que ellos son, "Asklepyo", los define así:

"El Archivo de la jerga contiene un montón de definiciones del término 'hacker', la mayoría de las cuales tiene que ver con la afición a lo técnico, y la capacidad de deleitarse en la solución de problemas y al sobrepujar los límites. Si Ud. quiere saber como transformarse en hacker, bien, sólo dos son realmente relevantes. Existe una comunidad, una cultura compartida, de programadores expertos y brujos de redes, que cuya historia se puede rastrear décadas atrás, hasta las primeras mini computadoras de tiempo compartido y los primigenios experimentos de ARPAnet. Los miembros de esta cultura acuñaron el término 'hacker'. Los hackers construyeron la Internet. Los hackers hicieron del sistema operativo UNIX lo que es en la actualidad. Los hackers hacen andar Usenet. Los hackers hacen que funcione la WWW. Si Ud. es parte de esta cultura, si Ud. ha contribuido a ella y otra gente lo llama a Ud. hacker, entonces Ud. es un hacker."[82]

Como vemos, su conducta es semejante a la de un niño que asegura actuar por tener a su alcance las herramientas proporcionadas por su padre, es decir ellos se consideran una especie de víctimas del sistema, si no tuvieran las herramientas en su poder no podrían haber actuado, pienso que son solo justificaciones de sus actos, sin duda que son conductas reprochables, que deben ser penadas, talvez solo como

---

[81] **CAMACHO LOSA,** Luis, citado por Claudio Magliona, en su obra Delincuencia y Fraude Informática, Pág. 61-62

contravenciones en un comienzo y en caso de reincidencias aplicar penas más drásticas.

* En el capítulo 4, pondremos ejemplos de las actuaciones de los hackers

Cracker. –

Aquel que accede a un sistema violentando sus seguridades, pero con fines ilícitos, no por curiosidad sino para causar daños, bien sea al sistema o bien a su operador o dueño y obtener de tales daños un beneficio personal o para terceros.

El cracker a diferencia del hacker, es el que accede a la información para aprovecharse de ésta, muchos suelen confundir los dos términos, se ha llegado a decir que son figuras delictivas sinónimas, pero cabe aclarar, que en este caso, el cracker ingresa al sistema no para demostrar sus habilidades, sino que tiene un objetivo, apoderarse de la información y sacar un beneficio lucrativo del mismo, los hacker son opuestos a la forma de actuar de un cracker, sobre el mismo tema Ripper dice que el cracker "tiene como intención destruir"[83], según el autor citado y férreo defensor de los hacker, lo que más molesta a estos, es encontrar en diversos artículos la confusión entre las dos figuras, no aceptan ser considerados como delincuentes, siendo los hackers los primeros a condenar la actuación de un cracker, por ser éste el que vulnera con fines delictivos los sistemas de seguridad de un operador.

La palabra cracker procede del verbo inglés "to crak", que significa "romper algo o descifrar un código"[84], pero un cracker no solo violenta la seguridad o la rompe sino que además busca adueñarse de la misma, para posteriormente sacar provecho, siendo causa de chantajes interminables.

---

[82] www.dva.com.ar
[83] www.delitos_infromáticos.com
[84] www.dva.com.ar

Existe una airada discusión sobre la diferencia entre los hacker y los cracker, unos a otros se acusan de sus actos, son opuestos entre sí, pero lo único cierto es que todo craker inicio siendo un hacker, que vio en tal actividad una forma de hacer dinero fácil, vendiendo información a gente interesada sobre la misma, pero sea cual sea la finalidad de unos u otros, la verdad de todo es que ambos proceden de la misma forma pese a ser su objetivo diferente, rompen las seguridades y acceden a información, y esa vulneración es la que la normativa penal debe tipificar como delito.

3. - Uso de la máquina como medio, para cometer otros daños

Piratería Informática. –

Si bien el término piratería esta más ligado con hazañas antiguas relacionadas con historias en alta mar, cometidas por piratas que buscaban riquezas, incluso así considerado por nuestra normativa penal vigente como el delito que se comete dentro de las aguas territoriales, trasladado este criterio más a un campo práctico que a una batalla acuática, se lo puede entender como una aprovechamiento de bienes exclusivos, para reproducirlos de manera ilegal.

Cabanellas dice que es "la destrucción o apoderamiento sin escrúpulos de los bienes ajenos"[85], en sentido informático se la ha considerado como el delito de reproducir programas sin autorización.

Es la forma más común y más fácil de cometer de este tipo de delincuencia, consiste en la reproducción sistemática y continua de programas de computación, en otros soportes similares como diskettes, CD, CD Rooms o DVD, mediante la utilización de otros computadores dotados del sistema de copia, que son

[85] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo VI, Pág. 250

comercializados en la mayoría de los casos a bajos precios, pero que no brindan las mismas garantías que los originales.

La piratería informática ha despertado gran interés, dentro de los tratadistas de la materia, debido a que no solo son conductas que afecten al área informática, como simple protección a un software o hardware, sino por que esta práctica se ha generalizado en otros ámbitos como el musical o literario, que llevan inmersos los derechos intelectuales a ser protegidos, como ejemplo de este accionar, lo podemos evidenciar en nuestro país, en cualquier lugar se puede observar a inescrupulosos que vende a vista y paciencia de todos los denominados discos compactos piratas, que se los adquiere a un costo relativamente bajo con relación a los originales, con una diferencia que oscila entre diez o doce dólares, pese a las acciones tomadas por las autoridades, es una utopía pensar que estos comerciantes informales abandonen su práctica ilegal, pero la más sorprendente es que, en los últimos meses este copia de productos se ha extendido al ámbito informático, así, no es raro observar en los lugares de expendios de revistas y periódicos la venta de algún software.

El problema implica que, el autor de la obra (CD, libro, Software, etc), no puede obtener los beneficios que por derecho le corresponden, según la Ley de Propiedad Intelectual de nuestro país, se protege las obras de entre otras clases "Art. 8 Lit. k) A los Programas de ordenador"[86], que son consideradas según la misma ley como "obras literarias y se protegen como tales"(Art. 20)[87], lo que abarca que sobre esa obra esta por detrás el intelecto, la creación imaginaria y materializada del

[86] **Ley de Propiedad Intelectual del Ecuador**
[87] **Ibid. Op. Cit.**

programa, la misma que es protegida, teniendo el autor el derecho de autorizar o no su reproducción y utilización.

Como dice Guibuorg, la creación de un software implica "inteligencia, imaginación y muchas horas de trabajo"[88], lo cual de algún modo debe reportar un beneficio a su autor, de lo contrario, tampoco sería justo aprovecharse de la creación, si bien el adquirir un programa (software) resulta costoso, los beneficios son muchos, por garantía, por seguridad y por saber que esa adquisición no implica un acto ilícito, pero que seguridad puede brindar una copia no autorizada?, a quien acudiremos a reclamar futuros daños en la máquina, bien cabe el término "Lo barato sale caro".

Muchas legislaciones consideran a la copia para uso personal solo como contravención, mientras que a la copia múltiple con fines comerciales, como un delito, sin embargo nos preguntamos, cuantas copias pueden hacerse de un programa original, con fines personales, sin duda que muchas, sin que implique que los diversos copiadores reproduzcan la misma con fines comerciales, es el caso de las empresas que adquieren un solo sistema original y que van reproduciéndolo en cada uno de sus ordenadores.

En nuestro país se aplico una normativa tendiente a regular este proceso ilícito, sin embargo no ha producido los resultados esperados, Horacio Fernández nos trae a colación acorde a lo estudiado, tres formas de cometer piratería informática:

1. – "Copia ilícita realizada por usuarios individuales
2. – Copia ilícita con fines comerciales
3. – Copia ilícita realizada por usuarios corporativos"[89]

[88] **GUIBOURG,** Ricardo, Manual de Informática Jurídica, Pág. 254
[89] **FERNÁNDEZ,** Horacio, Protección Jurídica del Software, Págs. 37-40-43

En este tipo de conductas, al contrario que la mayoría de los delitos informáticos, el sujeto activo de infracción puede ser cualquier persona, dotada simplemente de los aparatos necesarios para reproducir los programas, como el que posee una fotocopiadora y reproduce libros completos para la venta, y son tan modernos los medios electrónicos que su consumación resulta fácil para el autor.

El sujeto pasivo de esta infracción, es el autor, el creador de la obra, sin embargo existen otros agentes que facilitan dicha conducta, el consumidor final, el común de las personas que ven un ahorro significativo el adquirir programas ilegítimos (piratas), pese a las constantes advertencias de los futuros problemas, el único medio de evitar este delitos, es primero imponiendo drásticas sanciones a los infractores y fomentando una verdadera cultura ética sobre el daño que se causa al adquirir este tipo de productos.

Falsificación Informática. -

Doctrinariamente se entiende a la falsificación como "Adulteración, corrupción, cambio o imitación para perjudicar a otro u obtener ilícito provecho.// Delito de falsedad cometido en documento público o privado, en monedas, sellos o marcas"[90](77), como se advierte, es el hecho mismo de alterar algo, para luego utilizarlo dolosamente.

El Código Penal, hace referencias a tres tipos de falsificaciones:

1. – "Falsificación de monedas, billetes de banco, títulos al portador y documentos de crédito.
2. – Falsificación de sellos, timbres y marcas
3. - Falsificaciones de documentos en general"[91]

[90] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo IV, Pág. 13
[91] **Código Penal Ecuatoriano**

En lo que a nuestro estudio se refiere, podríamos encuadrar la norma penal en cualquiera de las figuras descritas, ya que es la utilización de un computador, con alto grado de resolución con el objetivo de fabricar documentos falsos, similares a los originales, para obtener beneficios dolosos del uso de tales documentos, muy utilizado para pasaportes, documentos de identificación, títulos universitarios, credenciales de manejo, etc.

Pero este concepto sería apegarnos a la analogía típicamente inaceptada en materia penal, lamentablemente nuestro Código Penal, no incluye la falsificación informática, el legislador no advirtió a tiempo que la falsificación desde hace alguno años atrás se la ha venido realizando con la utilización de medios informáticos, por las facilidades que este medio brinda, pero en esa lucha incansable por modernizar al Derecho, la nueva Ley de Comercio Electrónico, ha establecido una serie de reformas al Código Penal, en las que se incluye la falsificación electrónica y que al respecto dice: "**Artículo 61.-** A continuación del Art. 353, agréguese el siguiente artículo innumerado: **Falsificación electrónica.-** Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo." [92], pero no se refiere a la falsificación de documentos en general, sino a la información contenida en mensajes de datos, sin embargo consideramos necesario realizar una aclaración, ya que a nuestro criterio, este tipo de falsificación mas se asemejaría por la figura expuesta a la de fraude informático, o quizá a la violación de correo electrónico, entendiéndolo a éste como la mejor expresión de un mensaje de datos.

Para muchos autores el delito de falsificación informática, esta inmerso dentro del de piratería, pero como se anotó, éste posee otra característica, si bien pueden tener aspectos similares, como el hecho de reproducir algo, la falsificación a diferencia de la piratería, se caracteriza más por el beneficio que puede reportar no solo al autor material del delito sino también al intelectual, que es quien encomienda la labor, por lo que su diferenciación se hace imprescindible.

El número de casos de falsificación por medios informáticos, es interminable, incluso se puede programar a un ordenador para que reproduzca firmas, con rasgos tan precisos como el original,[93] y no se diga en los casos de falsificar documentos, este es aún mucho más palpable.

Como se dijo pueden existir dos sujetos activos, el que idea la acción y el que la materializa, siendo los dos altamente culpables, este último, el que realiza la falsificación, debe contar tan solo con un computador programado para tal función,

---

[92] **Ley de Comercio Electrónico, Mensaje de Datos y Firma Electrónica**
[93] **GUIBOURG,** Ricardo, Manual de Informática Jurídica, Pág. 279

un impresora, de preferencia tipo láser (con resolución de impresión muy alto), y obviamente con los distintos tipos de papeles según el documento a falsificar.

El sujeto pasivo puede variar, según el documento falsificado, y el objetivo que tenga el falsificador, pueden ser las personas jurídicas como los bancos, aduciendo falsas calidades, o las autoridades migratorias, para poder salir del país bajo identidad falsa, o cualquier persona natural como un comerciante al que se lo engaña haciéndose pasar por otra persona.

La figura es muy amplia, en nuestro estudio solo pretendemos demostrar como esta infracción acarrea graves daños a las personas que son víctimas de individuos maliciosos, que mediante la falsificación de documentos, ayudados por sistemas computacionales, pretenden causar perjuicios a terceros.

Homicidio informático. –

Guibourg dice "aunque que parezca increíble, es posible matar por computadora. Se han producido homicidios perpetrados mediante la modificación de las instrucciones dadas a un ordenador para un tratamiento médico"[94]

Si bien esta figura no ha sido considerada por la mayoría de autores, resulta importante y por demás interesante, saber que la computadora, puede ser un medio de cometer no solo delitos contra la propiedad, la intimidad, alterar o sustraer datos, sino que puede ser un medio idóneo para quitar la vida a otra persona, pese a lo espantoso que suena, sin duda que es una gran verdad, pese a no tener reportes sobre este delito, es simplemente una voz de alerta, especialmente para los grandes y modernos centros de salud, los cuales deben tomar las precauciones del caso en sus sistemas de seguridad informática, para evitar inconvenientes con sus pacientes

[94] **Ibid. Op. Cit.** Pág. 281

Hurto de tiempo. –

Uso indebido de centros o departamentos computacionales de instituciones por parte de los empleados, en horarios no autorizados, que si bien no pueden causar un daño a la empresa, pueden provocar la consumación de un delito mediante el uso de tales máquinas.

Esta modalidad suele ser tipificada en muchas legislaciones, como en el Estado de Virginia en el que se considera "propiedad" el "tiempo de computador o de servicio de procesamiento de datos"[95], se la considera incluso como un abuso de confianza, ya que los empleados pueden utilizar las máquinas con fines personales, como realizar trabajos ajenos a su actividad, pese a no correr graves riesgos el sistema, como se anoto se puede sin embargo cometer ilícitos como los mencionados anteriormente o aún peores, implicando en caso de ser descubiertos responsabilidad penal para la empresa de la que emano al acto ilícito.

En nuestro país la factibilidad de aplicación de esta conducta se vería inmersa más en sanciones administrativas que penales, cada institución debería restringir el uso de computadores a sus empleados para efectos personales ajenos a sus fines laborales, más la Ley podría simplemente establecer pautas para que las sanciones administrativas no atenten a las normas legislativas vigentes.

Hurto Informático. –

Previo al tratamiento de esta figura, bien vale la pena, hacer referencia de lo que el Hurto significa, en general esta comprendido dentro de los delitos contra la propiedad, "apoderamiento no autorizado de un bien mueble ajeno, con ánimo de

[95] **CORREA y otros,** Derecho Informático, Pág. 293

lucro, sin fuerza en las cosas ni violencia en las personas"[96], haciendo referencia a bienes muebles, ya que sobre bienes inmuebles operan otras figuras.

El Código Penal, tipifica al hurto en su Art. 547 "Son reos de hurto los que, sin violencias ni amenazas contra las personas, ni fuerza en las cosas, sustrajeren fraudulentamente una cosa ajena, con ánimo de apropiarse"[97], se recalca mucho respecto del no uso de fuerza en las cosas y amenaza a las personas, ya que de existir uno de estos supuestos la figura sería la del robo.

La doctrina penal entiende al hurto como el hecho en el "que se apodera de cosas muebles ajenas, sustrayéndolas al que las retiene, con el fin de sacar provecho de ellas para si o para otros"[98], en fin el hurto es el apoderamiento ilegal de una cosa ajena, pero sin que medien acciones violentas ni contra esa cosa ni contra su dueño, es decir, es una sustracción muy delicada de los bienes muebles ajenos.

La Ley de Comercio Electrónico si bien no indica como infracción la figura del hurto informático, nos presenta la siguiente figura, "**Artículo 63.-** A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados: **Art. Inn.- Apropiación Ilícita.-** Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas

---

[96] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo IV, Pág. 320
[97] **Código Penal Ecuatoriano**
[98] **MAGGIORE,** Giuseppe, Derecho Penal, Tomo V, Pág. 14

informáticos, sistemas informáticos, telemáticos o mensajes de datos."[99], dándonos una semblanza muy diferente de la tipificación normal del hurto que habla de la apropiación de cosas, en materia de delitos informáticos, se refiere a la apropiación de información, y por tal razón debemos asemejar y considerar a la información como un bien intangible susceptible de protección penal.

Esta diferenciación más de forma que de fondo, se refiere exclusivamente a la manera de establecer la infracción, es decir mientras en unos Estados o para una parte de los doctrinarios la figura sería la del Hurto informático, para el legislador ecuatoriano se convierte en una apropiación ilícita, pese a estar incluido en el capítulo del Robo.

Sobre el hurto informático, se podría decir que es la obtención de información no autorizada, mediante la vulneración de las seguridades del sistema, para acceder a datos, copiarlos de manera fácil, con fines ilícitos, que buscan provocar un daño a un tercero.

El Hurto Informático, es el delito mediante el cual se pueden apoderar de información, generalmente cuando se efectúan transacciones comerciales por medios informáticos, como la compra – venta de productos en el Internet.

Sin embargo, considerar que esta figura se verifica exclusivamente en este tipo de transacciones resulta ilógico, el Internet es solo uno de los tantos y variados métodos de cometer hurto informático, considerado tal vez el más frecuente y conocido, pero la figura misma puede encasillarse como una consecución de varios delitos, siendo ésta el objetivo final, es decir la sustracción o apoderamiento.

---

[99] **Ley de Comercio Electrónico**

Cuando de realizan compras por vía electrónica, se suele concretar la operación, mediante le pago de tarjetas de crédito, la empresa comercializadora verifica la seguridad de los datos consignados por el comprador, y procede a materializar la venta, pero que sucede cuando esas empresas no poseen medios de seguridad eficientes, estos datos (No. de tarjeta), son descubiertos por los infractores, estos se aprovechan de la misma y realizan varias compras, perjudicando a un tercero, en ningún momento hay uso de fuerza o violencia, todo lo contrario, este accionar es muy sutil, justamente para evitar ser descubiertos.

La figura del hurto informático, es muy sui generis y al mismo tiempo es muy debatida y analizada, se puede o no considerar al apoderamiento de la información como hurto, es una de las tantas preguntas que sobre el tema nos hacemos, como hemos venido diciendo la información debe y es considerada como un bien intangible, muchas veces apreciable en grandes cantidades de dinero, pero si para acceder a esa información se violentan los sistemas de seguridad, se podría decir que ya no hablaríamos de hurto, por que los actos previos desdibujan la figura penal, sin embargo, se considera más en el hecho de que violentar una seguridad no implica destrucción del sistema u ordenador, situación en la cual estaríamos frente a una figura no aceptada como el robo informático. Sin embargo esta determinación sería muy especulativa, por lo que apegados a la teoría sobre la materia nos atrevemos a decir que la figura del Hurto Informático esta bien establecida, la infracción es la misma que la establecida en el concepto de la clasificación de los delitos informáticos, por lo que sin duda que si podríamos llamar a esta figura en la legislación ecuatoriana y en general como Hurto, por la configuración de la infracción, por los efectos que esta produce y por las consecuencias de la misma.

La diferencia entre el robo y el hurto, es sin duda la utilización de la fuerza en las cosas o la amenaza a los propietarios de los bienes, para apoderarse de los mismos, sin embargo el robo informático más estaría sujeto a la figura misma del robo tratado por la doctrina y la ley penal, ya que el apoderamiento del bien puede recaer sobre el soporte físico (hardware) o sus accesorios (software), claro esta que también se puede cometer un hurto sin caer en la figura del robo, pero en el caso que nos compete, es la sustracción de bines ajenos (información), utilizando medios informáticos.

El sujeto activo es el que accede a los diversos datos y se aprovecha de los mismos, y el sujeto pasivo, puede ser un consumidor informático, o cualquier persona que posee información que puede significar beneficios lucrativos. El bien jurídico protegido en este caso es la información, el apoderarse de ella ilícitamente es que el configura al hurto informático.

Para algunos estudiosos sobre el Derecho Informático, y más sobre los delitos informáticos, resulta necesario establecer también la figura del robo informático, el robo como delito penal, es "Estrictamente, delito contra la propiedad, consistente en el apoderamiento de una cosa mueble ajena, con ánimo de lucro y empleando fuerza en las cosas o violencia en las personas"[100], y sobre el uso de la fuerza se refiere a la "desintegración, destrucción, demolición, rotura, fractura, alteración, etc., total o parcial"[101], como medio efectivo de consolidar la infracción y que lo difiere en su especie del hurto.

Nuestro Código Penal en su Art. 550 hace referencia la robo en los siguientes términos "El que, mediante violencias o amenazas contra las personas o

[100] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo VII, Pág. 249
[101] **MAGGIORE,** Giuseppe, Derecho Penal, Tomo V, Pág. 49

fuerza en las cosas, sustrajere fraudulentamente una cosa ajena, con ánimo de apropiarse, es culpado de robo, sea que la violencia tenga lugar antes del acto para facilitarlo, en el momento de cometerlo, o después de cometido para procurar su impunidad"[102], como advertimos esta tipificación no varía de la establecida por la doctrina penal, sin embargo nos vemos obligados a emitir nuestro criterio al respecto, no consideramos al robo como una conducta delictiva informática, el hurto informático, es el apoderamiento de la información, a la que consideramos necesariamente como un bien invalorable, el robo, es un apoderamiento material de una cosa tangible ajena, como entender entonces que pueda existir robo informático, muchos dirán porque se puede violentar una seguridad y acceder a información no autorizada, pero esa violación no se la verifica mediante el uso de una ganzúa que rompa un candado físico, sino es una serie de ordenes que violentan la seguridad del sistema, que puede causar daños, pero que de ninguna manera destruye el soporte material como tal, creemos firmemente que el robo, si lo queremos dar una connotación informática, sería la sustracción material de soportes informáticos (hardware, software), para apoderarse de estos y darles otros fines, incluso para verificar su información, pero ya no como delito informático, sino como un robo que lleva la consecuencia de sustraerse un computador, como parte misma de la infracción.

No obstante a lo anotado, gran parte de los estudiosos dicen que el hecho mismo de violentar una seguridad informática como por ejemplo el rompimiento de claves secretas (password), ya configuraría la infracción del Robo, sin embargo insistimos en la necesidad de asemejar la doctrina penal tradicional a esta figuras, si

[102] **Código Penal Ecuatoriano**

bien el Robo como tal esta ligado con la utilización de la fuerza y la violencia en las cosas para apropiarse de un bien ajeno, mal podríamos entender el romper claves, violentar seguridades de redes como un acto susceptible de apreciación visual, a la clave secreta se puede acceder de muchas formas, que el afectado no podría ni darse cuenta desde cuando ha estado afectado su interés o patrimonio, por lo que sería muy aventurero el considerar la figura como tal, una recomendación para normar estas conductas sería la de incrementar la sanción penal y pecuniaria en el caso de cometerse Hurto Informático, como una figura agravante del Hurto normal.

Violación de la Intimidad. –

La intimidad, significa "parte personalísima y reservada de un caso o una persona. Su divulgación puede originar responsabilidad cuando cause perjuicio o haya dolo o grave imprudencia."[103], se relaciona directamente con lo propio, lo personal, *lo más intimo* de una persona, lo que más cuida y preserva, que por razones naturales debe ser protegida.

La palabra intimidad viene del término "latino *intimus,* interior o interno"[104] además de manera extensiva se refiere también a la vida familiar o las diversas asociaciones de las que el hombre puede formar parte, pero que igual forma parte de la reserva legal.

El derecho a la intimidad esta protegido y consagrado en casi todas las constituciones del mundo, en el Ecuador no es la excepción, en el Art. 23 sobre los derechos reconocidos y garantizados por el Estado, entre otros No. 8 se establece "El derecho a la honra, a la buena reputación y a **la intimidad personal y familiar**. La

[103] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo IV, Pág. 485
[104] **LEON,** Fernando, De la comunicación a la Informática Jurídica penal, Pág. 82

ley protegerá el nombre, la imagen y la voz de la persona"[105], todas los seres humanos en el transcurso de nuestra vida nos vemos obligados a proteger ciertos datos que sin ser ilícitos, para nosotros resultan valiosos, muchas veces tan importantes que de ellos podrían depender futuros negocios.

El derecho a la intimidad dentro del ámbito informático esta ligado también con la protección de los datos, como se dijo, una persona puede consignar dentro de un computador una serie de documentos importantes, que posean información sensible, desde esta perspectiva debemos entender a la violación de intimidad por medios informáticos, como una de las formas de cometer este tipo de infracción.

Es el acceso no autorizado de un sistema, para conocer información de una persona, con fines ilícitos, generalmente de chantaje. Como dice Guibourg, "La introducción de datos personales en un archivo, su modificación, su copiado, empleo o destrucción pueden constituir actos ilegales"[106], y más aún la divulgación mal intencionada, es la que realmente configura la infracción.

La intimidad, como derecho constitucional consagrado, se convierte en una figura jurídica protegida, dentro del mundo informático los usuarios de los diversos sistemas son los más propensos a sufrir este tipo de acciones dolosas, estos datos requieren estar inmersos dentro de sistemas de seguridad, pero como muchas de las veces esto es casi imposible, se deben establecer normas que por lo menos garanticen que los mismos se encuentran debidamente protegidos por leyes especiales sobre la materia.

---

[105] **Constitución Política del Ecuador**
[106] **GUIBOURG,** Ricardo, Manual de Informática Jurídica, Págs. 280-281

Para muchos autores es tan simple como el "derecho a estar solo"[107], pero gracias a los sistemas computacionales esta información sobre las personas se transforman en los denominados bancos de datos automatizados, los cuales pueden estar bajo la custodia de diversas instituciones, dándole a la sociedad en general la posibilidad de conocer las características reales de un individuo, y precisamente esta facultad la que debe ser regulada, es decir, que nadie tanga la arbitrariedad de conocer a su libre albedrío la información confidencial de una persona sin su previo consentimiento.

A más de los datos establecidos con anterioridad, ciertos autores consideran también que deben estar protegidos jurídicamente dentro del ámbito de la intimidad y como trascendentales: "la toma de fotografías no autorizadas en lugares cerrados al público; el empleo de ciertas pruebas psicotécnicas en procesos de selección laboral o académica; y, la práctica secreta de análisis serológicos para detectar la infección por V.I.H."[108], entonces podríamos afirmar enfáticamente que todo lo que el hombre no desea que se ventile públicamente constituye su intimidad personal, y por lo tanto esta debe ser protegida por las normas legales.

Sin embargo no todo lo que el hombre protege esta en el marco de su intimidad, existen casos y situaciones en los que el Derecho, la Ley o la Costumbre, exigen que bajo ciertos parámetros el mismo hombre deba permitir que la autoridad acceda a esa información, debemos entender que la intimidad no implica únicamente información como bien protegido, sino que también la vida privada y los actos de las personas conllevan intimidad, pero estos actos deben estar dentro de la normativa legal, es por eso que las mismas leyes facultan a las autoridades a exigir de las

[107] **LEON,** Fernando, De la comunicación a la Informática Jurídica penal, Pág. 82
[108] **Ibid Op. Cit.** Pág 87

personas cierto tipo de comportamiento ante una determinada situación, y por eso tras el cumplimiento de formalidades legales, el Estado representado por sus funcionarios puede acceder lícitamente a la intimidad de las personas en los siguientes casos:

- Allanamiento para capturar al delincuente flagrante
- Allanamiento para capturar a la persona sobre la que pese orden de detención
- Allanamiento del lugar donde se está cometiendo un delito
- Allanamiento para rescatar a persona en inminente peligro
- Retención y apertura de la correspondencia en procesos judiciales
- Interceptar comunicaciones telefónicas
- Exhibición de documentos privados

Como vemos la intimidad esta ligada con la vida misma del hombre, esta debe y tiene que ser protegida por los medios legales, para evitar que la misma sea apropiada o divulgada en desmérito de los demás.

El antecedente normativo y constitucional de la protección del derecho de la intimidad es la figura del Habeas Data, sobre el cual se ha dicho que "...puede ser concebido como una acción judicial para acceder a registros o bancos de datos, conocer los datos almacenados y en caso de existir falsedad o discriminación corregir dicha información o pedir su confidencialidad"[109], como vemos es una figura que permite acceder a la información que sobre nuestros datos pueden o deban tener las diversas instituciones públicas o privadas, facultad que le permite al particular, de impedir la libre divulgación de sus datos, o la modificación de los mismos para no

[109] **PALAZZI,** Pablo, citado por Héctor Peñaranda, en su obra Iuscibernética Pág. 215

incurrir en futuros errores, es un mecanismo efectivo de la protección de los datos que involucran la intimidad de una persona.

Nuestra Constitución Política lo consagra de la siguiente manera "Art. 94. – Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como conocer el uso que se haga de ellos y su propósito.

Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización.

La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional"[110], el derecho a la intimidad esta ligado con esa privacidad personal a la que todos tenemos derecho en razón de nuestros intereses, si bien en nuestro lapso de vida dentro de una sociedad organizado, nos vemos obligados a consignar datos, como el nombre, la edad, la instrucción obtenida, u otros más sensibles, pero aunque ciertos datos son intrínsicos a nuestra condición misma de seres humanos, tenemos ese derecho a que si los mismos están mal consignados o han variado en el tiempo, como el cambio de estado civil, deben estar actualizados, para evitar problemas a futuro.

El concepto generalizado y ampliamente aceptado sobre lo que es el Habeas Data se refiere concretamente al derecho que tiene toda persona respecto de los datos que sobre si, posee o tiene otra persona, el colombiano Ramírez Suárez dice "El habeas data, o sea el derecho a conocer para los efectos de actualizar y rectificar

[110] **Constitución Política del Ecuador**

cualquier clase de información tergiversada en torno de la conducta de la persona, ya sea por razones individuales, de manejo bancario, crediticio y comercial, y sobre datos que puedan empañar la reputación o buen nombre de ellas y que están en poder de las diversas entidades públicas o privadas por cualquier causa. Informaciones en torno s récord educativo, a nivel de estudios primarios, secundarios y universitarios, récord sobre desarrollo de la salud, historial clínico y otros informes reservados, sobre actividades dentro del Estado como las sanciones dentro del régimen disciplinario, antecedentes policiales o penales..."[111]

Pero así como todos tenemos derecho a impedir que nuestros datos se divulguen libremente, todos también la posibilidad de recopilar libremente datos de los demás, y sin necesidad de violentar ningún derecho, justamente la autodeterminación de las personas, puede facilitar este objetivo, y es por eso que se debe normar, sin la autorización del interesado esta información se convierte en confidencial y sensible.

Es por esto que se han establecido ciertos criterios en base a los cuales las personas tiene derecho a conocer sobre sus datos:

1. – Derecho a acceder y obligación del poseedor a suministrar la información. – Es el que tiene toda persona de saber que clase de institución posee su información, y ha recibir de manera oportuna y célere la misma por parte de quien la tenga o la maneje.
2. – Derecho a rectificar y obligación del poseedor de cumplir. – Es el derecho que se tiene para solicitar a quien posee la información realice los cambios,

[111] **RAMÍREZ SUAREZ,** Jesús, citado por Fernando León en su obra De la Comunicación a la Informática Jurídica penal, Pág. 91 - 92

modificaciones o correcciones que sobre esos datos requiera el interesado cambiar, bien por ya no ser iguales o por ya no ser necesarios.

3. – Derecho al uso establecido y obligación del poseedor a cumplir lo mandado. – Facultad del interesado de exigir que la información que sobre si tiene el poseedor, sea destinada y utilizada para los fines requeridos.[112]

Otros delitos:

Existen otros tipos de delitos informáticos no contemplados por algunos tratadistas, ni incluidos en diversas legislaciones, bien por formar parte de otros delitos, o por ser consagradas ya como figuras independientes especialmente en las constituciones, o por ser considerados como parte de delitos penales ya existentes, pero de los cuales consideramos que deberían formar parte del tema de nuestra investigación.

La magnifica red de información como es el Internet, se ha prestado como herramienta para cometer infracciones no consideradas en el análisis anterior, por lo que a continuación expondremos lo que a nuestro juicio constituyen otros delitos informáticos no tratados por la doctrina y la informática penal.

Violación del correo electrónico "E- mail".-

Si bien podríamos incluirlo como una violación a la privacidad, esta figura básicamente forma parte de la violación de correspondencia normal como una carta, la misma que esta consagrada dentro de nuestra Constitución en el Art. 23 No. 13, el correo electrónico, es el mensaje que se envía desde un ordenador a otro utilizando los medios informáticos a través de la red (Internet). Es un medio de comunicación rápido y eficiente, pero que esta propenso a ser interceptado sin que

[112] **LEON,** Fernando, De la Comunicación a la Informática Jurídica penal, Pág. 93

significique que el mismo no llegará a su destinatario, sino que ese mensaje en el transcurso de su traslado de un ordenador a otro, viaja por una ruta dejando rastros, a los cuales pueden tener acceso otras personas ajenas al mensaje, y podrían interceptarlo, reproducirlo y darle un uso ilegítimo y doloso.

Los expertos en el tema recomiendan que para evitar acceder a un mensaje ajeno, se debe encriptar la información, la encriptación "Consiste en un mecanismo de codificación de la información a través de programas de encriptación, de modo tal, que pueda enviarse secretamente una información a través de las redes"[113], mediante los programas de encriptación se puede transformar la información legible en ilegible o incomprensible, lo que provoca que el interceptor del mensaje no pueda acceder al mismo, sin embargo esto requiere que tanto el emisor como el receptor del mensaje poseen los mismos programas y métodos de encriptación, para poder transformar la misma, el problema al que nos vemos expuestos, es que mientras no se posea este tipo de método, la correspondencia electrónica puede ser fácilmente violentada.

Existen aún problemas más graves, varias páginas Web ofrecen servicios de correo electrónico gratuito, sin necesidad de que el usuario deba suscribirse a un prestador de servicios de Internet y acceder a una cuenta personal proporcionada por esa empresa, si bien el servicio prestado brinda ciertas garantías, cualquier usuario incluso por error y por fallas en el sistema pueden acceder a una cuenta ajena, varios son los ejemplos de páginas que ofrecen estos servicios como: www.hotmail.com, www.latinmail.com, www.mixmail.com, las cuales presentan como atracción el término "mail" dentro de su nominación, en el Ecuador están páginas como

[113] **PEÑARANDA,** Héctor, Iuscibernética: Interrelación entre el Derecho y la Informática, Pág. 60

Ecuabox.com o Estaentodo.com, que pese a no indicar el término "mail", en ambos casos se pueden abrir cuentas de modo muy fácil, se consignan ciertos datos como nombre, dirección, teléfono, casilla postal, país de origen, edad, sexo, características físicas, etc, una vez aceptados se procede a solicitar al usuario una clave secreta "password", si no coincide con una ya existente, listo, ya posee una cuenta de correo electrónico gratuita, pero de que clave secreta hablamos, si el sistema de control de la página tiene acceso a la misma, con el ejemplo mencionado se desprende que si uno consigna una clave similar a otra, se nos solicita cambiar la misma por ya poseer otro usuario, los que manejan el control y mantenimiento de la página tienen acceso a dichas "claves secretas", y pueden ingresar a las cuentas y configurar el delito de violación del correo, y claro nunca sabremos que lo hicieron.

Pero hay problema más graves, estas mismas páginas ofrecen al usuario que olvido su clave, acceder a ciertos mecanismos que le permitan ingresar a su cuenta, la dirección electrónica en los últimos años se ha convertido en un dato más de cualquier persona, quien no lo posee no esta a la moda, y es muy común encontrarnos en tarjetas de presentación o en vallas publicitarias la dirección electrónica de una persona o empresa, eje: altamirano_fabian@hotmail.com o cfad@estaentodo.com, la primera parte corresponde al nombre o seudónimo del usuario, el signo @ que sirve para separar el nombre del usuario del nombre de la computadora en la cual reside el buzón del correo, y la última parte a la empresa que brinda el servicio, con solo saber la dirección, se ingresa a la página prestadora del servicio, y no se coloca nada en el espacio de la contraseña, clave o password, o se coloco cualquier palabra, inmediatamente el servidor le indica que la clave no corresponde con la original, y le da la opción que comúnmente dice "olvido su clave

personal, haga clic Aquí", se puede estar intentando cuantas veces lo desee el infractor y si tiene suerte en algún momento accederá a la información y mensajes del perjudicado, sin ser el usuario verdadero. Aún más fácil resulta si el delincuente informático tiene alguna relación con la víctima, podrá consignar datos relacionados con el usuario y el servidor le brindará la clave de acceso.

Pornografía y corrupción infantil. –

Para beneficio de unos y perjuicio de otros, el Internet no solo es una red de información, en la que encontramos acceso a páginas publicitarias, empresas comercializadoras, bibliotecas, deportes, servicios, etc, sino que lamentablemente y como bien dicen los expertos que el 80% aproximadamente de la información contenida tiene que ver con aspectos sexuales.

Pero no relacionado con temas de educación sexual, sino con verdadera pornografía a vista y paciencia de los usuarios que acceden a estas páginas, pero como bien se ha manifestado que la información en el Internet es libre para todos, mal podríamos impedir que esta se elimine, el problema no radica en sí por la información e imágenes contenidas, ya que cada persona es libre de permitir el uso y publicación de sus fotografías e historias, al igual que cualquier persona con criterio formado es libre de acceder a las mismas, pero lamentablemente el ingreso a estas páginas no esta regulado, si bien existen procedimientos mediante los cuales un usuario adulto puede limitar el ingreso a las mismas configurando su computador, también es cierto que son muy pocos los que se preocupan de hacerlo, dejando vía libre para que un menor de edad pueda ingresar.

Existen varias páginas en las cuales se advierte que el contenido de las mismas puede herir la susceptibilidad del usuario, o que contiene material exclusivo

para adultos e indican que si este no tiene la mayoría de edad según su país de origen debe salir, pero son solo simples enunciados, ya que con dar un clic en el lugar que dice "Ingresar", el problema esta resuelto, listo, como ellas dicen "Disfrute de nuestro contenido", y algo más grave "Recomiende esta página a un amigo", cualquier menor curioso ingresa y observa verdaderas obscenidades, cosas inimaginables incluso para un adulto, y peor aún se exhiben sin ninguna restricción fotografías no solo de hombres y mujeres desnudas que hacen gala de sus cuerpos, sino fotos de parejas teniendo relaciones sexuales (heterosexuales), y además otras de lesbianas u homosexuales, lo que podría desembocar en confusiones y desviaciones sexuales del menor, que puede asimilar como normales dichas actuaciones, existen algunas peores como relaciones zoofilias con animales, o los denominados fetichismos, es decir adoraciones a cierta clase de actividades sexuales que se convierten en agresiones.

Pero como dije, cada cual es libre de autorizar el uso de sus fotos e imagen como bien les parezca, y queda a libre criterio del usuario mayor de edad y con criterio formado el ingresar a estas páginas, incluso la libertad de preferencia sexual no limita el acceso a las mismas, ya que pueden haber personas con su preferencia sexual definida pero que pueden tener una mentalidad muy abierta, sin duda que en este caso no hablamos de pornografía infantil, sino de corrupción de menores, los cuales ingresan a las páginas sin restricción y disfrutan de su contenido, al respecto se ha previsto medidas de seguridad, en las cuales estos servicios deben ser otorgados bajo una prestación de dinero por parte del usuario, consignando el número de su tarjeta a la cuenta de la página, sin embargo siguen existiendo páginas a las cuales sin necesidad de pago se ingresa libremente a la información.

Pero que ocurre, cuando pese a las mismas restricciones sobre el tema, y pese a la realización de un pago previo, el usuario se encuentra con fotografías en las que esta un menor niño o niña teniendo relaciones sexuales con un adulto o entre menores, el cuadro es repugnante, no es necesario ser erudito en el tema para saber que ningún padre aceptaría la publicación de una foto de su hijo bajos esas circunstancias, sin fotos ilegales, en las que se fuerza al menor a realizarlas, bajo la dirección de verdaderos psicópatas sexuales, que disfrutan de esta cruel actividad, y claro, como "en gustos y sabores no mandan doctores", hay quienes disfrutan observando barbaries con menores, esta precisamente es la figura de la pornografía infantil de la red, existen muchos casos en los que se ha logrado detener a estos aberrantes, pero no existe un control por parte de las autoridades locales e internacionales, para impedir la publicación de este material lesivo para cualquier persona coherente, se debería implementar constantes investigaciones a los promotores de las páginas de adultos, para impedir la creciente ola delincuencial en materia de pornografía infantil.

A breves rasgos esta es una pequeña muestra de lo que en base a nuestra investigación, hemos podido establecer sobre los delitos informáticos, sin que sobre los mismos se haya dado la última palabra por parte de doctrinarios o legisladores, el tema es sumamente nuevo e interesante, y sobre él hay mucho camino por recorrer, tenemos la certeza que estos delitos con el tiempo se irán incrementando, o variaran especialmente en su forma de cometerlos, a lo que la sociedad en general debe estar alerta tomando medidas de seguridad, tendientes a proteger tanto a las personas naturales como jurídicas publicas o privadas de esta amenaza latente dentro del globalizado mundo en que vivimos.

El Código Penal ecuatoriano, establece los delitos de carácter sexual, estableciendo el proxenetismo y la corrupción de menores, sobre el primero el Art. 528.1 dice "El que promoviere o facilitare la prostitución de otra persona será sancionado con pena de prisión de uno a tres años, salvo que tuviere a su cargo una casa de tolerancia, establecida conforme a los reglamentos que la autoridad competente expidiere para esta clase de establecimientos"[114], si bien la figura de la pornografía infantil, no encuadra en esta figura, el Art. 528.2 agrava la pena según el Numeral 1ro, si "La víctima fuese menor de catorce años de edad" [115], pero advertimos que este es el caso de inducir a una persona a ejercer la más antigua de las profesiones, pero en nuestro estudio, establecimos el caso de la pornografía infantil a través del Internet, al respecto el mismo cuerpo legal en su Art. 528.6 indica que como corrupción de menores "Será sancionado con pena de uno a tres años de prisión:

1. – La exposición, venta o entrega a menores de catorce años de objetos, libros, escritos, imágenes visuales o auditivas obscenas, que puedan afectar gravemente el pudor o excitar o pervertir su instinto sexual; y,
2. – El que incitare a un menor de catorce años a la ebriedad o a la práctica de actos obscenos o le facilitare la entrada a los prostíbulos u otros centros de corrupción como cines o teatros que brinden espectáculos obscenos".[116]

El numeral uno establece la exposición de imágenes visuales o auditivas obscenas, libros, escritos u objetos con carácter sexual y como dijimos el Internet es una ventana abierta al sexo, no a la sexualidad educativa, sino a la libre exposición de actividades sexuales entre personas, pese a que como se anotó el proxenetismos

[114] **Código Penal Ecuatoriano**
[115] **Ibid. Op. Cit**

no encajaría en esta categoría, se ha establecido que ningún menor de edad, no solo de catorce años puede estar expuesto a riesgo sexuales, el consentimiento para que sea válido, lo debe dar una persona adulta y solo excepcionalmente un menor que tenga a criterio del juez, buen juicio de sus actos, pero que criterio puede tener un adolescente de quince años sobre los riesgos de su exposición sexual, creo que ninguna, incluso personas con criterio formado han sido víctimas de ultrajes y chantajes sexuales.

Al referirnos nosotros a lo obsceno hablamos de algo atentatorio a las buenas costumbres, "impúdico, torpe, inmoral como ofensivo para el pudor"[117], y la corrupción es la inducción a un acto ilegal, pero en el caso de la corrupción de menores, hablamos estrictamente en lo sexual, es el procurar la participación inmoral e ilegítima, incluso con consentimiento del menor, a la realización de actos tendientes a desarrollar la actividad sexual del mismo, para satisfacción de otro u otros, que gozan de dicha aberración.

Comúnmente se los conoce como pedófilos, sin embargo la figura a la que hacemos referencia no va dirigida a quienes disfrutan, sino a quienes corrompen a los menores, induciéndoles a esta actividad, y no solo como objetos sexuales, es decir procurando que participen en actividades sexuales, sino incitándoles a disfrutar de actividades ajenas a su edad y condición, por tal razón se tipifica y se pena la exposición a menores de materiales alusivos al sexo, aunque ya no solo el Internet se convierte en el mejor medio de acceder a esta clase de imágenes, ahora en nuestro país es muy común encontrar a la venta ya no solo revistas o libros de sexo, sino que se pueden adquirir a precios bajos películas en formato DVD, e imágenes en CD

---

[116] **Ibid. Op. Cit.**
[117] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo V, Pág. 643

Room, que poseen material pornográfico, los cuales se expenden a vista y paciencia de los menores, estas deberían ser también las imágenes, textos o escritos que pretende alcanzar la norma penal.

Creemos pues, que se debe regular el libre acceso a ciertas páginas de la red, para impedir la propagación, sino de la pornografía en general, ya que cada cual es libre de acceder a la información que desee, pero sí, de controlar el libre acceso de menores, y por sobre todo evitar esas imágenes infames de menores abusados sexualmente, y digo abusados, porque no creo que estén en libertad de expresar su consentimiento para tales actos, y menos para ser admirados por enfermos sexuales.

CAPITULO 2.- TRATAMIENTO INTERNACIONAL

2.1. – ORGANISMOS INTERNACIONALES. – Situación Internacional

El tema de los delitos informáticos ha despertado gran interés a nivel mundial, los países denominados del primer mundo, desarrollados o industrializados, han sido los primeros en preocuparse de este tipo de conductas y actuaciones, si bien el inicio mismo de estos actos no se ha podido determinar con precisión, los intentos por legislar sobre la materia datan aproximadamente desde finales de los años setenta, período durante el cual se evidenciaron varios casos, especialmente de fraudes a bancos, valiéndose del uso de sistemas informáticos.

Muchos aseguran que estas infracciones aparecieron con la llegada del Internet, pero mucho tiempo atrás, especialmente las instituciones financieras ya mantenían un sistema integrado de computadores a través de redes electrónicas, sin el uso de una terminal telefónica, sistema básico para el desarrollo y propagación del Internet, por lo que sería injusto y malintencionado pretender responsabilidad a este gran invento como el causante de las infracciones informáticas.

A nivel mundial, y más aún ahora que nos encontramos en proceso de globalización, en que los estados buscan salir de la autarquía, para alinearse en bloques que busquen el progreso económico, cultural, social y tecnológico, se hace necesario establecer normas claras que combatan actuaciones ilegales, que dificultan el desarrollo de los pueblos, la informática llegó para establecerse de manera indefinida y cada vez más futurista y realista acorde a las necesidades de la humanidad, los constantes cambios tecnológicos a los que nos vemos expuestos, demuestran este carácter indefinido de una ciencia, que por ningún motivo puede

estar al margen del Derecho, como ente regulador y vigilante de las diversas innovaciones que nos presentan día a día los investigadores de la rama.

Pero si intentamos poner un punto de partida al tratamiento que a nivel internacional se ha pretendido dar a los delitos informáticos, bien podríamos referirnos a los siguientes casos tratados por las diversas instituciones internacionales:

Para el año de 1977, el senador norteamericano Ribicoff, lanzo la primera iniciativa para legislar sobre los delitos informáticos, pero para 1983, la Organización para la Cooperación Económica y el Desarrollo (OCDE) en París, nombro un comité especializado para que traten el tema de la delincuencia relacionada con las computadores y se verifique la necesidad de reformar las legislaciones penales, lo que dio como resultado una serie de propuestas y recomendaciones a los países miembros, para que realicen ciertas modificaciones a sus normativas penales y se incluyan a los delitos informáticos.[118]

La OCDE, en el año de 1983, con la finalidad de evitar el uso no autorizado de programas computacionales, efectuó un estudio que posibilite establecer una armonía entre las diversas leyes penales, para que tengan vigencia en el ámbito internacional, lo que significo que para 1986 se publique el informe denominado: "Delitos de Informática: análisis de la normativa jurídica".[119], en la cual se prevé una lista mínima de varios ejemplos de usos indebidos que los países miembros podrían incluir en sus legislaciones para sancionarlas, esta lista incluía delitos como el fraude, la falsificación y sabotaje informáticos, alteración de datos, acceso no autorizado, reproducción de programas informáticos, a esto se sumo la

[118] www.stj-sn.gob.mx
[119] **Ibid. Op. Cit.**

petición la petición formulada por parte de la Comisión Política de Información, Computadores y Comunicaciones, para que se incluyan protecciones penales contra otros usos como el uso no autorizado de computadores, el robo de secretos comerciales entre otros, a lo que se llamo "lista optativa o facultativa" [120]

Por su parte el Consejo de Europa, en el año de 1989, y con el fin de continuar los avances en la materia, convoca a varios expertos sobre el tema, y emite la Resolución No. (88) 9, aceptada el 13 de septiembre del mismo año, la misma que "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.."[121], y en la cual ya se establece una lista de delitos que necesariamente deben incluirse en las legislaciones de los países miembros, y otra lista de posibles delitos, quedando a libre criterio de los mismos estados de incluirlos[122]

En el año de 1990, el tema de los delitos informáticos, fue ya considerado en el Octavo Congreso Criminal de las Naciones Unidas celebrado en la Habana Cuba, dentro del cual se estableció 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"[123], sin embargo este criterio fue emitido porque hasta ese momento los delitos informáticos todavía no alcanzaba su total desarrollo e injerencia negativa en la sociedad, más aún tan solo se reprochaban conductas tales como reproducción y difusión de programas sin autorización, y el uso indebido de

[120] www.stj-sin.gob.mx/Delitos_Informaticos2.htm
[121] **Ibid. Op. Cit**
[122] **Ibid. Op. Cit**
[123] **Ibid. Op. Cit**

cajeros automáticos, pero pese a lo expuesto el mismo Congreso ya estableció normas tendientes a mejorar los sistemas de seguridad de las computadoras para evitar futuras formas de delincuencia.

En este mismo año se celebró el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado (Montreal), que de igual forma considero que la creciente ola delictiva informática podría traer consigo graves consecuencias a los diversos Estados, posteriormente en el año de 1992, se celebro en Alemania la Conferencia de Wurzburgo, que también aborde el tema[124], adoptando nuevas recomendaciones sobre los delitos informáticos, en el sentido que mientras "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)"[125]. Finalmente, para septiembre de 1995, el Consejo de Europa, emite otra recomendación sobre los problemas del derecho procesal relacionados con la Información Tecnológica.[126]

Además, la preocupación a nivel mundial ha sido muy variada, por lo que la misma Organización de las Naciones Unidas, preparo un listado de los diversos delitos considerados en su seno, y que hasta cierto punto han servido de referencia por parte de las diversas legislaciones, para que estas se hagan eco del llamado, e instituyan en sus normativas penales los variados delitos aún no legislados. (Ver Pág. 25)

No obstante los variados intentos de la comunidad internacional por establecer las pautas y los riesgos que significa estar desprotegidos frente a la

[124] **Ibid.Op. Cit.**
[125] www.stj-sin.gob.mx/Delitos_Informaticos2.htm
[126] **Ibid. Op. Cit.**

delincuencia informática, existen grandes problemas que no permiten un total desarrollo de esta nueva tendencia de protección penal.

Los innumerables intentos, no solo de las organizaciones internacionales sino incluso dentro de los diferentes Estados por pretender establecer normas reguladoras y sancionadoras de estas conductas, han desembocado en airadas discusiones, especialmente entre doctrinarios tradicionalistas de la ciencia penal, que no consideran a estas conductas como nuevos delitos, sino como adaptaciones de los ya existentes, sin duda que la figura puede considerarse la misma en el fondo, pero no en la forma y en los medios para cometerlos, lo que conlleva a una falta de unidad de criterios, que no permiten dar paso a la impetuosa necesidad de legislarlos e incluirlos dentro de las legislaciones penales vigentes.

Por otro lado lo nuevo del tema, a incidido en una falta de criterios jurídicos unánimes sobre las diversas conductas, lo que para unos es sabotaje para otros es fraude, lo que implica una disparidad entre las diversas legislaciones que los han incluido en sus normas, los mismos legisladores han incurrido en la falta de preparación sobre la materia.

Sin embargo tampoco ha sido preocupación constante por parte de los organismos internacionales, el establecer un convenio grande y definitivo, que sea el eje orientador para que los Estados puedan armonizar sus leyes, las infracciones informáticas han alcanzado un nivel extraordinario de desarrollo y tecnificación, por lo que muchos países están en desventaja con otros, respecto de los diversos medios de protección y sanción, marcando aún más la diferencia entre los Estados industrializados y los que están en vías de desarrollo o tercer mundistas.

2.2.– LEGISLACIÓN DE OTROS PAISES

Muchos han sido los países en lo que realmente ha despertado una profunda preocupación el tema de los delitos informáticos, sin embargo pese a los altos y graves riesgos que se pueden sufrir, no todos los países han adoptado una legislación acorde al tema, para ser mas exactos, no en todos los Estados se han incorporado las mismas figuras delictivas, en algunos incluso solo se da prioridad a la protección del software, especialmente en los sudamericanos, sin embargo en la mayoría de lugares donde el temor a los ataques informáticos es realmente alto, es en donde las legislaciones tienen un gran avance, a continuación presentaremos una variada lista de países y sus normas, en cuanto se refiere a la mayor cantidad de infracciones que estos hayan introducido en sus legislaciones.

DIRECTIVA EUROPEA. –

El Concejo de Europa, que reúne a los países componentes de la llamada Unión Europea, conscientes de los terribles efectos que ha traído consigo el desarrollo de los delitos informáticos, tras varias reuniones, y con el fin de presentar ante sus países asociados una legislación de tipo comunitaria, desarrollo un estudio previo de estas conductas, y que dio como resultado una codificación de normas sobre la materia.

El convenio posee 48 artículos relacionados con los delitos informáticos, presentando un desarrollo extenso y más actual sobre los riesgos que produciría estar al margen de una legislación punitiva y efectiva.

El convenio a lo largo de sus articulados nos presenta varias innovaciones, desarrolla definiciones como *sistema informáticos, datos informáticos, proveedor de servicios, datos de tráfico,* a continuación hace referencia a las medidas

que deben tomar los Estados en su entorno nacional, considera dentro del Derecho Penal sustantivo los siguientes tipos de delitos:

- Acceso ilegal
- Intercepción ilegal
- Interferencia de datos
- Interferencia del sistema
- Mal uso de los dispositivos
- Falsificación relacionada con el uso de computadoras
- Fraude relacionado con el uso de computadoras
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con la violación de los derechos de autor y otros delitos relacionados

Posteriormente desarrolla una serie de recomendaciones sobre personas jurídicas, las diversas sanciones, los métodos de prevención y actuación judicial, normas sobre ayuda y cooperación interestatal, que faciliten la punición de las infracción, y las diversas instancias e instituciones a las que pueden recurrir los afectados. (ver Anexo No.1)

Sin duda que este documento, no solo que se ha convertido en referencial, sino en el convenio madre europeo en cuanto tiene que ver con los delitos informáticos, pese a que otros estados miembros de la Unión Europea con anterioridad ya incluyeron en sus normas penales ciertos delitos referentes a la delincuencia informática, el tratado de la OCDE no es más que una consecuencia lógica de ese estatus comunitario que se esta buscando implantar dentro de los países miembros.

Al introducirnos en un breve análisis de los artículos de la Resolución Europea encontramos una necesidad imperiosa de protegerse ante amenazas y ataques cibernéticos, así lo demuestra el acceso ilegal que pretende dar seguridad tanto a personas como instituciones comunitarias y nacionales de los diversos estados, con el fin de manejar sus sistemas sin interrupciones ni alteraciones, protegiéndose además los datos confidenciales y los secretos comerciales o industriales, pero el convenio va más allá, pretende dar una verdadera protección penal, como amenaza previa al autor del delito, sin dejar de lado las propuestas de mejorar las seguridades en los sistemas, cabe destacar que en este caso el acceso se refiere a cualquier intromisión no autorizada, bien desde una red interna (Itranet), bien desde computadores conectados entre si mediante redes de telecomunicación, o bien desde una red de comunicación externa (Internet).

La interceptación ilegal, pretende proteger la intimidad o privacidad de las comunicaciones que transportan datos, pero esta protección se brinda a todo tipo de comunicación que contenga datos importantes, cualquiera sea su medio de traslado, vía telefónica, fax, correo electrónico, etc. Los medios técnicos utilizados pueden ser muy variados, por tal razón se contempla como infracción el solo hecho de escuchar, de monitorear o vigilar la comunicación, pero la configuración de la infracción debe ser de manera intencional, con ánimo de cometer el delito, y de manera ilegal, sin autorización, ya que existen medios legales que permiten en los diversos estados, la intercepción de comunicaciones, cuando se presuma la posible consumación de un delito.

La interferencia de datos, esta íntimamente ligada con el daño, deterioro o eliminación de los datos contenidos en sistemas o soportes informáticos,

pretendiendo dar a la información ese carácter de bien, asimilado a una cosa corporal, lo que hemos denominado anteriormente al considerar a la información como un bien intangible susceptible de ser apreciado en dinero, además se incluye la alteración de los datos, lo cual se puede conseguir con la introducción de virus o gusanos que de alguna manera impidan el normal desarrollo de las actividades y de las cuales se desprenden datos diferentes a los reales, procurando un daño al operador o usuario de la máquina.

Otro de los delitos considerados es el de la interferencia de los sistemas, o lo que doctrinariamente se conoce como sabotaje informático, estableciendo como delito la obstaculización del normal funcionamiento de los sistemas informáticos y los diversos medios de comunicación por donde transita la información o los datos, la obstaculización debe ser intencional, ingresando, alterando, eliminando o suprimiendo los datos, lo cual configura la sanción penal, por su parte el mal uso de dispositivos hace referencia a la utilización indebida de ciertos datos o dispositivos informáticos que permitan cometer cualquiera de las infracciones antes descritas, mediante el uso de herramientas idóneas para la actividad, o que simplemente se las adquirió con el fin consumar la infracción, es lo que más se asemeja a la piratería informática, ya que también se sanciona, la venta, reproducción o distribución de dispositivos informáticos incluidos en soportes computacionales.

Sobre la falsificación relacionada con el uso de las computadoras, se pretende sancionar, no precisamente la información contenida en el documento o dato falso, sino más bien al autor de la infracción, este tipo de falsificación debe realizarse usando un sistema computacional, que permita que el sujeto activo de la infracción, altera de manera intencional y con fines ilícitos los datos contenidos en

los archivos, para que se obtenga una resultado contrario al requerido, por la necesidad que se tiene de saber que efectivamente los datos que contiene un soporte informático son reales, auténticos y confiables. La disposición además incluye en este artículo a todo tipo de dato, público o privado que pueda tener efectos legales.

El fraude relacionado con el uso de las computadoras, configura y establece que los datos ingresados en un sistema, pueden y deben ser considerados como bienes, tal es el caso de los fondos o depósitos, y que al igual que en la figura tradicional del fraude, se puede inducir al error a una persona para aprovecharse de dichos bienes y transferírselos a otro con fines ilícitos, mediante el engaño, esta delito se lo puede cometer mediante el ingreso da datos erróneos o la manipulación indebida de los mismos durante su tratamiento, y que, tiene como finalidad la trasferencia ilegal de fondos ajenos, lo que produce pérdidas económicas al sujeto pasivo de la infracción, por lo que se establece una vez más que los delitos informáticos suelen tener un carácter económico y monetario.

Algo que siempre ha sido motivo de preocupación en diversos países del mundo es la pornografía infantil, y aún más en estados como los europeos donde el criterio sobre la vida sexual es muy amplio, la Resolución no se ha quedado atrás en este sentido, por lo que ha incorporado normas relativas con este delito, la finalidad cumbre de establecer como infracción a la pornografía infantil, es la protección a los menores de edad, y de manera especial evitar su explotación sexual, establece como infracción la posesión, producción y distribución electrónica de material sexual alusivo con menores, lo cual preocupa más por la creciente ola de trasmisiones vía Internet, se sanciona el ofrecimiento no solo como oferta sino también como demanda, tanto al productos como al receptor del material, al hablar de distribución,

se entiende a todo acto tendiente a la propagación por medio de sistemas electrónicos de esta información, y por último, la posesión puede ser por cualquier medio que comprenda inequívocamente su utilización en un sistema computacional, como un disquete o un CD Room, todas esta normas amparadas en declaraciones internacionales que rechazan este tipo de prácticas. "La frase "conducta sexual explícita" abarca al menos las siguientes alternativas ya sea en forma real o simulada: a) relaciones sexuales ya sea en forma genital-genital, oral-genital, anal-genital u oral-anal, entre menores, o entre un adulto y un menor, del mismo sexo o del sexo opuesto; b) bestialidad; c) masturbación; d) abusos sádicos o masoquistas en un contexto sexual; o e) exhibición lasciva de los genitales o de la zona púbica de un menor. No es relevante el hecho de que la conducta descripta sea real o simulada."[127], abarcando el criterio más amplio respecto de lo que tanto la doctrina como las diversas leyes han pretendido dar a este tipo de conductas.

Finalmente la Resolución establece como otra de las infracciones informáticas a las violaciones relacionadas con los derechos de autor, brindado especial atención a los derechos de los autores que se afectan por la publicación sin autorización de obras protegidas a través del Internet, sean estas literarias, fotográficas, musicales o audiovisuales, debemos entender que cada vez que el autor de una obra intelectual, que reviste originalidad tanto en su expresión como en su contenido, invierte tiempo y dinero en la producción y elaboración de la misma, por lo que cada vez que adquirimos un producto parte de lo que pagamos regresa al autor como recompensa al esfuerzo realizado, y por más gran invento que revista el Internet, y por más pública que se la quiera considerar a la información incluida en la

[127] **Resolución del Consejo de Europa**

red, esta se ha convertido en el medio más eficaz para reproducir obras de todo tipo, sin que los autores de las obras puedan acceder a los derechos patrimoniales y morales a los que tiene derecho, diferimos sin duda sobre esto último, ya que la convención no habla del respeto a los derechos morales, el autor puede oponerse a toda publicación y distribución de la obra sin su autorización, lo que implica que además de afectar su patrimonio, también se puede afectar sus derecho a la paternidad de la obra.

No obstante este convenio reviste gran importancia por su contenido, por su estructura y por ser uno de las más amplios y diversos sobre la tipificación y sanción de las infracciones informáticas.

ALEMANIA. –

En el mes de agosto de 1986, se introdujo la segunda Ley para la Lucha contra la Criminalidad Económica, la que posee 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)[128]

Según los estudiosos de la materia, Alemania ha logrado introducir un buen número de infracciones, sin llegar tan lejos como los Estados Unidos, ya que dejaron de lado el acceso no autorizado a sistemas computacionales, y el uso indebido de equipos computacionales.

En cuanto se refiere a la estafa informática, esta tiene una especial particularidad, ya que se ha pretendido establecer un equivalente análogo sobre los tres requisitos de acción de engaño, provocación de error y disposición patrimonial, asimilándolo al computador, es decir, procurar que al soporte se lo pueda inducir a error para configurar la acción delictiva, estableciéndose como infracción la obtención de un resultado falso producto de la incorrecta aplicación del programa o sistema ya sea utilizando datos falsos, incorrectos o incompletos, o mediante una intervención ilícita de los datos. Uno de los problemas a los que se vieron avocados las autoridades alemanas y los legisladores, fue en determinar en donde radicaban los problemas para la aplicación del Derecho Penal tradicional en el ámbito informático y cuales serían los bienes jurídicos a proteger, llegando a la conclusión salomónica de determinar que si bien los medios y sistemas informáticos y electrónicos han propulsado nuevas formas delictivas, solo constituyen una nueva forma de operar en la consumación de los mismos, apegado a nuestro estudio y criterio anterior resalta lo previamente mencionado que los delitos informáticos son los mismos establecidos por la doctrina penal tradicional y lo que cambia es el medio o forma de cometerlos, pero que deben estar bien tipificados para evitar su impunidad, sin embargo también se consideró que no todos los bienes afectados encuadrarían en la denominación

[128] http//tiny.uasnet.mx

normal, por lo que especialmente en materia económica estos revisten mayor importancia.

En la legislación alemana el bien jurídico por excelencia es el patrimonio, sin menoscabo de la vida particular y la privacidad (intimidad), pero tiene sus falencias ya que si bien sanciona el espionaje de datos, excluye de esta categoría a los datos almacenado y trasmitidos vía electrónica, lo que deja prácticamente sin protección al espionaje informático, tampoco existen sanciones a la intromisión indebida, al delito de hacking, o a la violación del correo electrónico, por lo que se demuestra las falencias que contempla esta ley.

En cuanto a la protección de datos, en Alemania Federal, se adopto el 27 de enero de 1977 la Ley contra el uso ilícito de datos personales, dividida en seis capítulos, la cual se aplica tanto a registros manuales como automáticos, que poseen información de personas físicas del sector público y privado, cada entidad tiene la obligación de entregar a pedido del interesado o por autorización legal los datos necesarios, al igual que debe mantener estricta protección sobre los mismos.[129]

Pero más actual es la Ley Federal adoptada el 1ro de Agosto de 1997, la cual hace referencia a los principios que se deben observar en cuanto a la protección de datos, los mismos solo podrán ser recolectados, procesados y utilizados bajo las siguientes condiciones:

1. – Por los proveedores de servicios de telecomunicación, cuando la ley así lo permita y el usuario manifieste expresa o tácitamente su voluntad;
2. – No se podrá utilizar ni recolectar datos personales, en la creación de aparatos que este destinados a la prestación de tele - servicios

[129] **CORREA**, y otros, Derecho Informático, Pág. 268 - 269

3. – El usuario deberá ser oportunamente informado del uso y destino que se vayan a dar los datos consignados, pudiendo éste acceder en cualquier momento a dicha información por mandato legal
4. – El usuario además deberá ser informado de su derecho a retirar cuando él lo desee la información consignada.

Esta ley además ordena que, los proveedores no podrán recolectar datos a su arbitrio, sino exclusivamente cuando sus fines sociales así lo ameriten, sin que se permita tampoco el cruce de datos entre empresas similares, por lo que podemos afirmar que en cuanto a la protección de datos, la seguridad que se brinda es realmente efectiva y alentadora, para evitar las violaciones a los derechos de los ciudadanos.

AUSTRIA. –

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

- Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión. [130] Estableciéndose una multa para el que sin autorización acceda a datos o intencionalmente los borre.

[130] http//tiny.uasnet.mx

Como podemos advertir, lo escueto y corto de la ley no permite mayor comentario, cabe señalar que se han dejado de lados verdaderas infracciones mucho más peligrosas, pese a no ver sido tomadas en cuenta infracciones más bien de daño informático contra soportes o sistemas, brindándose mayor atención a la protección de datos, por la estructura misma de la ley, pese a los antecedentes que a continuación relatamos.

Al igual que en Alemania, también existe una Ley contra la protección de datos, sancionada el 18 de octubre de 1978, dividida en dos capítulos, que posee una alternación de disposiciones constitucionales y otras ordinarias de la misma ley, la protección se da a los datos reposados en instituciones públicas y privadas, pero los organismos públicos, solo podrán recoger datos, bajo autorización legal y para el fiel cumplimiento de sus fines, indicando además el uso jurídico que se va a dar a dichos datos, además existen limitaciones al acceso de datos en los siguientes casos:

- Protección de instituciones constitucionales y administración de justicia penal
- Asegurar la moral del Ejército federal
- Defensa general del país[131]

Recalcando una vez más que los artículos antes mencionados sobre infracciones informáticas, brindan más atención a la protección de datos que a las infracciones materia de nuestro análisis.

FRANCIA. –

La Ley número 88-19 del 5 de enero de 1988 contiene las siguientes normas sobre el fraude informático:

[131] **CORREA** Y otros, Derecho Informático, Pág. 270

- 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.[132]

Al analizar estos artículos encontramos que en Francia la situación es un poco más alentadora que la del restos de sus parciales europeos analizados, la inclusión de figuras tales como el acceso fraudulento a sistemas informáticos, el sabotaje informáticos, la destrucción y falsificación de datos, encuadran en su estructura figuras más acorde a los delitos informáticos, en el primero se podría

[132] http//tiny.uasnet.mx

sancionar figuras como el hacking o el cracking e incluso es espionaje informático, ya que se sanciona la intromisión indebida a sistemas informáticos, sobre el sabotaje la figura encaja en la establecida por la doctrina penal informática, en cuanto a la destrucción de datos esta se encasilla a la protección de los mismos, tanto en su manejo y tratamiento con la finalidad de evitar la modificación, alteración o destrucción de los datos, y evitar resultados erróneos, estableciéndose además como uno de los bienes jurídicos protegidos a la intimidad, y finalmente la falsificación que sanciona la alteración maliciosa e intencional de documentos informáticos.

Aquí cabe un comentario sobre la falsificación, en casi todas las legislaciones encontramos que se sanciona la falsificación de documentos informáticos, sin embargo nosotros hemos manifestado que también se debe considerar como falsificación el resultado que se obtiene mediante el uso de computadores, es decir, que se puede falsificar todo tipo de documento usando sistemas computacionales que permitan copiar y reproducir documentos, lo cual también constituye una infracción informática, poco tomada en cuenta incluso por los tratadistas y legisladores.

El 6 de enero de 1978, se adopto la ley relativa a la informática, los ficheros y las libertades, en la que se da especial atención a la protección de datos personales incluidos en registros automatizados que posean datos de personas físicas, tanto del sector privado y del sector público, dicho acceso es ilimitado a petición de la persona interesada, salvo en el caso de registros que se lleven en razón de la defensa y seguridad estatal, existe además prohibición expresa, de recolectar o conservar información sensible sobre: raza; opinión política, filosófica o religiosa; pertenencia a sindicatos; circunstancias penales; salvo autorización expresa del

interesado.[133] Sobre este tema bien vale señalar que los artículos en mención, ya establecen una protección jurídica a los datos, por lo que como simple referencia nos hemos remitido a esta ley.

GRAN BRETAÑA. –

Tras un ataque efectuado por un hacker en 1991, se introdujo la Computer Misuse Act (Ley de Abusos Informáticos), que estableció el acceso no autorizado, mediante la cual el alterar datos informáticos es penado hasta con cinco años de prisión, se incluye además la liberación de un virus, con sanciones de un mes hasta cinco años de prisión.[134]

Pacheco Klein dice: "Esta cláusula de la ley fue, principalmente, una reacción a la publicidad y al medio en torno a los virus de las computadoras. El Art. 3 inciso 2 establece que la persona tiene que tener intención de "modificar el contenido de cualquier computadora", y de esa manera:

a. Impedir la operación de cualquier computadora; o
b. Impedir o dificultar el acceso a cualquier programa, o la confianza de esos datos
c. Impedir la ejecución de cualquiera de esos programas, o la confianza de esos datos"[135]

La ley fue reformada en 1994, para permitir el acceso a la policía y a las agencias especializadas.

Pese al poco éxito que ha provocado esta ley, las sanciones realmente han sido efectivas, considerando además que ya se comienza a definir como una infracción la liberación y propagación de los virus, que son los delitos informáticos

[133] **CORREA**, y otros, Derecho Informático, Pág. 274
[134] www.monografias.com/trabajos/legisdelinf/

por excelencia no solo por su antigüedad sino también por los efectos y pérdidas que producen.

En cuanto a la protección de datos en el Reino Unido, debemos remitirnos a las fuentes más actuales que las regulan: Data Protection Bill de 1997; Data Protection Act de 1998, la primera resultante de los tratados internacionales como el de la Convención de Estrasburgo de 1981, contempla ciertos principios y requisitos, que configuran la protección, tales como: el sujeto afectado de la infracción debe ser *viviente*, lo cual deberá ser legalmente comprobado, los datos a protegerse son "origen étnico o racial; opiniones políticas; creencias religiosas o de otro carácter; si el sujeto se encuentra sindicado o no; condición de salud física y/o mental; vida sexual; la comisión o imputación de un delito y los detalles procesales del mismo"[136] además de propósitos especiales tales como periodismo, arte o literatura.

Por su parte la Data Protection Act, establce los derechos de los ciudadanos y la defensa eventual de sus derechos en cuanto se refiera a la protección de datos, sancionándose la obtención ilícita de datos personales tanto públicos como privados, regulándose además la transferencia de soportes informáticos.

HOLANDA. –

En este país, se introdujo el primero de marzo de 1993 la Ley de Delitos Informáticos, dentro de la cual se penalizan los siguientes delitos:

- Hacking
- Preacking (utilizar servicios de telecomunicación, evitando el pago total o parcial de los mismos)

---

[135] **PACHECO KLEIN**, citado por María José Viega, Pág. 17
[136] www.it-cenit.org.ar

- Ingeniería social (Arte de convencer a la gente que entregue información que normalmente no la entregaría)
- Distribución de virus, penada según la forma de distribución, si fueron por accidente o con fines dañosos, en el primer caso la pena no supera el mes de prisión, y el segundo caso puede llegar hasta cuatro años de prisión[137]

ESPAÑA. –

En nuevo Código Penal aprobado por Ley – Orgánica 10/1995, del 23 de noviembre / BOE número 281, del 24 de noviembre de 1995, incluye algunos delitos ligados con la materia de nuestro estudio, los cuales son sancionados con diversos tipos de penas y multas, a saber:

- El Art. 197 numeral 1, hace referencia al apoderamiento de mensajes de correo electrónico o intercepción de telecomunicaciones, para descubrir secretos o vulnerar la intimidad; numeral 2, apoderamiento, utilización o modificación de datos reservados personales o familiares incluidos en ficheros o soportes informáticos, electrónicos o telemáticos, sea el registro público o privado; numeral 4, la pena también se impone si lo descrito lo realizan las personas que tiene a su cargo dichos ficheros o soportes; numeral 5, y si los datos contiene información sensible como ideología, religión, creencias, salud, origen racial o vida sexual, o si la víctima fuere menor de edad o incapaz.
- Art. 198, también será penada la autoridad que sin mediar causa legal y valiéndose de su cargo efectúe cualquiera de las conductas anteriores.

[137] www.monografias.com/trabajos/legisdelinf/

- Art. 199, habrá sanción al que revelare secretos ajenos en razón de su oficio o situación laboral, o al profesional que incumpla con el sigilo o reserva, y divulgue los secretos ajenos.
- Art. 200, No solo se protege a las personas naturales sino también a las jurídicas, el que revele sus secretos sin consentimiento de sus representantes será igualmente penado.
- Art. 201, Previo al inicio de la acción penal, es necesaria la denuncia de la persona afectada, y en el caso de menores de edad o incapaces cabe la denuncia del Ministerio Fiscal. No se requiere denuncia si se han afectado intereses colectivos, el perdón del ofendido extingue la acción.
- Art. 211, "La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante"[138], este artículo presenta un debate muy interesante, ya que ¿se puede o no considerar al Internet como otro medio de eficacia semejante?, considero conveniente hacer la siguiente reflexión, hoy en día la red de comunicación y expresión más importante y eficiente es el Internet, a través de este podemos publicar reportajes incluso en páginas privadas o personales, aún más, existen páginas de opinión que poseen foros abiertos a los cibernautas, los cuales pueden dejar plasmada su opinión para que sea libremente accedida por otros usuarios, entonces si podemos afirmar que esta red de información, posee los requisitos de ser un medio semejante de eficacia.

[138] www.ctv.es/USERS/mpq/delitos.html

- Art. 238, se considera reo de robo con fuerza en las cosas los que realizan el acto con alguna de las siguientes circunstancias, numeral 4, uso de llaves falsas, numeral 5, inutilización de sistemas específicos de alarma o guarda, y en concordancia con lo expuesto el Art. 239, dice que se consideran como llaves falsas entre otras, las tarjetas magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia, similar a la actuación de un Cracker, que busca alterar la seguridad del sistema, sin estar frente a un computador.
- Art. 248, es reo de estafa, el que, con ánimo de lucro y mediante alguna manipulación informática o medio semejante, consiga la transferencia no consentida de una activo patrimonial.
- Art. 256, será penado el que sin autorización y causando perjuicio económico al afectado haga uso de cualquier terminal de telecomunicaciones, consideramos como medio de comunicación a una computadora conectada al Internet, o mediante la cual se realiza una llamada telefónica al exterior mediante el sistema denominado net2fon.
- Art. 264, comprendido dentro del capítulo *De los daños*, se sanciona al que por cualquier medio destruya, altere, inutilice o dañe los datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos.
- Art. 270. es penada la reproducción, plagio, distribución o comunicación pública, total o parcial de obras literarias, artísticas o científicas, dentro del cual también se protegen a los programas de ordenador.
- Art. 278, es delito el apoderamiento de datos, documentos escritos o electrónicos, soportes informáticos, con el fin de descubrir los secretos de una

empresa, su difusión o revelación, sin perjuicio de la pena por apoderamiento o destrucción de soportes informáticos.

- Art. 288, las sentencias que se emitan, tras la comisión de cualquiera de estos delitos deberá ser publicada en los periódicos oficiales, y por orden judicial bajo pedido del perjudicado, en cualquier otro medio informativo a costa del condenado.

Si bien esta recopilación de los delitos informáticos, parece ser extensa, reparamos en considerar a la misma como muy simplista, no se hace clara referencia de los alcances de este tipo de conductas, dando mucho redundancia especialmente en la violación a la intimidad y a la protección efectiva de los datos.

España pese a poseer uno de los Códigos Penales más actualizados en el continente europeo, su tipificación no alcanza para sancionar delitos como el sabotaje, la reproducción de virus, la intromisión a sistemas computacionales, hacking, sin embargo en mayo de 1996, entro a regir un nueva Ley Orgánica, con algunas modificaciones a los artículos existentes a la época, pero que no han llenado este vacío de la legislación penal informática.

En cuanto a la protección de datos de carácter personal, la constitución española en su Art. 18 numeral 4 indica "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[139], con el fin de cumplir este mandato el 29 de octubre de 1992 se dictó la ley 5/92 de Regulación de Tratamiento Automatizado de datos de carácter personal, la cual fue reemplazada el 15 de diciembre de 1999 por la Ley de Protección de Datos 15/99, la cual contempla varias normas referidas especialmente

[139] **FERNÁNDEZ,** Horacio, Protección jurídica del Software, Pág. 84

al uso que se deben dar a ciertos datos de tipo personal que incluyan en ficheros sean o no automatizados o informáticos, excepto los que se mantiene en razón de actividades personales, o de investigación de terrorismo o delincuencia organizada. La utilización de estos datos solo puede ser compatible con actividades lícitas y con autorización de sus titulares aquellos datos de tipo sensible (religión, ideología, sindicato, etc).[140]

ESTADOS UNIDOS. -

En los Estados Unidos en 1994 se introdujo el Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. esta nueva acta establece como infracción "la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas.(18 U.S.C.: Sec. 1030 (a) (5) (A)"[141]. Se considera a la nueva ley como un adelanto porque está directamente en contra de los actos de transmisión de virus.

Hace una modificación respecto del tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Estableciéndose a dos niveles:

a. 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
b. Para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.[142]

Se indica además que el creador de un virus no podrá alegar su falta de conocimiento sobre el daño que puede causar, que lo envió por error o que pretendió

[140] **Ibid Op, Cit**, Pág. 84 - 85
[141] www.monografias.com/trabajos/legisdelinf/

enviarlo como un mensaje, estableciéndose la figura jurídica, que la falta de conocimiento de una ley, no es causa de excusa por parte de la persona, y en materia informática mucho menos, ya que el crea un virus sabe perfectamente para que lo realiza.

Le legislador norteamericano sin duda, que va más allá de establecer una sanción pura a los virus, sino a la forma de crearlos, trasmitirlos, desarrollarlos y los efectos que estos producen. Posteriormente de realizaron reformas a la Sección 502 del Código Penal relativas a los delitos informáticos en las 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."[143]

Se contempla además 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."[144]

En cuanto de refiere a la protección de datos a diferencia de otros países especialmente europeos, no hay una ley general sobre el tema, sin embargo existe la Ley sobre libertad de información Freedom of Information Act, adoptada en 1966, que consagra que los datos contenidos en documentos públicos son de libre acceso, pero se exceptúan aquellos datos que contengan información sobre la vida privada de

---

[142] **VIEGA,** María José, Un nuevo desafío jurídico Pág. 16
[143] www.monografias.com
[144] **VIEGA,** María José, Un nuevo desafío jurídico Pág. 16 - 17

las personas.[145], la Privacy Act de 1974 establece la protección que se debe dar a los datos sobre la vida privada de las personas físicas contenidos en registros manuales y automáticos, teniendo el individuo derecho a conocer sobre los mismos, limitándose dicho acceso a los registros de la CIA, FBI, servicios migratorios y lucha contra el tráfico de drogas.

VENEZUELA. –

En la República Bolivariana de Venezuela, la Asamblea Nacional dicto la Ley Especial contra Delitos Informáticos, la cual fue publicada en la Gaceta Oficial No. 37.313 del 30 de octubre del 2001, que sin duda constituye una de las más modernas legislaciones sobre la materia, no solo por su contenido sino por su actualidad indiscutible, incluye una terminología adecuada que para muchos resulta inconstitucional, ya que posee textos en inglés, y las leyes nacionales solo permiten el uso del idioma castellano dentro de sus normas, sin embrago consideramos que esta alusión resulta retrograda, ya que bien cabe señalar que los inicios y desarrollo de la informática tiene ascendencia anglosajona, y es precisamente en Norteamérica y en Europa donde se evidencia el desate de estas conductas, mal podríamos darles un significado castizo a palabras técnicas que en la mayoría de los países del mundo así se las viene abordando, dejando de lado este comentario y centrándonos en esta legislación diremos también que abarca la mayoría de los distintos tipos de delitos, dentro de los cuales podemos destacar los siguientes:

Delitos contra los sistemas que utilizan tecnologías de información. –

- Art. 6. Acceso indebido. - Se pena el acceso, intercepción, interferencia o uso de sistemas informáticos, apegado a lo que la doctrina como conoce

[145] **CORREA**, y otros, Derecho informático, Pág. 277

como intromisión indebida, aunque de manera muy general, se pretende sancionar todo tipo de ingreso no autorizado, es esa generalidad la que demuestra el alcance mismo de la norma, no es restrictiva sino extensiva, brinda mayores garantías no solo al sistema informático sino también al usuario.

- Art. 7. Sabotaje o daño a sistemas. – La norma sanciona la destrucción, daño o modificación que altere o inutilice el normal funcionamiento del sistema, haciendo alusión, y siendo una innovación en Latinoamérica, que si los efectos son producidos por la creación o propagación de un virus la pena se incrementara. Si bien la figura misma del sabotaje de causar la destrucción total o parcial del sistema, sus archivos o información contenida en su soporte, es mucho más apropiada para sancionar, el hecho de incluir el término *altere,* ya supone una destrucción parcial, por lo que mencionamos que a nuestro criterio, la norma resulta completa.
- Art. 8. Sabotaje o daño culposos. – Se habla de culpa, ya que en el caso anterior el daño debe ser producido con dolo, es decir con el ánimo e intención de irrogar el daño, en cambio la culpa se produce imprudencia, negligencia, impericia o inobservancia, sin ánimo de causar daño, por lo que en este caso la pena se reduce a la mitad de la establecida.
- Art. 9. Acceso indebido o sabotajes a sistemas protegidos. – En este caso la figura sigue siendo la misma, provocar la destrucción de soportes informáticos, pero la pena se aumenta entre la tercera parte o la mitad, si los perjuicios se causan en datos destinados a funciones públicas, o sobre datos personales o patrimoniales de personas tanto naturales como jurídicas.

- Art. 10. Posesión de equipos o prestación de servicios de sabotaje. – La figura del sabotaje sigue siendo la conducta penada, pero en los casos anteriores se sanciona al sujeto activo de la infracción, al que produjo inequívocamente el acto, en este artículo se pena a la persona que posea, obtenga, venda, reproduzca o utilice programas destinados a la consumación del sabotaje, o que ofrezca tales servicios, una vez más lo innovador de la Ley sale a flote, ya que no solo se sanciona al que realiza la infracción sino al que se ofrece a realizarla, incluso sin haber perpetrado la comisión del delito, por el solo hecho de que sus actos son atentatorios a la ley, la moral y las buenas costumbres.
- Art. 11. Espionaje Informático. – En este caso se hace una clara diferencia entre el que obtiene, revele o difunda la información ajena contenida en un sistema informático, y lo que lo hace para obtener un beneficio personal, en este caso la pena se agrava de un tercio a la mitad, y en el caso de poner en riesgo la seguridad del Estado la pena se aumentara de la mitad a dos tercios, aquí se pretende proteger los datos, sin que necesariamente implique violación a la intimidad, ya que la norma no limita la información susceptible de apropiación y divulgación, bien puede ser confidencial, pública, privada o secretos de fábrica o comerciales.
- Art. 12. Falsificación de documentos. – Al igual que las leyes europeas, se sanciona la creación, modificación o alteración de documentos que consten en sistemas informáticos, dejando de lado a lo que tanto hacemos referencia, que es la falsificación de documentos como resultado del uso de sistemas computacionales

Delitos contra la propiedad. –

- Art. 13. Hurto – La figura tipificada es la misma mencionada por la doctrina y por las demás leyes sobre la materia existentes, pero llama la atención que no solo se considera el hurto de información o de bienes intangibles como valores, sino que también habla de bienes tangibles, que comprendan el patrimonio de una persona.
- Art. 14- Fraude. – En este caso, el fraude se comete introduciendo instrucciones falsas o fraudulentas al sistema con el fin de obtener resultados falsos, para provecho injusto en prejuicio ajeno, si bien en los delitos informáticos, al que realmente se engaña es al usuario y no a la máquina, bien cabría una rectificación de la norma, ya que a simple vista hace aparecer como que el delito se comete induciendo a la máquina al error, ésta solo procesa datos, el beneficio se obtiene del resultado, más no del engaño, sino de la introducción de ordenes adversas.
- Art. 15. Obtención indebida de bienes o servicios
- Art. 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos
- Art. 17 Apropiación de tarjetas inteligentes o instrumentos análogos
- Art. 18. Provisión indebida de bienes o servicios
- Art. 19. Posesión de equipos para falsificaciones

Estos cinco artículos hacen referencia al mal manejo de se dan a las tarjetas magnéticas (de crédito o de debito), bien para obtener beneficios, bien para falsificarlas o duplicarlas, o para acceder a bienes mediante sus uso, en nuestro estudio no hemos considerado como parte de los delitos informáticos al fraude que se comete mediante el uso de tarjetas magnéticas, por ser delitos ya tipificados con

anterioridad al surgimiento de las infracciones informáticas como doctrina, y por que sus sanciones fueron establecidas más en leyes bancarias que de otra índole.

Delitos contra la privacidad de las personas y de las comunicaciones

- Art. 20. Violación de la privacidad de la data ("hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado"[146]) o información de carácter personal. – Más que una violación a la privacidad, es, lo que se conoce como alteración indebida de datos, cuando el sujeto activo de la infracción se apodera, modifica o elimina datos de otra persona, los datos incluso pueden ser públicos, entonces de que privacidad podemos hablar, tal ves el legislador venezolano pretendió darle un significado más amplio, pero la verdad se ha quedado fuera de los alcances mismos de lo que la violación de la privacidad significa.
- Art. 21. Violación de la privacidad de las comunicaciones. – Igual comentario merecería este artículo, la diferencia es que en el anterior es sobre información, y en este caso es sobre la comunicación, como medio de transmitir la información.
- Art. 22. Revelación indebida de data o información de carácter personal. – En este caso no solo se sanciona al autor de la infracción, sino también al que divulgue o revele la información aún sin formar parte de la comisión del delito.

[146] **Ley de delitos informáticos de Venezuela**

Delitos contra niños, niñas o adolescentes. –

- Art. 23. Difusión o exhibición de material pornográfico. – La sanción va dirigida al que exhiba o difunda material apto para adultos, sin las advertencias necesarias, para evitar el acceso a menores, será sancionado por tales actos.
- Art. 24. Exhibición pornográfica de niños o adolescentes. – Por su parte esta norma hace referencia a lo que realmente es preocupante con el auge del Internet, la pornografía infantil, en la cual se exhibe imágenes de menores en actos sexuales, es la realmente debería estar tipificada, incluso más extensamente por los peligrosos alcances de estos actos, ya que la anterior hace más referencia a lo que sería la corrupción de menores

Delitos contra el orden económico. –

- Art. 25. Apropiación de propiedad intelectual. – Si bien se pretende sancionar en parte lo que ha sido motivo de nuestra crítica, la piratería de software, la norma resulta incompleta, ya que solo se sanciona al que reproduce, vende o distribuye obras del intelecto sin autorización de su creador, pero siempre que las haya obtenido mediante el acceso a sistemas informáticos, dejando de lado la sanción de aquel que adquiere por medios legítimos una obra, para su posterior copiado y reproducción.
- Art. 26. Oferta engañosa. - [147] Es más una sanción para los diversos comercializadores por la red, que ofrecen productos diferentes a los que realmente entregan, más que una infracción informática es una advertencia tanto para el oferente como para el adquirente.

[147] **Ley de delitos informáticos de Venezuela,** http://comunidad.derecho.org/pantin/g37313.html

La ley venezolana, resulta muy interesante, pese a cierto errores a nuestro criterio considerados, no obstante no deja de ser un modelo para el resto de legislaciones latinoamericanas, por lo casi completa de la misma y por que sus sanciones van más acorde al mundo en el que actualmente nos desenvolvemos.

PERU. –

Las leyes peruanas dentro del concepto de los delitos informáticos, incluyen las siguientes infracciones en su normativa penal:

- Art. 154. Delito de violación a la intimidad
- Art. 161. Delito de violación de correspondencia
- Art. 186. segundo párrafo No. 3. Delito de hurto agravado por transferencia electrónica de fondos , de la telemática en general, o la violación del empleo de claves secretas.[148]
- Art. 216. Delitos contra los derechos de autor de software
- Art. 427. Delitos de falsificación de documentos

Peor en el Código Penal peruano mediante el Artículo Único de la Ley No. 27309, publicado el 17 de julio de 2000, se introdujo un capítulo específico para la sanción de los delitos informáticos:

Artículo 207-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

[148] www.minjus.gob.pe/legislacion/codpenal.htm

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207-B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

Artículo 207-C.- En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.[149]

Analizando estos tres artículos, vemos claramente la intención del legislador peruano de dotar a sus administrados una protección efectiva, sobre manera en la protección de datos y el acceso que se pueda tener a los mismos, sin que de ninguna manera esta tipificación de lo que han denominado Delitos Informáticos, sea la más adecuada o ajustada a lo que realmente significan estas conductas, llama la atención que entre una de las penas se establezca la prestación de servicios comunitarios, práctica muy generalizada en países con sistema jurídico anglosajón, no obstante en cuanto a la tipificación de los artículos, bien vale señalar que no es tan limitada como parece, ya que a más de proteger los datos, también se protege en parte la intimidad, cuando se refiere a la intercepción de datos en tránsito,

[149] www.minjus.gob.pe

pero reitera mucho sobre la destrucción de bases de datos, más no de sistemas informáticos ni de los soportes que poseen esos datos.

CHILE. –

Este país fue el primero en Sudamérica en sancionar una Ley sobre Delitos Informáticos No. 19.223, la misma que entro a regir el 7 de junio de 1993, pese a que se dice que dichas normas deberían formar parte de la normativa sustantiva penal, ya que son la adaptación de las infracciones anteriores, y lo que cambia es el medio o forma de cometerlos, llama mucho la atención la poca extensión que tiene la ley, tan solo son los siguientes cuatro artículos:

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

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

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

Art. 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.

Art. 4. El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre

en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."[150]

Al hablar del término *maliciosamente*, comprendemos que la intención es la de causar daño, es decir que se actúa con dolo, por lo que se configura con más precisión la figura penal, las conductas descritas en el articulado hacen referencia a cuatro tipos de delitos, sabotaje informático, espionaje informático, protección de datos y la revelación o divulgación de secretos, estos dos últimos ligados con la violación de la intimidad.

Como se puede apreciar, pese a ser muy corta la ley no deja de ser importante e interesante, a decir de Fernández Delpech cuando realiza un análisis del articulado en mención "resulta que el delito se configura por la realización, tanto en cuanto al hardware como con relación al software, de diferentes acciones llevadas a cabo contra un sistema de tratamiento de información"[151], pero la ley más que buenos comentarios, lo que ha recibido es durísimas criticas, ya se la considera como "insuficiente para combatir el delito informático"[152], especialmente por que no incluye una figura fundamental dentro del estudio y tipificación de estas infracciones, como es el fraude informático.

URUGUAY. –

Pese a los variados tratadistas de origen uruguayo, este país no posee una legislación específica sobre la materia, su Código Penal, tipifica normas tradicionales como el Hurto (Art. 340), Estafa (Art. 347), Daño (Art. 358), entre otros, a los que se podría darles una semejanza al tratamiento informático, no obstante si ha sido

---

[150] **Ley de delitos informáticos chilena**, citada por Magliona Claudio en su obra Delincuencia y Fraude Informático, Pág.138
[151] **FERNÁNDEZ,** Horacio, Protección Jurídica del Software, Pág. 117
[152] **MAGLIONA,** Claudio, Delincuencia y Fraude Informático, Pág. 178

preocupación del legislador uruguayo el dotar de una normativa eficiente sobre el tema, existen por lo menos dos proyectos de ley, el primero que data desde noviembre de 1987 , el cual posee tres artículos, en los que se sanciona con penas de dos a seis años las conductas maliciosas que sin autorización recibiere, interfiera, altere, destruye, etc., un sistema o red de computadores, un soporte lógico o programa o bases de datos, para cometer fraude, obtener lucro y perjudicar a un tercero.[153]

El otro proyecto que busca obtener una legislación, es el que ya paso por el parlamento uruguayo y que no ha sido aprobado, el cual sancionaría las siguientes infracciones:

- Art. 1. Acceso doloso
- Art. 2 Acceso culposo
- Art. 3. Fraude informático
- Art. 4. Hurto Informático
- Art. 5. Dolo a través de medios de comunicación[154]

A nivel internacional, existen muchos otros países que poseen normas relativas a los delitos informáticos, además también organismos internacionales en sus diversos convenios multilaterales han incorporado variadas formas de protección jurídica ante estas infracciones, que no solo atañen al uso indebido de las computadoras o las redes de información, sino también a protecciones al software, más en el marco de la propiedad intelectual, pero que para dar una mayor expresión al tema de nuestro estudio resulta importante mencionar algunas instituciones u organismos:

---

[153] **VIEGA,** María José, Un nuevo desafío jurídico, Pág. 21
[154] **FERNÁNDEZ,** Horacio, Protección jurídica del Software Pág. 121 - 122

1. – La Organización Mundial de Propiedad Intelectual (OMPI), posee un proyecto de tratado sobre la protección del soporte lógico, y el Tratado sobre Derechos de Autor adoptado el 20 de diciembre de 1996
2. – El Acuerdo General de Aranceles Aduaneros y Comercio (GATT), en el marco de la Ronda de Uruguay, incluyo el tema sobre los programas de ordenador y compilación de datos (bases de datos), los cuales deben ser protegidos como obras literarias, conforme a los diversos derechos de autor.

2.3. – COMPARACION. -

El efectuar un estudio comparativo sobre las diversas legislaciones que poseen normas relativas a los delitos informáticos resultaría sumamente complejo, porque muchos delitos se encuentran tipificados de manera similar bajo otras denominaciones, lo que para algunas leyes es derecho de protección de datos, para otras es delito de violación de la intimidad, sin duda, ambas tiene un mismo fin, que es el proteger el uso indebido de datos sensibles de un tercero.

En el siguiente cuadro, sin que signifique precisamente una comparación entre varias legislaciones, hemos incluido las diversas infracciones contenidas y sancionadas en normas legales y constitucionales que pueden o no ser consideradas según los países que consideramos dentro de nuestro estudio, cabe destacar que en algunos estados, sus leyes son más actuales que otros, especialmente en los sudamericanos, que en relación a los europeos adoptaron leyes penales informáticas con posterioridad, tras sufrir una serie de ataques que involucraron empresas públicas y privadas, y que vieron la necesidad de contar con leyes efectivas que castiguen estas conductas antijurídicas.

	ALEMANIA	*AUSTRIA*	*FRANCIA*	*HOLANDA*	*ESPAÑA*	*ESTADOS UNIDOS*	*DIRECTIVA EUROPEA*	*VENEZUELA*	*PERU*
ESPIONAJE INFORMATICO	X							X	
ESTAFA INFORMATICA	X	X			X				
FALSIFICACIÓN DE DATOS	X		X				X	X	X
ALTERACIÓN DE DATOS	X				X				
SABOTAJE INFORMATICO	X		X				X	X	
DESTRUCCIÓN DE DATOS		X	X		X				X
USO DE DOCUMENTOS FALSOS			X						
HACKING				X					
PREACKING				X					
INGENIERIA SOCIAL				X					
DISTRIBUCION DE VIRUS				X		X	X	X	
PROTECCIÓN DE DATOS (DERECHO A LA INTIMIDA)	X	X	X		X	X	X	X	X
PIRATERÍA INFORMATICA					X			X	
ACCESO ILEGAL							X	X	X
FRAUDE INFORMATICO							X	X	
PORNOGRAFIA INFANTIL							X	X	
HURTO INFORMATICO								X	X
VIOLACIÓN DE CORRESPONDENCIA									X

Como podemos apreciar, pese a la variedad de delitos, y a la generalidad de los mismos, aceptada especialmente por parte de los tratadistas, los estados, con ciertas excepciones, no se han hecho eco de esta clasificación, por nosotros ya tratada, es decir, no tipifican a los diversos tipos de delitos, sino que realizan una adaptación de los mismos, o bien a sus normas ya existentes, como el caso del hurto o fraude, o crean nuevas figuras como la ingeniería social, única en su especie en la legislación holandesa, y ni remotamente aparejada a otras.

Advertimos también el gran desarrollo de la legislación venezolana, que por ser muy reciente se ha percatado de incluir en su ley, la mayor cantidad posible de delitos informáticos, bien vale señalar, que delitos como el de violación de la correspondencia (e-mail), esta generalmente incluido, dentro de las constituciones, como un derecho fundamental de cada ciudadano.

A lo que más énfasis brindan los estados, dentro de sus normas, es al derecho de protección de datos y la violación de la intimidad, aquellos que no los incluyen en sus leyes penales informáticas, los establecen, incluso dentro de normas específicas sobre el tema, dándoles un tratamiento importante en lo que se refiere al uso de sistemas informáticos para cometer cualquier infracción relacionada.

De igual forma otro de los delitos que poco se lo ha tratado pese a ser de los más alarmantes es el de la pornografía infantil, el delito de hacking, es generalmente introducido en el espionaje informático, mientras que el de cracking, en el de sabotaje informático, la figura del hurto no es muy aceptada dentro de las legislaciones, pero de igual forma se la establece más bien dentro del fraude informático, como medio de apoderarse de bienes ajenos, a la piratería informática no se la toma mucho en cuenta, considerando que este tipo de delito se encuentra

establecido más en Convenios Internacionales como los de la Organización Mundial de Propiedad Intelectual (OMPI).

CAPITULO 3.- TRATAMIENTO NACIONAL

En el Ecuador la situación respecto a los delitos informáticos, ha sido un poco tenue y diversa, el legislador ecuatoriano demoró algún tiempo en comprender los verdaderos riesgos que significaba el no contar con una normativa eficaz sobre el tema.

Sin embargo, más por gestiones por parte de personas y organismos ajenos a la función legislativa, que por los mismos legisladores, se ha logrado obtener una respuesta positiva, y en la actualidad el país cuenta con una ley que regula de algún modo este tipo de infracciones.

Haciendo una comparación respecto de las normas de otros países, debemos señalar que, pese a no existir una ley únicamente sobre delitos informáticos, se han introducido reformas al Código Penal, que permiten sancionar a los sujetos activos de estas conductas, cabe indicar, que si bien el proyecto inicial estuvo preparado, la demora en debatir y expedir la ley, duró aproximadamente casi 18 meses, lo que alguna manera, demuestra el poco interés que tuvo por parte del legislador, el dotar al país de una ley efectiva.

3.1 LEY DE COMERCIO ELECTRONICO

Como hemos manifestado la Ley de Comercio Electrónico, previa a su debate y publicación en el Registro Oficial, paso por un largo camino de arreglos y modificaciones hasta llegar a su texto final vigente, entre los primeros antecedentes para lograra obtener esta ley podemos mencionar los siguientes:

En el mes de marzo de 1999, el Ing. Carlos Vera, miembro de la Corporación Ecuatoriana de Comercio Electrónico (CORPECE), manifestó su inquietud, de la necesidad de contar en el país con una ley en materia de comercio electrónico, lo que motivo a varias personas interesadas en el tema preparar un anteproyecto de ley, el mismo que fue presentado ante el H. Congreso Nacional en el mes de Septiembre del mismo año, pero no sería sino hasta junio del 2000, en que se presentaron observaciones de este proyecto, las mismas que fueron acogidas casi un año después de su presentación ante el Parlamento Ecuatoriano, por lo que para septiembre del 2000, se volvió analizar las diversas observaciones presentadas y se retomo la depuración del proyecto.

Para el mes de febrero de 2001, el Consejo Nacional de Telecomunicaciones del Ecuador (CONATEL), convoca oficialmente a varias instituciones tanto públicas como privadas, para que conjuntamente analicen y presenten las recomendaciones que más convenientemente les parezcan, todo con la finalidad de obtener una ley efectiva, este proceso de apoyo al CONATEL, duro aproximadamente cuatro meses, y ya para el mes de mayo del 2001, se presento el proyecto con todas las modificaciones y arreglos ante el H. Congreso Nacional de la República, por lo que posteriormente paso a ser conocido por la Comisión especializada de lo Civil y Penal, la cual, conforme a la Ley es la competente para conocer y analizar este proyecto de ley, por el contenido y estructura del mismo.

Pese al apoyo, en el seno de la comisión por parte de los legisladores que conforman la misma, y tras ser por varias veces revisado el proyecto, este recién paso a formar parte de la orden del día del Parlamento en el mes de enero de 2002, y para

finales del febrero del mismo año, se terminaba de debatir el último artículo integrante de la Ley.[155]

Esta nueva ley entro en vigor en el Ecuador el 17 de abril del año 2002, y fue publicada en Registro Oficial Suplemento No. 557, la misma contiene normas, como su nombre lo indica sobre la normalización del comercio electrónico, firma digital, y mensajes de datos, además presenta una serie de reformas al Código Penal, en cuanto a la normalización de las denominadas por la misma ley como Infracciones Informáticas.

TITULO V

DE LAS INFRACCIONES INFORMÁTICAS

CAPÍTULO I

DE LAS INFRACCIONES INFORMATICAS

Artículo 58.- Infracciones Informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente Ley.

Reformas al Código Penal

Artículo 59.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

Artículo ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con

[155] www.dlh.hora.com.ec

prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

La figura descrita hace alusión, e incluye por su tipología a cuatro tipos de delitos perseguibles bajo la misma norma, a saber, intromisión indebida, espionaje informático, hacking y divulgación de información confidencial, incluidas en nuestra categoría de delitos que procuran un daño teniendo como fin a la máquina.

La intromisión indebida, se verifica cuando no teniendo autorización del propietario de la información se accede a esta, por cualquier medio, va de la mano la divulgación de la misma, estableciéndose tres clases de información y dos clases de sujetos activos de la infracción, en cuanto a los tipo de información, esta puede privada, atendiendo a la persona afectada, industrial o comercial y la seguridad nacional, sobre los infractores, estos pueden ajenos a la información, es decir el que

procura el daño sin mediar su actividad laboral, y los que conforme a su función tienen a su cargo la información, agravando según el caso la pena y la multa.

Sin embargo la estructura peculiar del artículo sanciona figuras altamente peligrosas, como el espionaje informático, al establecer que comete infracción el que por cualquier medio electrónico o informático, violentare claves o seguridades para obtener información protegida, secreta, reservada o confidencial contenida en soportes o sistemas informáticos.

Finalmente el mismo artículo sanciona el delito de Hacking, al establecer que igual comete le delito, aquel que simplemente violentare la seguridad, infracción muy discutida por parte de los defensores de la libertad de información, en los dos primeros casos propuestos lo que realmente se protege es la información, considerada ésta como bien intangible, concordantemente con el derecho a la reserva e intimidad de las personas, y además en todos los casos se protege los sistemas de seguridad, la figura tipifica y sanciona tanto la obtención de datos, como la destrucción de mecanismos de protección de los sistemas informáticos.

Artículo ...- Obtención y utilización no autorizada de Información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

En este caso si bien nuevamente el bien jurídico protegido es la información, la sanción va dirigida a la divulgación, publicación, transferencia, etc, de la misma, ya que la obtención no autorizada, esta ya sancionada con el artículo anterior, pero siempre y cuando esta obtención sea a través de medios informáticos,

por lo reparamos en considerar que lo que realmente se esta protegiendo es la obtención de datos en general, sea o no por medios informáticos o electrónicos, es lo que doctrina y varias legislaciones denominan como "La protección de datos", sin que implique violación al derecho de la intimidad, ya que no necesariamente pueden ser datos sensibles, sino cualquier tipo de información consignada por una persona, ya que sin su autorización no es factible tal transferencia, es muy común que las personas reciban llamadas de empresas que de algún modo han conseguido sus datos, ofreciéndoles premios, regalos o beneficios a cambio de cierta prestación o inscripción a un club, y realmente no se conoce el alcance de tales ofertas, por lo que de algún modo se pretende precautelar tanto la integridad, como el patrimonio de las personas, y consideramos pertinente que este incluidos en esta categoría de infracciones informáticas, por las bases de datos de manejan estas empresas, son trasladadas entre si, y las mismas están incluidas en sistemas o soportes informáticos sin la autorización del titular de los datos.

Creemos pertinente indicar que a más de las sanciones, se deberían establecer los mecanismos necesarios, para que los afectados tengan el derecho de exigir que sus datos sean eliminados cuando pese a ser realmente cedidos por ellos se los este dando un fin distinto del solicitado.

Estos dos artículos se incluyen a los delitos contra la inviolabilidad del secreto, según lo establece la estructura misma del Código Penal. Dentro de esta tipificación de delitos incluidos en nuestra normativa penal vigente, se establece la violación de correspondencia entendiéndose por tal a cartas o partes telegráficos, sin embargo el legislador no ha normado uno de los más comunes delitos cometidos a través de medios informáticos como es la violación del correo electrónico, si bien en

la actualidad el sistema de traslado de correspondencia aún se lo sigue realizando por medios tradicionales, las proyecciones tecnológicas no se equivocan en considerar que en los próximos diez o quince años venideros, el traslado de este tipo de información se lo realizara en su forma mayoritaria por medios electrónicos, lo que evidencia la necesidad de establecer como infracción la violación del correo electrónico (e mail), ya que los sistemas de seguridad que hoy en día poseen los diferentes ordenadores resultan insuficientes para impedir este tipo de infracciones, lo que de alguna manera significa que esta nueva ley ya nace con ciertos vacíos.

Artículo 60.- Sustitúyase el Art. 262 por el siguiente:

Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo.

Dentro del Título III de los delitos contra la Administración Pública, el capítulo V del Código Penal, se refiere a la "Violación de los deberes de los funcionarios públicos, la usurpación de atribuciones y de los abusos de autoridad", debiendo sustituirse el Art. 262, sobre la destrucción maliciosa de documentos, pero más que una sustitución es una reforma al contenido del artículo, ya que lo novedoso del actual, es la introducción de otras formas de documentos que no estén en soporte manuales, sino en soportes informáticos, el anterior se limitaba a señalar que la destrucción es únicamente de documentos y títulos, a lo cual se suman los programas, datos, bases de datos, información contenidos en sistemas

computacionales o redes electrónicas, lo cual implica una regularización más estricta de los documentos que el funcionario maneje. Pero esta regulación debería ser aún más estricta, ya que por el hecho mismo de que el funcionario tenga a su cargo un dispositivo electrónico y lo altere o destruya, los medios de prueba resultan insuficientes para establecer la real participación en la infracción.

La tipificación del artículo habla del funcionario público que maliciosa y fraudulentamente destruya o suprima documentos, es decir, establece como agravante la figura del dolo, y decimos el dolo ya que la culpa es actuar con negligencia, imprudencia o impericia, sin ser justificativo, no todo funcionarios, especialmente en nuestro país está capacitado para manejar un computador o dispositivos electrónico, generalmente los computadores en sector privado vinieron para reemplazar a los archivos manuales o a las máquinas de escribir, tal vez con el fin de alivianar el trabajo de los funcionarios, por lo que se debe dejar en claro, que la figura establece la mala intención, el dolo, la mala fe con la que obra el empleado público, pero no solo se debería sancionar al empleado, sino también al que ordenó o insinuó el cometimiento de la infracción, bien sea de la misma función pública o ajena a ésta, ya que sería una especie de corrupción o más acorde a la normativa penal vigente se incurriría en la figura del Cohecho Agravado (Art. 286 C.P.), ya que como se dijo la destrucción maliciosa de todo tipo de documento puede ser hecha por insinuación de parte interesada.

Artículo 61.- A continuación del Art. 353, agréguese el siguiente artículo innumerado:

Artículo Innumerado.....- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un

perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo.

Los Delitos contra la Fe Pública, contienen un capítulo sobre las "Falsificaciones de Documentos en General", las reformas incluyen el presente artículo al final de este capitulo, la norma expresada sin duda, que se constituye en el delito que más fehacientemente se apega a la variada clasificación que hemos dado con anterioridad sobre los delitos informáticos, sin pretender destruir el espíritu mismo del capítulo, el legislador introduce una nueva forma de cometer el delito de falsificación, pero a través de medios informáticos, dándole además un carácter más amplio, al indicar que el delito se comete por *cualquier medio,* brindándole al juez, la posibilidad de sancionar la infracción con un criterio más amplio, ya que no limita el medio para cometer la falsificación.

El artículo, a nuestro criterio recalca sobre manera la falsificación en el sentido de alterar o modificar mensajes de datos o la información incluida en estos,

no se refiere a la falsificación electrónica de documentos, podemos entender como mensajes de datos aquellos enviados por medios electrónicos o informáticos, de un ordenador a otro, en el caso del correo electrónico, o, de hecho la información debe estar contenida en un soporte material, sistema de información o telemático, la telemática es la "información automatizada enviada a distancia vía telefónica o por satélite, con soportes de voz e imagen"[156], la falsificación electrónica en el Ecuador supone tres formas distintas de cometer para que se configure la infracción;

- Alterando un mensaje de datos, la alteración a simple criterio significa modificación, cambio, aumento o disminución de lo que realmente el mensaje indica, desde aquí parte nuestro análisis, alterar, o modificar un mensaje, requiere previamente la intercepción del mismo, o por lo menos saber a ciencia cierta lo que contiene el mensaje, para establecer lo que hay que cambiar o modificar, lo que de alguna forma agravaría la infracción, pero esta alteración realmente se la puede relacionar exclusivamente con los mensajes electrónicos, los cuales constantemente son interceptados para cambiar su texto original.
- Simulando un mensaje de datos, en este caso más que una falsificación del mensaje es una suplantación del mismo, cambiando en todo o en parte su contenido inicial, para obtener un beneficio o causar un perjuicio.
- Suponiendo en un acto la intervención de personas ajenas al mensaje, es aquí donde ingresa la parte de los mensajes telemáticos, ya que se puede vía teléfono o vía satélite con voz e imagen, suplantar a una persona para que emita ordenes o envíe datos erróneos que beneficien a un tercero o a si

[156] **LEON,** Fernando, De la comunicación a la informática jurídica penal bancaria, Pág. 26

mismo, en el primer caso vía teléfono, sería tan sencillo como simular la voz de otro, para obtener el beneficio, y en el segundo caso, por ese retardo que mantienen las señales satelitales de aproximadamente 4 o 6 segundos, el mensaje podría ser alterado, simulado o supuesto, configurando al mismo tiempo los diversos modos de falsificación electrónica.

El delito de falsificación acorde a la doctrina penal, significa toda tipo de alteración sea total o parcial de un documento, no solo de funcionarios públicos sino también de personas que con tal acto pretendan inducir a error a cualquier persona y obtener un provecho del mismo, en materia informática resulta mucho más eficiente cometer una falsificación, ya que los medios que brindan los programas de ordenador facilitan la consecución de tales actos, a manera de ejemplo, si se desea falsificar una escritura pública tan solo se requiere un computador, un scanner, una impresora y papales iguales o similares o los originales, y la infracción esta consumada, pero nuevamente volvemos a lo ya mencionado, en nuestro país en la actualidad no contamos con peritos expertos en esta materia que puedan de manera eficiente determinar la falsedad de un documento realizado con la ayuda de medios informáticos, por lo que vemos la necesidad de no solo incluir reformas al código penal, sino también a los diversos medios de prueba tanto civiles como penales, que de alguna forma faciliten la investigación de tales hechos.

Artículo 62.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

Artículo Innumerado.....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o

cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Uno de los más comunes delitos informáticos, es el de Daño al sistema (software), jamás la doctrina se ha referido al daño del soporte material (hardware), que incurriría en otras figuras ajenas en sí a las infracciones en estudio, el delito de daño informático establecido en nuestra ley, brinda una amplia gama de cometer el delito, configurando a nuestro criterio dos conductas o dos infracciones muy diversas, la de sabotaje informático y la creación o propagación de virus, gusanos, rutinas cáncer o bombas lógicas.

El sabotaje informático, y conforme a la norma expuesta, significa la destrucción o inutilización de los sistemas, programas y datos incluidos en un soporte material informático, e incluso la destrucción misma de dicho soporte físico[157], violentando las seguridades del sistema, el artículo indica que puede ser sancionado el que destruya, altere, inutilice, suprime o dañe, los programas, datos, bases de datos, información o cualquier mensaje incluido en el sistema, por lo quede acuerdo a la doctrina la figura encuadra claramente en el concepto propuesto, el bien jurídico protegido, ya no solo es la información, entendiéndola a esta como datos, bases de

[157] **ROMEO CASABONA,** Carlos, citado por Claudio Magliona en su obra Delincuencia y Fraude Informático, Pág. 175

datos o mensajes, sino también los programas de ordenador, cuando se afecta al sistema se causa perjuicio tanto a los programas como a los archivos que contiene la información, y la ley es muy clara al indicar si es temporal o definitivo el daño, sin que la pena tenga que disminuir por el daño causado, ya que lo que se sanciona es la conducta, más no el resultado de tiempo de la misma. A lo que además se le debería sumar como infracción la intromisión indebida, porque para causar el daño, previamente se debió destruir las seguridades o claves del sistema.

Conveniente sería además tipificar dentro de este artículo que no solo se reprimirá el daño a los sistemas lógicos, sino también a los soportes materiales del sistema, para no solo encuadrar la norma con la doctrina, sino también para brindar mayores garantías a los propietarios de los computadores.

Pero el artículo resulta más amplio de lo que aparentemente indica, ya que menciona como forma de causar el daño, la *utilización de cualquier medio,* por lo que nosotros incluimos a los virus, gusanos, rutinas cáncer o bombas lógicas, en nuestra clasificación de los delitos, establecimos como conductas ilícitas, aquellas que procuren causar daño al sistema, sea por el medio que fuere, y es por eso la diferenciación que hicimos del sabotaje, ya que en los casos propuestos no se requiere la vulneración de las seguridades, por la estructura misma de un virus o gusano, este se puede transmitir vía correo electrónico, o accediendo físicamente al sistema e infectándolo, lo que también provoca un daño al sistema, la modalidad de los virus es tan variada y diversa, que estos casos se configuraría más la infracción, por los efectos temporales o definitivos del daño, ya que cualquiera de las infecciones al sistema, puede provocar daños sistemáticos, sin necesidad que sea inmediatos, sino posteriores dependiendo del continuado uso que se de la programa.

Artículo Innumerado.....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.

Estos dos artículos se incluyen dentro del Título V DE LOS DELITOS CONTRA LA SEGURIDAD PUBLICA, Capítulo VII, Del incendio y otras destrucciones, De los deterioros y daños, si bien estas infracciones, se refieren a la destrucción de bienes destinados al uso público, y a bienes muebles o inmuebles privados, el legislador encuentra pertinente incluirlos dentro de estos delitos, ya que la tipificación de los artículos en estudio hacen clara referencia a los daños en sistemas informáticos, y va más allá, a lo que a nuestro criterio consideramos como una innovación, ya que se establece como delito informático la destrucción de las instalaciones físicas necesarias para la transmisión de los mensajes, lo que sin duda constituye un avance sobre el tema de los delitos informáticos, ya que ni la doctrina, ni las diversas leyes de otros países han considerado este delito como infracción informática, clara esta que por el hecho mismo de producirse un atentado un sistema de transmisión, la misma ley penal le aplicaría una sanción punitiva, lo importante es que se considera directamente como acto ilegitimo la destrucción de las diversas instalaciones que permiten el libre envío y recepción de mensajes, como puede ser una antena de transmisión, una red sincronizada de mensajes, una central informática, etc.

Y la misma ley establece que *si no se tratare de un delito mayor,* y hace esta diferenciación, ya que los daños a las infraestructuras, se los puede realizar con

fines informáticos, para impedir la transmisión de los mensajes o impedir las comunicaciones, lo que se consideraría como infracción informática por los alcances que se pretenden con el delito, sin embargo si el delito fuere mayor o con otras finalidades, estaríamos frente a otras infracciones, que implican la seguridad del Estado o la establecida en el Art. 422 del Código Penal, de la interrupción de comunicaciones.

Artículo 63.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados:

Artículo Innumerado.....- Apropiación Ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

El Título X DE LOS DELITOS CONTRA LA PROPIEDAD, establece y conforme a nuestro estudio dos clases de delitos como son el Hurto y Robo, tanto la doctrina como las diversas leyes han adoptado estas dos figuras en lo que se refiere a la consumación de infracciones informáticas, el debate entre los tratadistas, de si se trata de hurto o robo ha dado como consecuencia que según el autor o ley que se trate o se estudie la figura varíe según su criterio o conveniencia, bien se ha dicho que para configurar el delito de robo se debe cumplir con el requisito fundamental, de apropiarse ilegítimamente de un bien ajeno, pero con el uso de fuerza en las cosas,

violencias o amenazas en las personas, esto último que lo diferencia del hurto, también es cierto que para los entendidos en la rama informática, la figura del robo es la que más se apega a sus necesidades.

Podríamos inicialmente decir que esta infracción, no debería estar incluida en le capítulo del Robo, sino más bien en el del Hurto, ya que en ningún momento se habla de la utilización de fuerza o violencia a los sistemas para obtener el provecho deseado, sin embargo la título del artículo habla de "Apropiación Ilícita", con la finalidad de mantener cierta concordancia con las disposiciones pertinentes al Robo, especialmente con la norma del Art. 553, que habla de que también se asimila a robo la sustracción de cosa ajena hecha con fraude y ánimo de apropiarse, y el nuevo artículo, al referirse a la apropiación ilícita, dice que esta debe ser realizada por medios fraudulentos, por lo que con fines más de fondo que forma se incluye esta norma en dicho capítulo.

Artículo Innumerado.....- La pena será de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1.- Inutilización de sistemas de alarma o guarda;

2.- Descubrimiento o descifrado de claves secretas o encriptadas;

3.- Utilización de tarjetas magnéticas o perforadas;

4.- Utilización de controles o instrumentos de apertura a distancia;

5.- Violación de seguridades electrónicas, informáticas u otras semejantes.

Pero si en el artículo anterior, quedaba la duda del porque de su ubicación en el capítulo del robo, este otro artículo nos la absuelve de manera efectiva, cuando habla de apropiación ilícita, tan solo se esta tipificando la

infracción, su sanción y consecuencias, más, el subsiguiente ya configura explícitamente el delito de Robo informático, y aclara el porque de su inclusión en dicho capítulo, nos presenta cinco formas que agravan el delito, y en cada una se puede incurrir en los requisitos para cometer robo, así tenemos:

1. – Inutilización de sistemas de alarma o guarda. – El mencionar la palabra inutilizar ya significa, objetivamente destrucción, o por lo menos alteración, pero para alterar algo, necesariamente debemos acceder a ese algo y provocar un daño que impida que el sujeto activo sea delatado, es decir, al inutilizar los sistemas de alarma o guarda el infractor ya provoca un daño al sistema, sea mediante fuerza o violencia en ese sistema de seguridad.
2. – Descubrimiento o descifrado de claves secretas o encriptadas. – Si bien este numeral no establece los requisitos mismos del robo, bien vale señalar que para poder descubrir una clave o desencriptar la información, el infractor debe poseer altos conocimientos sobre estas técnicas, sin embargo se sanciona el resultado de apropiarse ilegítimamente de bien ajeno, por lo que si mediante estos procedimientos se logra el objetivo, el robo esta consumado.
3. – Tanto la utilización de tarjetas magnética o perforadas, así como el uso de controles remotos que permitan acceder a un bien ajeno, violentando el sistema, de igual forma configuran el delito de robo, pese a no haber violencia ni fuerza, lo que el legislador pretende es no dañar el espíritu mismo de la ley.
4. – Violación de seguridades electrónicas, informáticas u otras semejantes. – Esta es la que más se apega a lo que a nuestro estudio se refiere, la palabra

clave es *violación de seguridades*, el término violación en el ámbito jurídico significa "Infracción, quebrantamiento o transgresión de la ley o mandato"[158], pero asemejándolo al requisito del robo, sobre la utilización de violencia para consumar la infracción, la violación de la seguridad implica, el uso de violencia o fuerza en las cosas para procurar el apoderamiento ilegítimo del bien.

Finalmente diremos que si bien no se establece como delito ni el Robo ni el Hurto informático, podríamos entender que en ambos artículos se los esta sancionando y tipificando a la vez, lo que realmente interesa es el bien jurídico a proteger, que es la propiedad, el medio por el que se lo haga, con o sin violencia, fuerza o amenaza, no comprende el análisis, ya que la sanción no varía, sea cual fuere el medio utilizado.

Artículo 64.- Añádase como segundo inciso del artículo 563 del Código Penal el siguiente:

Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.

El artículo 563 del Código Penal sanciona la Estafa, este segundo inciso tipifica la Estafa Informática, ya que la figura misma no varía en lo absoluto, pero se hace referencia a una nueva forma de cometerlo, mediante el uso de sistemas electrónicos o telemáticos, pero indicando que la pena será la máxima prevista, es decir cinco años, y en cuanto a la multa, esta también es superior al monto

[158] **CABANELLAS,** Guillermo, Diccionario de Derecho Usual, Tomo VIII, Pág. 383

establecido, que es de cincuenta a mil sucres (cuatro centavos de dólar), en este caso sería de quinientos a mil dólares.

La estafa informática consiste en "el provecho ilícito que se obtiene con daño patrimonial, mediante el empleo de artificios o engaños idóneos para inducir a otro en error, sirviéndose a su vez de una computadora o vulnerado sus seguridades"[159], por lo que y en referencia la artículo en estudio, el sujeto activo de la infracción es aquel que suplanta a otra persona, pero obviamente manteniendo una conexión con una computadora, bien por medios informáticos (Internet), o directamente frente a ella, aduciendo calidades falsas, suplantado al operario o dueño, y procurando obtener un beneficio lucrativo de tal actividad.

Artículo 65.- A continuación del numeral 19 del Art. 606 añádase el siguiente:

..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

El legislador ha considerado la violación al derecho a la intimidad dentro de las contravenciones de tercera clase, que están penadas con prisión de dos a cuatro días, y multa de uno a ciento veinte sucres (menos de un centavo de dólar), creemos conveniente hacer una crítica sobre esta infracción, el derecho a la intimidad ha traído en materia de delitos informáticos un arduo debate, no por la forma de tipificarlo y sancionarlo, sino porque, a través de medios informáticos es mucho más fácil acceder a información confidencial y causar grave peligro y daño a la persona afectada, justamente el estudio de estas infracciones parte de que los diversos ciber – delincuentes, aprovecharon las fallas en los sistemas de seguridad, para acceder a información privilegiada, si bien la intimidad solo se la puede atribuir a una persona

[159] **LEON,** Fernando, De la comunicación a la Informática Jurídica penal bancaria, Pág. 208 - 209

natural, sería muy injusto establecer una pena tan irrisoria al delincuente, creemos sin duda, que es una de las más comunes infracciones que se suelen cometer, y que dentro de la normativa penal de otros estados se encuentra severamente sancionada, estaríamos dejando de lado una sanción a una infracción altamente peligrosa.

3.2. – CODIGO PENAL ECUATORIANO

Si bien podríamos afirmar que el Ecuador a dado un paso gigante con la inclusión dentro del Código Penal de las infracciones informáticas, también podríamos decir que nuestro legislador pese a sus buenas intenciones se ha quedado un poco corto en cuanto a la tipificación de estos delitos, no solo por que se pudo haber tomado en consideración otras legislaciones que sobre el tema son muchos más extensas, y que incluso poseen leyes exclusivas sobre los delitos informáticos, sino porque no ha considerado otras infracciones si establecidas en la ley penal y que son susceptibles de ser cometidas por medios informáticos como pueden ser los siguientes:

- Falsificación de moneda usando medios informáticos, al igual que los sellos, timbres y marcas.
- El delito de intimidación, que se lo realiza por escrito, considerando que se puede mediante el uso del Internet enviar mensajes amenazantes, sin que necesariamente la dirección de la que se remita sea la del agresor.
- La instigación a delinquir, al igual que en el supuesto anterior, pero incluso por medios más efectivos y consecuencias más graves, ya que a través de una página Web, se puede instigar a las personas, especialmente a los menores a cometer delitos, incluso bajo retribución de premios.

- Delitos contra la Honra, que se los puede cometer de la misma manera que los delitos antes mencionados, bien por vía de correo electrónico o por publicaciones realizadas en páginas electrónicas.
- Pornografía infantil, o más acorde a nuestro Código Penal, corrupción de menores, ya que sería pertinente reformar el artículo indicando que la exposición o venta de material que incite a prácticas sexuales también se lo puede realizar por medios informáticos.

Estas figuras son a manera de ejemplos, algunas formas de infracciones que también pueden ser cometidas por medios informáticos, no obstante debemos señalar que no solo se debería realizar este tipo de reformas añadiduras, sino que también se deberían incluir otros delitos que nuestro Código Penal no posee como serían:

- Cracking, como figura agravante del delito de hacking
- Plagio informático, considerando como tal a la edición, venta o reproducción de una obra ajena como propia usando medios informáticos
- Piratería informáticas, siendo la reproducción y venta de todo tipo de artículos sin la autorización del autor, tales como copias de discos compactos, DVD y programas de ordenador.

Bien vale señalar que en los dos últimos casos propuestos existen leyes especiales que sobre los mismos establecen sanciones, como es la Ley de Propiedad Intelectual.

3.3. –CONSTITUCION POLÍTICA DEL ECUADOR

Nuestra Constitución, a criterio personal muy moderna y completa a nivel Latinoamericano, si bien no establece como es lógico una tipificación de delitos

informáticos, si posee en su normativa una serie de derechos que están consagrados a favor de todos los ciudadanos de la nación, y a lo largo de este estudio hemos venido tratando una serie de conductas que afectan o pueden afectar al común de las personas, y tras establecer los delitos informáticos vigentes y los que deberían ser considerados, dentro de este cuerpo legal, supremo por excelencia, también encontramos normas que de una u otra manera forman parte de lo que estamos tratando.

Así, nos vemos obligados a determinar que la Constitución ecuatoriana posee ciertos derechos que pueden ser afectados a través de medios informáticos, tal es el caso del Art. 23 el cual señala que *"Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes"*, No 8 *"El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona"*[160], en cuanto al derecho a la honra y a la buena reputación, como se dijo debería también considerarse dentro de las posibles infracciones informáticas susceptibles de ser cometidas por medios informáticos, pero sobre la violación al derecho de intimidad la ley deja muchos vacíos por llenar, a más de lo ya anotado sobre el tema cuando analizábamos las reformas al Código Penal de la Ley de Comercio Electrónico, creemos conveniente indicar que por el solo hecho de ser un derecho consagrado por la constitución, el legislador no lo incluyo en los delitos informáticos, ya que se debería sobrentender que esta violación puede ser cometida por cualquier medio, incluido el informáticos, pero si bien esta protección sería un poco extensiva, consideramos necesario que el legislador a

[160] **Constitución Política de la República del Ecuador**

manera de concordancia con la carta constitucional, incluyera dentro de la infracciones informáticas la violación de la intimidad de manera expresa. Al efecto el mismo artículo en su No. 21 establece que toda persona tiene derecho a guardar reserva sobre sus convicciones tanto políticas como religiosas, ni sobre datos referentes a su salud y vida sexual, como advertimos con anterioridad en cuanto se refiere al derecho a la intimidad, durante el transcurso de vida de los seres humanos, por el hecho de ser tales, nos vemos obligados a mantener para nosotros una serie de datos personales incluso personalísimos, que bajo ninguna naturaleza nos pueden obligar a revelar, como es el caso de convicciones políticas, religiosas, estado de salud, preferencia sexual, ligación sindical, que configuran la vida privada e intima de los seres humanos.

Todo esto concuerda con el Art. 9 de la Ley de Comercio Electrónico, que se refiere a la confidencialidad y reserva, para los mensajes de datos, cualquiera sea su forma, medio o intención, que si bien garantiza y protege la información y la intimidad, insistimos una vez más en la necesidad de que este derecho sea establecido expresamente como infracción informática, por la facilidad de violarlo por medios electrónicos, informáticos e inclusive telemáticos

Igualmente en concordancia con las normas que a nuestro criterio se debería aumentar, el No.9 inciso segundo del mismo artículo consagra que toda persona afectada por afirmaciones si pruebas publicadas en cualquier medio de comunicación (Internet, e mail), tiene derecho a que por ese mismo medio se hagan las rectificaciones del caso para salvaguardar su buen nombre.

Finalmente el mismo artículo 23 No. 13 norma la inviolabilidad y el secreto a la correspondencia, indicando además que este principio se verificará con

cualquier otro tipo o forma de comunicación, de lo cual desprendemos que si bien dentro de la ley penal no se establece la violación del correo electrónico de manera expresa la constitución así lo consagra, al indicar que podrá ser también por cualquier otro medio, a lo cual nosotros incluimos al correo electrónico en todas sus formas, sea gratuito o contratado.

Como concordancia final del derecho a la intimidad, pese a ya ser analizado bien vale señalar, que además la Constitución en el Art. 94 establece el Habeas Data, que como se estudio es el antecedente más próximo de lo que en la actualidad conocemos como derecho a la intimidad.

3.4. –SITUACION NACIONAL

Hasta hace unos pocos meses atrás nuestro país no contaba con una legislación en materia de delitos informáticos, pero el 17 de abril de 2002, en el Registro Oficial Suplemento. 557, se publico la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, la cual en su Título V incluye lo que se han denominado Infracciones Informáticas, estableciendo varias reformas a nuestro ordenamiento penal vigente, las mismas que han sido motivo de análisis previo, sin embargo en el Ecuador este tipo de conductas han afectado gravemente no solo a personas naturales sino también a personas jurídicas, especialmente a instituciones del sector público.

Si bien en la actualidad gracias a gestiones particulares de personas interesadas en el tema, podemos contar con una serie de normas penales relacionadas con situaciones informáticas, también es cierto que estas normas aún resultan insuficientes, ya que no se ha establecido una ley específica en delitos informáticos, tal y como lo han venido implementando países europeos y otros como Venezuela, el

legislador ecuatoriano, ha pretendido según se nota en el espíritu mismo de la Ley, no incurrir en el cotidiano sistema de implantar en el país más leyes, que por su naturaleza contengan sanciones penales, es decir, existen leyes como las tributarias que por su naturaleza misma contienen a más de las propias de la materia, otras normas penales, no tipificadas en el Código Penal, por lo que advertimos que si bien la intención ha sido buena, de establecer en un mismo cuerpo legal a las infracciones informáticas, resulta un poco ilógico pensar que estas normas tengan la total eficiencia que se espera, ya que hablamos que al incluir estas conductas, nos referimos a la modernización que el derecho requiere, pero hasta la actualidad, nuestro Código Penal, cuenta con sanciones irrisorias en cuanto al pago de multas se refiere, y las nuevas normas introducidas, por su parte poseen sanciones mucho más acorde a la realidad de nuestra sociedad, no solo por ser más justas, sino porque el infractor en parte podría reparar el daño causado a la victima.

Los ataques a ordenadores sufridos en nuestro país, prácticamente han perdido la cuenta, los mismos lamentablemente han quedado en la impunidad, justamente por esa falta de normativa sobre la materia, pero pese a que ya existe, la falta de conocimiento por parte del común de las personas de igual forma no permite establecer una certera cifra de cuantos han sido los ordenadores afectados, por los diversos y variados ataques que se producen, además por la falta de probidad en la función judicial, la gente no se acerca a denunciar este tipo de infracciones.

La promulgación de la Ley de Comercio Electrónico, en cuanto se refiere a los delitos informáticos, ha sido un logro muy importante, pero los medios para hacerla efectiva resultan insuficientes, no basta con tener tipificado cierto número de conductas, si los procedimientos para castigarlas no están bien definidos, el Código

de Procedimiento Penal en su Art. 32 divide el ejercicio de la acción penal en tres clases:

- Pública de instancia oficial
- Pública de instancia particular
- Privada

Dentro de los delitos susceptibles de ejercer la acción penal pública de instancia particular, y conforme a nuestro estudio establece los siguientes: Revelación de secretos de fábrica, Estafa, Hurto y Robo (apropiación ilícita), y en los de acción privada a delito de daño en propiedad privada, estableciéndose presupuestos claros sobre los pasos ha seguir para la sanción de estas conductas, en los de acción pública de instancia particular se deberá contar con un fiscal, figura esta muy discutida por el papel que en la actualidad están desempeñando, se supone que la Fiscalía debería ya contar con un departamento técnico y especializado en este tipo de infracciones, porque de nada sirve tener una ley que realmente se ha vuelto inaplicable, y no solo por la falta de personal capacitado que puede hacer efectiva una investigación que la situación amerite, sino porque tampoco de han definido bien cuales podrían ser los medios de prueba eficientes en estos casos.

Peor aún en la acción privada, a la cual se accede solo mediante acusación particular y ante un Juez penal, el cual por sobradas razones no posee tampoco los medios suficientes para una prolija investigación y sanción de estas conductas, es decir la situación del país realmente es crítica, la indefensión en la que se encuentra la sociedad es alarmante, porque como se ha expuesto no solo la falta de medios judiciales es impedimento, sino también que las víctimas no miran con buenos ojos las actuaciones de esta función, por su falta de probidad y celeridad, en otros casos

las denuncias no se las llega a realizar, especialmente por parte de las instituciones, por temor a perder credibilidad, pero caso muy especial es el del Municipio del Distrito Metropolitano de Quito, el cual la noche del 5 y madrugada del 6 de febrero de 2001, sufrió un ataque a su página en Internet (www.quito.gov.ec), y las autoridades si bien no pudieron presentar ninguna denuncia justamente por la falta de una ley en ese tiempo, no tuvieron reparo en dar a conocer a la comunidad la situación ocurrida, incluso a través de los medios de prensa.

El Ecuador ha dado un paso importante, al introducir normas penales informáticas, pero aún nos falta mucho por hacer, como establecer medios efectivos y suficientes que garanticen el éxito rotundo de la Ley, implementando departamentos técnicos en la materia no solo en la función judicial o en la fiscalía, sino también a nivel policial, procurar una campaña masiva de difusión de la Ley, y de las consecuencias nefastas de los ataques, y por sobre todo a las autoridades demostrar que la situación es preocupante y que los medios judiciales serán efectivos en procurar una justa pena a los infractores.

CAPITULO 4.- CASOS Y JURISPRUDENCIA

En el presente capítulo, pretendemos dar a conocer casos reales sobre delitos informáticos, ocurridos en varios países, cuales han sido las sanciones a los mismos, o cuales deberían ser las penas de acuerdo a nuestro ordenamiento penal vigente sobre la materia, además indicaremos una serie de infracciones que se dan a conocer por diversos medios y que de alguna manera reflejan el grave peligro que significan este tipo de conductas.

Durante la investigación de nuestro estudio nos hemos preocupado de recopilar información necesaria tendiente a demostrar que las infracciones informáticas realmente existen y sus medios de propagación son tan diversos como delitos existen, por lo que gracias a un sitio Web, especializado en la materia, se ha logrado acceder a información de varios países, que han sufrido los denominados ataques informáticos en sus diversas formas, como virus, gusanos, sabotajes, espionajes, pornografía infantil, hackers y crackers, en definitiva lo que pretendemos demostrar es que este tipo de conductas delictivas son más comunes de lo que nos imaginamos, y diariamente existen denuncias sobre las mismas, por lo menos en los países desarrollados, donde además de una efectiva sanción punitiva, existen los medios suficientes e idóneos para proceder a la investigación, detención y sanción de los sujetos activos de las infracciones.

4.1. CASOS

A continuación estableceremos la mayor cantidad de casos posibles reales, relatando un resumen del caso y cual sería su tratamiento conforme a nuestra legislación:

CASO # 1

Redada contra la pornografía infantil en Austria. –

El 22 de abril del año 2002, se ha llevado en Austria una de las más grandes redadas contra la pornografía infantil en el Internet, con el agravante de que en este país es penado judicialmente la tenencia de material pornográfico, durante este proceso fueron investigados 329 registros domiciliarios pertenecientes a 283 personas, según lo determina el Jefe de la Sección de denuncias de pornografía infantil, incluso uno de los implicados, luego del registro que la Policía realizara en su domicilio se suicido, esta investigación se inició en Texas (EEUU) a una empresa que se dedicaba a la distribución de este tipo de material, los mismos investigadores tan solo en Viena llegaron a intervenir más de 400 computadores, estando además implicados en el caso funcionarios públicos y periodistas.[161]

CASO # 2

La ONG "Todos son inocentes", se querella contra el portal de Internet TERRA, por publicar pornografía infantil. –

El Presidente de la ONG "Todos son inocentes", con fecha 7 de mayo de 2002, ha presentado una denuncia contra el Presidente del Consejo de Administración del Portal TERRA, ya que se han publicado imágenes de pedofilia, teniendo el portal antecedentes de publicaciones similares con anterioridad, la primera denuncia fue presentada el 13 de marzo, y la segunda el 8 de abril, ya que se presentaron imágenes de menores que no superan los cinco años de edad, la ONG planea presentar denuncias en los diferentes países en que tiene la sede dicha

[161] www.delitosinformaticos.com

organización e incluso contra el Gobierno español, por negligencia en el cumplimiento del Protocolo de la Convención de los Derechos del Niño, que fue ratificada por este gobierno.[162]

CASO # 3

La Guardia Civil clausura dos sitios con pornografía infantil. –

El 7 de mayo de 2002, la Guardia Civil española, ha logrado detectar y clausurar dos sitios web españoles que contenían pornografía infantil, dichos sitios poseían más de 7000 fotografías con escenas explicitas de menores, cuyas edades fluctuaban entre los cinco meses y los quince años, los cuales simulaban o tenían relaciones sexuales con adultos, o escenas de agresiones corporales, esta clausura fue posible gracias a los controles permanentes que realiza la Guardia Civil en la red, sin embargo se ha llegado a determinar que el servidor que proveía las imágenes era Norteamericano.[163]

CASO # 4

Cuatro personas detenidas por difundir pornografía entre menores en la Red. –

Cuatro jóvenes entre 20 y 24 años de edad fueron detenidos el 16 de junio de 2002, por el Cuerpo Nacional de Policía española por estar relacionados con la difusión de pornografía con destino para menores, utilizando para el efecto un canales juveniles de Chat, enviando continuos mensajes, y si el menor pinchaba el mensaje inmediatamente se conectaba con el sitio, el cual además facturaba una

[162] **Ibid. Op. Cit.**
[163] **Ibid. Op. Cit.**

tarifa elevada, uno de los detenidos es un experto en elaboración de páginas web y tiene altos conocimientos en programación.[164]

CASO # 5

Joven chileno detenido en un ciber café por utilizar y difundir pornografía infantil. –

Agentes de la comisaría informaron que el día 24 de marzo de 2002, fue detenido un estudiante de Derecho, al interior de un ciber café, al cual se lo acusa de difundir por Internet pornografía infantil, el cual formaba parte de una red con intereses comunes en pedofilia denominada "Regreso de la familia", de la cual además forman parte un mexicano que hacía gala de tener relaciones con su prima menor de edad, y, otra mujer que abusa de los niños que tiene a su cargo.[165]

Estos delitos que por su naturaleza mismos más que reprochables son despreciables, podemos evidenciar algunas fallas en los procedimientos, en el primer caso se ha logrado detener a los autores del mismo, y que mejor evidencia que el suicidio de uno de los implicados, pero en los otros dos casos queda de lado la sanción, no basta el retiro efectivo de las imágenes o la clausura de los sitios sino una drástica sanción contra los propietarios o administradores de los sitios, relevante función tanto de la ONG, como de la Guardia Civil española, ésta última que ha demostrado real capacidad de investigación en cuanto tiene que ver con el cibercrimen.

Dentro de nuestra legislación, el Código Penal sanciona la corrupción de menores, con una pena de uno a tres años de prisión, tanto la exposición, venta o entrega a menores de material obsceno, como la incitación a un menor a la práctica

[164] **Ibid. Op. Cit.**
[165] **Ibid. Op. Cit**

de actos obscenos, lamentablemente las reformas a este cuerpo legal, tras la publicación y entrada en vigencia de la Ley de Comercio Electrónico, no se contempla el delito de pornografía infantil a través de medios informáticos, sin embargo trasladando las normas penales, bien se podría indicar que cabría una sanción privativa de la libertad contra quines de cualquier forma expongan esta tipo de material, considerando que para dicha exposición se han utilizado a menores de edad, lo que encuadraría la figura para la sanción penal.

CASO # 6

Desmantelado anillo de piratas informáticos en EE.UU.. –

La denominada Operación Cibertormenta, efectuada por el FBI, ha dado como resultado la detención de 27 personas residentes en San Francisco, Washington y Oregon, la misma que a durado aproximadamente dos años de investigación, los detenidos en su mayoría de origen taiwanes se dedicaban a la piratería de software informático, dentro de los programas que se dedicaban a piratear figuran el Office 2000 y Windows NT de la empresa Microsoft, y de Adobe Systems (Adobe Photoshop, Adobe Illustrator y Adobe Go-Live).[166]

CASO # 7

Detenido joven pirata por comercializar a través del Internet películas en formato CD Room. –

Un joven español fue detenido el 20 de abril de 2002, porque se dedicaba a la piratería (copia y reproducción) y venta de películas en formato CD Room de

[166] www.delitosinformáticos.com

manera no autorizada, utilizando anuncios en páginas de subastas, indicando el servicio que brindaba e incluyendo su dirección electrónica para que lo contacten, para realizar sus copias el implicado utilizaba un programa denominado DeCSS, que provoca la ruptura de los códigos de seguridad que poseen los DVD que los alquilaba a una video club local, su detención fue posible ya que además se pudo constatar que tenía una gran cantidad de clientes en todo el territorio español, además se encontró en su poder varios programas que facilitan este tipo de actos y diversos soportes informáticos. Sin embargo fue puesto en libertad con cargos continuando el desarrollo del caso en juzgado español.[167]

En estos dos casos, la figura del delito se encuadra en el denominado de Piratería Informática, que consiste en la reproducción no autorizada de programas informáticos o similares, mediante el uso de soportes computacionales aptos para tal actividad, nuevamente nos vemos abocados a mencionar la falta de tipificación en materia penal sobre la piratería en general, como proceso de reproducción de obras sin autorización del autor, como manifestamos anteriormente, una de las falencias que posee nuestra normativa penal, es que no solo existen sanciones penales dentro del Código de la materia, sino que estas se encuentran en otros cuerpos legales, en los casos planteados la sanción la encontraremos en la Ley de Propiedad Intelectual, la cual además impone multas y sanciones civiles como el comiso de los bienes pirateados y los artefactos con los que se los realizó, a más de la reparación de daños y perjuicios a favor del autor o autores.

Sin embargo por no ser materia de nuestro estudio, nos limitamos a establecer las pautas tendientes a la reparación de los daños que estas conductas

[167] **Ibid. Op. Cit**

causan, pero los hemos incluido ya que forman parte de la cadena delictiva informática, determinada así por la doctrina y por ciertas legislaciones vigentes en el resto del mundo, y además porque configuran y forman parte de la clasificación de los delitos informáticos.

CASO # 8

Hackers atacan servidores del gobierno americano. –

El 10 de mayo de 2002, una banda de hackers denominados a si mismo "Deceptive Duo", ingresaron a servidores de las líneas aéreas americanas Midwest Express, pero la grave del caso, es que son ellos mismos los que informaron que ingresaron al servidor y robaron información de usuarios, nombres, direcciones de e mail y contraseñas, quedando aún por establecerse si realmente obtuvieron dicha información.[168]

CASO # 9

Hacker ataca la página chilena www.atichile.cl. –

Entre diciembre de 2001 y enero de 2002, un joven chileno de 21 años, ingreso a la cuneta general de la empresa Ati Chile, intercepto y se apropio de direcciones electrónicas de usuarios y sus nombres, destruyo los archivos y creo otra página con mensajes ofensivos, apropiándose además de datos sensibles de la empresa, el cual tras una larga investigación ha sido detenido, juzgado y sentenciado.[169]

---

[168] **Ibid. Op. Cit.**
[169] **Ibid. Op. Cit.**

CASO # 10

Detenido Cracker por daños informáticos en Barcelona – España. –

Una mujer acusada de producir daños informáticos fue detenida el 9 de mayo de 2002, por parte del Grupo de Delitos Informáticos de la Jefatura Superior de Policía, la cual inutilizo cuentas de acceso, destruyo archivos, revelo secretos de varias instituciones en las que había trabajado anteriormente, la investigación inicio tras la denuncia de que desde el mes de julio de 2001, los archivos informáticos de las instituciones habían sido destruidos, imposibilitando el normal funcionamiento del sistema, y pare febrero se detecto que las cuentas de acceso habían sido arbitrariamente cambiadas, tras las investigaciones respectivas se llego a determinar que la causante era una mujer cubana de 32 años, que había trabajado en todas las organizaciones afectadas.[170]

El delito de hacking o el de cracking dentro de nuestra legislación no se encuentra establecido como tal, sin embargo existen figuras a las que se los podría asimilar para evitar la impunidad de los mismos, según los estudiosos del tema se ha logrado determinar que este tipo de infracción es la más común, ya que los medios de cometerla es mucho más sencilla, el Art. 59 de la Ley de Comercio Electrónico establece como infracción la violentación de sistemas informáticos para acceder a información no autorizada, siendo la pena de seis meses a un año de prisión y multa de quinientos a mil dólares americanos, si bien la figura como tal no establece la determinación del sujeto activo como hacker o cracker, esta por demás entender que al momento del juzgamiento de la infracción, el autor se ajusta a la conducta descrita, esto en el supuesto de los dos primeros casos, pero como agravante a la infracción en

[170] www.delitosinformáticos.com

el tercer caso, a más de violentar las seguridades y violar el derecho a la intimidad se produce el delito de daño informático, el cual esta sancionado por la misma Ley con una pena de seis meses a tres años de prisión y multa se 60 a 150 dólares, tal y como lo señala el Art. 62.

CASO # 11

Virus Klez, se propaga a gran velocidad y se lo cataloga ya como epidemia. –

En el mes de abril de 2002, en China fue descubierto el denominado virus Klaz, en su última y más moderan versión, el cual ya se ha logrado propagar en más de 130 países, y el Centro de Alerta Temprana sobre virus informáticos, por su alta peligrosidad y rápido desplazamiento lo ha catalogado como una verdadera epidemia, similar a los daños causados por el virus Sircam, el grado de peligrosidad a decir del centro es de 4, Alta es decir "Amenaza peligrosa y difícil de contener", se propaga vía correo electrónico y puede afectar carpetas y directorios compartidos, además procura eliminar antivirus y sistemas de seguridad de los computadores para dejarlos indefensos.[171]

CASO # 12

Aparece nuevo virus o gusano denominado "Operación Triunfo". –

Pretendiendo engañar a los usuarios, este virus se propaga a través del correo electrónico, y hace cree al receptor del mensaje que le ha llegado información acerca del popular programa televisivo "Operación Triunfo", siendo un enganche para que el usuario abra su correo y el virus se pueda propagar, el archivo denominado

---

[171] **Ibid. Op. Cit**

OperaciónTrinufo,scr- llega con un mensaje que dice "Mira esto jajaja, te vas a reir !!" y el resto del mensaje indica "Jajaja !!! Es la osita !!Miralo!!", pretendido instalarse en varios archivos, en busca de que el usuario cada vez que inicie o reinicie su sistema, el gusano actúe destruyendo la mayor cantidad posible de archivos, especialmente los que tiene extensión .exe, borrando además archivos con extensión: .ace, .jpg, .zip, .mp3, entre los más comunes.[172]

CASO # 13

Nuevo gusano ataca a servidores SQL de Microsoft. –

Un gusano denominado "SQLsnake", se esta reproduciendo y propagando rápidamente a través del Internet, por lo que los dueños de las viejas versiones del software SQL Server de Microsoft, has sido advertidos para que cambien la configuración de su contraseña, se han reportado ya más de quince mil computadoras infectadas con un promedio de cien infecciones por hora, siendo estos ataques más frecuentes en Estados Unidos y Corea, teniendo graves repercusiones en los sistemas afectados.

Los presentes casos respecto de otro de los graves problemas informáticos a los que nos vemos sometidos, se refieren a la creación y divulgación de virus o gusanos, especialmente por medio del Internet, muy pocos son los Estados en los que esta modalidad de crimen esta penada, en nuestro país, no se ha establecido como figura delictiva, pese a los casi diarios casos de infección de computadoras por la introducción de virus, sin embargo se podría asimilar la conducta al delito de daños informáticos, por los graves problemas que ocasionan los mismos.

---

[172] **Ibid. OP. Cit.**

CASO ECUATORIANO

Hackers destruyen página web del Municipio de Quito. –

La noche del 5 al 6 de febrero de 2001, personas hábiles en informática destruyeron la página web del cabildo, la cual había tenido un gran éxito en cuanto a información, que incluso recibió más de 26.000 consultas durante el mes de enero, pero para sorpresa de quienes ingresaron a la página el martes siguientes, se encontraron con la desagradable sorpresa que en vez de la página aparecía un pescado, se presume que quienes atacaron la página ingresaron por el Internet al servidor central del municipio, los técnico se demoraron aproximadamente 48 horas en volver a poner en servicio la página. (Ver anexo No. 2)

Este caso más palpable en nuestro país, puso de manifiesto el riesgo que corríamos al no contar con una ley, en este caso los culpables quedaron impunes por falta de normativa, pero simplemente lo hemos establecido, para dejar en claro que el Ecuador no esta al margen de la delincuencia informática.

Para muestra un botón, así versa un dicho popular muy arraigado en nuestra sociedad, con la exposición de los casos mencionados, hemos querido dejar establecido que todo el mundo, es decir quines habitamos en el planeta estamos expuestos a la criminalidad informática, no solo las grandes potencias mundiales, sino todos y cada uno de los Estados en los cuales la tecnología se ha desarrollado de manera desmesurada, sin un ordenamiento jurídico que la regule, y la lista sigue, y seguirá en aumento si no ponemos un alto, con sanciones efectivas y verdaderas.

Sin embargo no solo son personas sin escrúpulos las dedicadas a esta actividad, bien para demostrar sus habilidades con los sistemas informáticos, o para efectivamente aprovecharse de sus conocimientos y obtener réditos económicos de tales actividades, sino que también las entidades estatales en la actualidad están formando parte de este tipo de infracciones, especialmente en cuanto tiene que ver a la violación del derecho a la intimidad, así lo demuestra un estudio presentado por la cadena de noticias CNN, en la cual se establece que a tras los atentados del 11 de septiembre en los Estados Unidos, y luego de siete meses de publicada la ley para combatir el terrorismo, se han multiplicado las peticiones de las autoridades para que las compañías proveedoras de servicios de Internet, les permitan espiar a ciertos usuarios, catalogados como presuntos miembros de comunidades terroristas, esto sin duda a causado gran conmoción, ya que se estaría atentando contra uno de los derechos fundamentales de los seres humanos, como es la privacidad y la intimidad, pese a la necesidad comprensible de lucha contra el terrorismo, se teme mucho que estas medidas afecten otros intereses que nada tengan que ver con dicha lucha, como discriminación racial, social, sindical o religiosa, utilizando dicha información en contra de las personas afectadas, a lo que se suma que toda intervención deberá ser previa autorización judicial, sin embargo se establecido con certeza que todas las peticiones de intervención electrónica han sido aceptadas sin mediar nada más que la simple sospecha, procediéndose a la intervención incluso antes de que la orden sea autorizada, en nuestro caso, no solo que se violaría el derecho a la intimidad sino también al debido proceso, consagrado en la Constitución de la República.

Sin embargo estas medidas podrían estar bien justificadas si nos remitimos a ciertos informes del Departamento de Defensa norteamericano del cual se desglosan los siguientes datos:

- Marzo de 1999. – Las computadoras del Pentágono se ven sometidas al asedio organizado de intrusos. Todos los días, el Departamento de Defensa registra entre 60 y 80 ataques cibernéticos
- Mediados de 1999. – En un plazo de tres meses, los piratas informáticos contrarios al gobierno de Estados Unidos accedieron de forma ilegal a las páginas electrónicas del Senado, la Oficina Federal de Investigación (FBI), el Ejército, la Casa Blanca y varios departamentos ministeriales
- Enero de 2000. – Durante el año anterior, las empresas de todo el mundo dedicaron 12.100 millones de dólares a combatir el "terrorismo económico" realizado mediante los virus informáticos
- Agosto de 200. – En el Reino Unido, un intruso penetró en sitios virtuales de una agencia oficial y de las autoridades locales.[173]

Los temores de las autoridades mundiales por futuros ataques terroristas revisten necesariamente una tendencia informática, por ser el medio más rápido y eficaz para enviar y recibir información, por que los sistemas electrónicos y las redes de telecomunicaciones son el eje propulsor de esta nueva era, y por que no cabe la menor duda de que la mejor arma que poseen los hombres es n computador, a través de él se puede aprender a manejar desde un auto hasta el más sofisticado avión de combate, nada es difícil para la tecnología computacional, sin embargo lo desmedido

[173] **Revista DESPERTAD,** mayo 2001

de las leyes atentatorias al derecho a la intimidad tendrán un gran rechazo dentro de la comunidad internacional.

Pero no solo las intromisiones oficiales por parte de autoridades afectan al común de las personas o de las empresas, y sin necesidad de establecer un caso en concreto, los intrusos cibernéticos son un grave peligro para la estabilidad financiera, solo en mayo los intrusos cibernéticos robaron cientos de número de tarjetas de crédito del sitio TheNerds.net y obtuvieron acceso a datos de más de 265.000 empleados públicos en California, disparándose la cifra en un casi 400 por ciento superior a lo ocurrido en 1999.[174]

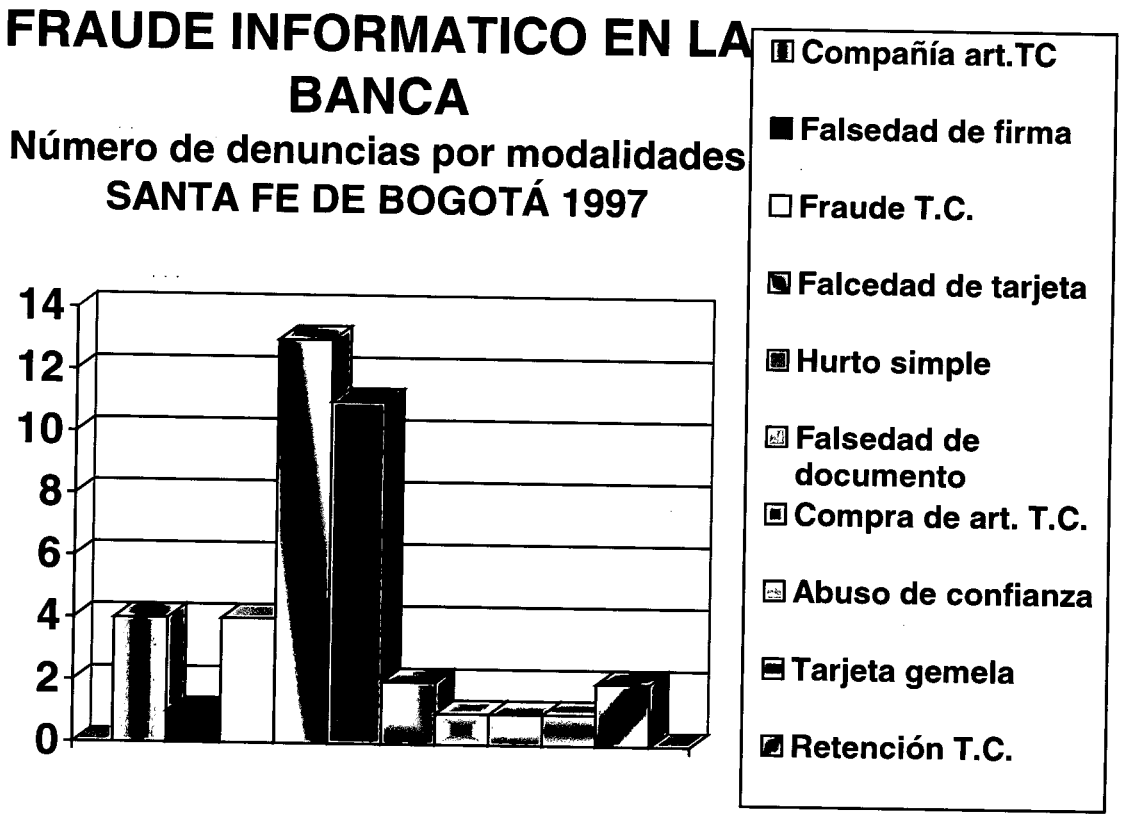
Los problemas de la delincuencia informática son realmente alarmantes, en Europa por ejemplo estos delitos aumentaron en un diez por ciento en el último semestre del 2001, el estudio fue llevado a cabo en empresas industriales, de comercio y de servicios, en España, Francia, Alemania, Reino Unido y Sudáfrica, tan solo en España el número de compañías afectadas supero el 40%, sufriendo entre dos a cinco ataques, lo asombrante de la situación es la que mayoría de infracciones se reportan de ataques internos, por parte empleados descontentos con su empresa (insiders), mientras que la mayoría de ataques externos ni siquiera son percibidos, lo que pone de manifiesto la falencia de los sistemas de seguridad.

Por otro lado el temor más grande que tiene las empresas, especialmente las más influyentes y poderosas, es la pérdida de información de sus archivos, entre los problemas más comunes están: virus 77%, fallas internas 71%, errores de usuario 59%. Es así, de esta forma como podemos darnos cuenta de los terribles problemas

[174] **Artículos del Diario "La Gaceta"**, junio 2002

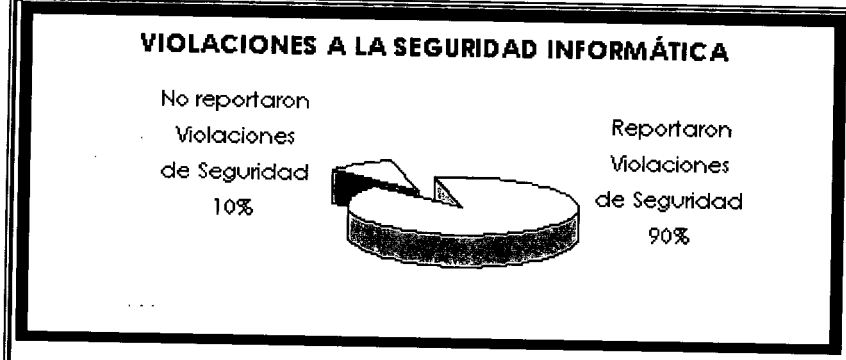
que causa el denominado cibercrimen, sus secuelas son enormes, los daños son generalmente irreparables y las pérdidas de tipo financiera son incalculables.

Otro de los casos alarmantes es el encontrado en Colombia donde uno de los delitos más comunes es el de Fraude Informático en todas sus formas y más aún en la banca o sistema financiero tal y como lo demuestra el siguiente cuadro estadístico:[175]



Otro de los estudios reportados sobre la delincuencia informática, realizado en los Estado Unidos de Norteamérica por parte del Instituto de Seguridad de Computadoras (CSI), denominado "Estudio de Seguridad y Delitos Informáticos" efectuado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno, en cooperación con la Agencia Federal de Investigaciones (FBI), de San Francisco, División de delitos informáticos, arroja los siguientes datos:

"Violaciones a la seguridad informática:

Respuestas	PORCENTAJE (%)
No reportaron Violaciones de Seguridad	10%
	
Reportaron Violaciones de Seguridad	90%

- 90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.
- 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados, por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

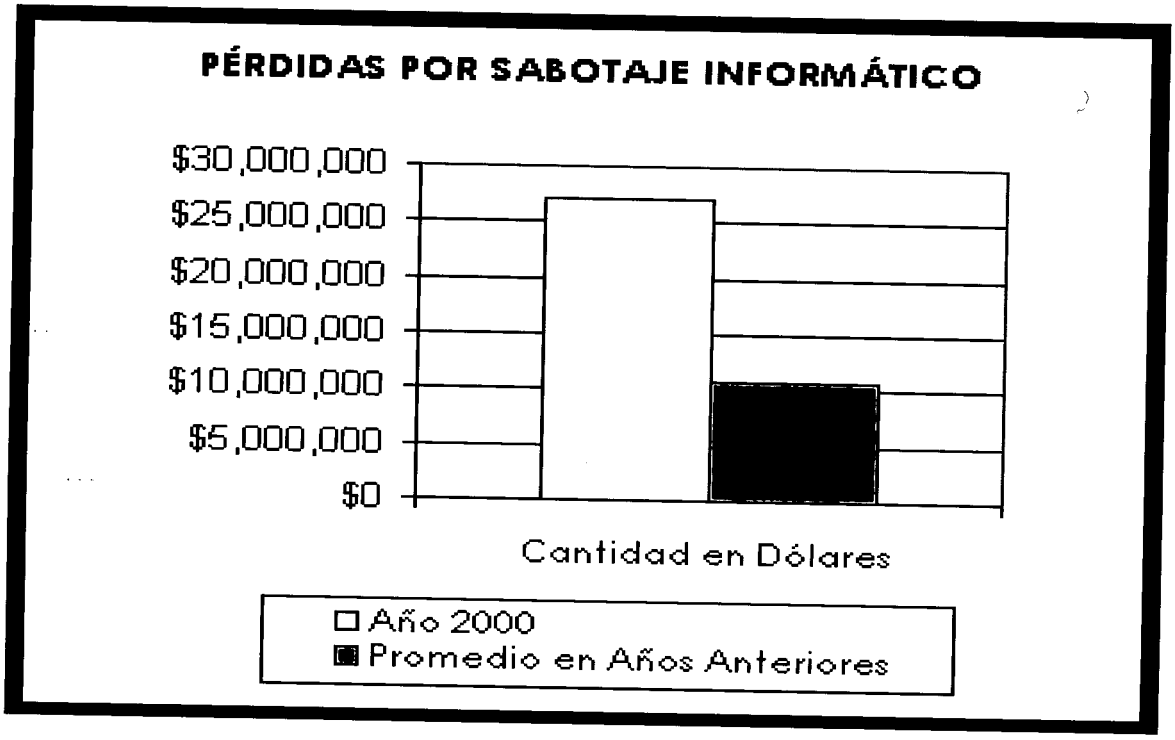
Pérdidas Financieras:

- 74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

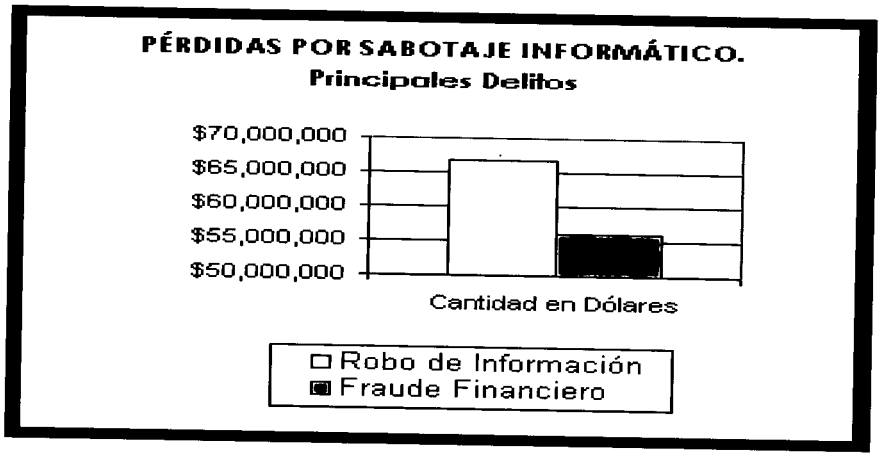
---

[175] **GUERRERO,** María Fernanda y otros, Penalización de la Criminalidad Informática, Pág. 155

- Las pérdidas financieras ascendieron a $265,589,940 (el promedio total anual durante los últimos tres años era $120,240,180).

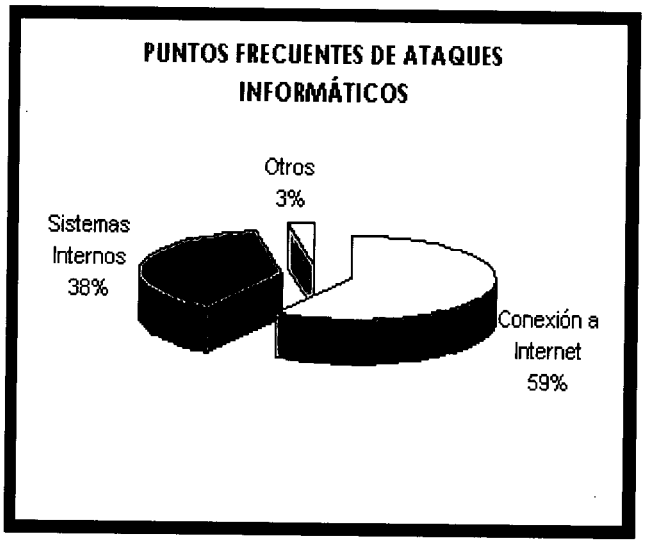


- 61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10,848,850.



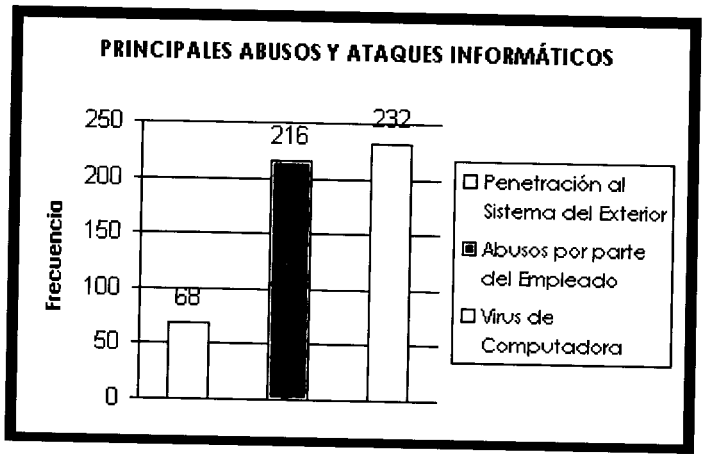
- Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000).
- Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

Accesos no autorizados:



- 71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38%.
- Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del "Estudio de Seguridad y Delitos Informáticos 2000" confirman que la amenaza del

crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.



Los encuestados detectaron una amplia gama a de ataques y abusos. Aquí están algunos otros ejemplos:

- 25% de encuestados descubrieron penetración al sistema del exterior.
- 79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).
- 85% descubrieron virus de computadoras."[176]

Con estos ejemplos, pretendemos dar a conocer los graves perjuicios, no solo de imagen sino también económicos que se corre con los ataques tan variados de los ciber delincuentes, los cuales cada vez atentan a la salud financiera, tanto de empresas privadas como gubernamentales, incluso en países, donde las sanciones a estas conductas son severamente sancionadas, pero que las cifras reflejan alarmantes pérdidas monetarias.

[176] www.monografias.com

4.2. JURISPRUDENCIA

La jurisprudencia, a más de ser una de las fuentes del derecho al entender de todo aquel que esta relacionado con el mundo jurídico, se la considera como "La Ciencia del Derecho"[177], aunque se la debe entender más bien como "el hábito que se tiene de juzgar según igual forma una misma cuestión"[178], es decir, cada vez que se administra justicia por parte del Tribunal de última instancia en un determinado Estado, en el caso del Ecuador la interposición del Recurso de casación, el cual ya no tiene apelación alguna, siendo tal fallo el último y definitivo, se dice que se esta sentando jurisprudencia, y cuando exista un caso similar, éste deberá ser sentenciado conforme al anterior que provoco la existencia de la jurisprudencia, en definitiva es el fallo reiterativo de casos diferentes sobre una misma cuestión.

En materia de delitos informáticos por lo novísimo del tema, aún no se ha podido establecer una real y significativa jurisprudencia, la cual pueda dirimir asuntos similares, incluso por lo diverso de la infracciones, los fallos deberían ser diferentes, sin embargo, una vez que se ha sentenciado un caso, éste pasa a formar parte de la normativa jurídica vigente, es por eso que a continuación presentaremos fallos ocurridos en el juzgamiento de infracciones informáticas en diversos países.

SENTENCIA # 1

Chile: Primer caso de hacking juzgado por la nueva reforma procesal. –

Esta primera sentencia esta relacionada con uno de los casos antes presentados, respecto de la detención y juzgamiento de un joven de 21 años por violación de la intimidad, revelación de datos y sabotaje informático, por haber ingresado

[177] **CABANELLAS, Guillermo,** Diccionario de Derecho usual, Tomo V, Pág. 55
[178] **Ibid. Op. Cit,** Pág. 55

ilegalmente y obstaculizado el servidor de la empresa Ati, Chile www.atichile.cl, el caso fue juzgado por la Ley 19.233 con el agravante de que las acciones cometidas encuadran en todas las infracciones por la Ley establecida (ver Pág. 93), a más del delito de violación al derecho de la intimidad.

El Abogado de la empresa afectada señalo que la fiscalía durante la audiencia de juzgamiento acepto todos y cada uno de los ilícitos denunciados en la querella particular presentada.

SENTENCIA # 2

Estados Unidos: Condenan a 20 meses de cárcel al creador del virus Melissa. –

El primero de mayo de 2002, David Smith, de 33 años, creador del virus Melissa, fue condenado por un tribunal de Nueva Jersey a 20 meses en una prisión federal, por provocar pérdidas estimadas en aproximadamente 1.363,63 millones de euros al trastornar en marzo de 1999 los sistemas mundiales de correo electrónico de un millón de ordenadores.

SENTENCIA # 3

Francia: Individuo condenado por envío de pedofilia a través de correo electrónico. –

Un tribunal francés condenó a ochos meses de prisión, a un ex empleado de la Universidad de Lieja (Bélgica), por "difundir imágenes de carácter pornográfico que incluían a menores", el mismo que admitió los cargos en su contra y que además fue conminado al pago de una multa de 1.500 euros, el caso se inició ya que el autor de la infracción, enviaba por correo electrónico fotografías pedófilas, las cuales por

error fueron recibidas por un estudiante, el cual dio aviso a las autoridades de su instituto educativo, las mismas que presentaron la respectiva denuncia, y la policía tras varios meses de investigación logro dar con la procedencia de las mismas.

Estos breves resúmenes de sentencias dictadas en contra de los sujetos activos de diversas infracciones informáticas, demuestran que, si es factible la imposición de una sanción, y algo más, que efectivamente se puede encontrar a los delincuentes informáticos, situación que ha sido motivo de muchas discusiones, porque se ha puesto en tela de duda la posibilidad de sanción a los mismos, pero queda demostrado que con una pronta denuncia, una prolija investigación y un juzgamiento eficiente, los delitos informáticos no quedan impunes, sin embargo como no todo es siempre bueno, y como la administración de justicia se la puede realizar desde varias ópticas, pese a la sana crítica con la que deben obrar los jueces al momento de sancionar una conducta, existen también fallos contrarios al espíritu de nuestro estudio, es decir que se ha dado la razón a los infractores, bien por no haber tipificación de la conducta, bien porque la valoración de las pruebas no ha demostrado la real participación del denunciado o porque simplemente no fueron lo suficientemente contundentes para aplicar una sanción, así lo demuestra el siguiente fallo argentino:

SENTENCIA # 4

Argentina: Juez falla a favor de ciberintrusos. –

El 11 de abril de 2002, un juez argentino, aduciendo falta de tipificación que castiguen la conducta reclamada, fallo a favor a programadores piratas que violaron la página web de la Corte Suprema, este grupo conocido como "X – Team", irrumpió

el sitio del máximo tribunal de justicia con el fin de acusar a los jueces de encubrir un caso relativo a los derechos humanos, el juez estableció que no hubo daños a cosas, personas o animales, indicando además que no hay ilícitos en el campo informático.

Esta sentencia puso de manifiesto un "grave vacío legal", que no permite la sanción de estos hechos, por más que a los ojos de la comunidad informática jurídica se haya cometido un evidente delito informático, pero en Argentina los fallos judiciales no sientan precedentes jurisprudenciales, por lo que cualquier otro juez podría fallar de manera distinta en un caso similar.

Este grupo ingreso ilegalmente al sitio de Internet de la Corte Suprema en 1998, altero su contenido y coloco en su lugar una foto de un periodista asesinado, e incluyendo declaraciones que culpaban al tribunal de encubrir su muerte.(Ver anexo # 3)

Ante esta situación con fecha 4 de mayo de 2002, la justicia Argentina ha hecho un pedido formal para que se reforme el Código Penal y se considere el "crackeo" de páginas web como un delito.

Con las sentencias mencionadas es fácil colegir que si es posible determinar a los infractores informáticos, pero siempre y cuando se realice una prolija investigación al amparo de los procedimientos pertinentes, vigentes y legales, que no atenten contra ningún derecho de los sospechosos, so pena de nulidad del proceso.

4.3. METODOS DE PROTECCION

Los ataques cibernéticos a más de ser delitos, se han convertido en verdaderos dolores de cabeza, especialmente para grandes y medianas empresas, las mismas que según las estadísticas son las más afectadas, por delitos como el hackeo, la

intromisión indebida, violación de secretos, virus, gusanos, ataques internos y externos, pero una de las alternativas que nos brinda la misma que tecnología, de la cual se han valido los delincuentes para cometer sus infracciones, es una serie de recomendaciones, que van desde simples actuaciones del usuario, hasta la utilización de programas o software, que permiten mejorar los sistemas de seguridad de redes tanto individuales como colectivas.

Instituciones financieras son las que más han hecho uso de este tipo de procedimientos, a decir de los técnicos en seguridad informática, uno de los problemas a los que nos vemos avocados el común de usuarios y de internautas en la red, es la facilidad con la que se pueden realizar los ataques, pero más grave aún, es que los mecanismos de protección resultan tener un costo muy elevado, por lo incluso se ha llegado a determinar que es más barato reparar la máquina afectada o contaminada, que adquirir un dispositivo de seguridad, el cual esta al alcance de consorcios empresariales con un alto poder económico.

A continuación presentaremos una serie de recomendaciones muy simples que los usuarios pueden seguir a fin de reducir los riesgos de ataques o contaminaciones en sus computadores:

- Instalar puntualmente las actualizaciones que recomiendan las casas productoras de software.- Especialmente de los sistemas operativos como el Windows y de las diversas aplicaciones que permiten la conexión al Internet, en los casos de los productos de Microsoft es recomendable la utilización de Windows Update para automatizar el proceso de actualización.
- Utilizar un buen antivirus y actualizarlo periódicamente. – Es conveniente utilizar antivirus que tengan en lo posible actualización diaria y un buen

sistema de servicio al cliente, y que además este certificado por instituciones afines al mundo informático

- Realizar copias de seguridad. – Es recomendable efectuar respaldos de los archivos que poseen información confidencial o sensible, bien sea en formato de disquete o en CD Room.
- Establecer contraseñas seguras y largas. – Al momento de introducir una contraseña para acceso a cualquier programa, es conveniente que esta posee caracteres largos y con palabras que no se identifiquen con el usuario, de preferencia palabras que no puedan encontrar fácilmente en un diccionario.
- Evitar el uso de archivos con formatos potencialmente peligrosos. – Se recomienda no descargar o abrir archivos desde las páginas web con formato .exe, y procurar el envío de correo por los medios efectivos y no a través de correos gratuitos, más propensos al despliegue de virus.
- No abrir ni remitir correo de una dirección desconocida. – Es muy común recibir en las direcciones de e mail, varios mensajes que no corresponden a remitentes conocidos, en tales casos es mejor eliminar o borrar dichos mensajes, porque generalmente traen consigo virus.
- Estar bien informado sobre las posibles proliferaciones de virus. – En la actualidad los medios de comunicación están realizando una labor destacable al informar constantemente de posibles ataques informáticos, es conveniente estar atento a toda información para evitar problemas posteriores.

Si bien estas recomendaciones no garantizan la infección de una máquina a pequeños usuarios, son simples consejos útiles a seguir por parte de aquellos que utilizan la computadora en sus actividades cotidianas.

CAPITULO 5. -

PROPUESTA, OBJETIVOS Y CONCLUSIONES

En el presente capítulo, una vez que hemos analizado la doctrina sobre los delitos informáticos y hecho un recuento de lo que a nuestro criterio resultan las más importantes infracciones, al igual que de las más destacadas legislaciones internacionales sobre la materia, y procurando dar una análisis de las diversas infracciones incluidas en nuestra normativa penal, nos resta por presentar una propuesta personal, del tratamiento actual que se debería dar a esta infracciones, plantear los posibles objetivos no solo del Ecuador sino de la comunidad internacional, en cuanto se refiere a una normalización más eficiente de esta conductas, y finalmente establecer las conclusiones a las que hemos llegado tras este breve estudio.

5.1.- PROPUESTA

Las actuales condiciones en las que se desenvuelve el mundo en general, han sido las más propicias para el desarrollo y crecimiento de las tecnologías, procurando mantener una equidad en los diversos campos en los que la Informática expresa su mayor auge, el hablar de una Era Informática o Electrónica, no es más que apegarnos al criterio dado por historiadores sobre las diferentes épocas en las que el hombre ha vivido, y por tal razón, a cada una de esas eras se las ha ido denominando conforme a las herramientas e instrumentos que se utilizaba, hoy en día, las nuevas tecnologías obligan al ser humano a adaptarse a las nuevas condiciones de comunicación, aprendizaje, lenguaje, escritura y expresión.

Los diversos postulados modernos sobre mundialización o globalización, nos llevan a determinar que los seres humanos caminamos hacia un mundo sin

barreras o fronteras virtuales, desde los intentos por conquistar el espacio, hasta la necesidad de captar consumidores a nivel internacional, reflejan esa necesidad de las personas, estados y empresas, por darse a conocer en todo el planeta, gracias a la creación de la red de información denominada Internet, es cuando surge la necesidad de establecer normas legislativas que rebasen las fronteras de los países, y es cuado la Informática encuentra su máximo grado de interrelación con el Derecho, todo lo que al hombre le es intrínseco encarna una norma jurídica, su vida personal, laboral y comercial, tiene que ver necesariamente con normas positivas.

Sin duda que la globalización pretende la internacionalización de la sociedad en todos sus campos, cultural, artístico, literario, informático o jurídico, los estados en la actualidad buscan alinearse en bloques que les permitan alcanzar un crecimiento económico, político y social relevante, y tanto la Informática como el Derecho, le brindan a la comunidad de estados adentrarse más a fondo en una solución que hace algunos años atrás se veía muy lejana.

El desarrollo inimaginable que han alcanzado las nuevas tecnologías, en materia comercial, industrial, cultural e informativa, bajo ningún concepto pueden estar al margen de una normatividad legal, que permita aún más dicho crecimiento, por las garantías que ofrece un sistema jurídico eficaz, por lo que vemos la necesidad de establecer y propulsar la internacionalización de las normas jurídicas, muchos dirán que es una utopía o quimera el pretender implantar una legislación internacional en una determinada materia, y lo cierto es que si ni en nuestro país, para debatir una ley se ponen de acuerdo, considerando que los intereses son mutuos, peor aún podríamos alcanzar una ley internacional entre diversos Estados, por la variedad de criterios existentes.

Pero el ser humano es un animal de costumbres y se adapta al medio por conveniencia o necesidad, y justamente aquí donde parte nuestra propuesta, la creciente ola delictiva que asota ala humanidad entera, encontró en los delitos informáticos su mejor expresión y manera de cometer infracciones, tan diversas como las establecidas en las normas penales y estudiadas por doctrinarios tradicionales, pero como dijimos, ni siquiera nosotros que estamos viviendo esta nueva era, somos capaces de imaginarnos hasta donde llegara a desarrollarse la tecnología, tampoco estamos en condiciones de establecer hasta que punto las infracciones se van a seguir desarrollando.

Es esta inquietud la que nos obliga a proponer la creación de una legislación internacional en materia de delitos o infracciones informáticas, ya como hemos estudiado, estas se las puede cometer a distancia, sin imaginar los terribles daños que provocan fuera de las fronteras en las que se cometió, y entran en discusión teorías tales como la extraterritorialidad de la ley, la persecución del delito por el daño causado, el juzgamiento del infractor, y no son las normas del Derecho Internacional Público, las que de mejor manera puede normar estas conductas, sino una efectiva legislación internacional, ratificada por todos y cada uno de los Estados miembros de la Organización de la Naciones Unidas, la que va ha permitir sancionar de manera efectiva, en igualdad de condiciones al infractor, ya que el delito puede ser provocado en un estado, consumado en otro y el delincuente capturado en otro, lo que de alguna manera garantizaría la sanción punitiva del mismo, sea cual fuere su origen o nacionalidad.

Creemos pues, que al establecerse una legislación de este tipo, necesariamente se deben considerar temas como la extradición, la igualdad de

sanción y la prescripción de la infracción, claro está que la presenta propuesta debe transitar un arduo y duro camino de debates y acuerdos, debe existir la apertura de las potencias mundiales, así como de los países en vías de desarrollo, comprendiendo la necesidad de establecer a nivel mundial, una norma que garantice a todos la sanción del delincuente.

Por lo que dejamos de lado todo criterio pesimista y miramos hacia el futuro, con la única intención de vivir en un mundo más seguro, y porque no, dar la pauta inicial para la unificación de los diversos derechos y legislaciones existentes en el mundo.

5.2. -OBJETIVOS

Previo al desarrollo del presente estudio, nos plateamos una serie de objetivos, tendientes a propulsar un adecuado tratamiento de las infracciones informáticas, y una vez que hemos concluido nuestra investigación, nos hemos dado cuenta que esas intenciones pretendidas, hoy más que nunca son necesarias, no solo para una efectiva sanción de los delitos, ni para establecer la necesidad de que todos los países cuenten con una legislación similar, sino por lo comprendido y aprendido de este análisis, así consideramos dejar establecidos los siguientes objetivos:

- Pese haber sido motivo de nuestra propuesta, nos queda a los nuevos abogados el objetivo y la obligación de ser los propulsores de una legislación internacional, que será el mejor legado que podamos dejar a nuestra sociedad, a nuestra familia y a nuestro planeta.
- Procurar que en el Ecuador, la legislación penal, aumente de manera significativa otros tipos de delitos informáticos no considerados en la ley

inicial, y mantener una constante actualización de las futuras infracciones que se puedan llegar a cometer.

- Establecer en nuestro país, los medios más idóneos, que permitan la efectiva sanción y punición de los infractores, ya que en las actuales condiciones, las normas incluidas en el Código Penal, realmente no tendrían la función para las cuales han sido creadas.
- Verificar y reestructura los medios de prueba, ya igualmente se vería mermada la facultad y posibilidad de sanción de estas conductas.
- Obligar a todos y cada uno de los empleados de la Función Judicial, a formar parte de este proceso de modernización de la justicia, más aún que nos encontramos en la era informática, y que nuestro país esta sufriendo los embates de la delincuencia electrónica.
- Capacitar tanto a peritos, jueces y magistrados sobre los reales alcances de las nuevas normas, para que no sea su desconocimiento en cuanto a la estructura misma de los delitos, la que impida la imposición de una pena.
- Fomentar una amplia campaña de información sobre la nueva ley, para que los ciudadanos sepan que si son objeto de estas conductas, puedan acudir a los organismos pertinentes en búsqueda de justicia.
- Desarrollar métodos de protección informática, que estén al alcance de las personas, ya que los costos de implementación de los sistemas de seguridad son muy elevados, considerando además que el Ecuador es uno de los principales exportadores de software en Latinoamérica, propulsando por parte del Estado esta actividad, y siendo uno de los objetivos del gobierno, la

seguridad ciudadana no solo en las calles, sino también en el uso de sistemas computacionales.

- Promover además el respeto a los derechos fundamentales, que son constantemente violados por medios electrónicos.
- Como objetivo final, consideramos necesario el establecimiento al interior del Ministerio Fiscal, de un departamento técnico, capacitado y especializado en esta materia, al igual que dentro de las estructuras de la Policía Nacional, para que conjuntamente actúen en la investigación y persecución de estos delitos.

5.3. - CONCLUSIONES

A las conclusiones que hemos llegado son las siguientes:

- Las infracciones informáticas, son un mal cada vez más creciente, por lo que muchos países que no cuentan con sanciones a esta conductas, afrontarán en un futuro cercano graves problemas de juzgamiento.

Es por este motivo, nuestra preocupación e intención de promover a todo nivel la creación de una ley comunitaria, que permita la efectiva sanción de estas infracciones, no solo en los Estados que cuentan con leyes sobre la materia, sino también en aquellos, en los que dicha tipificación no existe o esta en vías de establecerse, lo que de alguna manera garantice a la comunidad internacional la protección a los diversos tipos de ataques que se pueden sufrir, incluso, y porque no, con la creación de un Tribunal Internacional especializado en Derecho Penal Informático, que sea el eje impulsador de la sanción de estas conductas.

- La doctrina sobre la materia resulta muy pequeña, en relación a lo que realmente significan estas infracciones, por lo que muchas de las veces pasan desapercibidas.

Esto se debe sin duda, al poco interés tanto de los estudiosos del Derecho, como de aquellos que lo practican, ya que sus pensamientos tradicionalistas, no les permite ver más allá de lo ya establecido, pocos han sido los que realmente se preocupan de dar pautas para el tratamiento y normalización de estas infracciones, quizá por ser modernistas y visionarios, pero debemos entender que de a poco el mundo entero comprenderá los verdaderos riesgos que implica estar inmersos en esta nueva era, y que por lo tanto el Derecho, como norma de conducta de la sociedad en general, deberá establecer los parámetros por los cuales las nuevas tecnologías deberán transitar.

- La falta de unificación de criterios sobre los diversos modos de cometer los delitos informáticos, conlleva una confusión, tanto para dar su concepto, como para legislarlos.

Si bien por un lado el poco interés que ha despertado esta nueva forma de cometer delitos, resulta incomprensible por los nuevos cambios que esta viviendo la humanidad, resulta también poco entendible, porque, aquellos a los que si les interesa esta modalidad peculiar de aprovecharse de los demás, no ha desembocado en una unidad de criterios, es fácil suponer que por el hecho de hablar de normas positivas, la disparidad entre varias legislaciones sea evidente, no es muy lógico tampoco que la poca doctrina varíe demasiado, por lo que sería muy adecuado convocar a nivel internacional, a todos y cada de los escritores, autores y estudiosos para que, justamente con el propósito de alcanzar una legislación comunitaria e internacional, este expongan sus criterios y llegar a una comunidad de criterios que permitan un mejor tratamiento y análisis de los denominados delitos informáticos.

- El poco interés que han despertado estas infracciones, especialmente en legisladores y juristas tradicionales del derecho, merma de alguna manera los alcances y consecuencias de las mismas.

Como anotamos, no solo los autores tradicionales del Derecho que han dado poco realce a estas conductas, quizá por considerarlas iguales a las ya comúnmente tratadas a lo largo del desarrollo del Derecho, han sido la causante del mínimo interés por legislarlas, sino también los creadores e impulsadores de las leyes o normas positivas de los Estados, se convierten en cómplices de que estas infracciones no tengan el real sentido que se les ha pretendido dar en nuestro estudio, y sin necesidad de introducirnos en problemas legislativos ajenos, el mejor ejemplo lo tenemos en nuestro país, donde la Ley que incluye las reformas al Código Penal para normalizar y tipificar los delitos informáticos, demoró en ser aprobada casi dos años, tras su presentación ante el Parlamento, por lo que es necesario que tanto estudiosos como legisladores sean concientes de lo peligroso que resulta no poseer una ley efectiva, es menester indicar que debemos adaptarnos a las innovaciones que la tecnología nos presenta día a día, por lo que los parlamentarios nacionales y mundiales deben ser más modernistas que tradicionalistas para así procurar una debida seguridad a la sociedad.

- La falta de cooperación, por parte de quienes han sufrido ataques, especialmente de las empresas por temor a perder credibilidad, hace que las buenas intenciones por sancionarlos sean ineficientes.

No solo el contar con una buena o efectiva ley sobre delitos informáticos, garantiza a la sociedad la seguridad requerida, sino que se necesita de la buena predisposición por parte de aquellos que han sufrido ataques a sus sistemas o sus

empresas, para realmente hacer valedera la intención de sancionar, de nada sirve tener una ley, si esta no cumple con su finalidad, y no por ineficacia de la misma sino por la falta de denuncia ante los delitos sufridos. Claro está que para que la sociedad se sienta protegida, debe confiar en el sistema judicial de su país, siendo necesaria una modernización de los procesos jurídicos no solo en el Ecuador sino en todo el mundo, para que así el ofendido, acuda ante las autoridades, a sabiendas que derecho a la justicia esta garantizado.

- Las normas incluidas en nuestro ordenamiento penal, poseen términos muy técnicos, lo cual implica confusión, tanto al momento de interpretarla como al momento de sancionarla.

La ley según nuestro ordenamiento jurídico vigente, debe ser entendida por todos, sin que su desconocimiento sea excusa para cometer una infracción, sin embargo reparamos en considerar que en cuanto se refiere a las infracciones informáticas, y no solo en nuestro país, sino en casi todas las legislaciones existentes sobre la materia, contienen términos muy técnicos, muchas de las veces relacionadas con el mundo de la informática, y no todas las personas están en capacidad de conocer dichos términos, por lo que a manera de recomendación, se debería utilizar palabras sinónimas que expresen o posean un mismo sentido sin tanto tecnicismo, o incurriríamos en extremos como el venezolano, en donde se pretendió declarar a la ley el carácter de inconstitucional por no utilizar palabras en español que es lo que exige la Constitución de Venezuela, para la elaboración de sus leyes.

- Si bien los artículos, en su estructura encierran otros delitos, la falta de especificación podría provocar la impunidad del infractor.

En el Ecuador la tipificación de las infracciones informáticas, resulta un poco peculiar, ya que en un mismo artículo se pueden sancionar varias conductas, si bien la intención del legislador ha sido buena, no solo por incorporar este tipo de normas, sino también por dotar al país de esta seguridad, la estructura misma de los artículos debería ser más explícita para así, diferenciar y penar conducta por conducta para evitar que al momento de juzgar y sancionar se omitan la sigularización de una infracción.

- Los organismos internacionales, resultan ineficientes al momento de establecer normas por las cuales los países puedan regirse para legislar estos delitos.

La intención nuestra de proponer una legislación internacional, tiene sus trabas además en las Organizaciones Internacionales, ya que estas al igual que muchos detractores de los delitos informáticos, han demostrado su poco interés en establecer pautas y normas sobre las cuales los países pueden basarse, para adoptar internamente en sus leyes penales las modificaciones que sobre las infracciones informáticas se requiere.

Como conclusión final diremos que, corresponde a las nuevas generaciones de abogados y juristas, la implementación de mecanismos necesarios tendientes a mejorar la efectiva sanción de los delitos informáticos, introduciéndonos de manera eficiente a la modernización del Derecho y sus normas, alejándonos de antagonismos y doctrinas tradicionales que no permiten la correcta aplicación y sanción de estas normas.

El mundo moderno espera más de nosotros, la sociedad entera aguarda grandes cambios, que nos permitan vivir en comunidad, no solo el Derecho tiene este

gran reto, sino también las demás ciencias a las cuales la tecnología se ve avocada a integrarse, este cambio estructural de la humanidad tendrá su efecto valedero cuando nos demos cuenta de que estos cambios son necesarios para nuestro cotidiano convivir.

ANEXO 1

RESOLUCIÓN DE LA DIRECTIVA EUROPEA

CONVENIO PRELIMINAR SOBRE DELITOS INFORMÁTICOS

Preámbulo Los Estados Miembro del Consejo de Europa y los demás Estados signatarios del presente, Considerando que la finalidad del Consejo de Europa es alcanzar una mayor unidad entre sus miembros; Reconociendo la importancia de fomentar la cooperación con los demás Estados signatarios del presente

Convenio; Convencidos de la necesidad de buscar, como cuestión prioritaria, una política penal común destinada a la protección de la sociedad contra los delitos informáticos, aprobando entre otras cosas una legislación apropiada y fomentando la cooperación internacional; Concientes de los cambios profundos ocurridos como producto de la digitalización, la convergencia y la globalización permanente de las redes informáticas; Preocupados ante el riesgo de que las redes informáticas y la información electrónica puedan también ser utilizadas para cometer delitos penales y que las pruebas relacionadas con dichos delitos puedan ser almacenadas y transferidas por estas redes; Reconociendo la necesidad de cooperación entre los Estados y la industria privada para combatir los delitos informáticos y la necesidad de proteger los intereses legítimos relacionados con el uso y el desarrollo de las tecnologías de la información; Persuadidos de que una lucha eficaz contra los delitos informáticos requiere una cooperación internacional en materia de delitos mayor, rápida y que funcione correctamente; Convencidos de que el presente Convenio es necesario para detener las acciones dirigidas contra la confidencialidad, la integridad y la disponibilidad de sistemas, redes y datos informáticos, así como también contra el mal uso de dichos sistemas, redes y datos, estableciendo la penalización de dichas conductas, conforme se lo describe en el

mismo, y la aprobación de facultades suficientes para combatir eficazmente dichos delitos penales, facilitando la detección, la investigación y el procesamiento de dichos delitos penales tanto a nivel nacional como internacional y estableciendo acuerdos para lograr una rápida y confiable cooperación internacional; Concientes de la necesidad de asegurar un apropiado equilibrio entre los beneficios de aplicar las leyes y respetar los derechos humanos fundamentales, conforme lo establecido en el Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales del Consejo de Europa de 1950, el Pacto Internacional de Derechos Civiles y Políticos de Naciones Unidas de 1966, así como también en otros tratados internacionales sobre derechos humanos pertinentes, que reafirman el derecho de cada individuo a expresar sus opiniones sin interferencias, al igual que el derecho a la libertad de expresión, que incluye la libertad de buscar, recibir y comunicar información e ideas de todo tipo, traspasando las fronteras geográficas, y los derechos relacionados con el respeto a la privacidad; [Concientes también de [la necesidad de reconciliar los beneficios de la asistencia mutua internacional y] la protección de los datos personales, según lo estableció por ej., el Convenio para la Protección de las Personas respecto del Procesamiento Automático de Datos Personales del Consejo de Europa de 1981] ; Considerando la Convención sobre los Derechos del Niño de las Naciones Unidas de 1989 y el Convenio sobre la prohibición de las Peores Formas de Trabajo Infantil de la Organización Internacional del Trabajo de 1999; Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en el campo pena, así como también los tratados similares que existen entre los Estados miembro del Consejo de Europa y otros Estados y poniendo énfasis en que el presente Convenio pretende complementar

dichos acuerdos con el fin de que las investigaciones y los procedimientos penales concernientes a los delitos penales relacionados con los sistemas y los datos informáticos sean más eficaces y para posibilitar la recopilación de pruebas electrónicas relacionadas con un delito penal; Acogiendo con entusiasmo los recientes desarrollos que facilitan la comprensión y la cooperación internacional respecto de combatir los delitos informáticos, incluyendo las acciones de las Naciones Unidas, la OCDE, la Unión Europea y el Grupo de los 8; Recordando la Recomendación N° R (85) 10 concerniente a la aplicación práctica de la Convención Europea sobre Asistencia Mutua en Asuntos Penales con respecto a los exhortos para la interceptación de telecomunicaciones, la Recomendación N° R (88) 2 sobre piratería en materia de derechos de autor y otros derechos relacionados, [la Recomendación N° R (87) 15 que regula el uso de los datos personales por parte de la policía, la Recomendación N° R (95) 4 sobre la protección de los datos personales en el área de los servicios de telecomunicaciones, haciendo referencia en particular a los servicios telefónicos] así como también la Recomendación N° R (89) 9 sobre los delitos relacionados con las computadoras que proporciona lineamientos para las legislaturas nacionales respecto de la definición de ciertos delitos informáticos y la Recomendación N° R (95) 13 concerniente a los problemas del derecho procesal penal en relación con la Tecnología de la Información; Teniendo en cuenta la Resolución No. 1 aprobada por los Ministros de Justicia Europeos en su 21ª Conferencia (Praga, junio de 1997), que recomendaba al Comité de Ministros que apoyara el trabajo llevado a cabo por el Comité Europeo para los problemas de la Delincuencia (CDPC) respecto de los delitos informáticos con el fin de que las disposiciones nacionales en materia de derecho penal sean lo más parecidas

posibles entre sí y posibilitar el uso de medios eficaces de investigación con respecto a dichos delitos, así como también la Resolución N° 3 aprobada en la 23ª Conferencia de Ministros de Justicia Europeos (Londres, junio de 2000), que alentó a las Partes negociadoras a continuar con sus esfuerzos con vistas a encontrar soluciones apropiadas para posibilitar que la mayor cantidad posible de Estados sean Partes intervinientes en el Convenio y reconoció la necesidad de contar con un rápido y eficiente sistema de cooperación que tenga en cuenta debidamente los requerimientos específicos que debe tener la lucha contra los delitos informáticos; Habiendo tenido en cuenta también el Plan de Acción aprobado por los Jefes de Estado y de Gobierno del Consejo de Europa, en ocasión de realizarse su Segunda Cumbre (Estrasburgo, 10 al 11 de octubre de 1997), para buscar respuestas comunes al desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa; Hemos acordado lo siguiente:

Capítulo I - Uso de los términos

Artículo 1 - Definiciones A los efectos del presente Convenio: a. "sistema informático" significa todo dispositivo o grupo de dispositivos interconectados o relacionados, de los cuales uno de ellos o más, conforme a un programa, realiza el procesamiento automático de datos; b. "datos informáticos" significa toda representación de hechos, información o conceptos en un formato que pueda ser procesado a través de un sistema informático, incluyendo un programa que pueda hacer que un sistema informático realice una

función; c. "proveedor de servicios" significa: (i) cualquier ente público o privado que provea a los usuarios de su servicio la capacidad para comunicarse por intermedio de un sistema informático y (ii) cualquier otra entidad que procese o almacene datos informáticos en nombre de dicho servicio de comunicaciones o de los usuarios de dicho servicio. d. "datos de tráfico" significa todos los datos informáticos relacionados con una comunicación efectuada a través de un sistema informático, generados por un sistema informático que formaba parte de una cadena de comunicación, que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente.

Capítulo II - Medidas que deben tomarse a nivel nacional

Sección 1 - Derecho penal sustantivo

Título I - Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos

Artículo 2 - Acceso ilegal Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delito penal en virtud de sus leyes nacionales, cuando se efectúe de manera intencional, el acceso a un sistema informático o a una parte del mismo sin permiso. Una Parte puede requerir que el delito sea cometido infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención dolosa o en relación con un sistema informático que esté conectado con otro sistema informático.

Artículo 3 - Interceptación ilegal Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delitos penales en virtud de sus leyes nacionales, cuando se efectúe de manera intencional, una interceptación sin permiso, a través de medios técnicos, de las transmisiones de datos informáticos de carácter no público efectuada a, desde o dentro de un sistema informático, incluyendo las emisiones electromagnéticas desde un sistema informático que transporta dichos datos informáticos. Una Parte puede requerir que el delito sea cometido con intención dolosa, o en relación con un sistema informático que esté conectado con otro sistema informático.

Artículo 4 - Interferencia de los datos 1. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delitos penales en virtud de sus leyes nacionales, cuando se efectúen de manèra intencional, daños, eliminaciones, deterioros, alteraciones o supresiones de datos informáticos sin permiso. 2. Una Parte puede reservarse el derecho de requerir que las conductas descriptas en el inciso 1 tengan como resultado un perjuicio serio.

Artículo 5 - Interferencia del sistema Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delitos penales en virtud de sus leyes nacionales, cuado sea cometida de manera intencional, la obstaculización seria y sin permiso del correcto funcionamiento de un sistema informático mediante el ingreso, la transmisión, el daño, la eliminación, el deterioro, la alteración o la supresión de datos informáticos.

Artículo 6 - Mal uso de los dispositivos 1. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delitos penales en virtud de sus leyes nacionales, cuando sean cometidos de manera intencional y sin permiso: (a) la producción, venta, obtención para uso personal, importación, distribución o demás actos similares que pongan a disposición: 1. un dispositivo, incluyendo un programa informático, diseñado o adaptado principalmente con el fin de cometer cualquiera de los delitos establecidos conforme a los Artículos 2 a 5; 2. una clave para ingresar a una computadora, un código de acceso, o cualquier otro dato similar por medio del cual pueda accederse a un sistema informático o a parte del mismo con la intención de ser utilizados con el fin de cometer cualquiera de los delitos establecidos conforme a los Artículos 2 a 5; y (b) la posesión de uno de los ítems mencionados en los incisos (a)(1) o (2) ut supra, con la intención de ser utilizado para cometer alguno de los delitos establecidos en los Artículos 2 a 5. Una Parte puede requerir por ley la posesión de una determinada cantidad de dichos ítems antes de que corresponda aplicar la responsabilidad penal. 2. No deberá interpretarse que este artículo impone una responsabilidad penal cuando la producción, venta, obtención para uso, importación, distribución y demás actos similares relacionados con disponer de o poseer un ítem mencionados en el inciso 1 de este Artículo no tienen la intención de cometer un delito conforme a lo establecido en los artículos 2 a 5 de este Convenio, tales como la verificación o protección autorizada de un sistema informático. 3. Cada Parte puede reservarse el derecho a no aplicar el inciso 1 del presente Artículo, siempre que la reserva no concierna a la venta, distribución u otra manera similar de poner a disposición los ítems mencionados en el inciso 1(a) (2).

Título 2 - Delitos relacionados con el uso de computadoras

Artículo 7 - Falsificación relacionada con el uso de computadoras Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delitos penales en virtud de sus leyes nacionales, cuando se efectúe de manera intencional y sin permiso, el ingreso, la alteración, la eliminación o la supresión de datos informáticos, que tenga por resultado la producción de datos no auténticos con la intención de que sean considerados como auténticos y que se obre en consecuencia con fines legales, sin tener en cuenta si los datos son directamente legibles e inteligibles. Una Parte puede requerir que exista la intención de cometer fraude o una intención dolosa similar antes de que corresponda aplicar la responsabilidad penal.

Artículo 8 - Fraude relacionado con el uso de computadoras Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delitos penales en virtud de sus leyes nacionales, cuando se cause de manera intencional y sin permiso, la pérdida de un bien a otra persona debido a: (a) cualquier ingreso, alteración, eliminación o supresión de datos informáticos, (b) cualquier interferencia con el funcionamiento de un sistema de computación, con la intención dolosa o fraudulenta de procurar, sin permiso, un beneficio económico para sí o para un tercero.

Título 3 - Delitos relacionados con los contenidos

Artículo 9 - Delitos relacionados con la pornografía infantil 1. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delitos penales en virtud de sus leyes nacionales, cuando se lleven a cabo de manera intencional y sin permiso, las siguientes conductas: (a) producir pornografía infantil a los fines de

ser distribuida a través de un sistema informático; (b) ofrecer o poner a disposición pornografía infantil a través de un sistema informático; (c) distribuir o transmitir pornografía infantil a través de un sistema informático; (d) procurar pornografía infantil a través de un sistema informático para sí o para un tercero; (e) poseer pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informático. 2. A los fines del inciso 1 ut supra el término "pornografía infantil" incluirá todo material pornográfico que visualmente represente: (a) un menor que participe en una conducta sexual explícita; (b) una persona que parezca ser un menor de edad que participa en una conducta sexual explícita; (c) imágenes realistas que representen a un menor que participa en una conducta sexual explícita. 3. A los fines del inciso 2 ut supra, el término "menor" incluirá a todas las personas menores de 18 años. Sin embrago, una Parte puede requerir un límite de edad menor, el que no podrá ser inferior a 16 años. 4. Cada Parte puede reservarse el derecho de no aplicar, en todo o en parte, los incisos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Título 4 - Delitos relacionados con la violación de los derechos de autor y otros derechos relacionados

Artículo 10 - Delitos relacionados con la violación de los derechos de autor y otros delitos relacionados 1. Las Partes deberán adoptar las medidas legales y de otra índole que sean necesarias para establecer como delito penal en virtud de sus leyes nacionales, la violación de los derechos de autor, según lo establezcan las leyes de esa Parte conforme a las obligaciones que haya asumido en virtud de la Paris Act del 24 de julio de 1971 de la Convención de Berna para la protección de las Obras Literarias y

Artísticas, el Acuerdo sobre los aspectos relacionados con el Comercio de los Derechos de Propiedad Intelectual y el Tratado sobre los Derechos de Autor de la WIPO (Organización Mundial de la Propiedad Intelectual), con excepción de los derechos morales conferidos por dichas Convenciones cuando dichos actos sean cometidos con intención, [al menos] con carácter comercial y a través de un sistema informático. 2. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delito penal en virtud de sus leyes nacionales, la violación de derechos relacionados, según lo establecido en las leyes de esa Parte, conforme a las obligaciones que haya contraído en virtud de la Convención Internacional sobre la Protección de los Artistas, Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión celebrada en Roma (Convención de Roma), el Acuerdo sobre los aspectos relacionados con el Comercio de los Derechos de Propiedad Intelectual y los Tratados de la WIPO sobre Interpretaciones, Ejecuciones y Fonogramas, con excepción de los derechos morales conferidos por dichas Convenciones cuando dichos actos sean cometidos con intención, [al menos] con carácter comercial y a través de un sistema informático. 3. Una Parte puede reservarse el derecho de no imponer ninguna responsabilidad penal en virtud de los incisos 1 y 2 de este artículo en circunstancias limitadas, siempre que se cuente con otros recursos eficaces disponibles y que dicha reserva no derogue las obligaciones internacionales contraídas por la Parte establecidas en los instrumentos internacionales mencionados en los incisos 1 y 2 de este artículo.

Título 5 - Responsabilidad y sanciones auxiliares

Artículo 11 - La tentativa y ayudar o instigar 1. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delitos penales en virtud de sus leyes nacionales, cuando de manera intencional, se brinde ayuda o se instigue la comisión de cualquiera de los delitos establecidos conforme a los Artículos 2 a 10 del presente Convenio con la intención de cometer dichos delitos. 2. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer como delito penal en virtud de sus leyes nacionales, cuando se realice de manera intencional, toda tentativa de cometer cualquiera de los delitos establecidos conforme a los Artículos 3 a 5, 7 y 9 (1) a y 9 (1) c de este Convenio. 3. Cada Estado se puede reservar el derecho a no aplicar, en todo o en parte, el inciso 2 de este artículo.

Artículo 12 - Responsabilidad de las personas jurídicas 1. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para asegurar que una persona jurídica pueda ser considerada responsable de cometer un delito penal, conforme lo establecido por esta Convención, cometido para su beneficio por cualquier persona física, que actúe ya sea individualmente o como parte de un órgano de la persona jurídica, que tenga una posición importante dentro de la persona jurídica basándose en: (a) la facultad de representar a la persona jurídica; (b) la facultad para tomar decisiones en nombre de la persona jurídica; (c) la facultad para ejercer controles dentro de la persona jurídica. 2. Además de los casos ya contemplados en el inciso 1, cada Parte deberá tomar las medidas que estime necesarias para asegurar que una persona jurídica pueda ser considerada responsable cuando la falta de supervisión o de control por parte de una persona física como se menciona en el inciso 1 ha hecho posible la comisión de

un delito penal conforme a lo establecido por esta Convención para beneficio de esa persona jurídica por parte de una persona física que actuó bajo su autoridad. 3. Sujeta a los principios legales de la Parte, la responsabilidad de la persona jurídica puede ser penal, civil o administrativa. 4. La persona jurídica será plausible de dicha responsabilidad sin perjuicio de la responsabilidad penal que corresponda a las personas físicas que hayan cometido el delito.

Artículo 13 - Sanciones y medidas 1. Cada Parte deberá tomar las medidas necesarias para asegurar que los delitos penales establecidos de acuerdo con los Artículos 2 a 11 sean punibles mediante sanciones eficaces, proporcionadas y disuasivas, que incluyan la privación de la libertad. 2. Cada Parte deberá asegurar que las personas jurídicas consideradas responsables de acuerdo con el Artículo 12 estén sujetas a sanciones o medidas eficaces, proporcionadas y disuasivas, de carácter penal o no, incluyendo sanciones monetarias.

Sección 2 - Derecho procesal

Título 1 - Disposiciones comunes

Artículo 14 - Alcance de las disposiciones procesales 1. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para establecer las facultades y los procedimientos previstos en esta Sección a los efectos de realizar investigaciones o procedimientos penales específicos. 2. Salvo cuando esté establecido específicamente de otra manera en el Artículo 21, cada Parte deberá aplicar las facultades y los procedimientos mencionados en el inciso 1 a: (a) los delitos penales establecidos conforme a los artículos 2 a 11 de este Convenio; (b) otros delitos penales cometidos a

través de un sistema informático y (c) la recopilación de pruebas en formato electrónico de un delito penal. 2. Cada Parte puede reservarse el derecho de aplicar las medidas a que hace referencia el Artículo 20 sólo en el caso de delitos o categorías de delitos especificados en la reserva, siempre que el alcance de dichos delitos o categorías de delitos no sea más restringido que el alcance de los delitos a los que corresponde aplicar las medidas mencionadas en el Artículo 21. Cada Parte deberá considerar restringir una reserva tal para posibilitar la aplicación más amplia posible de la medida mencionada en el Artículo 20.

Artículo 15 - Condiciones y salvaguardas 1. Cada Parte deberá asegurar que el establecimiento, la implementación y la aplicación de las facultades y procedimientos previstos en esta Sección estén sujetos a las condiciones y salvaguardas previstas en virtud de sus leyes nacionales, las que deberán contemplar la adecuada protección de los derechos y las libertades humanas, incluyendo los derechos que surjan conforme a las obligaciones que haya contraído cada Parte en virtud del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales del Consejo de Europa de 1950, el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 1966 y otros documentos internacionales sobre derechos humanos pertinentes y deberán incorporar el principio de proporcionalidad. 2. Dichas condiciones y salvaguardas deberán, según corresponda en vista de la naturaleza de la facultad o procedimiento concerniente, incluir, entre otras cosas, la supervisión del poder judicial o de otro poder independiente, los motivos que justifiquen su aplicación y la limitación del alcance y la duración de dicha facultad o procedimiento. 3. En la medida en que sea coherente con el

interés público, en particular con la firme administración de justicia, cada Parte deberá considerar el impacto de las facultades y procedimientos a que hace referencia esta Sección con respecto a los derechos, las responsabilidades y los legítimos intereses de terceros.

Título 2 - Pronta preservación de los datos informáticos almacenados

Artículo 16 - Pronta preservación de los datos informáticos almacenados 1. Cada Parte deberá adoptar las medidas legales y de cualquier otra índole que sean necesarias para posibilitar que sus autoridades competentes ordenen u obtengan de manera similar la pronta preservación de datos informáticos específicos, incluyendo los datos de tráfico que hayan sido almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que los datos informáticos son particularmente vulnerables a su pérdida o modificación. 2. Cuando una Parte aplica el inciso 1 por medio de una orden a una persona para que preserve datos informáticos específicos almacenados que estuvieren en posesión de dicha persona o cuyo control ejerciera, la Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para obligar a dicha persona a preservar y mantener la integridad de dichos datos informáticos por el período de tiempo que sea necesario, hasta un máximo de 90 días, para posibilitar que las autoridades competentes procuren su revelación. Una Parte puede establecer que dicha orden sea renovable. 3. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para obligar a la persona encargada de custodiar los datos informáticos o a cualquier otra persona encargada de preservar los mismos a mantener la confidencialidad de dichos procedimientos por el período de tiempo que establezcan sus

leyes nacionales. 4. Las facultades y procedimientos a que hace referencia este artículo deberán estar sujetos a los Artículos 14 y 15.

Artículo 17 - Pronta preservación y revelación parcial de los datos de tráfico 1. Cada Parte deberá adoptar, con respecto a los datos de tráfico que han de preservarse en virtud del Artículo 16, las medidas legales y de otra índole que sean necesarias para: (a) asegurar que dicha pronta preservación de los datos de tráfico esté disponible sin tener en cuenta si uno o más proveedores de servicios estuvieron involucrados en la transmisión de esa comunicación y (b) asegurar la pronta revelación a la autoridad competente de la Parte, o a la persona designada por esa autoridad competente, de una cantidad suficiente de datos de tráfico para que la Parte pueda identificar los proveedores de servicio y el trayecto a través del cual se transmitió la comunicación. 2. Las facultades y los procedimientos a los que hace referencia este artículo deberán estar sujetos a los Artículos 14 y 15.

Título 3 - Orden de suministrar

Artículo 18 - Orden de suministrar 1. Las Partes deberán adoptar las medidas legales y de otra índole que sean necesarias para facultar a sus autoridades competentes a ordenar: (a) a una persona que se encuentre dentro de su territorio que suministre los datos informáticos específicos que dicha persona posea o controle, que estén almacenados en un sistema informático o en un medio de almacenamiento de datos informático; y (b) a un proveedor de servicios que ofrezca sus servicios en el territorio de la Parte a suministrar información sobre sus abonados en relación con los servicios que dicho proveedor de servicios posea o controle. 2. Las facultades y los procedimientos a que

hace referencia este artículo deberán estar sujetos a los Artículos 14 y 15. 3. A los fines del presente Artículo, "información sobre sus abonados" significa toda información, contenida en forma de datos informáticos o en cualquier otro formato, que posea el proveedor de servicios en relación con los abonados a sus servicios, además de la información relacionada con los datos de tráfico o de contenidos, por medio de la cual se pueda establecer: (a) el tipo de servicio de comunicaciones utilizado, las disposiciones técnicas tomadas y el período de servicio; (b) la identidad del abonado, el domicilio postal o geográfico, el número telefónico y otros números de acceso e información relacionada con la facturación y el pago que esté disponible conforme al contrato o acuerdo de servicio; (c) cualquier otra información que se pueda obtener relacionada con la instalación de equipos de comunicaciones disponible conforme al contrato o acuerdo de servicio.

Título 4 - Allanar el lugar donde se encuentren y secuestrar datos informáticos almacenados

Artículo 19 - Allanar el lugar donde se encuentren y secuestrar datos informáticos almacenados 1. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para facultar a sus autoridades competentes a allanar el lugar donde se encuentren o acceder de manera similar a: (a) un sistema informático o a una parte del mismo y a los datos informáticos almacenados en el mismo; y (b) un medio de almacenamiento de datos informático en el que pueda haber almacenados datos informáticos, que se encuentre dentro de su territorio. 2. Cada Parte deberán adoptar las medidas legales y de otra índole que sean necesarias para asegurar que en caso de que

sus autoridades deban allanar o acceder de manera similar a un sistema informático específico o a parte del mismo, conforme a lo establecido en el inciso 1 (a), y tengan motivos para creer que los datos buscados están almacenados en otro sistema informático o parte del mismo que se encuentre dentro de su territorio y que a esos se puede acceder legalmente desde el sistema inicial, dichas autoridades podrán extender con toda prontitud el allanamiento o la manera similar de acceder al otro sistema. 3. Cada Parte deberá adoptar las medidas legales y de otra índole que sean necesarias para facultar a sus autoridades competentes para secuestrar o conseguir de manera similar los datos informáticos a los que se ha tenido acceso conforme a los incisos 1 o 2. Estas medidas deberán incluir la facultad para: (a) secuestrar u obtener de manera similar un sistema informático o parte del mismo o un medio de almacenamiento de datos informático; (b) hacer y conservar una copia de dichos datos informáticos; (c) mantener la integridad de los datos informáticos almacenados relevantes; y (d) impedir el acceso a o eliminar los datos informáticos que se encuentren en el sistema informático al que se accedió. 4. Cada Parte deberá adoptar las medidas legales y de cualquier otra índole que sean necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que tenga conocimiento acerca del funcionamiento del sistema informático o de las medidas que se utilizan para proteger los datos informáticos contenidos en el mismo, a proveer, como es razonable, la información necesaria para posibilitar se tomen las medidas a que hacen referencia los incisos 1 y 2. 5. Las facultades y los procedimientos a los que hace referencia este artículo deberán estar sujetos a los Artículos 14 y 15.

Título 5 - Recopilación de datos informáticos en tiempo real

Artículo 20 - Recopilación de datos informáticos en tiempo real 1. Cada Parte deberá adoptar las medidas legales y de cualquier otra índole que sean necesarias para facultar a sus autoridades competentes a: (a) recopilar o registrar mediante la aplicación de medios técnicos dentro del territorio de dicha Parte y (b) obligar a un proveedor de servicios, conforme a su capacidad técnica existente, a: i. recopilar o registrar mediante la aplicación de medios técnicos dentro del territorio de esa Parte, o ii. cooperar y ayudar a las autoridades competentes en la recopilación o el registro de, datos de tráfico, en tiempo real, asociados con comunicaciones específicas transmitidas dentro de su territorio a través de un sistema informático. 2. En caso de que una de las Partes, debido a principios establecidos de su sistema legal nacional, no pueda adoptar las medidas a que hace referencia el inciso 1 (a), puede adoptar en cambio las medidas legales o de cualquier otra índole que sean necesarias para asegurar la recopilación o el registro en tiempo real de los datos de tráfico asociados con comunicaciones específicas efectuadas en su territorio a través de la utilización de medios técnicos en ese territorio. 3. Cada Parte deberá adoptar las medidas legales y de cualquier otra índole que sean necesarias para obligar a un proveedor de servicios a mantener la confidencialidad de los hechos y de cualquier otra información con respecto al ejercicio de cualquier facultad prevista en este Artículo. 4. Las facultades y los procedimientos a que hace referencia este artículo deberán estar sujetos a los Artículos 14 y 15.

Artículo 21 - Interceptación de datos de contenidos 1. Cada Parte deberá adoptar las medidas legales y de cualquier otra índole que sean necesarias, en relación con una serie de delitos mayores a ser determinados por las leyes nacionales, para facultar a sus

autoridades competentes a: (a) recopilar o registrar mediante la aplicación de medios técnicos dentro del territorio de la Parte y (b) obligar a un proveedor de servicios, conforme a su capacidad técnica existente, a: i. recopilar o registrar mediante la aplicación de medios técnicos dentro del territorio de esa Parte, o ii. cooperar y ayudar a las autoridades competentes en la recopilación o el registro de los datos de contenidos, en tiempo real, de comunicaciones específicas efectuadas en su territorio transmitidas por medio de un sistema informático. 2. En caso de que una de las Partes, debido a principios establecidos de su sistema legal nacional, no pueda adoptar las medidas a que hace referencia el inciso 1 (a), puede adoptar en cambio las medidas legales o de cualquier otra índole que sean necesarias para asegurar la recopilación o el registro en tiempo real de los datos de contenidos asociados con comunicaciones específicas efectuadas en su territorio a través de la utilización de medios técnicos en ese territorio. 3. Cada Parte deberá adoptar las medidas legales y de cualquier otra índole que sean necesarias para obligar a un proveedor de servicios a mantener la confidencialidad de los hechos y de cualquier otra información con respecto al ejercicio de cualquier facultad prevista en este Artículo. 4. Las facultades y los procedimientos a que hace referencia este artículo deberán estar sujetos a los Artículos 14 y 15.

Sección 3 - Jurisdicción

Artículo 22 - Jurisdicción

1. Cada Parte deberá adoptar las medidas legales y de cualquier otra índole que sean necesarias para establecer la jurisdicción respecto de cualquier delito establecido conforme con los Artículos 2 a 11 de este Convenio, cuando el delito es cometido: (a)

dentro de su territorio; o (b) a bordo de un barco de su bandera; o (c) a bordo de una aeronave registrada en virtud de las leyes de esa Parte; o (d) por uno de sus ciudadanos, si el delito es punible en virtud del derecho penal que rige en el lugar donde se cometió o si el delito es cometido fuera de la jurisdicción territorial de cualquier Estado.

2. Cada Estado puede reservarse el derecho de no aplicar o de aplicar sólo en casos o condiciones específicos las normas referentes a la jurisdicción establecidas en los incisos 1 (b) a 1(d) del presente artículo o cualquier parte del mismo.

3. Cada Parte deberá adoptar las medidas que sean necesarias para establecer la jurisdicción con respecto a los delitos a que hace referencia el Artículo 24, inciso (1) de este Convenio, en aquellos casos en que el presunto acusado se encuentre dentro de su territorio y no lo extradite a otra Parte, únicamente en base a su nacionalidad, después de un pedido de extradición.

4. Este Convenio no excluye ninguna jurisdicción penal ejercida conforme a las leyes nacionales.

5. Cuando más de una Parte reclame tener jurisdicción sobre un presunto delito establecido de acuerdo a este Convenio, las Partes involucradas deberán, cuando fuere apropiado, efectuar una consulta con miras a determinar la jurisdicción más apropiada donde llevar a cabo el procedimiento penal.

Capítulo III - Cooperación internacional

Sección 1 - Principios generales

Título 1 - Principios generales relacionados con la cooperación internacional

Artículo 23 - Principios generales relacionados con la cooperación internacional Las Partes deberán cooperar entre sí, conforme con las disposiciones de este capítulo y mediante la aplicación de los documentos internacionales pertinentes sobre cooperación internacional en materia de asuntos penales, los acuerdos celebrados en base a una legislación uniforme y recíproca y las leyes nacionales en el sentido más amplio posible a los efectos de realizar las investigaciones o los procedimientos concernientes a los delitos penales relacionados con el empleo de sistemas y datos informáticos o para la recopilación de pruebas en formato electrónico de un delito penal. Título 2 - Principios relacionados con la extradición

Artículo 24 - Extradición

1. (a) Este artículo se aplica a la extradición entre Partes por los delitos penales establecidos conforme a los Artículos 2 a 11 de este Convenio, siempre que sean punibles en virtud de las leyes de ambas Partes involucradas mediante la privación de la libertad por un período máximo de al menos un año, o mediante una pena más severa (b) Cuando se deba aplicar una pena mínima diferente en virtud de un acuerdo convenido en base a una legislación uniforme o recíproca o a un tratado de extradición, incluyendo el Convenio Europeo sobre Extradición (ETS N° 24), aplicable entre dos o más partes, corresponderá aplicar la pena mínima provista en virtud de dicho acuerdo o tratado.

2. Los delitos penales descriptos en el inciso 1 de este Artículo serán considerados para ser incluidos como delitos extraditables en virtud de cualquier tratado de extradición existente entre las Partes. Las Partes se comprometen a incluir dichos delitos como delitos extraditables en todo tratado de extradición a celebrarse entre ellas.

3. Si una Parte que condiciona la extradición a la existencia de un tratado recibe un pedido de extradición de otra Parte con la que no tiene un tratado de extradición, puede considerar este Convenio como la base legal para conceder la extradición con respecto a cualquier delito penal al que haga referencia el inciso 1 de este Artículo.

4. Las Partes que no condicionan la extradición a la existencia de un tratado deberán reconocer los delitos penales a los que hace referencia el inciso 1 de este Artículo como delitos extraditables entre las mismas.

5. La extradición deberá estar sujeta a las condiciones establecidas por las leyes de la Parte a la que se le requiere la misma o a los tratados de extradición aplicables, incluyendo los motivos en base a los cuales la Parte a la que se le solicita la extradición puede denegarla.

6. Si la extradición por uno de los delitos penales a los que hace referencia el inciso 1 de este Artículo es rechazada sólo debido a la nacionalidad de la persona buscada, o porque la Parte a la que se le solicita la misma considera que tiene jurisdicción sobre el delito, esta Parte deberá someter el caso, a pedido de la Parte solicitante, ante las autoridades competentes a fin de que lleven a cabo el procedimiento penal y deberá informar el resultado final a la Parte solicitante a su debido tiempo. Esas autoridades deberán dictar sentencia y conducir sus investigaciones y procedimientos en la misma forma que con cualquier otro delito de naturaleza comparable en virtud de las leyes de esa Parte.

7. (a) Cada parte deberá, al momento de firmar o cuando presente su instrumento de ratificación, aceptación, aprobación o adhesión, comunicar al Secretario General del Consejo de Europa el nombre y los domicilios de cada autoridad responsable de solicitar

o recibir un pedido de extradición o de arresto provisional en ausencia de un tratado. (b) El Secretario General del Consejo de Europa deberá establecer y llevar un registro actualizado de las autoridades designadas a tal efecto por las Partes. Cada Parte deberá asegurar que los detalles incluidos en el registro sean correctos en todo momento.

Título 3 - Principios generales relacionados con la asistencia mutua

Artículo 25 - Principios generales relacionados con la asistencia mutua

1. Las Partes deberán proporcionarse asistencia mutua en el sentido más amplio posible a fin de realizar las investigaciones o procedimientos concernientes a los delitos penales relacionados con el empleo de sistemas y datos informáticos, o para la recopilación de pruebas en formato electrónico en relación con un delito penal.

2. Cada Parte deberá adoptar también las medidas legales y de cualquier otra índole que sean necesarias para cumplir con las obligaciones establecidas en los Artículos 27 a 35.

3. Cada Parte, en circunstancias urgentes, puede pedir la asistencia mutua o efectuar las comunicaciones relacionadas con dicho pedido mediante medios de comunicaciones rápidos, incluyendo el fax o el correo electrónico, en la medida en que dichos medios proporcionen niveles apropiados de seguridad y autenticación (incluyendo el uso de la encripción, de ser necesaria), quedando pendiente una confirmación formal, de ser requerida por la Parte a la que se le efectúa el pedido de asistencia mutua. La Parte a la que se le efectúa el pedido deberá aceptar y responder al mismo mediante dichos medios rápidos de comunicaciones.

4. Excepto cuando un Artículo de este Capítulo establezca específicamente lo contrario, la asistencia mutua deberá estar sujeta a las condiciones establecidas en las leyes de la Parte a la que se le solicita la asistencia mutua o a la aplicación de tratados de asistencia mutua, incluyendo los motivos en base a los cuales la Parte a la que se le requiere la asistencia mutua puede denegar la cooperación. La Parte a la que se le efectúa el pedido de asistencia no deberá ejercer el derecho a denegar la asistencia mutua basándose exclusivamente en que el pedido está relacionado con un delito que ella considera un delito fiscal.

5. Cuando, conforme con las disposiciones de este capítulo, la Parte a la que se le efectúa el pedido de asistencia mutua puede condicionar la asistencia mutua a la existencia del requerimiento de que el delito sea considerado como tal en ambas jurisdicciones (doble criminalidad), esa condición se considerará cumplida, sin tener en cuenta si sus leyes ubican el delito dentro de la misma categoría de delitos o lo denominan con la misma terminología que la Parte solicitante, si la conducta implícita en el delito por el cual se solicita la asistencia constituye un delito penal en virtud de sus leyes.

Artículo 26 - Información espontánea 1. Una parte puede, dentro de los límites de sus leyes nacionales, sin previa solicitud, enviar a otra Parte información obtenida dentro del marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte que la recibe para iniciar o realizar investigaciones o procedimientos concernientes con los delitos penales establecidos conforme a este Convenio o que pudieran conducir a un pedido de cooperación efectuado por dicha Parte

en virtud del presente capítulo. 2. Antes de proveer dicha información, la Parte que la provee puede solicitar que sea mantenida en forma confidencial o que sea utilizada sujeta a ciertas condiciones. Si la Parte que la recibe no puede cumplir con dicho requerimiento, deberá notificar a la Parte que provee la información, la que luego determinará si la información será no obstante suministrada. Si la parte que la recibe acepta la información sujeta a ciertas condiciones, deberá ajustarse a las mismas.

Título 4 - Procedimientos que corresponde aplicar a los pedidos de asistencia mutua ante la ausencia de acuerdos internacionales pertinentes.

Artículo 27 - Procedimientos que corresponde aplicar a los pedidos de asistencia mutua ante la ausencia de acuerdos internacionales pertinentes

1. Cuando no exista un tratado o acuerdo de asistencia mutua en base a una legislación uniforme o recíproca vigente entre las Partes que solicitan y a las que les solicitan un pedido de asistencia mutua, corresponde aplicar las disposiciones de los incisos 2 al 10 de este artículo. Las disposiciones de este artículo no se aplicarán cuando dichos tratados, acuerdos o legislación estén disponibles, salvo que las Partes involucradas acuerden aplicar parte o todas las disposiciones restantes de este Artículo en lugar de los mismos.

2. (a) Cada Parte deberá designar una autoridad o autoridades centrales que serán responsables de efectuar y responder los pedidos de asistencia mutua, la ejecución de dichos pedidos o la transmisión de los mismos a las autoridades competentes para llevarlos a cabo. (b) Las autoridades centrales deberán comunicarse entre sí de manera directa. (c) Cada Parte deberá, cuando firme o cuando presente su instrumento de

ratificación, aceptación, aprobación o adhesión comunicar al Secretario General del Consejo de Europa el nombre y los domicilios de las autoridades designadas en cumplimiento de este inciso. (d) El Secretario General del Consejo de Europa deberá establecer y llevar un registro actualizado de las Autoridades centrales designadas a tal efecto por las Partes. Cada Parte deberá asegurar que los detalles incluidos en el registro sean correctos en todo momento.

3. Los pedidos de asistencia mutua en virtud de este Artículo deberán ser llevados a cabo conforme con los procedimientos especificados por la Parte que los solicita excepto cuando sean incompatibles con las leyes de la Parte a la que se los solicitan.

4. La Parte a la que le solicitan un pedido de asistencia mutua puede, además de los motivos de denegación disponibles en Virtud del Artículo 25, inciso (4), denegar la asistencia si: (a) el pedido es concerniente a un delito que la Parte a la que se le efectuó el pedido considera un delito político o un delito relacionado con un delito político; o (b) considera que la ejecución del pedido es probable que perjudique su soberanía, la seguridad, el orden público u otros intereses esenciales.

5. La Parte a la que se le efectuó el pedido puede posponer el tomar medidas en relación a un pedido si dichas medidas pudieran perjudicar investigaciones o procedimientos penales que estén realizando sus autoridades.

6. Antes de denegar o posponer la asistencia, la Parte a la que se le efectúo el pedido de asistencia deberá, cuando fuere apropiado después de consultar con la parte que efectúa el pedido, considerar si el pedido puede ser concedido en forma parcial o sujeto a determinadas condiciones, según lo considere necesario.

7. La Parte a la que se le efectúa el pedido deberá informar a la brevedad a la Parte solicitante el resultado de la ejecución del pedido de asistencia. Si el pedido es denegado o pospuesto, se deberán explicar las razones para dicha denegación o postergación. La Parte a la que se le solicita el pedido deberá efectuar también a la Parte solicitante las razones por las cuáles es imposible la ejecución del pedido o por las cuáles es probable que el cumplimiento del mismo se demore significativamente.

8. La Parte solicitante puede requerir que la otra Parte mantenga la confidencialidad de forma y de fondo de cualquier pedido efectuado en virtud de este Capítulo excepto en la medida de lo necesario para llevar a cabo el pedido. Si la Parte a la que se le solicita el pedido no puede cumplir con el requisito de confidencialidad, deberá informar a la brevedad a la Parte solicitante, la que luego determinará si el pedido será no obstante llevado a cabo.

9 .(a) En caso de urgencia, los pedidos de asistencia mutua o las comunicaciones relacionadas con los mismos, podrán ser realizados directamente por las autoridades judiciales de la Parte que efectúa el pedido a las autoridades de la otra Parte. En esos casos se deberá enviar una copia simultáneamente a la autoridad central de la Parte a la que se le efectúa el pedido por intermedio de la autoridad central de la Parte solicitante. (b) Todo pedido o comunicación en virtud de este inciso puede ser efectuado a través de la INTERPOL (International Criminal Police Organization). (c) Cuando se efectúa un pedido conforme al inciso (a) y la autoridad no es competente para encargarse del pedido, deberá referir el mismo a la autoridad nacional competente e informar lo hecho directamente a la Parte solicitante. (d) Los pedidos o comunicaciones efectuados en

virtud de este inciso que no impliquen tomar medidas coercitivas pueden ser transmitidos directamente por las autoridades competentes de la Parte solicitante a las autoridades competentes de la otra Parte. (e) Cada Parte puede, al momento de firmar o al presentar su instrumento de ratificación, aceptación, aprobación o adhesión informar al Secretario General del Consejo de Europa que, por razones de eficiencia, los pedidos efectuados en virtud de este inciso han de ser dirigidos a su autoridad central.

Artículo 28 - Confidencialidad y limitaciones de uso

1. Cuando no exista un tratado o acuerdo de asistencia mutua en base a una legislación uniforme o recíproca vigente entre las Partes intervinientes en un pedido de asistencia mutua, corresponde aplicar las disposiciones de este artículo. Las disposiciones de este artículo no se deberán aplicar cuando dichos tratados, acuerdos o legislación estén disponibles salvo que las Partes involucradas acuerden aplicar parte o todos los artículos restantes en lugar de los mismos.

2. La Parte a la que se le solicitó la información puede suministrar información o material en respuesta a un pedido que depende de la condición de que: a) sea mantenida en forma confidencial cuando el pedido de asistencia mutua no pudiera ser cumplido ante la ausencia de dicha condición, o b) no sea utilizada para otras investigaciones o procedimientos distintos a los establecidos en el pedido.

3. Si la Parte que efectúa el pedido no puede cumplir con la condición a que hace referencia el inciso 2, deberá informar a la brevedad a la otra Parte, la que luego determinará si no obstante se ha de proveer la información. Cuando la parte que efectúa el pedido acepta la condición, deberá cumplirla con carácter obligatorio.

4. Toda Parte que suministre información o materiales sujetos a la condición a que hace referencia el inciso 2 puede requerir que la otra Parte explique, en relación con esa condición, el uso que ha hecho de dicha información o material.

Sección 2 - Disposiciones específicas

Título 1 - Asistencia mutua con respecto a medidas provisionales

Artículo 29 - Pronta preservación de datos informáticos almacenados

1. Una Parte puede solicitar a otra Parte que ordene u obtenga la pronta preservación de los datos almacenados por medio de un sistema informático, que esté ubicado dentro del territorio de la mencionada parte y respecto de los cuales la parte solicitante pretende presentar un pedido de asistencia mutua para poder allanar el lugar donde se encuentren o acceder al mismo de manera similar, secuestrar o procurar de manera similar o revelar los datos.

2. Un pedido de preservación efectuado en virtud del inciso 1 deberá especificar: (a) la autoridad que requiere la preservación; (b) el delito por el cual se lleva a cabo la investigación o el procedimiento penal y una breve síntesis de los hechos relacionados; (c) los datos informáticos almacenados a ser preservados y su relación con el delito; (d) toda información disponible para identificar a la persona encargada de custodiar los datos informáticos almacenados o la ubicación del sistema informático; (e) la necesidad de la preservación; y (f) que la Parte tiene intención de presentar un pedido de asistencia mutua para efectuar un allanamiento o acceder de manera similar, secuestrar o procurar de manera similar, o revelar los datos informáticos almacenados.

3. Ante la recepción de un pedido de asistencia mutua de otra de las Partes, la Parte a la que se le efectuó el pedido deberá tomar todas las medidas apropiadas para preservar rápidamente los datos especificados conforme con sus leyes nacionales. A los fines de responder a un pedido, no se requerirá como condición que el delito sea considerado como tal por ambas partes (doble criminalidad) como condición para efectuar dicha preservación.

4. Una parte que requiere la doble criminalidad como condición para responder a un pedido de asistencia mutua para efectuar un allanamiento o acceder de manera similar, secuestrar o procurar de manera similar o revelar los datos puede, con respecto a otros delitos que no sean los establecidos conforme con los artículos 2 a 11 de este Convenio, reservarse el derecho de denegar el pedido de preservación en virtud de este Artículo en aquellos casos en que tenga motivos para creer que al momento de revelar los datos la condición de doble criminalidad no puede cumplirse.

5. Además, un pedido de preservación puede ser denegado sólo en caso de que: (a) el pedido sea concerniente a un delito que la Parte a la que se le solicita el pedido considere un delito político o un delito relacionado con un delito político; o (b) la Parte a la que se le solicita el pedido considera que el cumplimiento del pedido es probable que perjudique su soberanía, la seguridad, el orden público u otros intereses esenciales.

6. Cuando la Parte a la que se le efectuó el pedido considere que la preservación no garantizará la disponibilidad futura de los datos o que amenazará la confidencialidad de los mismos, o que de lo contrario perjudicará la investigación de la Parte solicitante,

deberá informarlo a la brevedad a la Parte solicitante, la que determinará luego si se deberá no obstante cumplir con el pedido.

7. Toda preservación efectuada en respuesta al pedido a que hace referencia el inciso 1 deberá realizarse por un período no inferior a 60 días con el fin de posibilitar que la Parte solicitante presente un pedido de allanamiento o para acceder de manera similar, secuestrar o procurar de manera similar o revelar los datos. Una vez recibido dicho pedido, los datos deberán continuar siendo preservados hasta que se tome una decisión en relación con ese pedido.

Artículo 30 - Pronta revelación de los datos de tráfico preservados 1. Cuando, mientras se lleva a cabo un pedido efectuado en virtud del artículo 29 para preservar datos de tráfico concernientes a una comunicación específica, la parte a la que se le efectuó el pedido descubre que un proveedor de servicios de otro Estado estuvo involucrado en la transmisión de la comunicación, la Parte a la que se le efectuó el pedido deberá revelar con la mayor rapidez posible a la Parte solicitante una cantidad suficiente de datos de tráfico con el fin de identificar a ese proveedor de servicios y el trayecto a través del cual se transmitió la comunicación. 2. La revelación de los datos de tráfico en virtud del inciso 1 sólo se podrá retener si: (a) el pedido es concerniente a un delito que la Parte a la que se le efectuó el pedido considera un delito político o un delito relacionado con un delito político; o (b) la Parte a la que se le efectuó el pedido considera que la ejecución del pedido es probable que perjudique su soberanía, la seguridad, el orden público u otros intereses esenciales.

Título 2 - Asistencia mutua con respecto a las facultades de investigación

Artículo 31 - Asistencia mutua con respecto a acceder a datos informáticos almacenados 1. Una Parte puede solicitar a otra que efectúe un allanamiento o acceda de manera similar, secuestre o que procure de manera similar y que revele datos almacenados por medio de un sistema informático ubicado dentro del territorio de la Parte a la que se le efectúa el pedido, incluyendo datos que han sido preservados conforme al artículo 29. 2. La Parte a la que se le efectuó un pedido deberá responder al mismo mediante la aplicación de los instrumentos internacionales, acuerdos y leyes a que hace referencia el artículo 23 y conforme con otras disposiciones pertinentes de este capítulo. 3. El pedido deberá ser respondido a la brevedad cuando: (a) existan motivos para creer que los datos pertinentes son particularmente vulnerables a sufrir alguna modificación o la pérdida de los mismos; o (b) los instrumentos, los acuerdos y las leyes a que hace referencia el inciso 2 establecen una cooperación inmediata.

Artículo 32 - Acceso transfronterizo a datos almacenados con consentimiento o cuando estén disponibles al público Una Parte puede, sin necesidad de obtener autorización de otra Parte: (a) acceder a datos informáticos almacenados que estén disponibles para el público (fuente abierta), sin importar la ubicación geográfica de los mismos; o (b) acceder o recibir, a través de un sistema informático en su territorio, datos informáticos almacenados ubicados en otra Parte, si la Parte obtiene el consentimiento legal y voluntario de la persona que posee las facultades legales para revelar los datos a la Parte a través de ese sistema informático.

Artículo 33 - Asistencia mutua con respecto a la recopilación de datos de tráfico en tiempo real

1. Las partes deberán proveerse asistencia mutua con respecto a la recopilación de datos de tráfico en tiempo real asociados con comunicaciones específicas efectuadas en su territorio transmitidas por medio de un sistema informático. Sujeta al inciso 2, la asistencia deberá regirse por las condiciones y los procedimientos establecidos en virtud de las leyes nacionales.

2. Cada Parte deberá proveer dicha asistencia al menos con respecto a los delitos penales para los cuales la recopilación de los datos de tráfico en tiempo real estaría disponible en un caso nacional de similares características.

Artículo 34 - Asistencia mutua con respecto a la interceptación de los datos de contenido Las Partes deberán proveerse asistencia mutua con respecto a la recopilación o al registro en tiempo real de los datos de contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que las leyes nacionales y los tratados aplicables lo permitan.

Título 3 - Red 24/7

Artículo 35 - Red 24/7

1. Cada Parte deberá designar un punto de contacto que esté disponible las 24 horas, los 7 días de la semana con el fin de asegurar la provisión de ayuda inmediata con el fin de realizar las investigaciones o los procedimientos concernientes a los delitos penales relacionados con sistemas y datos informáticos o para la recopilación de pruebas en formato electrónico de un delito penal. Dicha asistencia deberá incluir facilitar o, si las leyes nacionales y la práctica lo permiten, directamente llevar a cabo: (a) la provisión de

asistencia técnica; (b) la preservación de los datos conforme a los artículos 29 y 30; y (c) la recopilación de pruebas, brindar información legal y ubicar a los sospechosos.

2. (a) El punto de contacto de una Parte deberá tener la capacidad de efectuar comunicaciones con el punto de contacto de la otra Parte en forma inmediata. (b) Si el punto de contacto designado por una Parte no es parte de la autoridad o autoridades responsables de esa Parte para la asistencia mutua o la extradición, el punto de contacto deberá garantizar que puede coordinar su accionar con dicha autoridad o autoridades en forma inmediata.

3. Cada Parte deberá asegurar que cuenta con personal capacitado y equipado con el fin de facilitar la operación de la red.

Capítulo IV - Disposiciones finales

Artículo 36 - Firma y entrada en vigencia

1. Este Convenio estará abierto para su firma por los Estados miembro del Consejo de Europa y por los Estados no miembro que han participado en su elaboración.

2. Este Convenio está sujeto a su ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación serán depositados ante el Secretario General del Consejo de Europa.

3. Este Convenio entrará en vigencia en el primer día del mes que siga al vencimiento del período de tres meses contados a partir de la fecha en que cinco Estados, incluyendo al menos tres Estados miembro, del Consejo de Europa, hayan manifestado su

consentimiento a obligarse en virtud de este Convenio conforme con las disposiciones de los incisos 1 y 2.

Artículo 37 - Adhesión al presente Convenio Después de la entrada en vigencia del presente Convenio, el Comité de Ministros del Consejo de Europa, después de consultar con los Estados Firmantes del Convenio y con el consentimiento unánime de los mismos, puede invitar a cualquier Estado que no sea miembro del Consejo y que no haya participado en la elaboración del Convenio a adherirse al mismo. La decisión deberá ser tomada por la mayoría establecida en el artículo 20 (d) del estatuto del Consejo de Europa y por el voto unánime de los representantes de los Estados Firmantes con derecho a participar en el Comité de Ministros.

2. Con respecto a cualquier Estado que se adhiera a este Convenio en virtud del inciso 1 ut supra, el Convenio entrará en vigencia en el primer día del mes siguiente al vencimiento de un período de tres meses contados a partir de la fecha en que se presente el instrumento de adhesión ante el Secretario General del Consejo de Europa.

Artículo 38 - Aplicación territorial

1. Cualquier Estado puede, al momento de firmar o de presentar su instrumento de ratificación, aceptación, aprobación o adhesión, especificar el territorio o territorios a los que corresponde aplicar el Convenio.

2. Cualquiera de las Partes puede, en una fecha posterior, por medio de una declaración dirigida al Secretario General del Consejo de Europa, extender la aplicación de este Convenio a cualquier otro territorio especificado en la declaración. Con respecto a dicho

territorio el Convenio entrará en vigencia en el primer día del mes siguiente al vencimiento de un período de tres meses contados a partir de la fecha de recepción de la declaración por parte del Secretario General.

3. Toda declaración efectuada en virtud de los dos incisos precedentes puede, con respecto de cualquier territorio especificado en dicha declaración, ser dejada sin efecto mediante una notificación dirigida al Secretario General del Consejo de Europa. La misma entrará en vigencia en el primer día del mes siguiente al vencimiento de un período de tres meses contados a partir de la fecha de recepción de dicha notificación por parte del Secretario General.

Artículo 39 - Efectos del Convenio

1. La finalidad del presente Convenio es complementar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluyendo las disposiciones de: - el Convenio Europeo sobre Extradición abierto para su firma en Estrasburgo el 13 de diciembre de 1957 (ETS N° 24); - el Convenio Europeo sobre Asistencia Mutua en Asuntos Penales abierto para su firma en Estrasburgo el 20 de abril de 1959 (ETS N° 30); - el Protocolo Adicional al Convenio Europeo sobre Asistencia Mutua en Asuntos Penales abierto para su firma en Estrasburgo el 17 de marzo de 1978 (ETS N° 99).

2. Si dos o más Partes ya han celebrado un acuerdo o tratado sobre las cuestiones a que hace referencia este Convenio o han establecido de algún otro modo sus relaciones con respecto a dichas cuestiones, o deberían hacerlo en un futuro, deberán también estar facultadas para aplicar dicho acuerdo o tratado o para regular dichas relaciones en consecuencia. Sin embargo, cuando las Partes establecen sus relaciones respecto de las

cuestiones consideradas en el presente Convenio de otro modo que no sea el incluido en el mismo, deberán hacerlo de manera tal que no contradiga los objetivos y principios del Convenio.

3. Ningún contenido del presente Convenio deberá afectar otros derechos, restricciones, obligaciones y responsabilidades de la Parte.

Artículo 40 - Declaraciones Mediante una notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado puede, al momento de firmar o de presentar su instrumento de ratificación, aceptación, aprobación o adhesión declarar que se reserva para sí la posibilidad de requerir elementos adicionales como lo establecen el Artículo 2, el Artículo 3, el Artículo 6, inciso 1 (b), el Artículo 7, el Artículo 9, inciso 3 y en el Artículo 27, inciso 9 (e).

Artículo 41 - Cláusula federal Un Estado federal puede notificar al Secretario General que este asumirá las obligaciones que surgen en virtud de este Convenio de manera coherente con los principios fundamentales que rigen la relación entre su gobierno central y los Estados que lo componen u otras entidades territoriales similares. Al efectuar una declaración, un Estado federal deberá proveer una declaración con respecto a la naturaleza de su sistema federal y al efecto que su carácter federal pueda tener en la implementación del Convenio.]

Artículo 42 - Reservas Mediante una notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado puede, al momento de firmar o cuando presente su instrumento de ratificación, aceptación, aprobación o adhesión declarar que se reserva para sí las reservas establecidas en el Artículo 4, inciso 2, el Artículo 6, inciso

3, el Artículo 9, inciso 4, el Artículo 10, inciso 3, el Artículo 11, inciso 3, el Artículo 14, inciso 3, el Artículo 22, inciso 2, el Artículo 29, inciso 4. No pueden efectuarse otras reservas.

Artículo 43 - Estado y remoción de las reservas

1. Una Parte que ha hecho una reserva conforme al Artículo 42 puede remover en todo o en parte la misma por medio de una notificación dirigida al Secretario General. Dicha remoción entrará en vigencia a partir de la fecha de recepción de dicha notificación por parte del Secretario General. Si la notificación establece que la remoción de la reserva ha de entrar en vigencia en la fecha especificada en la misma, y dicha fecha es posterior a la fecha en que la notificación es recibida por parte del Secretario General, la remoción entrará en vigencia en dicha fecha posterior.

2. Una Parte que ha hecho una reserva conforme al Artículo 32 deberá remover dicha reserva, en todo o en parte, ni bien las circunstancias lo permitan.

3. El Secretario General puede periódicamente consultar a las partes que han efectuado una o más reservas conforme al Artículo 42 con respecto a las posibilidades de remover dichas reservas.

Artículo 44 - Modificaciones

1. Las modificaciones a este Convenio pueden ser propuestas por cualquiera de las partes y deberán ser comunicadas por el Secretario General del Consejo de Europa a los Estados miembro del Consejo de Europa, a los Estados que no sean miembro pero que han participado en la elaboración de este Convenio, así como también a cualquier Estado

que se haya adherido, o que haya sido invitado a adherirse a este convenio conforme a las disposiciones del artículo 37.

2. Toda enmienda propuesta por una parte deberá ser comunicada al Comité Europeo para los Problemas de la Delincuencia (CDPC), el que presentará su opinión con respecto a la modificación propuesta ante el Comité de Ministros.

3. El Comité de Ministros deberá considerar la modificación propuesta y la opinión presentada por el Comité Europeo para los Problemas de la Delincuencia (CDPC) y después de consultar con las Partes intervinientes en este Convenio que no sean Estados miembro, puede adoptar la modificación.

4. El texto de cualquier modificación adoptada por el Comité de Ministros conforme con el inciso 3 del presente artículo deberá ser enviado a las Partes para su aceptación.

5. Cualquier modificación adoptada conforme al inciso 3 del presente artículo entrará en vigencia en el trigésimo día después de que todas las partes hayan informado al Secretario General respecto de su aceptación de la misma.

Artículo 45 - Resolución de controversias

1. Se deberá informar al Comité Europeo para los Problemas de la Delincuencia (CDPC) con respecto a la interpretación y aplicación del presente Convenio.

2. En caso de controversias entre las Partes con respecto a la interpretación o a la aplicación del presente Convenio, las mismas buscarán una resolución de la controversia a través de la negociación o de cualquier otro medio pacífico de su elección, incluyendo el sometimiento de la controversia al Comité Europeo para los Problemas de la

Delincuencia (CDPC), a un tribunal arbitral cuyas decisiones serán obligatorias para las partes, o al Tribunal Internacional de Justicia, según lo acuerden las partes involucradas.

Artículo 46 - Consultas de las Partes Las Partes deberán, de ser apropiado, efectuar consultas periódicas con vistas a facilitar: (a) el uso y la implementación efectiva de este Convenio; (b) el intercambio de información sobre importantes desarrollos legales, políticos y tecnológicos relacionados con los delitos informáticos y la recopilación de pruebas en formato electrónico; (c) la consideración de un posible suplemento o modificación del presente Convenio.

2. Se deberá informar periódicamente al Comité Europeo para los Problemas de la Delincuencia (CDPC) con respecto al resultado de las consultas a que hace referencia el inciso 1.

3. El Comité Europeo para los Problemas de la Delincuencia (CDPC) deberá, de ser apropiado, facilitar las consultas a que hace referencia el inciso 1 y tomar las medidas necesarias para asistir a las Partes en sus esfuerzos para complementar o modificar el Convenio. Pasados tres años a partir de que el presente Convenio entre en vigencia, el Comité Europeo para los Problemas de la Delincuencia (CDPC) deberá, en cooperación con las Partes, efectuar una revisión de todas las disposiciones del Convenio y, de ser necesario, recomendar las modificaciones apropiadas.

4. Salvo cuando los asuma el Consejo de Europa, los gastos incurridos en cumplimiento de las disposiciones del inciso 1 serán afrontados por las Partes en la manera que las mismas determinen.

5. Las Partes serán asistidas por la Secretaría del Consejo de Europa en el desempeño de sus funciones conforme al presente Artículo.

Artículo 47 - Terminación

1. Cualquiera de las Partes puede, en cualquier momento, dar por terminado este Convenio por medio de una notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha terminación entrará en vigencia en el primer día del mes siguiente al vencimiento del período de tres meses contado a partir de la fecha de recepción de la notificación por parte del Secretario General.

Artículo 48 - Notificación El Secretario General del Consejo de Europa deberá notificar a los Estados miembro del Consejo de Europa, a los Estados que no sean miembro pero que han participado en la elaboración del presente Convenio, así como también a cualquier estado que se haya adherido, o que haya sido invitado a adherirse al presente Convenio acerca de: (a) toda firma; (b) la presentación de un instrumento de ratificación, aceptación, aprobación o adhesión; (c) la fecha de entrada en vigencia de este Convenio conforme con los Artículos 36 y 37; (d) toda declaración efectuada en virtud de los Artículos 40 [y 41] o de las reservas hechas conforme al Artículo 42. (e) Todo otro acto, notificación, o comunicación relacionada con este Convenio.

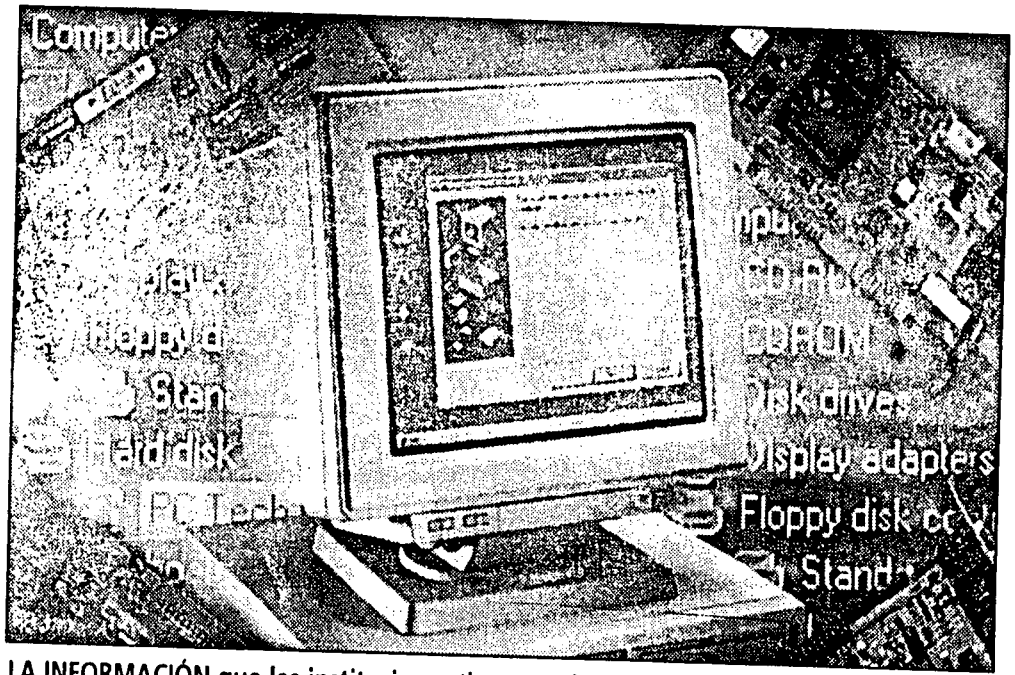
En fe de lo cual los abajo firmantes, debidamente autorizados a tal efecto, han firmado el presente Convenio.

Celebrado en Estrasburgo, ... de 2001, en idioma inglés y francés, considerándose ambos textos igualmente auténticos, en una única copia la que será depositada en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa deberá entregar copias certificadas a cada uno de los Estados miembro del Consejo de Europa, a los Estados que no sean miembro pero que han participado en la elaboración del presente Convenio y a todo Estado invitado a adherirse al mismo.

ANEXO 2

BOLETÍN DE PRENSA
MUNICIPIO DE QUITO

Pagina WEB del Muncipio destruida por 'crackers'



LA INFORMACIÓN que las instituciones tienen en la gran red mundial no están a salvo de atentados. Ni siquiera los programas internos son invulnerables a los ataques de los "cibervándalos".

EL MUNICIPIO de Quito denunció que la página web (www.quito.gov.ec) fue atacada la noche del 5 y 6 del presente mes por personas desconocidas pero hábiles en informática.

Al parecer, ciberpiratas "crackers" (especialistas en romper seguros de la red y destruir toda la información de un programa) lograron ingresar en el sistema y acabar con toda la información allí colocada durante mucho tiempo.

En lugar de la página web aparecía un pez. Inmediatamente, los técnicos iniciaron el arreglo e indicaron que pronto volverá el servicio.

Los técnicos del Municipio explicaron que las personas que atacaron la página lo hicieron a través de los enlaces de internet a la computadora central de la Alcaldía y borraron el contenido.

"Son personas que quieren hacer daño al Municipio. Los hackers, como se conoce a las personas que atacan a las páginas web y que son conocedoras de informática, generalmente, buscan provecho personal o impiden que se difunda la información".

UN CONTENIDO VALIOSO SE HA PERDIDO

● LA PÁGINA web contenía información sobre Quito, sus atractivos turísticos, servicios, incluso, la ciudadanía podía consultar el valor del impuesto predial. Mediante este canal también la ciudadanía puede escribir cartas y enviar invitaciones al alcalde, Paco Moncayo.

En 48 horas funcionará nuevamente la página web y esta vez con más seguridad para evitar este tipo de daños, aseguraron los técnicos.

Boletín de Prensa

HACKERS DESTRUYEN PÁGINA WEB DEL MUNICIPIO DE QUITO

La página web del Municipio de Quito (www.quito.gov.ec) fue atacada la noche del 5 al 6 de Febrero de 2001 por personas desconocidas hábiles en informática que la destruyeron, informó el Departamento de Comunicación Social del Municipio.

La página web del Municipio es un éxito de información ciudadana, tanto que recibió 26.000 consultas durante el mes de enero. En esa página podía consultarse, entre otras cosas, el monto del impuesto predial de cualquier persona, con solo digitar el nombre.

Los visitantes de la mañana de este martes encontraron que en vez de la página del Municipio lo que aparecía era un pescado. Ahora los técnicos municipales pusieron un aviso que dice que la página está en reparación y que pronto volverá a estar en servicio.

Quienes atacaron la página deben haber entrado, a través de los enlaces de Internet, a la computadora central (server) del Municipio y borraron el contenido del home page, explicaron los técnicos de Informática del Municipio del Distrito Metropolitano de Quito. Borrada la home page, o página de inicio, nadie puede acceder a la abundante y detallada información con que se contaba.

Nadie se explica en el Municipio a qué se debe ese ataque. "Los hackers, como se conoce a las personas que atacan a las páginas web y que son conocedoras de informática, generalmente buscan un provecho personal, o impedir que se difunda información", dijeron los técnicos de la municipalidad. "No puede ser coincidencia", dijo otro de los técnicos. "Son personas que quieren hacer daño al Municipio o al alcalde".

La página de Internet también proveía información sobre la ciudad de Quito, sus atractivos así como sobre el Municipio, sus servicios y sus dependencias y fue iniciada por el Alcalde de Quito, Gral. Paco Moncayo, como un sistema adicional de información a la ciudadanía y venía siendo mantenida por personal de Informática, Comunicación Social y la antigua Dirección de Planificación, hoy Dirección de Gestión del Desarrollo.

Era también el sistema por el cual cualquier persona podía escribir al Alcalde, sistema que había alcanzado mucho éxito, pues cada día decenas de personas enviaban por ese medio solicitudes, quejas, felicitaciones, pedidos o invitaciones al Alcalde.

Los técnicos de informática se comprometieron en volver a poner "al aire" la página en 48 horas. "Estamos trabajando arduamente para que la página vuelva a funcionar lo más pronto posible", dijeron los expertos municipales. "Y esta vez pondremos más seguridades para que no les sea tan fácil destruir una información tan vital". FIN

ANEXO 3

FALLO ARGENTINO
A FAVOR DE CIBER INTRUSOS

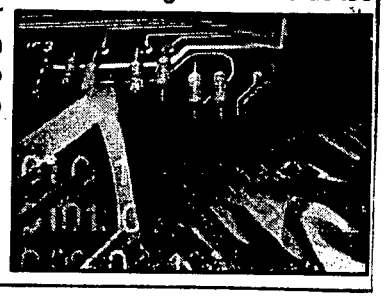
TECNOLOGIA

Juez falla a favor de ciberintrusos en Argentina

Los intrusos informáticos pueden ser el flagelo de la era digital, pero en Argentina encontraron un curioso aliado: el sistema judicial que ellos mismos menosprecian. Al aducir un "grave vacío legal" que torna difícil el enjuiciamiento de delitos digitales, un juez resolvió que la ciberintrusión es legal en este país sudamericano porque no hay normas que la castiguen.

La decisión favorecería a programadores piratas que violaron el sitio de Internet de la Corte Suprema. Con la justificación de que la ley sólo abarca los delitos cometidos sobre "personas, cosas y animales" y no los ilícitos en el campo informático, un juzgado federal declaró inocentes a varios argentinos conocidos como "X-Team", que irrumpieron en el sitio del máximo tribunal para acusar a los jueces de encubrir un caso relativo a los derechos humanos.

"El juez dictó que no hubo daños a cosas, personas o animales y que entonces no correspondía aplicar la ley", explicó Antonio Mille, abogado de la filial argentina de Microsoft. El fallo fue publicado el 11 de abril. La sentencia no fue apelada, dijeron abogados. "Esto nos permite sostener (...) que hay un grave vacío legal que hoy en día no permite reprimir los hechos", dijo el juez que redactó la resolución. En Argentina los fallos judiciales no sientan precedentes legales y otro juez puede resolver en forma distinta sobre la legalidad o no de los intrusos informáticos. El "X-Team" fue acusado de haber entrado ilegalmente al sitio de Internet de la Corte Suprema en 1998 y de haber puesto en su lugar una foto del fotógrafo asesinado José Luis Cabezas, además de haber colocado declaraciones culpando al tribunal de encubrir su muerte.



Cabezas fue encontrado muerto, quemado, dentro de su auto en enero de 1997. La investigación de su crimen involucró a un empresario con vínculos cercanos al ex presidente Carlos Menem.

SENTENCIA DEL JUEZ DEL JUZGADO FEDERAL EN LO CROMINAL Y CORRECCIONAL N° 12 DE BUENAS AIRES, ARGENTINA DE FECHA 20 MARZO SOBRE SUPUESTO DELITO DE HACKEO.

Buenos Aires, marzo 20 de 2002. Autos Y Vistos: Para resolver en las presentes actuaciones que llevan el N° 8515/98 caratuladas "---------- y otros s/delito de acción pública" del registro de la Secretaría N° 24, de este Juzgado Nacional en lo Criminal y Correccional Federal N° 12, y respecto de la situación procesal de ----------, argentino, titular del DNI ----------, nacido el día ----de------ de------en esta ciudad, estudiante, soltero, hijo de ----------, domiciliado realmente en la ----------, y constituido a los efectos legales en la----------, ambos de esta ciudad;; ----------, argentino, titular del DNI ---------- nacido el día------ de ---------- de ---------- en el partido de----------, Provincia de Buenos Aires, soltero, empleado, hijo de ----------, domiciliado en la calle ----------, Provincia de Buenos Aires, y constituido a los efectos legales en la ---------- de esta Ciudad; ----------, argentino, titular del DNI ----------, nacido el día------- de ---------- de ---------- en el ----------, provincia de Buenos Aires, soltero, analista de sistemas, desocupado, hijo de ----------, domiciliado realmente en la Calle ----------, Provincia de Buenos Aires, y constituido a los efectos legales en la ---------- de esta ciudad; ----------, argentino, titular del DNI ----------, nacido el día-------de--- de-----en el Partido de ----------, Provincia de Buenos Aires, hijo de ---------- ----------, domiciliado en la calle---------- partido de ----------, provincia de

Buenos Aires, y constituido en ---------- de esta ciudad; ----------, argentina, titular del DNI ----------, nacida el día ----de ------ de------ en el partido de -------, provincia de Buenos Aires, soltera, empleada, hija de----------, domiciliada realmente en la calle ---------- partido de ----------, provincia de Buenos Aires, y constituido en la calle ----------de esta ciudad; y----------, argentino, titular del DNI----------, nacido el día --- de ---- de ----- en la provincia de Buenos Aires, soltero, estudiante;

Y CONSIDERANDO: Que las presentes actuaciones tienen su raíz el día 31 de agosto del año 1998, en virtud de la remisión de testimonios del expediente administrativo Nº 20-01576/98 dispuesta por la Corte Suprema de Justicia de la Nación, el que fuera labrado por la Secretaría de Auditores del máximo tribunal.--Tal expediente fue tramitado a los efectos de efectuar una información sumaria respecto de la violación detectada de la seguridad del sistema de la página de Internet del tribunal de mención el día 26 de enero de ese mismo año. En efecto en la fecha señalada se advirtió que la página inicial había sido reemplazada por una alusiva al aniversario del fallecimiento del periodista ----------.

Durante la instrucción del sumario en cuestión se produjeron diversas medidas probatorias, las que le permitieron a los Sres. Secretarios Letrados de la CSJN concluir que en los hechos que fueran motivo de pesquisa no había intervenido personal del Poder Judicial de la Nación. Arribadas las actuaciones a conocimiento de este tribunal, se corrió vista al Sr. Agente Fiscal en los términos del artículo 180 del Código Procesal Penal de la Nación, oportunidad en la que formuló el pertinente requerimiento de

instrucción. .Así las cosas, comenzó la etapa instructora produciendo las medidas conducentes a los efectos de ahondar en la pesquisa.

En tal sentido, en la inteligencia que luego de la violación del sistema se recibió un correo electrónico -a través del cual se informaban los motivos en virtud de los cuales se había alterado la página inicial del sitio de la CSJN- el cual habría sido enviado a través del servidor Startel, cuyo usuario emisor habría sido la firma Buenos Aires Diseños S.R.L., se le recibió declaración testimonial a ----------, titular de dicha empresa. (Fs. 84/5).En dicha oportunidad, el nombrado expresó que por problemas con el servicio prestado por Startel, en diversas oportunidades se había visto en la obligación de dar a conocer la clave asignada, recordando que en una oportunidad se había comunicado con uno de los empleados de dicha firma de nombre ----------.

Por tal razón, luego del informe requerido a Startel, se le recibió declaración testimonial a los empleados de dicha firma que tenían el nombre de pila en cuestión, de las que no surgieron elementos de interés para la presente pesquisa. (ver fs. 112, 114/6, 118, 134/6).El día 3 de marzo del año 1999 se le recibió declaración testimonial a ----------, periodista de la revista "Siglo XXI", quién publicara una nota relacionada a los hechos materia de investigación. De dicho acto puede destacarse que la periodista de mención se había entrevistado con miembros del Grupo de "Hackers" denominado "Xteam", quienes se habían atribuido la violación del sistema de la Corte Suprema de Justicia de la Nación. Por otra parte se solicitó colaboración en la presente pesquisa a la Secretaría de Inteligencia del Estado, a los efectos de ahondar en la investigación, en virtud de lo cual, se propusieron diversas medidas de prueba a tales efectos. (fs. 165).

Así también se le dio intervención al Departamento Análisis Delictivo de la PFA a los efectos de practicar diversas tareas de inteligencia, cuyos informes se encuentran glosados a fs. 170, 174/89, y 241/3. El día dos de mayo de dos mil se le recibió declaración testimonial a ----------, perteneciente a la Secretaría de Inteligencia del Estado, quién proporcionó las medidas de prueba que a su entender resultaban necesarias para ahondar en la investigación (Fs. 273).Posteriormente con fecha nueve del mismo mes y año se delegó la instrucción del presente sumario al Sr. Fiscal de la Fiscalía Federal N° 1, quién continuó con la pesquisa de autos, disponiendo las diligencias tendentes a determinar el origen de la violación al sitio Web del máximo Tribunal, como así también del correo electrónico remitido al día siguiente.

Así también habrá de destacarse que continuó la colaboración del personal especializado de la Secretaría de Inteligencia del Estado, y se dio intervención a la División Informática de la Policía Federal Argentina. Por otra parte se encomendó la realización de una pericia a los efectos de individualizar a los integrantes del grupo "XTeam" que surgían de la nota periodística obrante a fs. 138/40.De dicho estudio surge que la persona que participó de la nota periodística, resulta ser "muy probablemente ----------". (ver fs. 375/82).Continuando con las tareas encomendadas al personal interventor, partiendo de los datos que surgían de la nota en cuestión, logró la individualización de diversos números de registro del sistema ICQ de quienes podrían formar parte del grupo "Xteam" (ver fs. 397/8).-También se logró individualizar el sitio www.geocities.com/wences, ingresando posteriormente a la dirección de la página web http.//www.iwences.web.com, procediéndose a imprimir la totalidad de los datos que

surgieron de los mismos. (fs. 408).Posteriormente la División Informática de la PFA, a través de las diligencias practicadas logró identificar fehacientemente a ----------
---como aquel que participara de la nota periodística, como así también el que surgiera del sitio y página web detalladas, obteniéndose posteriormente los elementos necesarios para obtener un acabado conocimiento de sus datos filiatorios. (ver fs. 427/33, 455/63, 479/85).

Toda vez que de las tareas señaladas se habían obtenido de los abonados telefónicos que habitualmente eran utilizados por el citado --------, se dispuso su intervención a los efectos de tomar un acabado conocimiento de las actividades por él desarrolladas -abonados 4259-6757, 4207-4197, y 4206-1366- (ver fs. 549).A fs. 635/74 y fs. 742 se incorporaron listados de llamadas entrantes y salientes de los diversos abonados telefónicos que resultaban de interés para la presente pesquisa. Así también se incorporaron las escuchas telefónicas obtenidas a partir de la intervención de los abonados en cuestión (ver fs 677/723, 737/8, 756/60, y 768/923).

Del análisis efectuado sobre los listados de llamadas entrantes y salientes y las escuchas obtenidas, se logró determinar que en el horario en que se habría producido la violación del sitio de la Corte Suprema de Justicia de la Nación, desde el abonado telefónico del domicilio de ---------- se habían efectuado gran cantidad de llamados a diversos medios de comunicación. Así también se registraron dos llamadas entrantes a dicho abonado provenientes del N° 4309-7591 correspondiente al Diario Clarín. Por otra parte, de dicho estudio se vislumbró la relación existente entre dos personas llamadas -------- y ------ que trabajaban en la Firma Copde y conforme los contactos mantenidos con el

encartado ---------, podría presumirse que las nombradas tenían un acabado conocimiento de las actividades desplegadas por el citado------.

En razón de lo expuesto, en el entendimiento que existían elementos suficientes para sospechar que ---------- habría participado en el hecho materia de investigación, el día 4 de enero del pasado año se dispuso recibirle declaración indagatoria en los términos del artículo 294 del Código procesal de la Nación. Debe señalarse que tal acto se difirió hasta tanto fuera habido el nombrado quien, conforme las tareas de inteligencia practicadas, residía en los Estados Unidos de América, y se encontraba en aprestos para retornar al País. Así las cosas el día 18 del mismo mes y año se dispuso la detención de---------, quien regresaba del país de mención en la fecha señalada, ordenándose asimismo el secuestro de los efectos que el nombrado pudiere poseer. Por otra parte se dispusieron los allanamientos de las fincas donde residían ----------, las hermanas ---------- y ----------, como así también el domicilio de la Firma COPDE SA.A fs. 971/81 se agregaron las constancias de llamados entrantes a la firma Startel, como consecuencia del requerimiento efectuado por la instrucción a los efectos de determinar las conexiones existentes con dicho servidor al momento en que se llevara a cabo la violación del sistema de la CSJN, como así también al momento en que se enviara el correo electrónico posterior. Posteriormente se incorporaron al presente sumario nuevas transcripciones de las escuchas telefónicas producidas por la prevención. (ver fs 983/4, 1000/2, 1007/8, 1017/9, 1022/1122, 1126/37, y 1165/84).Conforme fuera señalado en los párrafos precedentes, el día 19 de enero del pasado año se llevaron a cabo diversos allanamientos y detenciones.

Así, obran a fs. 1188/92, las actuaciones labradas por el personal interventor, con motivo de la detención de --------- --------, y el secuestro de los efectos de interés para la investigación. Cabe precisar que entre sus pertenencias se afectaron a las presentes actuaciones una note book, diskettes y una máquina marca "Palm", todo lo cual, posteriormente fue sometido al correspondiente estudio pericial. Así también en la misma fecha se procedió al allanamiento del domicilio ocupado por la Firma COPDE --- ---------- , Partido de ----------, provincia de Buenos Aires- producto del cual se secuestraron dos CPU y otros elementos informáticos, los que se hallan detallados en el acta labrada glosada a fs. 1197.Por otra parte se llevó a cabo el registro domiciliario en la finca sita en la calle ---------- de la localidad de ----------, provincia de Buenos Aires- el cual era ocupado por los padres de ----------, quien también residía en dicho lugar en los períodos en que se encontrara en el País.

Con motivo de dicho registro se logró el secuestro de gran cantidad de elementos de computación tales como un gabinete Minitower incompleto, y gran cantidad de diskettes, como así también diversos elementos de interés para la presente pesquisa. (ver acta de fs. 1202)En la misma fecha señalada se procedió al allanamiento de la finca sita en el ----------, de la localidad de ------ --------, provincia de Buenos Aires, en virtud del cual se afectaron a esta causa dos CPU, gran cantidad de diskettes, y agendas personales (ver fs. 1211).Así las cosas, el día 23 de enero del pasado año se encomendó al Sr. titular de la División informática de la PFA la realización de una pericia sobre la gran cantidad de elementos de computación secuestrados.

En la misma fecha el personal interventor recibió declaración a los testigos presenciales de los diversos procedimientos arriba señalados, quienes a su vez oficiaron como tales al momento en que se procedió a la apertura de los elementos secuestrados en autos. (ver fs. 1283/8, 1291/6 y acta de fs. 1289/90).Cabe destacar que en tanto se continuaba la intervención de los abonados telefónicos de interés, se agregaron a la presente causa las transcripciones de las conversaciones mantenidas a través de los mismos, de los cuales fueron surgiendo diversos elementos de interés para la presente pesquisa. (fs. 1301/7, 1324/43, 1353/8, 1363/84, 1389/1401, 1409/31, 1448/53).

Asimismo, se agregaron a fs. 1314/9 vistas fotográficas de ---------- obtenidas a través de los procedimientos dispuestos por este Tribunal en la que se lo puede observar acompañado de la persona de sexo femenino conocida como ------, de quien ya existían indicios que hicieran presumir su colaboración con el encartado de mención. Por otra parte se incorporaron diversos artículos periodísticos publicados por distintos medios gráficos, alguno de los cuales encontraban correlato con contactos telefónicos que los autores de los mismos habían mantenido con los imputados o bien con personas allegadas a éstos. (fs. 1433/42).Ahora bien, en virtud del estudio practicado por el personal interventor con motivo del peritaje que le fuera encomendado sobre el director o del disco rígido de la computadora portátil que le fuera secuestrada a ------ y del archivo del programa denominado ICQ -el cual contenía diversas conversaciones, conocidas como "Chats", mantenidas entre el nombrado y distintas personas-, y de su relación con el análisis de las escuchas telefónicas obtenidas, el Titular de la División Informática de la PFA, logró la individualización de los miembros del grupo "Xteam", y

el rol que cumplirían cada uno de ellos dentro de dicha organización. En tal sentido, se sindicó a ----------cuyo seudónimo resultaba ser Niko- como manager del grupo de mención. En efecto se logró individualizar dos identificaciones en el programa ICQ, donde pudieron obtenerse sus datos filiatorios.

A tal efecto se valoraron las conversaciones mantenidas con "wences" -apodo atribuido al encartado -------- como así también aquellas mantenidas vía conducto telefónico. En segundo término se individualizó como miembro del "XTeam" a ----------, de quien se obtuvieron sus datos filiatorios, y su identificación en el programa ICQ, a través del cual había mantenido conversaciones y donde figuraba la dirección de e-mail ---------- Por último se determinó que el nombrado utilizaba los seudónimos de Bash, Kurt y None. En tercer lugar se sindicó como miembro del grupo en cuestión a ----------, poseedor de la dirección de correo electrónico ---------- quien utilizara el seudónimo de Quato al momento de comunicarse mediante el programa ya citado.

Al respecto cuadra destacar que desde los inicios de la presente pesquisa surgían indicios que hacían presumir que el nombrado participaba en las actividades del grupo, y su consecuente vinculación con el hecho materia de investigación. Por otra parte se identificó a ----------, quien actuara de diseñador gráfico del grupo, individualizado en el programa ICQ bajo el apodo de Tommy Tomato, en el cual figuraba su dirección de e-mail (Tomatelo@consoda.com.ar), específicamente de las conversaciones mantenidas por este medio entre Wences y Bash. Así también se sindicó a una persona de sexo femenino de nombre ---------- como miembro de este grupo.

Tal afirmación se fundó en las conversaciones mantenidas a través de los abonados telefónicos intervenidos en autos. Por último se logró la individualización de ---------- --------- quien se identificara como Manuk en el programa de comunicación citado. Al respecto cuadra destacar que conforme las constancias colectadas en estas actuaciones se desprendía que "Manuk" habría sido quien había enviado el correo electrónico a la Corte Suprema de Justicia de la Nación el día posterior a la violación del sitio web de dicho Tribunal. (ver constancias de fs. 1460/73, y 1476/89).A su vez pudo corroborarse de los listados de llamadas entrantes y salientes del abonado utilizado por ---------- que éste se habría comunicado en reiteradas oportunidades con el utilizado por----------, al momento en que se habría producido la violación a la página de la CSJN. (fs. 1497).

En razón de lo expuesto este Tribunal dispuso el allanamiento de las fincas ocupadas por los encartados, a los efectos de lograr el secuestro de cualquier elemento informático que utilizaren los nombrados a los efectos de llevar a cabo las actividades desplegadas por el grupo "Xteam". Fs. (1502/5).A fs. 1524/32 se agregaron copias de la nota publicada por la Revista "Veintitrés", y a fs. 1616 la publicada en la revista "Rolling Stone" relativas al hecho materia de investigación. Por otra parte se incorporaron al presente sumario las actas labradas con motivo del peritaje encomendado como así también imágenes obtenidas en dicha oportunidad, de la computadora portátil que le fuera secuestrada a ---------- (ver fs. 1678/98).El día 22 de febrero del pasado año, con motivo de lo dispuesto por este Tribunal, se procedió a la detención de A----------, en momentos en que asistía a la sede de la División Informática Federal a los efectos de participar de la pericia en la que había sido designado por ---------- como

perito de parte, (ver declaraciones testimoniales y acta de detención obrantes a fs. 1700/4.)

En la misma fecha se procedió al allanamiento de la finca sita en la ---------- de esta ciudad, procediéndose al secuestro de diversos elementos de computación tales como un disco rígido marca Segate, noventa y cinco diskettes y nueve Compact discs. Por otra parte, se procedió al secuestro de diversos elementos y envoltorios que contenían una sustancia vegetal símil a la marihuana. (Ver acta y declaraciones testimoniales agregadas a fs. 1709/17).Así también se llevó a cabo el registro de la finca sita en la calle ---------- del partido de -------, Provincia de Buenos Aires, lugar donde se procedió a la detención de ----------, y se logró el secuestro de diversos elementos de informática, entre los que se pueden destacar diversos discos rígidos, CPU, una notebook, y gran cantidad de diskettes. (ver acta, declaraciones testimoniales y vistas fotográficas obtenidas en dicha oportunidad obrantes a fs. 1724/37).Asimismo, se procedió al allanamiento de la finca sita en la calle ---------- del partido de ----------, provincia de Buenos Aires, lugar de residencia de ----------.

Inspeccionando que fuera el lugar, se logró el secuestro de un CPU, una agenda, soportes magnéticos y gran cantidad de fotografías. (ver acta y declaraciones obrantes a fs. 1742/4). Se destaca que el registro efectuado sobre el inmueble sito en la calle ---------- del Partido de ----------, provincia de Buenos Aires, arrojó resultado negativo, en tanto en dicho domicilio no vivía ni era conocido ----------, ni se logró el secuestro de elemento alguno de interés para esta causa. (ver fs. 1746/50).Por último, el día 23 de febrero del año próximo pasado se llevó a cabo el allanamiento de la finca sita en la -----

---------- de esta ciudad, lugar de residencia de ----------, quien no se hallaba en el inmueble. Sin perjuicio de ello se logró el secuestro de gran cantidad de material informático, tal como CPU, diskettes, Compact Discs, como así también un bolso con la inscripción "Decidir.com", (ver constancias de fs. 1783/7).

El día 8 de marzo del mismo año se le recibió declaración testimonial en dependencia policial a ---------- quien en su carácter de Gerente General de la Firma Decidir.com, señaló que ---------- había trabajado como colaborador eventual de una subsidiaria de dicha firma en el exterior, en virtud de la recomendación que efectuara ----------, quien sí fuera empleado de dicha empresa. Se agregó a fs. 1837/46 el informe pericial elevado por el encartado ----------, quien conforme se expresara en su oportunidad, actuó como perito de parte en el estudio dispuesto por este Tribunal, en razón del cargo que le fuera conferido por el imputado ---------, remitiéndome a sus conclusiones en honor a la brevedad. Continuando con la instrucción del presente sumario el Sr. Agente Fiscal dispuso recibirle declaración testimonial a todos aquellos periodistas que hubieren publicado artículos relacionados con el hecho materia de investigación.

Así, prestó testimonio ----------, periodista del Diario Clarín, quien manifestó ser autor de las notas glosadas a fs. 1433 y 1435, ratificando el contenido de cada una de ellas. Así también se le recibió declaración testimonial a ----------, empleado del mismo periódico, quien expresó haber sido el autor de la nota cuya copia obra a fs. 435. Al respecto manifestó haber recibido un llamado telefónico de un "hacker" quien lo anotició que llevaría a cabo un ingreso ilegítimo a la página de la Corte Suprema de

Justicia de la Nación, lo cual ocurrió pasados unos veinte minutos de haberse producido el llamado. El día veintidós de marzo del pasado año se le recibió declaración a ----------, quien indicó que era de su autoría el artículo periodístico agregado a fs. 393/6 de las presentes actuaciones. Lucen a fs. 1928/44 copias de los artículos obtenidos de la Red internet relacionado con el hecho materia de pesquisa en la presente causa. Con fecha 14 de marzo del pasado año prestó declaración testimonial ----------, apoderado de la Firma Criteria SA, quien expresó que ---------- y---------- habían trabajado para dicha firma desde el mes de diciembre de 1997 hasta el mes de mayo o junio del año 1999 (fs. 1956).

Por otra parte, se agregó a fs. 1971/2 el acta de informe pericial, en la cual se detallan los diversos datos obtenidos de los elementos informáticos secuestrados en autos, entre los que se pueden destacar los glosados a fs. 1973/2013.El día 18 de abril del pasado año se le recibió declaración testimonial a ---------- y a ----------, ambos periodistas, quienes ratificaron la autoría y el contenido de diversas notas periodísticas incorporadas a esta causa.A fs. 2063/137 se agregaron actuaciones labradas por el personal preventor. Las mismas están compuestas por informes remitidos por el Ministerio de Relaciones Exteriores y Culto de la Nación, listados de llamadas entrantes y salientes de abonados telefónicos, transcripciones de escuchas telefónicas y conversaciones mantenidas a través de ICQ, y del análisis efectuado por la dependencia policial. Finalmente, el día 17 de diciembre del pasado año, se dispuso recibirle declaración indagatoria a los encartados en autos, en los términos del artículo 294 del Código Procesal Penal de la Nación. Cabe destacar que----------, ----------, ----------, ----------

----- y ----------, optaron por el derecho a negarse a declarar. (ver fs. 2308/10, 2311/13, 2315/6, 2323/5, y 2334/6).

Por su parte ---------- al momento de efectuar su descargo negó toda participación o vinculación con el hecho que se le imputó. Asimismo, señaló que los mensajes de ICQ que se le atribuyen le correspondieran. Por último, señaló haber conocido el grupo "Xteam" a partir de su participación en los peritajes dispuestos por este tribunal. Calificación Penal. Ahora bien, conforme se desprende de las distintas declaraciones indagatorias recibidas en la presente causa se les imputa a los encartados haber participado, de diversa manera, en la violación del sistema de seguridad de la página Web de la Corte Suprema de Justicia de la Nación, alterando la página inicial la que fue reemplazada por una alusiva al aniversario del fallecimiento del periodista ----------, afectando de tal forma el sitio de mención.

Así, desde el punto de vista del derecho de fondo se debería encuadrar el hecho mencionado en la figura penal básica prevista por el artículo 183 del Código Penal, debiendo, asimismo, determinar si el mismo se encuentra contemplado en el agravante descripto por el artículo 184 inciso 5° del mismo cuerpo legal. Cabe destacar que la primer norma citada reprime con pena de prisión de 15 días a un año al que "destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno...".Por su parte el agravante previsto por el artículo 184 inciso 5° del Código Penal establece que la pena será de tres meses a cuatro años de prisión si el daño atípico se ejecuta "... en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público..."De la enunciación

de ambos artículos, se desprende, y así lo ha sostenido la doctrina, que la acción de dañar está compuesta por todo ataque a la materialidad, utilidad o disponibilidad de las cosas. La primer variante se da cuando se altera su naturaleza, forma o calidades, mientras que la utilidad se ataca cuando se elimina su aptitud para el fin o los fines a que estaba destinada. Por último, entiéndase que se ataca a la disponibilidad de la cosa cuando el acto de la gente impide que su propietario pueda disponer de ella. (Carlos Creus, "Derecho Penal" parte especial, Tomo I, pág. 609).

De lo expuesto, puede afirmarse que en el caso bajo estudio se vislumbra la existencia una de las variantes de la acción típica prevista por la norma en cuestión, cual es el ataque a la materialidad en tanto conforme surge de las constancias de autos, la página Web del máximo Tribunal de justicia de la Nación, fue alterada, reemplazándosela -conforme fuera señalado precedentemente- por una alusiva al aniversario de ----------. Sin embargo, claro es advertir que al profundizar el encuadre legal nos encontramos con un obstáculo, el cual radica en el objeto del delito, que llevara al suscripto a sostener la atipicidad del hecho investigado. Ello así, en tanto a mi entender no es dable considerar a la página Web de la Corte Suprema de Justicia de la Nación, como una "cosa", en los términos en que esta debe ser entendida. A los efectos de lograr un claro significado jurídico de la palabra "cosa" debemos remitirnos al artículo 2311 del Código Civil de la Nación que define a ésta como los objetos materiales susceptibles de tener un valor. A su vez, prescribe que las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación. Debemos señalar que la doctrina no ha sido pacífica en lo que respecta a los elementos característicos de la cosa.

En efecto, un sector doctrinario que entendió que aquellos son su corporeidad y su valor patrimonial. Sin embargo el concepto de corporeidad no es unánimemente reconocido por la doctrina, ya que para algunos existe la ocupación de un lugar en el espacio -concepto sostenido por Soler- mientras que para otros resulta ser condición suficiente su materialidad, de manera que bastaría que un objeto pueda ser detectado materialmente para que sea considerado "cosa" -criterio adoptado por Núñez-.Ahora bien, sentado lo expuesto, puede advertirse que se opte por uno u otro concepto, una página web no puede asimilarse al significado de "cosa". Ello así, en tanto y en cuanto por su naturaleza no es un objeto corpóreo, ni puede ser detectado materialmente. Cabe destacar que una interpretación extensiva del concepto de cosa, a punto tal que permita incluir a la página Web dentro del mismo, comprendería una acepción que implicaría un claro menoscabo al principio de legalidad establecido en el artículo 18 de nuestra Constitución Nacional. Claro es advertir que nos encontramos con un claro vacío legal que ocupa en la actualidad a nuestros legisladores, conforme se desprende de sendos proyectos y anteproyectos de ley que se han presentado.

Entre ellos podemos señalar el proyecto de ley del Senador Antonio Berhongaray, el cual en su capítulo III titulado "Daño a datos informáticos", artículo 5 reprime con prisión de seis a tres años a quien "sin expresa autorización del propietario de una computadora o sistema de computación y del propietario de los datos, o excediendo los límites de la autorización que le fuera conferida, ya sea a través del acceso no autorizado, o de cualquier otro modo, voluntariamente y por cualquier medio, destruyere, alterare en cualquier forma, hiciere inutilizables o inaccesibles, o produjera o

diere lugar a la pérdida de datos informáticos".Asimismo, el artículo 6 establece los agravantes de la figura básica prevista en el artículo arriba señalado. (Diario de asuntos Entrados del Senado de la Nación, Año XV nro 3 pág.68 y siguiente, Buenos Aires, 1999).Por otra parte, el anteproyecto de ley publicado en el Boletín Oficial el día 26 de noviembre del pasado año, en su artículo 2, bajo el título Daño informático reprime con prisión de un mes a tres años al que "... ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un sistema o dato informático."Como se ve, tanto el proyecto como el anteproyecto de ley, intentan crear una figura penal, símil al daño previsto por el artículo 183 del Código Penal Argentino, pero que tengan como objeto del delito, ya no a la "cosa", sino a datos o sistemas informáticos.

Esto nos permite sostener que, también los legisladores advierten el grave vacío legal que hoy en día no permite reprimir los hechos como el que fuera motivo de pesquisa en la presente causa, en tanto los datos y sistemas informáticos, al igual que las páginas Web, resultan ser extrañas al significado jurídico de la palabra cosa contemplado en nuestro ordenamiento legal vigente. Por lo demás, habrá de destacarse que el hecho motivo de pesquisa no tiene encuadre legal en figura penal alguna prevista en nuestro Código Penal de la Nación ni en las leyes complementarias. Por ello, y en punto a resolver la situación procesal de los encartados en autos, habré de adoptar un temperamento de carácter conclusivo a su respecto, en tanto, conforme fuera adelantado, a entender del suscripto el hecho investigado no constituye delito.

Así las cosas, entiendo que corresponde y así; Resuelvo:

I. Sobreseer a ----------, de las demás condiciones personales obrantes en autos, en orden al hecho por el cual fuera indagado, en tanto no encuadra en figura legal alguna, dejando expresa mención que la formación del presente sumario en nada afecta el buen nombre y honor que gozare. (artículo 336 inc. 3° del C.P.P.N.).

II.Sobreseer a----------, de las demás condiciones personales obrantes en autos, en orden al hecho por el cual fuera indagado, en tanto no encuadra en figura legal alguna, dejando expresa mención que la formación del presente sumario en nada afecta el buen nombre y honor que gozare. (artículo 336 inc. 3° del C.P.P.N.).

III.Sobreseer a ----------, de las demás condiciones personales obrantes en autos, en orden al hecho por el cual fuera indagado, en tanto no encuadra en figura legal alguna, dejando expresa mención que la formación del presente sumario en nada afecta el buen nombre y honor que gozare. (artículo 336 inc. 3° del C.P.P.N.).

IV.Sobreseer a ----------, de las demás condiciones personales obrantes en autos, en orden al hecho por el cual fuera indagado, en tanto no encuadra en figura legal alguna, dejando expresa mención que la formación del presente sumario en nada afecta el buen nombre y honor que gozare. (artículo 336 inc. 3° del C.P.P.N.).

V. Sobreseer a ----------, de las demás condiciones personales obrantes en autos, en orden al hecho por el cual fuera indagado, en tanto no encuadra en figura legal alguna, dejando expresa mención que la formación del presente sumario en nada afecta el buen nombre y honor que gozare. (artículo 336 inc. 3° del C.P.P.N.).

VI. Sobreseer a ----------, de las demás condiciones personales obrantes en autos, en orden al hecho por el cual fuera indagado, en tanto no encuadra en figura legal alguna, dejando expresa mención que la formación del presente sumario en nada afecta el buen nombre y honor que gozare. (artículo 336 inc. 3° del C.P.P.N.).

VII. Notifíquese mediante sendas cédulas de notificación y firme que sea archívese.-- Fdo.: Dr. ----------

SUMARIO: "...Ello así, en tanto a mi entender no es dable considerar a la página Web de la Corte Suprema de Justicia de la Nación, como una "cosa", en los términos en que esta debe ser entendida. A los efectos de lograr un claro significado jurídico de la palabra "cosa" debemos remitirnos al artículo 2311 del Código Civil de la Nación que define a ésta como los objetos materiales susceptibles de tener un valor. A su vez, prescribe que las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación. Debemos señalar que la doctrina no ha sido pacífica en lo que respecta a los elementos característicos de la cosa. En efecto, un sector doctrinario que entendió que aquellos son su corporeidad y su valor patrimonial. Sin embargo el concepto de corporeidad no es unánimemente reconocido por la doctrina, ya que para algunos existe la ocupación de un lugar en el espacio -concepto sostenido por Soler- mientras que para otros resulta ser condición suficiente su materialidad, de manera que bastaría que un objeto pueda ser detectado materialmente para que sea considerado "cosa" -criterio adoptado por Núñez. Ahora bien, sentado lo expuesto, puede advertirse que se opte por uno u otro concepto, una página web no puede asimilarse al significado de "cosa". Ello así, en tanto y en cuanto por su naturaleza no es

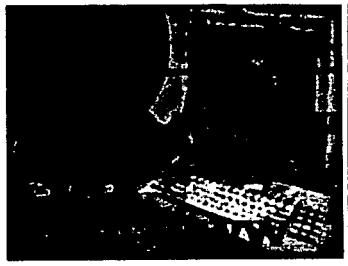
un objeto corpóreo, ni puede ser detectado materialmente. Cabe destacar que una interpretación extensiva del concepto de cosa, a punto tal que permita incluir a la página Web dentro del mismo, comprendería una acepción que implicaría un claro menoscabo al principio de legalidad establecido en el artículo 18 de nuestra Constitución Nacional. Claro es advertir que nos encontramos con un claro vacío legal que ocupa en la actualidad a nuestros legisladores, conforme se desprende de sendos proyectos y anteproyectos de ley que se han presentado..."

ANEXO 4

CASOS

TECNOLOGIA

Los intrusos cibernéticos atentan contra salud financiera, dicen expertos



Advertencia: los intrusos cibernéticos serían peligrosos para su salud financiera. Eso es lo que están diciendo los expertos en informática a las empresas afectadas por una constante cadena de infecciones de virus y otras vulnerabilidades que golpean a sus computadoras.

Más allá de una simple incomodidad, los intrusos y los virus están amenazando con arrastrar a las empresas de Estados Unidos con una seguridad insuficiente a una pesadilla legal que podría competir con los famosos procesos judiciales de las tabacaleras en los últimos años. Los expertos advierten que en el futuro cercano, las mismas empresas podrían enfrentar cuentas mucho mayores de abogados y aseguradoras, mientras al predecir una oleada de procesos judiciales por este tema en dos años."Va a ser una carrera a los estrados de la corte, como una persecución de ambulancia", advirtió Ed McPherson, director de la empresa de práctica de seguridad tecnológica PricewaterhouseCoopers en Atlanta. "Va a ser como un efecto dominó, cuando caiga el primer caso legal, se producirá un efecto multiplicador en todo el país".

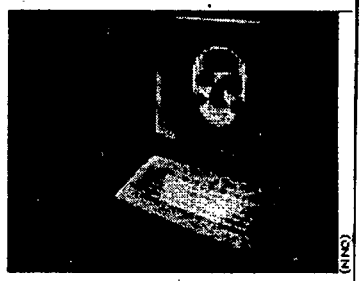
Con tal enredo informático de posibles demandas y miles de millones de dólares en juego, los expertos predicen que los procesos podrían alcanzar los procesos de las tabacaleras en Estados Unidos. Recientes fallas de seguridad ilustran el alcance del problema. Sólo en mayo, los intrusos cibernéticos robaron cientos de números de tarjetas de crédito del sitio TheNerds.net y obtuvieron acceso a datos de 265.000 empleados públicos en California. La cifra de incidentes de seguridad se disparó 400 por ciento desde 1999, a 52.658 casos en el 2001, según el equipo de respuesta de emergencias informáticas de la firma Carnegie Mellon.

Y según un sondeo difundido en abril por la Oficina Federal de Investigaciones (FBI) y el Instituto de Seguridad Informática de San Francisco, cerca del 90 por ciento de más de 500 compañías y agencias del gobierno encuestadas dijo que habían experimentado fallas de seguridad en el último año, con daños que superaron los 450 millones de dólares. "Parte de la razón por la que aún no hemos visto (demandas) es el estigma que viene con ser víctima de un ataque", dijo Lawrence Walsh, editor gerente de Information Security Magazine. Pero dada la rigidez de la economía, el aumento de las fallas de redes y las pérdidas resultantes, las empresas buscarán las cortes para obtener compensación, dijo Walsh.

"Tenemos evidencia de que las compañías en todo el país están analizando sus alternativas cuando ha habido un daño sostenido", agregó McPherson,

TECNOLOGIA

Nuevo gusano ataca a servidores SQL de Microsoft



Los dueños de viejas versiones del software SQL Server de Microsoft recibieron una advertencia para que cambien la configuración por omisión de la contraseña del administrador para evitar una infección con lo que se cree es un gusano de Internet.

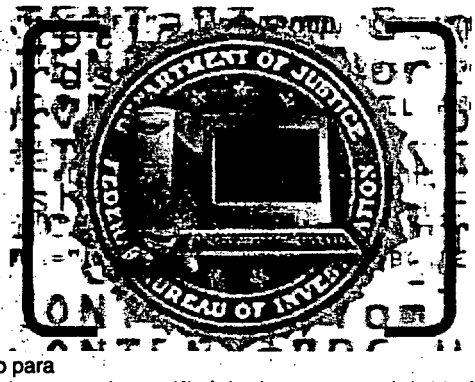
El gusano "SQLsnake" busca computadoras que operen el software de base de datos de Microsoft SQL Server 7. Este fue entregado por Microsoft sin una contraseña de administrador por omisión.

Elias Levy, presidente de tecnología del proveedor de servicios de seguridad SecurityFocus, explicó que si el gusano no encuentra una contraseña de administrador, el gusano crea su propia cuenta, así como una contraseña, y envía a una dirección gratuita de correo electrónico un mensaje con una lista de nombres de usuarios y contraseñas que toma del sistema. "Hemos visto hasta entre 1.400 a 1.600 máquinas infectadas", y cerca de 100 nuevas infecciones por hora, dijo Levi. "Obviamente, alguien está utilizando esto para recoger cuentas que puedan usar luego para entrar al sistema". Las dos fuentes principales de los ataques son Estados Unidos y Corea, pero eso no significa, necesariamente, que el gusano se originó en uno de esos dos países, agregó.

El SQL Server 2000, que fue lanzado a finales del 2000, contiene una contraseña codificada, y por lo tanto no es vulnerable a los ataques, explicó Mark Miller, un especialista de seguridad en servicios de productos de apoyo de Microsoft. La compañía advirtió de un incremento en la lectura digital de puertos de SQL Servers en Internet la semana pasada, y comenzó a informar inmediatamente de los riesgos potenciales, indicó Miller.

Al menos ha habido otras dos versiones de gusanos que atacan al SQL Server, según expertos y cibersitios proveedores de antivirus. La mayoría de los gusanos atacan a programas de correo electrónico o software que sustentan los sitios de Internet y navegadores. Pero el gusano más reciente de SQL Server es peligroso porque se dirige a las bases de datos en las que los sitios de comercio electrónico almacenan información importante, explicó Amit Yoran, presidente ejecutivo del proveedor de servicios de administración de seguridad RipTech. "Los gusanos ya no van más tras los usuarios en sus casas o los sitios de Internet", dijo Yoran. "Ellos van tras las aplicaciones de comercio electrónico", agregó.

Aumenta el espionaje gubernamental por Internet en Estados Unidos



CNN.- En los siete meses posteriores a la aprobación de una ley para combatir el terrorismo, se multiplicaron las peticiones presentadas por las autoridades a las compañías de Internet para que les permitan espiar a ciertos suscriptores.

Los defensores del derecho a la privacidad temen que las libertades civiles de Estados Unidos se vean afectadas por una combinación de factores como los mayores poderes policiales -- ampliados por la llamada Ley Patriótica --, una supervisión menos estricta y una creciente cooperación entre el gobierno, las redes telefónicas del sector privado y los proveedores de Internet.

Las nuevas leyes no sólo se aplican al terrorismo, sino también a otros delitos. "La tendencia hasta el 11 de septiembre era proteger la privacidad", dijo Al Gidari, un abogado en Seattle, que representa a algunas compañías de Internet y telecomunicaciones. "Ahora parece que todo eso se metió en una caja... y se echó a un rincón", agregó.

Las autoridades consideran que necesitan una mayor supervisión electrónica para seguir las huellas a los delincuentes dotados de mayores adelantos técnicos, y recalcan que esas acciones son selectivas, lo que implica que no necesariamente buscan en todos los proveedores todos los mensajes electrónicos que mencionen a Osama bin Laden.

En la mayoría de las ocasiones, lo que necesitan es identificar la fuente o el destinatario de un mensaje amenazador o sospechoso.

Los defensores de las libertades individuales están de acuerdo en que es preciso combatir el terrorismo, pero temen que las medidas tomadas con ese fin afecten a ciudadanos inocentes.

"Lo que tememos es el surgimiento de un sistema que almacene vastas cantidades de información acerca de la gente y luego la use con propósitos diferentes de los que motivaron su creación", dijo Alan Davidson, director asociado del Centro para la Democracia y la Tecnología.

Los funcionarios de justicia aseguran que toda búsqueda debe ser aprobada por un juez, y que muchos de los cambios han hecho más estrictos ciertos procedimientos que brindaban ventajas a los delincuentes en el uso de Internet.

Sin embargo, los críticos sostienen que casi todas las solicitudes para intervenir comunicaciones suelen recibir aprobación, y que los únicos informes públicos acerca del proceso no han indicado si las peticiones son excesivas.

Las solicitudes de información se han quintuplicado con respecto a los niveles observados antes del 11 de septiembre, según Gidari, entre cuyos clientes figura el proveedor de Internet America Online, así como las telefónicas AT&T Wireless y Cingular.

En Quantum Computer Services, un proveedor de correo electrónico gratuito en el estado de Luisiana, las solicitudes de información por parte de las autoridades se duplicaron después de los atentados terroristas, dijo la gerente Sheila Keller.

"Algunas cuentas creadas en Arabia Saudita y en Medio Oriente fueron de infraestructura de Internet, las solicitudes de información "se han disparado", dijo un ejecutivo de seguridad, quien pidió que ni él ni su compañía fueran identificados.

La mayoría de las peticiones buscan identificar a los operadores de una dirección específica de Internet de la que deben reunirse evidencias a juicio de las autoridades, señaló el directivo.

El portavoz de AOL, Nicholas Graham, declaró que hubo un alza luego de los atentados terroristas, pero que la compañía ha vuelto a los niveles normales de trabajo en cooperación y cumplimiento con las autoridades".

El espíritu de colaboración entre las compañías de Internet y las autoridades se intensificó incluso antes del 11 de septiembre, lo que representó un cambio sustancial respecto a los primeros días de la industria, expresó Gidari.

Las compañías "no son ya el bastión de la protección a los consumidores contra incursiones del gobierno en su información privada", dijo. "La percepción general es de una mayor coincidencia y deseo de ayudar", agregó. Un investigador del FBI especializado en delitos informáticos dijo que algunos proveedores de servicios de Internet en el área de San Francisco mantienen sus registros de conexiones por mayores períodos sólo en caso de que los agentes lo soliciten.

Normalmente, los agentes entregan una carta en la que dicen que se proponen solicitar una orden judicial, y el proveedor de Internet comienza a buscar la información incluso antes de que la petición sea aprobada, explicó el investigador, que pidió mantener el anonimato.

Sue Ashdown, presidenta de la Asociación Estadounidense de Proveedores de Servicio de Internet, dijo que las compañías deben insistir en la presentación de una orden judicial. "Tienen una responsabilidad grave si entregan información sin causa suficiente", agregó.

Las compañías como Quantum, AOL y Earthlink dicen que no tienen otra alternativa que cooperar cuando las autoridades proporcionan los documentos necesarios.

Sin embargo, la ley de supervisión permite que los operadores y proveedores entreguen voluntariamente información en casos de emergencias.

"Ahora todo es una emergencia", dijo Gidari.

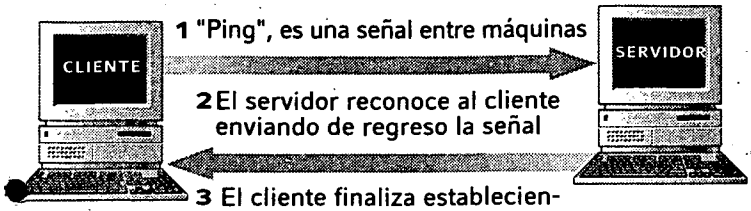
VIENE DE LA PÁG. B8

Los informáticos que desean aprender

Los 'hackers' rompen las seguridades

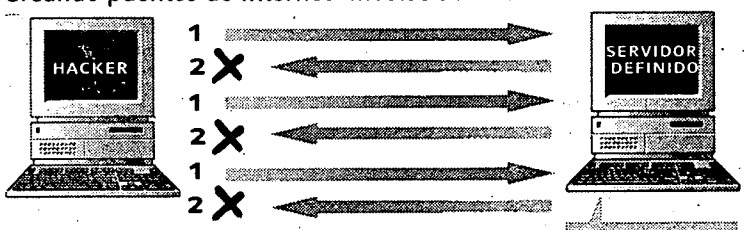
Una conección normal de Internet

El cliente y el servidor cambian un set de sequencias de mensajes para hacer una conexión



Uno a uno la negación de servicio ataca

Creando puentes de Internet "medias abiertas"

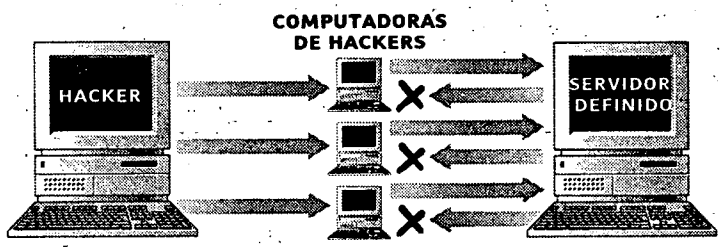


1 Envía una serie de "pings"

2 Si el ping se despliega en la dirección real, el servidor definido no puede retornar las señales para hacer un enlace. Se demora unos instantes, y luego desiste

Ataques distribuidos

Las computadoras que utilizan los hackers envían cientos de pings a los sistemas. Estos se encuentran en una locación remota.



Fuente: KRT; EL COMERCIO

"Todos los hackers son buenos si siguen la filosofía original del movimiento" advierte el libro 'La ética del hacker' que describe el mundo de estos expertos en informática. "No somos los que introducen virus en las computadoras ni realizamos robos, ésos son los crackers. Nosotros tenemos una ética que, sin duda, cambiará el mundo, basada en el libre acceso a la información que circula en Internet y a los códigos fuente".

Armín Utreras sabe que los hackers solo se dedican a investigar y probar sistemas, porque él incursionó hace varios años en este mundo.

Este empresario, quien dejó el 'hacking' hace mucho tiempo, se estremeció varias veces al constatar la vulnerabilidad de muchos sistemas y durante varias ocasiones la puso en evidencia para que las empresas corrijan las fallas.

Sonríe cuando recuerda que sus conocimientos en este campo le sirvieron para crear programas más seguros. Gracias a ello lo contrataron en varias empresas de prestigio.

Por obvias razones el accionar de un hacker es clandestino, aunque, como este caso, hay muchas compañías que contratan los servicios de hacking para determinar su nivel de seguridad y hallar sus potenciales debilidades.

En la actualidad, Utreras dirige su propia empresa especializada en brindar diversas soluciones informáticas.

Daniel también dominó este campo hace varios años.

Según él, es difícil estimar exactamente cuántos hackers operan en el Ecuador, pues hay una comunidad, como la Universitaria, donde varios estudiantes de sistemas asumen el reto de aprender y curiosear el tema de la seguridad. "Tengo algunos amigos que sienten empatía por este tema y comentamos sobre las nuevas herramientas y programas".

EL ESPECIALISTA DICE

■ **Cleiner Íñiguez**
CONSULTOR INFORMÁTICO

Personalmente me considero una persona con muchas inquietudes técnicas referentes al tema seguridad y siempre se aprende eso de la comunidad hacker. No he utilizado ese conocimiento para realizar incursiones que atenten por un lado la parte legal ni la información de las instituciones. Me inicié en este hobby en la universidad. Para mí fue un reto el dominar los sistemas aprendidos.
Al principio lo hice con un grupo de compañeros de clases. Queríamos lograr que los servidores del laboratorio donde recibíamos clases nos dejen la puerta abierta para crear cuentas adicionales de usuarios y enviar recordatorios a los amigos que utilizaban las otras máquinas.

ANEXO 5

LEY DE COMERCIO ELECTRÓNICO MENSAJES DE DATOS Y FIRMA DIGITAL

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS

Ley No. 67. RO Sup 557 de 17 de Abril del 2002.

CONGRESO NACIONAL

Considerando:

Que el uso de sistemas de información y de redes electrónicas, incluida la internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado;

Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos;

Que se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura;

Que a través del servicio de redes electrónicas, incluida la Internet, se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una ley especializada sobre la materia;

Que es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales; y,

En ejercicio de sus atribuciones, expide la siguiente.

LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS

TITULO PRELIMINAR

Art. 1.- Objeto de la ley.- Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

CAPITULO I

PRINCIPIOS GENERALES

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento.

Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Art. 4.- Propiedad intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto

profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.

Art. 6.- Información escrita.- Cuando la ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que este contenga sea accesible para su posterior consulta.

Art. 7.- Información original.- Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

Se considera que un mensaje de datos permanece integro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente.

Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Art. 8.- Conservación de los mensajes de datos.- Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

a. Que la información que contenga sea accesible para su posterior consulta;

b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;

c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,

d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

Art. .9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Art. 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguiente casos:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,

b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

Art. 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

a) Momento de emisión del mensaje de datos.- Cuando el mensaje de datos ingrese cuan sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto;

b) Momento de recepción del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,

c) Lugares de envío y recepción.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos.

Art. 12.- Duplicación del mensaje de datos.- Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

TITULO II

DE LAS FIRMAS ELECTRONICAS, CERTIFICADOS DE FIRMA ELECTRONICA, ENTIDADES DE CERTIFICACION DE INFORMACION, ORGANISMOS DE PROMOCION DE LOS SERVICIOS ELECTRONICOS, Y DE REGULACION Y CONTROL DE LAS ENTIDADES DE CERTIFICACION ACREDITADAS

CAPITULO I

DE LAS FIRMAS ELECTRONICAS

Art. 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba enjuicio.

Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular;

b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;

c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;

d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y,

e) Que la firma sea controlada por la persona a quien pertenece.

Art. 16.- La firma electrónica en un mensaje de datos.-

Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas, en dicho mensaje de datos, de acuerdo a lo determinado en la ley.

Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;

b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;

c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;

d) Verificar la exactitud de sus declaraciones;

e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;

f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,

g) Las demás señaladas en la ley y sus reglamentos.

Art. 18.- Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Art. 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por

: a) Voluntad de su titular;

b) Fallecimiento o incapacidad de su titular;

c) Disolución o liquidación de la persona jurídica, titular de la firma; y,

d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

CAPITULO II

DE LOS CERTIFICADOS DE FIRMA ELECTRONICA

Art. 20.- Certificado de firma electrónica.- Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Art. 21.- Uso el certificado de firma electrónica.- El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta ley y su reglamento.

Art. 22. - Requisitos del certificado de firma electrónica.- El Certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

a) Identificación de la entidad de certificación de información;

b) Domicilio legal de la entidad de certificación de información;

c) Los datos del titular del certificado que permitan su ubicación e identificación;

d) El método de verificación de la firma del titular del certificado;

e) Las fechas de emisión y expiración del certificado;

f) El número único de serie que identifica el certificado;

g) La firma electrónica de la entidad de certificación de información;

h) Las limitaciones o restricciones para los usos del certificado; e,

i) Los demás señalados en esta ley y los reglamentos.

Art. 23.- Duración del certificado de firma electrónica.- Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta ley.

Art. 24.- Extinción del certificado de firma electrónica.- Los certificados de firma electrónica, se extinguen, por las siguientes causas:

a) Solicitud de su titular;

b) Extinción de la firma electrónica, de conformidad con lo establecido en el artículo 19 de esta ley; y,

c) Expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Art. 25.- Suspensión del certificado de firma electrónica.- La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley;

b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,

c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Art. 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley, cuando:

a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,

b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada.

La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

Art. 27.- Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

Art. 28.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta ley y su reglamento.

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

CAPITULO III

DE LAS ENTIDADES DE CERTIFICACION DE INFORMACION

Art. 29.- Entidades de certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

Art. 30.- Obligaciones de las entidades de certificación de información acreditadas.- Son obligaciones de las entidades de certificación de información acreditadas:

a) Encontrarse legalmente constituidas, y estar registradas en Consejo Nacional de Telecomunicaciones;

b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;

c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información,

d) Mantener sistemas de respaldo de la información relativa a los certificados;

e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en esta ley;

f) Mantener una publicación del estado de los certificados electrónicos emitidos;

g) Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;

h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados; e,

i) Las demás establecidas en esta ley y los reglamentos.

Art. 31.- Responsabilidades de las entidades de certificación de información acreditadas.- Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no

hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.

Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio.

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Art. 33.- Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Conejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros.

Art. 34.- Terminación contractual.- La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor.

Art. 35.- Notificación de cesación de actividades.- Las entidades de certificación de información acreditadas, deberán notificar al Organismo de Control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto.

CAPITULO IV

DE LOS ORGANISMOS DE PROMOCION Y DIFUSION DE LOS SERVICIOS ELECTRONICOS, Y DE REGULACION Y CONTROL DE LAS ENTIDADES DE CERTIFICACION ACREDITADAS

Art. 36.- Organismo de promoción y difusión.- Para efectos de esta ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior.

Art. 37.- Organismo de regulación, autorización y registro de las entidades de certificación acreditadas.- El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas. En su calidad de organismo de autorización podrá además:

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones;

b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; y

c) Las demás atribuidas en la ley y en los reglamentos.

Art. 38.- Organismo de control de las entidades de certificación de información acreditadas.- Para efectos de esta ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas.

Art. 39.- Funciones del organismo de control.- Para el ejercicio de las atribuciones establecidas en esta ley, la Superintendencia de Telecomunicaciones tendrá las siguientes funciones:

a) Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y las prácticas comerciales restrictivas, competencia desleal y protección al consumidor, en los mercados atendidos por las entidades de certificación de información acreditadas;

b) Ejercer el control de las entidades de certificación de información acreditadas en el territorio nacional y velar por su eficiente funcionamiento;

c) Realizar auditorías técnicas a las entidades de certificación de información acreditadas;

d) Requerir de las entidades de certificación de información acreditadas, la información pertinente para el ejercicio de sus funciones;

e) Imponer de conformidad con la ley sanciones administrativas a las entidades de certificación de información acreditadas, en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio;

f) Emitir los informes motivados previstos en esta ley;

g) Disponer la suspensión de la prestación de servicios de certificación para impedir el cometimiento de una infracción; y,

h) Las demás atribuidas en la ley y en los reglamentos.

Art. 40.- Infracciones administrativas.- Para los efectos previstos en la presente ley, las infracciones administrativas se clasifican en leves y graves.

Infracciones leves:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por el organismo de control; y,

2. Cualquier otro incumplimiento de las obligaciones impuestas por esta ley y sus reglamentos a las entidades de certificación acreditadas.

Estas infracciones serán sancionadas, de acuerdo a los literales a) y b) del artículo siguiente.

Infracciones graves:

1. Uso indebido del certificado de firma electrónica por omisiones imputables a la entidad de certificación de información acreditada;

2. Omitir comunicar al organismo de control, de la existencia de actividades presuntamente ilícitas realizada por el destinatario del servicio;

3. Desacatar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción;

4. El incumplimiento de las resoluciones dictadas por los Organismos de Autorización Registro y Regulación, y de Control; y,

5. No permitir u obstruir la realización de auditorías técnicas por parte del organismo de control.

Estas infracciones se sancionarán de acuerdo a lo previsto en los literales c) y d) del artículo siguiente.

Las sanciones impuestas al infractor, por las infracciones graves y leves, no le eximen del cumplimiento de sus obligaciones.

Si los infractores fueren empleados de instituciones del sector público, las sanciones podrán extenderse a la suspensión, remoción o cancelación del cargo del infractor, en cuyo caso deberán observarse las normas previstas en la ley.

Para la cuantía de las multas, así como para la gradación de las demás sanciones, se tomará en cuenta:

a) La gravedad de las infracciones cometidas y su reincidencia;

b) El daño causado o el beneficio reportado al infractor; y,

c) La repercusión social de las infracciones.

Art. 41.- Sanciones.- La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

a) Amonestación escrita;

b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;

c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y,

d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica;

Art. 42.- Medidas cautelares, En los procedimientos instaurados por infracciones graves.- Se podrá solicitar a los órganos judiciales competentes, la

adopción de las medidas cautelares previstas en la ley que se estimen necesarias, para asegurar la eficacia de la resolución que definitivamente se dicte.

Art. 43.- Procedimiento.- El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones.

TITULO III

DE LOS SERVICIOS ELECTRONICOS, LA CONTRATACION ELECTRONICA Y TELEMATICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PUBLICOS

CAPITULO I

DE LOS SERVICIOS ELECTRONICOS

Art. 44.- Cumplimiento, de formalidades.- Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

CAPITULO II

DE LA CONTRATACION ELECTRONICA Y TELEMATICA

Art. 45.- Validez de los contratos electrónicos.- Los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Art. 46.- Perfeccionamiento y aceptación de los contratos electrónicos.- El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.

La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

Art. 47.- Jurisdicción.- En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario.

Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta ley y demás normas legales aplicables.

Cuando las partes pacten someter las controversias a un procedimiento arbitral en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje.

CAPITULO III

DE LOS DERECHOS DE LOS USUARIOS O CONSUMIDORES DE SERVICIOS ELECTRONICOS

Art. 48.- Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o

mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

Art. 49.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,

b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;

2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;

3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,

4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

Art. 50.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.

Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.

La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la internet, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.

En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o Servicio de que se trate.

En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente ley.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.

CAPITULO IV

DE LOS INSTRUMENTOS PUBLICOS

Art. 51.- Instrumentos públicos electrónicos.- Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente.

Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables.

TITULO IV

DE LA PRUEBA Y NOTIFICACIONES ELECTRONICAS

CAPITULO I

DE LA PRUEBA

Art. 52.- Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

Art. 53.- Presunción.- Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

Art. 54.- Práctica de la prueba.- La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;

b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de

firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados; y,

c) El facsímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

Art. 55.- Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Art. 56.- Notificaciones Electrónicas.- Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo

electrónico, de un abogado legalmente inscrito, en cualquiera de los Colegios de Abogados del Ecuador.

Las notificaciones a los representantes de las personas jurídicas del sector público y a los funcionarios del Ministerio Público que deben intervenir en los juicios, se harán en las oficinas que estos tuvieren o en el domicilio judicial electrónico en un correo electrónico que señalaren para el efecto.

TITULO V

DE LAS INFRACCIONES INFORMATICAS

CAPITULO I

DE LAS INFRACCIONES INFORMATICAS

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:

"**Art...-** El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art...- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Art. 59.- Sustitúyase el artículo 262 por el siguiente:

"**Art...- 262.-** Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo".

Art. 60.- A continuación del artículo 353, agréguese el siguiente artículo innumerado:

"**Art....-** Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

4.- El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.".

Art. 61.- A continuación del artículo 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"**Art...-** Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art...- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.".

Art. 62.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados:

"**Art...-** Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art...- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptadas;

3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,

5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

"... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

DISPOSICIONES GENERALES

Primera.- Los certificados de firmas electrónicas, emitidos por entidades de certificación de información extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.

Segunda.- Las entidades de certificación de información acreditadas podrán prestar servicios de sellado de tiempo. Este servicio deberá, ser acreditado técnicamente por el Consejo Nacional de Telecomunicaciones. El reglamento de aplicación de la ley recogerá los requisitos para este servicio.

Tercera.- Adhesión.- Ninguna persona está obligada a usar o aceptar mensajes de datos o firmas electrónicas, salvo que se adhiera voluntariamente en la forma prevista en esta ley.

Cuarta.- No se admitirá ninguna exclusión, restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en la presente ley y su reglamento.

Quinta.- Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor.

Sexta.- El Consejo Nacional de Telecomunicaciones tomará las medidas necesarias, para que no se afecten los derechos del titular del certificado o de terceros, cuando se produzca la revocatoria del certificado, por causa no atribuible al titular del mismo.

Séptima.- La prestación de servicios de certificación de información por parte de entidades de certificación de información acreditadas, requerirá de autorización previa y registro.

Octava.- El ejercicio de actividades establecidas en esta ley, por parte de instituciones públicas o privadas, no requerirá de nuevos requisitos o requisitos adicionales a los ya establecidos, para garantizar la eficiencia técnica y seguridad jurídica de los procedimientos e instrumentos empleados.

Novena.- Glosario de términos.- Para efectos de esta ley, los siguientes términos serán entendidos conforme se definen en este artículo:

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

Red electrónica de información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Servicio electrónico: Es toda actividad realizada a través de redes electrónicas de información.

Comercio electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley.

Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona,

organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Certificado electrónico de información: Es el mensaje de datos que contiene información de cualquier tipo.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Dispositivo de emisión: Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.

Emisor: Persona que origina un mensaje de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Quiebra técnica: Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta ley y su reglamento.

Factura electrónica: Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

Décima.- Para la fijación de la pena en los delitos tipificados mediante las presentes, reformas al Código Penal, contenidas en el Título V de esta ley, se tomarán en cuenta los siguientes criterios: el importe de lo defraudado, el quebranto económico causado, los medios empleados y cuantas otras circunstancias existan para valorar la infracción.

DISPOSICIONES TRANSITORIAS

Primera.- Hasta que se dicte el reglamento y más instrumentos de aplicación de esta ley, la prestación del servicio de sellado de tiempo, deberá cumplir con los requisitos de seguridad e inalterabilidad exigidos para la firma electrónica y los certificados electrónicos.

Segunda.- El cumplimiento del artículo 56 sobre las notificaciones al correo electrónico se hará cuando la infraestructura de la Función Judicial lo permita, correspondiendo al organismo competente de dicha Función organizar y reglamentar los cambios que sean necesarios para la aplicación de esta ley y sus normas conexas.

Para los casos sometidos a Mediación o Arbitraje por medios electrónicos, las notificaciones se efectuarán obligatoriamente en el domicilio judicial electrónico en un correo electrónico señalado por las partes.

DISPOSICION FINAL

El Presidente de la República, en el plazo previsto en la Constitución Política de la República, dictará el reglamento a la presente ley.

La presente ley entrará en vigencia a partir de su publicación en el Registro Oficial.

BIBLIOGRAFÍA

1. BUENAVENTURA, Ramón, *Las Respuestas, todo lo que usted siempre quiso preguntar sobre Internet,* Ed. Debate, Madrid, 1999
2. CABANELLAS, Guillermo, *Diccionario Enciclopédico de Derecho Usual,* Tomos, III, IV, VI, VII, Ed. HELIASTA, Edición No. 23
3. CARVAJAL, Ignacio, *Jurismatica,* Ed. Tinta & Papel, Quito, 2001
4. COBA, Santiago, *Los delitos informáticos en la legislación ecuatoriana,* Tesis PUCE, Quito, 2001
5. CORREA - NAZAR ESPECHE - CZAR DE ZALDUENO - BATTO, *Derecho Informático,* Ed. Depalma, Buenos Aires, 1994
6. FERNÁNDEZ DE CORDOVA, Pedro, *Estudios de Derecho Comparado,* Ed. Corporación de Estudios y Publicaciones, Quito, 2001
7. FERNÁNDEZ, Horacio, *Protección Jurídica del Software,* Ed. ABELEDO – PERROT, Buenos Aires, 2000
8. FERNÁNDEZ ALLER, Cecilia y Otro, *Informática para abogados,*
9. GUIBORG, Ricardo, *Manual de Informática Jurídica,*
10. GUERRERO, María Fernanda y Otros, *Penalización de la Criminalidad Informática,* Ed. Gustavo Ibáñez, Bogotá, 1998
11. JIMÉNEZ DE ASUA, Luis, *La Ley y el Delito,* Ed. Andrés Bello, Caracas, 1945
12. LEON, Fernando, *De la comunicación a la informática jurídica penal,* Ed. Doctrina y Ley, Bogotá, 2001

13. MAGGIORE, Guiseppe, *Derecho Penal,* Tomos I, IV, V, Ed. TEMIS, Bogotá, 1972

14. MAGLIONA, Claudio, y otra, *Delincuencia y Fraude Informático,* Ed. Jurídica de Chile, Santiago de Chile, 1999

15. PEÑARANDA, Héctor, *Iuscibernética: Interrelación entre el Derecho y la Informática,* Ed. FEDES, Maracaibo, 2001

16. RANIERI, Silvio, *Manual de Derecho Penal,* Tomos, I, V, VI, Ed. TEMIS, Bogotá, 1975

17. SABINO, Carlos, *Como hacer una tesis,* Ed. Panamericana, Bogotá, 2000

18. SOLANO, Orlando, *Manual de Informática Jurídica,* Ed. Gustavo Ibáñez, Bogotá, 1997

19. TÉLLEZ, Julio, *Derecho informático,* Ed. McGRAW-HILL, México, 1996

20. VIEGA, María José, *Un nuevo desafío jurídico: Los Delitos Informáticos*

21. ZABALA BAQUERIZO, Jorge, *Delitos contra la Propiedad,* Ed. EDINO, Bogotá

22. ZABALA BAQUERIZO, Jorge, *El Proceso Penal,* Ed. EDINO, Bogotá

23. Diccionario de Término de Computación, Ed. Pearson

24. CD ROOM, Enciclopedia Jurídica OMEBA

25. Constitución Política de la República del Ecuador

26. Código Penal Ecuatoriano

27. Código Civil Ecuatoriano

28. Código de Procedimiento Civil Ecuatoriano

29. Código de Procedimiento Penal Ecuatoriano

30. Ley de Propiedad Intelectual del Ecuador

31. Ley de Comercio Electrónico, mensajes de Datos y Firma Digital del Ecuador

32. Revista DESPERTAD, Mayo, 2001

33. Diario El Comercio

34. Diario La Gaceta

35. CD ROOM, Congresos de Derecho e Informática, Netley, Quito 2001

36. CD ROOM, Primer Congreso Mundial de Derecho Informático, Quito, 2001

37. www.stj-sin.gob.mx

38. http://tiny.uasnet.mx

39. www.ctv.es/USERS

40. www.dva.com.ar

41. www.delitos_informaticos.com

42. www.monografias.com

43. http://comunidad.derecho.org

44. www.it-cenit.arg.ar

45. www.minjus.gob.pe

46. www.dlh.hora.com.ec

47. www.legalia.com

48. www.bufetalmeida.com

49. http://personales.ciudad.com.ar

50. www.derecho-informatico.com

51. www.google.com

52. www.derecho.com

53. www.todaley.com

54. www.ulpiano.com/Recursos_delitos.htm

55. www.2600.com

56. www.omdi.com

57. www.alfa-redi.org

58. http://publicaciones.derecho.org

59. www.portaley.com

60. www.angelfire.com/la/legislaDir

61. http://fundesco.es

62. www.iacvt.com.ar/delitosinformaticos.htm

63. www.seguridad-la.com/e_delitos

64. www.bsa.org/europe-esp/policy/internet

65. www.eusKalnet.net/org/delitos

66. http://derechoinformatico.deamerica.net/?cat=Delitos