UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

SEMINARIO DE GRADUACIÓN EN CIENCIAS JURÍDICAS AÑO 2004

PLAN DE ESTUDIO 1993

LA PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS EN EL SALVADOR

TRABAJO DE GRADUACIÓN PARA OPTAR AL TÍTULO DE:

LICENCIADO EN CIENCIAS JURÍDICAS

PRESENTAN:

BENAVIDES SALAMANCA, LEO BLADIMIR

HERNÁNDEZ ANZORA, MARLON IBÁN

LEÓN ARDÓN, KENIA KATY

DIRECTORA DE SEMINARIO:

LICDA. STELLA DE LOS ANGELES PINEDA DE RODRÍGUEZ

CIUDAD UNIVERSITARIA, SAN SALVADOR, FEBRERO DE 2005

UNIVERSIDAD DE EL SALVADOR

RECTORA
DRA. MARÍA ISABEL RODRÍGUEZ

VICE-RECTOR ACADÉMICO
ING. JOAQUÍN ORLANDO MACHUCA GÓMEZ

VICE-RECTORA ADMINISTRATIVA
DRA. CARMEN ELIZABETH RODRÍGUEZ DE RIVAS

SECRETARIA GENERAL
LICDA. ALICIA MARGARITA RIVAS DE RECINOS

FISCAL GENERAL
LIC. PEDRO ROSALIO ESCOBAR CASTANEDA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

DECANA
LICDA. MORENA ELIZABETH NOCHEZ DE ALDANA

VICE-DECANO
LIC. OSCAR MAURICIO DUARTE GRANADOS

SECRETARIO
LIC. FRANCISCO ALBERTO GRANADOS HERNÁNDEZ

COORDINADORA DE LA UNIDAD DE SEMINARIO DE GRADUACIÓN
LICDA. BERTA ALICIA HERNÁNDEZ ÁGUILA

DIRECTORA DE SEMINARIO
LICDA. STELLA DE LOS ANGELES PINEDA DE RODRÍGUEZ

Te agradezco Madre, por haberme dado la vida con tu inagotable amor, por ser la mujer más bella que he conocido, porque todo lo que soy te lo debo a ti, por haberme enseñado que siempre debo seguir el camino de la verdad y hacer lo correcto conforme a mis convicciones e ideales, por enseñarme el valor de la vida, a ser ávido de conocimiento, a ser responsable, por brindarme tu ayuda cuando la necesito, por haberte sacrificado a cambio de mi felicidad, por ser mi ejemplo a seguir, por ser una excelente profesional…Madre, para ti siempre seré tu niño y te entregó mi corazón forjado por tu amor y sangre.

Te doy gracias Padre, por que siempre me has enseñado el bien, por ser mi padre amado, por mantener en alto tus ideales y convicciones, por instruirme en la vida, por preocuparte por mis problemas, porque nunca me fallaste, porque siempre puedo contar contigo, siempre estás ahí para mí, por ser modelo en mi vida, por siempre creer en mí y haberme apoyado en toda mi vida…Hombres como tú hay pocos, eres el padre ideal, y agradezco por tenerte en mi vida.

Padres, este trabajo es de ustedes, una muestra insignificante de todo lo que les agradezco, y de no ser por ustedes este triunfo no sería posible… los Amo.

Gracias a mi amada Ive, por todo el apoyo que me ha brindado, por haber estado presente cuando más te he necesitado, por escuchar siempre mis locuras y/o problemas, por todos los bellos momentos y el amor que me has dado…Gracias por todo, Te Amo.

Les agradezco a todos mis amigos(as), por estar conmigo en las buenas y en las malas, por haberme apoyado, por todos los momento de felicidad que hemos compartido, y muy especialmente, quiero agradecerles a Jaime, Nestor y Owyn, por esa amistad sincera que me han dado y por ser cómplices y secuaces de las diversas locuras que hemos hecho en esta vida… Gracias por ser mis amigos y estar siempre a mi lado, los quiero.

Gracias a mis compañeros de grupo por su apoyo y esmero para realizar un excelente trabajo, y juntos obtener este triunfo.

Y por último, pero no de menos, a todas las personas que me han ayudado y que forman parte de mi vida.

LEO BLADIMIR BENAVIDES SALAMANCA

ÍNDICE GENERAL

Pág.

INTRODUCCIÓN i

CAPITULO I

ANTECEDENTES HISTÓRICOS DE LA INFORMÁTICA Y DE LOS DELITOS INFORMÁTICOS

TITULO I

ANTECEDENTES DE LA INFORMÁTICA

1. La Informática. Generalidades 1

1.1. La Computadora y su historia 3

1.2. Antecedentes del Internet 20

1.3. Antecedentes del Internet en El Salvador 26

TITULO II

ANTECEDENTES DE LOS DELITOS INFORMÁTICOS

1. Surgimiento a nivel internacional 35

2. Diferentes definiciones de Delito Informático 38

2.1 Características de los Delitos Informáticos 42

2.2 Clasificación de los Delitos Informáticos 44

CAPITULO II

ANÁLISIS DE LOS TIPOS PENALES EN EL DERECHO COMPARADO

TITULO I

ANÁLISIS DE TIPOS PENALES

1. La Tipicidad y el Tipo 46

2. Tipos surgidos del Derecho Comparado 51

2.1. Bienes Jurídicos Protegidos 57

2.2. Sujetos de los Delitos Informáticos

2.2.1. El Sujeto Activo 65

2.2.2. El Sujeto Pasivo 83

3. Penas aplicadas a los delitos informáticos en el derecho comparado 85

3.1 Justificación de las penas 90

TÍTULO II

LEGISLACIÓN, NORMAS INTERNACIONALES, JURISPRUDENCIA Y CASOS EMBLEMÁTICOS SOBRE DELITOS INFORMÁTICOS

1. Países que actualmente cuentan con legislación sobre delitos informáticos 94

2. Regulación en el Derecho Internacional sobre Delitos Informáticos 117

3. Jurisprudencia y casos emblemáticos sobre Delitos Informáticos 122

CAPITULO III

ANÁLISIS DE DERECHO COMPARADO SOBRE DELITOS INFORMÁTICOS.

TÍTULO I

NECESIDAD DE LA TIPIFICACIÓN EN LA LEGISLACIÓN SALVADOREÑA

1. Análisis sobre la necesidad de la tipificación de delitos informáticos 151

1.1 ¿Son suficientes los tipos tradicionales del código penal para castigar acciones informáticas que dañan bienes jurídicos? 156

TÍTULO II

REGULACIÓN SOBRE DELITOS INFORMÁTICOS EN EL SALVADOR

1. Análisis sobre la regulación existente sobre delitos informáticos en El Salvador 160

2. Jerarquía de la legislación que los regulan 169

3. Aspectos no regulados con respecto al derecho comparado 170

CAPÍTULO IV

PROPUESTA PARA LA TIPIFICACIÓN DE DELITOS INFORMÁTICOS EN EL SALVADOR

TÍTULO I

FUNDAMENTACIÓN Y PROPUESTA DE LOS TIPOS PENALES

1. Hechos Históricos y perspectivas de futuro que justifican la necesidad de su tipificación 172

2. Fundamentación Constitucional para la regulación de los delitos informáticos 176

3. Inconveniencia de la dispersión e inflación jurídica: inclusión en el Código Penal 178

4. Propuestas de Tipos Penales a adoptarse en el Derecho Penal Salvadoreño 180

CAPITULO V

CONCLUSIONES

Conclusiones 192

BIBLIOGRAFÍA 194

CIBERBIBLIOGRAFÍA 197

INTRODUCCIÓN

En un momento de la historia en el que la informática penetra cada vez más el qué hacer de las instituciones públicas y privadas de nuestro país, es importante saber cómo enfrentarse a ella, pues todo el espacio, las facilidades y la velocidad que brinda esta tecnología, puede servir -como todo producto del ser humano-, para elevar la calidad de vida de la población salvadoreña, pero también puede ser utilizada para dañar o atacar aquellos valores más importantes para ésta.

En un país como el nuestro, en donde nos convertimos en eminentes receptores de esta tecnología, cuya introducción es siempre más lenta que en los países del primer mundo, debemos reaccionar ante las nuevas realidades sociales, culturales y, por supuesto, jurídicas, que esta penetración de tecnología provoca. Somos aquellos que formamos parte del gremio del derecho, a quienes nos corresponde detectar cuáles son las nuevas realidades y retos que la informática traerá a la sociedad, y en ese sentido, cómo se debe reaccionar desde el entramado jurídico para que dichos avances no se conviertan en dañinos para la sociedad, sino que por el contrario, sean fructíferamente utilizados para su beneficio.

En la medida que la tecnología de la informática entra a formar parte del qué hacer de las instituciones públicas y privadas de nuestro país, pasa a tener importancia clave para el desenvolvimiento de éstas, provocando que la mayoría de sus trámites, comunicación, información y diligencias se

realicen y archiven a través de esta tecnología, lo que hace que el manejo de ésta, pase a ser de suma importancia.

Otros países que ya han dado pasos más grandes en el desarrollo e implementación de la informática, han visto ya sus importantes beneficios, pero también los graves riesgos que implica la mala utilización de ésta, y es por eso que han profundizado en el análisis de las medidas que deben tomar para evitar estos riesgos, o al menos, cómo tratarlos cuando éstos ya se han efectuado. Es aquí donde el derecho debe jugar un papel importante, y particularmente el derecho penal, para intentar proteger aquellos bienes jurídicos que pueden ser perjudicados a través de la manipulación de la tecnología informática.

Las categorías de Delitos informáticos han nacido en países europeos con altos niveles de implementación y desarrollo informático, a través de los cuales han intentado estructurar normativas jurídico-penales que protejan a los bienes que pueden ser afectados a través de la informática. Es aquí que el derecho penal, procesal penal y la criminología tienen un gran reto, pues deben incorporar y reconocer nuevos conceptos, propios del desarrollo informático, así como también deben reconocer nuevas formas de proceder por parte de los delincuentes y sus posibles motivaciones, debiendo plantear soluciones jurídicas lo suficientemente depuradas para enfrentar un mundo que cambia constantemente y a velocidades estrepitosas, a través de las cuales puedan enmarcarse posibles nuevas mutaciones e innovaciones.

El derecho penal a nivel mundial, se ha enfrentado con la existencia de una tendencia claramente dominante en la legislación de varios países hacia la introducción de nuevos tipos penales, así como a una agravación de los ya existentes, que pueden englobarse en el marco general de la restricción, o la reinterpretación de las garantías clásicas del derecho penal sustantivo y del derecho procesal penal. Así también, esta tendencia ha creado nuevos bienes jurídico-penales, ha ampliado los espacios de riesgos jurídico-penalmente relevantes y ha flexibilizado las reglas de imputación, entre otros.

Es por ello, que como grupo de investigación nos hemos planteado como hipótesis principal que las actividades delincuenciales que pueden cometerse a través de la tecnología informática, no se encuentran suficientemente reguladas en el derecho penal salvadoreño, generando inseguridad jurídica para las personas naturales y jurídicas que la utilizan en su desempeño, e impunidad para quienes los cometen.

Para probar dicha hipótesis hemos desarrollado una investigación que contempla lo siguiente: *Capítulo I* - Antecedentes históricos de la informática y de los delitos informáticos, en el cual estudiaremos de manera breve aspectos relacionados a la Informática, La Computadora y su Historia, ya que es el instrumento principal en este tipo de delitos, Antecedentes de Internet, tanto mundial como en El Salvador, ya que el ciberespacio puede ser utilizado para la comisión de conductas ilícitas, y, se estudiará el Surgimiento de los Delitos Informáticos a nivel internacional,

así como definiciones, características y clasificación de los mismos; En el *Capítulo II* - Análisis de los tipos penales en el derecho comparado, se estudiará lo que respecta a los Tipos surgidos en el derecho comparado, los bienes jurídicos protegidos en esta clase de delitos, el sujeto activo y pasivo de los delitos informáticos, las penas y su justificación, y lo que se refiere a la legislación, normas internacionales, jurisprudencia y casos emblemáticos; En el *Capítulo III* - Análisis de derecho comparado sobre delitos informáticos, se estudiará lo que se refiere a la necesidad de tipificación de los delitos informáticos y si en realidad son suficientes los tipos penales tradicionales para sancionar estas acciones o delitos, la regulación existente en El Salvador sobre Delitos Informáticos, así como aspectos no regulados con respecto al derecho comparado; En el *Capítulo IV* - Propuesta para la tipificación de delitos informáticos en El Salvador, se estudiarán los hechos y perspectivas que justifican la tipificación de los Delitos Informáticos, la fundamentación constitucional para ello, la inconveniencia de la dispersión e inflación jurídica, y la propuesta de tipos penales a adoptar en el derecho salvadoreño; y, finalmente, en el *Capítulo V* – Conclusiones, se plantearán las conclusiones a las que hemos llegado como grupo durante la elaboración de la presente investigación.

Es por ello que a continuación podrán encontrar los razonamientos jurídicos, sociológicos y políticos en los que basamos las respuestas a nuestras hipótesis de trabajo, intentando aportar y generar una discusión teórico-jurídica sobre las nuevas realidades que plantea la informática, a las que inexorablemente debemos responder desde la perspectiva del derecho

penal, para así coadyuvar al imperio y profundización del Estado democrático de derecho por el cual ha apostado la sociedad salvadoreña.

LA PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS EN EL SALVADOR

CAPITULO I

ANTECEDENTES HISTÓRICOS DE LA INFORMÁTICA Y DE LOS DELITOS INFORMÁTICOS

TITULO I

ANTECEDENTES DE LA INFORMÁTICA

1. LA INFORMÁTICA. GENERALIDADES

La noción de "INFORMÁTICA", es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962.

En sentido general, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones.

Mora y Molino, la definen como un estudio que delimita las relaciones entre los medios es decir equipo, y los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado.

Mario G. Losano, caracteriza a la informática como un producto de la cibernética, en tanto un proceso científico relacionado con el tratamiento automatizado de la información en un plano interdisciplinario[1].

Derecho de la Informática

El Derecho a la Informática ha sido considerado por Valentín Carrascosa López como "el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas entorno a la informática y sus aplicaciones"[2]

Para Emilio Suñé, "es el conjunto de normas reguladoras del objeto informática o de problemas directamente relacionados con la misma"[3].

Para Juan José Ríos Estavillo, "es el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas"[4].

Julio Téllez Valdez, ha afirmado que "es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"[5].

---

[1] LOSANO, Mario G., Curso de Informática Jurídica, Tecnos. Madrid 1984.
[2] Citado por RÍOS ESTAVILLO, Juan José. "Derecho e Informática en México. Informática Jurídica y Derecho a la Informática", Universidad Nacional Autónoma de México, 1ª Edición, México, 1997, pág. 73
[3] Citado por RÍOS ESTAVILLO, Juan José, op. cit., pág. 73
[4] RÍOS ESTAVILLO, Juan José. op. cit., pág. 73
[5] TÉLLEZ Valdés, Julio. "Derecho Informático". Universidad Autónoma de México. 1ª Edición. México. 1991. Pág. 82

1.1. LA COMPUTADORA Y SU HISTORIA

El Ordenador o Computadora, es un dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

La computadora esta compuesta por dos elementos principales: el Hardware y el Software

El Hardware, es el equipo utilizado para el funcionamiento de una computadora. El hardware se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento. Los componentes de esas categorías están conectados a través de un conjunto de cables o circuitos llamados BUS[6] con el CPU[7] (Central Processing Unit por sus siglas en inglés, o Unidad Central de Procesamiento) del ordenador, y le proporciona capacidad de cálculo.

El soporte lógico o Software, en cambio, es el conjunto de instrucciones que un ordenador emplea para manipular datos: por ejemplo, un procesador de textos o un videojuego. Estos programas suelen almacenarse y transferirse al CPU, a

[6] Por BUS se entiende el conjunto de elementos de conexión que permiten la transmisión de información entre los distintos componentes de una computadora.

[7] Por CPU se entienden los circuitos que llevan a cabo los cálculos en las grandes computadoras; también se asigna este nombre al microprocesador integrado que cumple la misma función en máquinas de menor tamaño.

través del hardware de la computadora. El software también rige la forma en que se utiliza el hardware, como por ejemplo la forma de recuperar información de un dispositivo de almacenamiento. La interacción entre el hardware de entrada y de salida es controlada por un software llamado BIOS[8] (siglas en inglés de Basic Input Output System, o Sistema Básico de Entrada/Salida).

Aunque, técnicamente, los microprocesadores[9] todavía se consideran hardware, partes de su función también están asociadas con el software. Este hecho de que los microprocesadores presenten tanto aspectos de hardware como de software, hace que a veces se les aplique el término intermedio de microprogramación, o firmware[10].

Históricamente, el instrumento temprano de la informática más importante es el ábaco que ha sido conocido y ampliamente usado por más de 2,000 años. Simplemente es una percha de madera que sostiene alambres paralelos en los que se atan cuentas. Cuando estas cuentas se manipulan, siguen el alambre según reglas "programadas" que el usuario debe memorizar. Con base en estas, todas las operaciones de la aritmética ordinaria pueden realizarse. Otro instrumento de la informática, el astrolabio, también existía hace 2,000 años y se usaba para la navegación.

---

[8] El BIOS es el software básico que se encarga, tras encender el ordenador, de que éste se ponga en funcionamiento.

[9] El Microprocesador es un circuito constituido por millares de transistores integrados en un chip, que realiza alguna determinada función de los computadores electrónicos digitales.

[10] Por Firmware se entiende aquellos dispositivos que incorporan un software que controla algunos aspectos de su funcionamiento.

Blaise Pascal está ampliamente acreditado con la construcción de la primera "máquina calculadora digital" en 1642. Ésta realizaba sólo sumas de números entrada por medio de diales y se pensaba que ayudaba al padre de Pascal quien era un recolector de impuestos. En 1671, Gottfried Wilhelm von Leibniz inventó una computadora que se construyó en 1694, la cual podía sumar y, sumando sucesivamente y desplazando los dígitos del resultado, multiplicar. Leibniz inventó un mecanismo de "rueda escalonada" para introducir los sumandos, mecanismo todavía en uso. Los prototipos construidos por Leibniz y Pascal no se usaron ampliamente pero seguían siendo curiosidades después de hasta más de un siglo, cuando Tomas de Colmar (Charles Xavier Thomas) desarrolló (1820) la primera calculadora mecánica comercialmente exitosa que podía sumar, substraer, multiplicar, y dividir. Seguiría una sucesión de mejoras en las calculadoras mecánicas de escritorio por varios inventores, para que, aproximadamente por 1890, las operaciones disponibles incluyeran la acumulación de los resultados parciales, el almacenamiento y la reintroducción de resultados pasados, y la impresión de los resultados, cada uno requiriendo una iniciación manual. Estas mejoras fueron hechas para satisfacer a los usuarios comerciales, prestando muy poca atención a las necesidades de la ciencia, principalmente.

Mientras Tomas de Colmar estaba desarrollando la calculadora de escritorio, una serie de desarrollos muy notables en las computadoras comenzó en Cambridge, Inglaterra, debido a Charles Babagge. Charles Babbage (1793-

1871), visionario inglés y catedrático de Cambridge, hubiera podido acelerar el desarrollo de las computadoras si él y su mente inventiva hubieran nacido 100 años después. Adelantó la situación del hardware computacional al inventar la "máquina de diferencias", capaz de calcular tablas matemáticas. En 1834, cuando trabajaba en los avances de la máquina de diferencias Babbage concibió la idea de una "máquina analítica". En esencia, ésta era una computadora de propósitos generales. Conforme con su diseño, la máquina analítica de Babbage podía sumar, substraer, multiplicar y dividir en secuencia automática a una velocidad de 60 sumas por minuto. El diseño requería miles de engranes y mecanismos que cubrirían el área de un campo de fútbol y necesitaría accionarse por una locomotora. Los escépticos le pusieron el sobrenombre de "la locura de Babbage". Charles Babbage trabajó en su máquina analítica hasta su muerte. Los trazos detallados de Babbage describían las características incorporadas ahora en la moderna computadora electrónica. Las computadoras de Babbage jamás fueron completadas. Existieron varias razones para su fracaso, la mayoría frecuentemente asociadas a la falta de técnicas de maquinaria de precisión en el momento. Otra conjetura al respecto es que Babbage estaba trabajando en la solución de un problema que pocas personas en 1840 necesitaban resolver urgentemente.

Si Babbage hubiera vivido en la era de la tecnología electrónica y las partes de precisión, hubiera adelantado el nacimiento de la computadora electrónica por varías décadas. Irónicamente, su obra se olvidó a tal grado, que algunos pioneros en el desarrollo de la computadora electrónica ignoraron por completo

sus conceptos sobre memoria, impresoras, tarjetas perforadas y control de programa secuencial.

Un paso hacia el cómputo automatizado fue la introducción de tarjetas perforadas que se usaron para computar, por primera vez con éxito, en 1890 por Herman Hollerith y James Powers, trabajando para el Departamento del Censo de los E.U. Juntos desarrollaron dispositivos que podían leer la información que se había perforado en las tarjetas automáticamente, sin la intermediación humana. Se redujeron por consiguiente mayormente los errores de lectura, el flujo del trabajo se aumentó, y, de manera más importante, se pudieron usar pilas de tarjetas perforadas como una forma de almacenamiento de memoria accesible de capacidad casi ilimitada; además, diferentes problemas podían guardarse en diferentes lotes de tarjetas para trabajarse más adelante cuando fuera necesario. Hollertih fundó la Tabulating Machine Company y vendió sus productos en todo el mundo. La demanda de sus máquinas se extendió incluso hasta Rusia. El primer censo llevado a cabo en Rusia en 1897, se registró con el Tabulador de Hollerith. En 1911, la Tabulating Machine Company, al unirse con otras Compañías, formó la Computing-Tabulating-Recording-Company.

Los resultados de las máquinas tabuladoras tenían que llevarse al corriente por medios manuales, hasta que en 1919 la Computing-Tabulating-Recording-Company, anunció la aparición de la impresora/listadora. Esta innovación

revolucionó la manera en que las Compañías efectuaban sus operaciones. Para reflejar mejor el alcance de sus intereses comerciales, en 1924 la Compañía cambió el nombre por el de IBM (International Bussines Machines Corporation, por sus siglas en inglés, es decir Corporación Internacional de Máquinas de Negocios)

Durante décadas, desde mediados de los cincuentas la tecnología de las tarjetas perforadas se perfeccionó con la implantación de más dispositivos con capacidades más complejas. Dado que cada tarjeta contenía en general un registro (Un nombre, dirección, etc.) el procesamiento de la tarjeta perforada se conoció también como procesamiento de registro unitario.

Una antigua patente de un dispositivo que mucha gente creyó que era la primera computadora digital electrónica, se invalidó en 1973 por orden de un tribunal federal, y oficialmente se le dio el crédito a John V. Atanasoff como el inventor de la computadora digital electrónica. El Dr. Atanasoff, catedrático de la Universidad Estatal de Iowa, desarrolló la primera computadora digital electrónica entre los años de 1937 a 1942. Llamó a su invento la computadora Atanasoff-Berry, ó solo ABC (Atanasoff Berry Computer). Un estudiante graduado, Clifford Berry, fue una útil ayuda en la construcción de la computadora ABC.

Algunos autores consideran que no hay una sola persona a la que se le pueda atribuir el haber inventado la computadora, sino que fue el esfuerzo de muchas personas. Sin embargo en el antiguo edificio de Física de la Universidad de Iowa aparece una placa con la siguiente leyenda: "La primera computadora digital electrónica de operación automática del mundo, fue construida en este edificio en 1939 por John Vincent Atanasoff, matemático y físico de la Facultad de la Universidad, quien concibió la idea, y por Clifford Edward Berry, estudiante graduado de física."

Mauchly y Eckert, después de varias conversaciones con el Dr. Atanasoff, leer apuntes que describían los principios de la computadora ABC y verla en persona, el Dr. John W. Mauchly colaboró con J.Presper Eckert, Jr. para desarrollar una máquina que calculara tablas de trayectoria para el ejército estadounidense. El producto final, una computadora electrónica completamente operacional a gran escala, se terminó en 1946 y se llamó ENIAC (Por sus siglas en inglés, Electronic Numerical Integrator And Computer ó Integrador Numérico y Calculador Electrónico). La ENIAC construida para aplicaciones de la Segunda Guerra mundial, se terminó en 30 meses por un equipo de científicos que trabajan bajo reloj. La ENIAC, mil veces más veloz que sus predecesoras electromecánicas, irrumpió como un importante descubrimiento en la tecnología de la computación. Pesaba 30 toneladas y ocupaba un espacio de 450 metros cuadrados, llenaba un cuarto de 6 m x 12 m y contenía 18,000 bulbos, tenía que programarse manualmente

conectándola a 3 tableros que contenían más de 6,000 interruptores. La ENIAC requería una gran cantidad de electricidad. La leyenda cuenta que la ENIAC, construida en la Universidad de Pennsilvania, bajaba las luces de Filadelfia siempre que se activaba. La imponente escala y las numerosas aplicaciones generales de la ENIAC señalaron el comienzo de la primera generación de computadoras.

En 1945, John von Neumann, que había trabajado con Eckert y Mauchly en la Universidad de Pennsylvania, publicó un artículo acerca del almacenamiento de programas. El concepto de programa almacenado permitió la lectura de un programa dentro de la memoria de la computadora, y después la ejecución de las instrucciones del mismo sin tener que volverlas a escribir. La primera computadora en usar el citado concepto fue la llamada EDVAC (Por sus siglas en inglés, Eletronic Discrete-Variable Automatic Computer, es decir, Computadora Automática Electrónica de Variable Discreta), desarrollada por Von Neumann, Eckert y Mauchly.

Los programas almacenados dieron a las computadoras una flexibilidad y confiabilidad tremendas, haciéndolas más rápidas y menos sujetas a errores que los programas mecánicos.

Hasta este punto, los programas y datos podrían ser ingresados en la computadora sólo con la notación binaria, que es el único código que las

computadoras "entienden". El siguiente desarrollo importante en el diseño de las computadoras fueron los programas intérpretes, que permitían a las personas comunicarse con las computadoras utilizando medios distintos a los números binarios.

Primera Generación de Computadoras (1951 a 1958)

Las computadoras de la primera Generación emplearon bulbos para procesar información. Los operadores ingresaban los datos y programas en código especial por medio de tarjetas perforadas. El almacenamiento interno se lograba con un tambor que giraba rápidamente, sobre el cual un dispositivo de lectura/escritura colocaba marcas magnéticas. Esas computadoras de bulbos eran mucho más grandes y generaban más calor que los modelos contemporáneos.

Eckert y Mauchly contribuyeron al desarrollo de computadoras de la primera generación formando una compañía privada y construyendo UNIVAC I, que el Comité del censo utilizó para evaluar el censo de 1950. La IBM tenía el monopolio de los equipos de procesamiento de datos a base de tarjetas perforadas y estaba teniendo un gran auge en productos como rebanadores de carne, básculas para comestibles, relojes y otros artículos; sin embargo no había logrado el contrato para el Censo de 1950.

Comenzó entonces a construir computadoras electrónicas y su primera entrada fue con la IBM 701 en 1953. Después de un lento pero excitante comienzo la IBM 701 se convirtió en un producto comercialmente viable. Sin

embargo en 1954 fue introducido el modelo IBM 650, el cual es la razón por la que IBM disfruta hoy de una gran parte del mercado de las computadoras. La administración de la IBM asumió un gran riesgo y estimó una venta de 50 computadoras. Este número era mayor que la cantidad de computadoras instaladas en esa época en E.U. De hecho la IBM instaló 1000 computadoras. Aunque caras y de uso limitado las computadoras fueron aceptadas rápidamente por las Compañias privadas y de Gobierno. A la mitad de los años 50 IBM y Remington Rand se consolidaban como líderes en la fabricación de computadoras.

En 1952 Grace Murray Hoper una oficial de la Marina de E.U., desarrolló el primer compilador, un programa que puede traducir enunciados parecidos al inglés en un código binario comprensible para la maquina llamado COBOL (Common Business-Oriented Lenguage, por sus siglas en inglés, es decir, Lenguaje Común Orientado hacia Aplicaciones de Empresa).

Segunda Generación (1959-1964). El Transistor de Compatibilidad Limitada.

El invento del transistor hizo posible una nueva Generación de computadoras, más rápidas, más pequeñas y con menores necesidades de ventilación. Sin embargo el costo seguía siendo una porción significativa del presupuesto de una Compañía. Las computadoras de la segunda generación también utilizaban redes de núcleos magnéticos en lugar de tambores giratorios para el almacenamiento primario. Estos núcleos contenían pequeños anillos de

material magnético, enlazados entre sí, en los cuales podían almacenarse datos e instrucciones.

Los programas de computadoras también mejoraron. El COBOL desarrollado durante la primera generación estaba ya disponible comercialmente. Los programas escritos para una computadora podían transferirse a otra con un mínimo esfuerzo. El escribir un programa ya no requería entender plenamente el hardware de la computación. Las computadoras de la Segunda Generación eran sustancialmente más pequeñas y rápidas que las de bulbos, y se usaban para nuevas aplicaciones, como en los sistemas para reservación en líneas aéreas, control de tráfico aéreo y simulaciones para uso general. Las empresas comenzaron a aplicar las computadoras a tareas de almacenamiento de registros, como manejo de inventarios, nómina y contabilidad.

La marina de los Estados Unidos de Norteamérica utilizó las computadoras de la Segunda Generación para crear el primer simulador de vuelo. (Whirlwind I). HoneyWell se colocó como el primer competidor durante la segunda generación de computadoras. Burroughs, Univac, HoneyWell, los más grandes competidores de IBM durante los 60's se conocieron como el grupo BUNCH.

Tercera Generación (1964-1971). Circuitos Integrados, Compatibilidad con Equipo Mayor, Multiprogramación, Minicomputadora.

Las computadoras de la tercera generación emergieron con el desarrollo de los circuitos integrados (pastillas de silicio) en las cuales se colocan miles de componentes electrónicos, en una integración en miniatura. Las computadoras

nuevamente se hicieron más pequeñas, más rápidas, desprendían menos calor y eran energéticamente más eficientes.

Antes del advenimiento de los circuitos integrados, las computadoras estaban diseñadas para aplicaciones matemáticas o de negocios, pero no para las dos cosas. Los circuitos integrados permitieron a los fabricantes de computadoras incrementar la flexibilidad de los programas, y estandarizar sus modelos.

La IBM 360 una de las primeras computadoras comerciales que usó circuitos integrados, podía realizar tanto análisis numéricos como administración ó procesamiento de archivos.

Los clientes podían escalar sus sistemas 360 a modelos IBM de mayor tamaño y podían todavía correr sus programas actuales. Las computadoras trabajaban a tal velocidad que proporcionaban la capacidad de correr más de un programa de manera simultánea (multiprogramación).

Por ejemplo, la computadora podía estar calculando la nomina y aceptando pedidos al mismo tiempo.

Con la introducción del modelo 360, IBM acaparó el 70% del mercado, y para evitar competir directamente con IBM, la empresa Digital Equipment Corporation (DEC) redirigió sus esfuerzos hacia computadoras pequeñas. Mucho menos costosas de comprar y de operar que las computadoras grandes, las minicomputadoras se desarrollaron durante la segunda generación pero alcanzaron su mayor auge entre 1960 y 1970.

Cuarta Generación (1971 a la fecha). Microprocesador, Chips de memoria, Microminiaturización.

Dos mejoras en la tecnología de las computadoras marcan el inicio de la cuarta generación: el reemplazo de las memorias con núcleos magnéticos, por las de chips de silicio y la colocación de muchos más componentes en un Chip[11], esto producto de la microminiaturización de los circuitos electrónicos. El tamaño reducido del microprocesador y de chips hizo posible la creación de las computadoras personales.

Las tecnologías LSI (Integración a gran escala) y VLSI (integración a muy gran escala) permiten que cientos de miles de componentes electrónicos se almacenen en un chip. Usando VLSI, un fabricante puede hacer que una computadora pequeña rivalice con una computadora de la primera generación que ocupara un cuarto completo.

En la actualidad, la familia de procesadores Intel Pentium 4 con soporte a la Tecnología HT (Hyper-Threading) ofrece a los usuarios de computadoras de hogar y de oficina una experiencia computacional excepcional al mantener la computadora lista para responder de inmediato, mientras procesa otras tareas en un segundo plano. Por ejemplo, un usuario de hogar puede estar en un juego de inmersión mientras codifica audio o video, comprime imágenes o compone efectos especiales. Un gerente de tecnología informática puede ejecutar una aplicación en segundo plano como un escaneo constante de virus,

[11] Los chips son circuitos electrónicos complejos formados por componentes extremadamente pequeños formados en una única pieza plana de poco espesor de un material conocido como semiconductor.

la encriptación o compresión simultánea, mientras minimiza los trastornos para otros usuarios comprendidos en el mismo entorno computacional.

Intel Corporation lanzó nuevos procesadores basados en el proceso líder en la industria de 90 nanómetros[12], en producción de altos volúmenes. La tecnología de proceso de 90 nm es el proceso de fabricación de semiconductores más avanzado de la industria, construido exclusivamente en obleas de 300 mm. Este nuevo proceso combina mayor desempeño, transistores de menor consumo de energía, silicio forzado, interconectores de cobre de alta velocidad y nuevo material dieléctrico de bajo k. Esta es la primera vez que se integran todas estas tecnologías en un único proceso de fabricación. Los procesadores Intel Pentium 4 construidos con base en el proceso de 90 nm conservan las capacidades multi-tarea de la Tecnología Hyper-Threading (HT), e incluyen nuevas características como la microarquitectura Intel NetBurst mejorada, un caché[13] Nivel 2 (N2) más largo de 1 Mb[14] y 13 instrucciones nuevas.

Intel también ha acelerado la velocidad de su procesador Pentium 4 Extreme Edition con soporte a la Tecnología HT a 3.40 GHz[15]. Este procesador es construido en base a la tecnología de proceso de 0.13 micrones[16] de Intel, y

[12] Un nanómetro o nm, es la billonésima parte de un metro.
[13] El caché es una pequeña porción de memoria muy ágil que almacena los datos que se usan con mayor frecuencia, para que la cpu recurra a ella en vez de dirigirse a la memoria principal
[14] Mb es la abreviatura de Megabyte, unidad de medida de la memoria y la capacidad de almacenamiento de cualquier dispositivo de la computadora, y equivale a un millón de bytes, aproximadamente.
[15] Acrónimo de Gigahertz, el cual es una unidad de corriente alterna o frecuencia electromagnética de la onda, equivalente a mil millones de hertz (unidad de frecuencia de un ciclo por segundo), y mide la velocidad de los procesadores..
[16] Un micrón es igual a la millonésima parte de un metro.

está dirigido específicamente a jugadores de última generación y usuarios de alto poder computacional con sus 2 Mb de caché Nivel 3 (N3). Estos usuarios ahora pueden esperar una experiencia aún mejor cuando llevan a sus computadoras al límite de desempeño. El procesador Intel Pentium 4 Extreme Edition con Tecnología HT de 3.40 GHz ofrece el desempeño de procesador más elevado del mundo para sistemas de escritorio con Microsoft Windows XP.

Asimismo, el procesador AMD Athlon 64 FX integra una avanzada tecnología, la cual proporciona un extraordinario rendimiento y una incomparable experiencia de cómputo. El procesador AMD Athlon 64 FX opera bajo AMD64, una tecnología revolucionaria que 1) permite que el procesador ejecute aplicaciones de 32 bits[17] a gran velocidad, a la vez que el usuario efectúa la transición hacia la nueva generación de aplicaciones de software de 64 bits, y 2) proporciona protección optimizada contra virus (EVP) cuando se utiliza con la versión de Windows XP Service Pack 2 (SP2). La tecnología AMD64 abre las puertas hacia un nuevo y avanzado software de 64 bits y a un alto nivel de rendimiento del procesador. Los aficionados, jugadores y fanáticos que requieren poder puro pueden explotar todo el potencial de la tecnología AMD64, al mismo tiempo que disfrutan del extraordinario rendimiento del software de computadoras personales de hoy.

[17] Bit, en informática, acrónimo de Binary Digit (dígito binario), que adquiere el valor 1 o 0 en el sistema numérico binario. En el procesamiento y almacenamiento informático un bit es la unidad de información más pequeña manipulada por el ordenador, y está representada físicamente por un elemento como un único pulso enviado a través de un circuito, o bien como un pequeño punto en un disco magnético capaz de almacenar un 0 o un 1

La próxima generación de aplicaciones de juegos y creación de contenido digital exigirá un rendimiento excepcional, para ofrecer un extraordinario nivel de realismo, así como excelentes gráficos en tercera dimensión. Los sistemas basados en el procesador AMD Athlon 64 FX ofrecen un avanzado nivel de rendimiento para el software de entretenimiento y creación de contenido más exigente, tanto hoy como en el futuro. La tecnología AMD64 pone al alcance de los usuarios de PC[18] juegos verosímiles con gráficos de extraordinaria calidad tipo cinematográfica y edición de video de nivel profesional. Microsoft, Red Hat, SuSE y TurboLinux ya han anunciado sistemas operativos avanzados de 64 bits para la plataforma AMD64, los cuales se ejecutarán en procesadores con tecnología AMD64.

La protección EVP es una característica exclusiva de la tecnología AMD64. Esta función es habilitada por el sistema operativo, como por ejemplo el nuevo Windows XP SP2 y la Windows XP 64-bit Edition for Extended Systems, y está diseñada para contrarrestar un tipo malicioso de evento conocido como "desbordamiento del búfer" o "inundación del búfer". La protección EVP, junto con estos sistemas operativos, está diseñada para evitar que ciertos virus se esparzan, como MSBlaster y Slammer, reduciendo sustancialmente el costo e interrupciones asociados con virus similares, a la vez que optimiza la protección de computadoras e información personal para prevenir ciertos virus de PC.

[18] PC es el acrónimo de personal computer, es decir, computadora personal. Se utiliza para designar los ordenadores o computadoras personales.

El procesador AMD Athlon 64 FX es el único procesador de PC de 64 bits compatible con Windows y además es el procesador de PC más avanzado técnicamente en el mundo entero. Incluye innovaciones tecnológicas para que el usuario pueda disfrutar de una experiencia de cómputo realista y de calidad tipo cinematográfica. La arquitectura AMD64 duplica el número de registros SSE/SSE2 y de propósito general, para lograr un mejor rendimiento, a la vez que incrementa el procesamiento de multimedia con la tecnología 3DNow! Professional y la tecnología SSE2. La tecnología HyperTransport incrementa el rendimiento global del sistema, eliminando los cuellos de botella de E/S, aumentando el ancho de banda del sistema y disminuyendo la latencia. El controlador integrado de memoria DDR[19] de 128 bits, conjuntamente con la tecnología de memoria DDR estándar del mercado, proporcionan un ancho de banda superior de hasta 6.4 Gb[20] por segundo y reducen la latencia de memoria, lo cual mejora el rendimiento de prácticamente todas las aplicaciones. El procesador AMD Athlon 64 FX cuenta con el mejor sistema de memoria caché incorporado y de alto rendimiento para procesadores de PC del mercado, aumentando, de esta manera, el rendimiento de muchas aplicaciones, en especial, las que manejan grandes cargas de trabajo.

[19] Es un tipo de Memoria RAM (Memoria de acceso aleatorio o RAM, en informática, memoria basada en semiconductores que puede ser leída y escrita por el microprocesador u otros dispositivos de hardware tantas veces como se quiera) que trabaja al doble de velocidad en la transferencia de datos.

[20] Gb es el acrónimo de Gigabyte, y el significado exacto varía según el contexto en el que se aplique. En un sentido estricto, un gigabyte tiene mil millones de bytes. No obstante, y referido a computadoras, los bytes se indican con frecuencia en múltiplos de potencias de dos. Por lo tanto, un gigabyte puede ser bien 1.000 megabytes o 1.024 megabytes, siendo un megabyte 220 o 1.048.576 bytes.

1.2. ANTECEDENTES DEL INTERNET.

La definición que podemos dar del INTERNET, es que este no es un cuerpo físico o tangible, sino una red gigante que interconecta una innumerable cantidad de redes locales de computadoras. Es la red de redes.

También podemos considerar que Internet es un sistema internacional de intercambio de información que une a personas, instituciones, compañías y gobiernos alrededor del mundo, de manera casi instantánea, a través del cual es posible comunicarse, con un solo individuo, con un grupo amplio de personas interesadas en un tema específico o con el mundo en general. Es un medio de comunicación que tendrá un profundo efecto social, si tomamos en cuenta la teoría de la aldea global, del canadiense Marshall Muluhan.

En términos generales, Internet se ha convertido en un polémico escenario de contrastes en donde todo es posible: desde encontrar información de contenido invaluable, de alcances insospechados en el ámbito de la cultura, la ciencia y el desarrollo personal, hasta caer en el terreno del engaño, la estafa o la corrupción de menores.

Se calcula que Internet enlaza hoy día a 60 millones de computadoras personales en un extenso tejido electrónico mundial, lo cual hace necesario entenderla como un fenómeno social, dado el crecimiento exponencial que ha mostrado.

Entendiendo al Internet como la red de redes, donde como se mencionó entrelaza a 60 millones de computadoras personales a nivel mundial, sin tomar en cuenta la cantidad de personas que puedan conectarse a la red de redes sin tener una computadora personalizada, esto nos da una idea del desarrollo tan amplio que ha tenido en la última década. Así pues, se habla constantemente de los beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, más sin embargo, también dicho avance nos muestra otra cara de la moneda, siendo las conductas delictivas, pues se abrió la puerta a conductas antisociales que se manifiestan en formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas para infringir la ley, y ha creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

El inicio del INTERNET, se remonta a 1969, cuando la Agencia de Proyectos de Investigación Avanzada en Estados Unidos, conocida por sus siglas, "ARPA" (Advanced Research Projects Agency), desarrolló ARPANET, una especie de red que unía redes de cómputo del ejército y de laboratorios universitarios que hacían investigaciones sobre la defensa.

Esta red, permitió primero a los investigadores de Estados Unidos acceder y usar directamente súper computadoras localizadas en algunas universidades y laboratorios clave; después, compartir archivos y enviar correspondencia electrónica. A finales de 1970 se crearon redes cooperativas descentralizadas, como UUCP, una red de comunicación mundial basada en UNIX y USENET

(red de usuarios), la cual daba servicio a la comunidad universitaria y más adelante a algunas organizaciones comerciales.

En 1980, las redes más coordinadas, como CSNET (Acrónimo en inglés de Red de Ciencias de Cómputo), y BITNET (red de gran extensión que conecta instituciones de educación superior en E.E.U.U., usada principalmente para divulgar avances en investigaciones y noticias del ámbito académico. Su nombre proviene del inglés Because It´s Time Network, es decir, 'porque ya era hora'), empezaron a proporcionar redes de alcance nacional, a las comunidades académicas y de investigación, las cuales hicieron conexiones especiales que permitieron intercambiar información entre las diferentes comunidades. En 1986, se creó la Red de la Fundación Nacional de Ciencias (NSFNET, acrónimo en inglés), la cual unió en cinco macrocentros de computo a investigadores de diferentes Estados de Norte América, de este modo, esta red se expandió con gran rapidez, conectando redes académicas a más centro de investigación, remplazando así a ARPANET en el trabajo de redes de investigación. ARPANET se da de baja en marzo de 1990 y CSNET deja de existir en 1991, cediendo su lugar a INTERNET.

Esta red se diseñó para una serie descentralizada y autónoma de uniones de redes de computo, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa comercial alguna y con la habilidad

automática de reenrutar datos si una o más uniones individuales se dañan o están por alguna razón inaccesibles.

Cabe señalar que entre otros objetivos, el sistema redundante de la unión de computadoras se diseñó para permitir la continuación de investigaciones vitales y comunicación cuando algunas partes de ésta red se dañaran por cualquier causa.

Gracias al diseño de Internet, y a los protocolos de comunicación en los que se basan un mensaje enviado por éste medio puede viajar por cualquiera de diversas rutas, hasta llegar a su destino, y en caso de no encontrarlo, será reenrutado a su punto de origen en segundos.

Una de las razones del éxito de Internet, es su interoperatividad, es decir, su capacidad para hacer que diversos sistemas trabajen conjuntamente para comunicarse, siempre y cuando los equipos se adhieran a determinados estándares o protocolos, que no son sino reglas aceptadas para transmitir y recibir información.

Actualmente, cualquier persona puede ofrecer su propia página, un lugar virtual en el WWW[21] o abrir su propio foro de discusión, de los que hoy en día

[21] Acrónimo de World Wide Web, mecanismo proveedor de información electrónica para usuarios conectados a Internet.

existen alrededor de veinte mil y que abordan desde temas muy interesantes hasta muy deleznables, incluyendo comportamientos criminales.

El espíritu de la información que se maneja en Internet es que sea pública, libre y accesible a quien tenga la oportunidad de entrar a la red, lo cual marca un principio universalmente aceptado por los usuarios y que a dado lugar a una normativa sin fronteras y de lo cual podemos deducir, en términos jurídicos, cual sería la ratio iuris o razón de ser de esta especial normatividad.

Se intenta que Internet, sea, un medio interactivo viable para la libre expresión, la educación y el comercio. No existe institución académica, comercial, social o gubernamental que pueda administrarla. Son cientos de miles de operadores y redes de cómputo, que de manera independiente, deciden usar los protocolos de transferencia y recepción de datos para intercambiar comunicaciones, información. No existe un lugar que concentre o centralice la información de Internet. Sería técnicamente imposible.

Los individuos tienen una amplia gama de formas de introducirse al Internet, a través de los proveedores de acceso a Internet, conocidos en el medio de las telecomunicaciones como Internet Service Provider.

En términos de acceso físico, se puede usar una computadora personal, conectada directamente (por cable coaxial o de fibra óptica) a una red (un proveedor de servicios de Internet, por ejemplo), que éste a su vez, conectada a

Internet; o puede hacerse una computadora personal con un módem conectado a una línea telefónica a fin de enlazarse a través de ésta a una computadora más grande o a una red, que esté directa o indirectamente conectada a Internet.

Ambas formas de conexión son accesibles a las personas en una amplia variedad de Instituciones académicas, gubernamentales o comerciales. Lo cierto es que hoy en día el acceso a la red de Internet es cada vez más sencillo en Universidades, bibliotecas y cibercafeterías, lo cual está estrechamente relacionado con el número de proveedores de servicios de Internet.

Es previsible que el mundo virtual traiga consigo cambios de importancia en las instituciones jurídicas existentes, así como el desarrollo de instituciones jurídicas nuevas que regulen nuevos intereses y nuevas relaciones.

Los servicios mas importantes que brinda el INTERNET, en general son los siguientes: a) CORREO ELECTRÓNICO, siendo el servicio de mayor uso, de mayor tráfico y, por lo tanto, de mayor importancia para el surgimiento, en la actualidad, de diversas relaciones contractuales. Permite escribir y enviar mensajes a una persona o grupo de personas conectadas a la red; b) TRANSFERENCIA DE ARCHIVOS, el cual permite transferir archivos, los cuales pueden ser de texto, gráficas, hojas de cálculo, programas, sonido y vídeo. c) ACCESO REMOTO A RECURSOS DE COMPUTO POR INTERCONEXIÓN, (telnet), es una herramienta interactiva que permite

introducirse, desde una computadora en casa o en la oficina, a sistemas, programas y aplicaciones disponibles en otra computadora, generalmente ubicada a gran distancia y con gran capacidad; d) WORD WIDE WEB, el servicio más nuevo y popular de Internet, caracterizado por la interconexión de sistemas a través del hipertexto, por medio del cual pueden transmitirse textos, gráficas, animaciones, imágenes y sonido. Se le considera un elemento importante de mercadotecnia. e) GRUPOS DE DISCUSIÓN (Usenet), existen hoy día alrededor de quince mil grupos enfocados a diversos temas, en la actualidad se llega alrededor de cien mil mensajes por día; f) COMUNICACIÓN EN TIEMPO REAL, es la posibilidad de establecer diálogos inmediatos en tiempo real, a través de Internet, permitiendo a dos o más personas "dialogar" simultáneamente por escrito, sin importar la distancia geográfica. Esta forma de comunicación es análoga a la línea de teléfono, sólo que emplea el teclado o monitor en lugar del auricular.

1.3. ANTECEDENTES DEL INTERNET EN EL SALVADOR.

En septiembre de 1994 se gestionó, ante el IANA (Internet Assigned Numbers Authority, es decir, Autoridad de Número Asignados de Internet) y el InterNIC (Internet Network Information Center, es decir, Centro de Información de la Red Internet), respectivamente, un conjunto de direcciones IP, equivalentes a una clase B, y la administración del dominio de Nivel Superior correspondiente

a El Salvador, SV. Ese mismo mes y año, el grupo SVNet fue constituido por la Universidad Centroamericana UCA, el CONACYT (Consejo Nacional de Ciencia y Tecnología), la UES (Universidad de El Salvador), la Universidad Don Bosco, ANTEL (Agencia Nacional de Telecomunicaciones) y FUSADES (Fundación Salvadoreña del Desarrollo), con el fin de administrar ambos recursos.

En octubre de ese año se estableció un acuerdo con UUNet, en Virginia, EEUU, para manejar el tráfico de correo desde y hacia El Salvador, bajo el dominio SV. En diciembre se instaló y configuró exitosamente uno nodo UUCP (Unix to Unix Copy Program) de correo electrónico en el CONACYT con este propósito, y los primeros mensajes con direcciones terminadas en SV comenzaron a circular en Internet. Como anécdota curiosa, se puede referir que los primeros mensajes venían escritos en ruso, pues algunas personas pensaban que SV eran las siglas de la extinta Unión Soviética.

Anteriormente y junto a esta iniciativa, era posible intercambiar correos a través de Internet por vías tales como la ofrecida por ANTEL, usando el protocolo X.25, o a través de los servicios de otros nodos UUCP, como el llamado Huracán. La provisión del servicio de correo electrónico a los salvadoreños que así lo desearan, con direcciones SV, inició en marzo de 1995. Esto era realizado por medio de una llamada telefónica a medianoche a UUNet, en la que se intercambiaban los mensajes de y hacia nuestras direcciones SV y el resto del mundo.

En paralelo, y desde la constitución de SVNet, se había venido trabajando en la formulación de un proyecto a presentar a la OEA (Organización de Estados Americanos), en el marco del proyecto RedHUCyT (Red Hemisférica Universitaria de Ciencia y Tecnología). Finalmente, después de varias revisiones y ajustes, el proyecto salvadoreño fue presentado por SVNet a la OEA en septiembre de 1995.

Se llevaron a cabo varios eventos relacionados, entre ellos dos WorldNets, en la Embajada de los Estados Unidos (Julio y Octubre de 1995) con panelistas nacionales e internacionales vía satélite, varios cursos y seminarios organizados por diversas instituciones, un panel técnico sobre "Criterios para la gestión y desarrollo de la red Internet en El Salvador", y otros. La capacitación técnica a los miembros de SVNet fue realizada por los mismos salvadoreños, en noviembre.

Después del trabajo de conexión y pruebas realizadas en diciembre de 1995, ese mismo mes se firmó un convenio de mutua colaboración entre ANTEL y los demás miembros de SVNet, que posibilitó la instalación de líneas dedicadas a estas instituciones. Enero de 1996 vio un punto de presencia a Internet estable desde El Salvador, así como la recepción de los equipos que la OEA había financiado para iniciar la conectividad a Internet de nuestro país.

En febrero de 1996 ANTEL completó la instalación de los primeros enlaces dedicados a Internet en territorio salvadoreño, siendo éstos el de la

Universidad Centroamericana José Simeón Cañas y el de la Universidad Don Bosco. El siguiente mes vieron surgieron los sitios web[22] de estas dos universidades, así como los de SVNet y la página principal de El Salvador (www.sv), convirtiéndose así en los primeros sitios web de El Salvador que residían en un servidor ubicado fisicamente en El Salvador.

Desde entonces, el crecimiento de Internet en El Salvador ha sido, como en todo el mundo, gratamente acelerado.

En cuanto a la capacidad instalada, todos los proveedores de conectividad y servicios Internet han incrementado y modernizado continuamente dicha capacidad, motivados por la demanda, que también ha ido en crecimiento. Se estima que este crecimiento es del orden de un 20% anual. Por la misma razón, y para mantenerse activos en el mercado, todas las empresas desarrollan planes de expansión con una programación en el tiempo que consideran, acertadamente, una de sus piezas de información más celosamente guardadas.

En este campo, no es raro que las empresas vayan siendo absorbidas, vendidas o fusionadas por otras, en algunos casos internacionales, en otros por empresas que originalmente se hallan en otra línea de negocio pero desean explotar el servicio de conectividad en El Salvador.

[22] Un sitio web es una página multimedia basada en hipertextos que enlazan páginas sobre temas relacionados entre sí, aunque estén en diferentes servidores

Algunos de los equipos utilizados en la provisión del servicio por las empresas dedicadas a ello comprenden:

- Enrutadores Cisco 2500, 3600, 3640, 7206 para conexiones hacia proveedores y backbones.
- Equipos de enrutamiento Cisco 1720 para clientes dedicados.
- Equipos de Acceso Cisco AS5300 con capacidad de 4 E1s cada uno.
- Servidores Compaq para Mail Server, Web Server, Hosting, Monitoreo.
- Equipos con plataformas Solaris, Linux y AIX.

En cuanto a enlaces y anchos de banda, tanto hacia el exterior como los ofrecidos a clientes locales:

- Varios accesos a Internet, normalmente con redundancia entre enlaces satelitales y enlaces de fibra óptica.
- Si bien los anchos de banda hacia el exterior son variables de acuerdo al tamaño del proveedor, iniciando en 512 KBps, a manera de ejemplo, para una salida de 6 Mbps el tráfico mensual promedio es de 4,350 KBps.
- Los anchos de banda ofrecidos a clientes dedicados son, en su mayoría, de 128 KBps, pero también se proveen de 256 KBps, 512 KBps y más, siempre en múltiplos de 64 KBps. Se utilizan tecnologías de fibra óptica, cobre y microondas.
- Los precios de estos servicios oscilan alrededor de $350 a $ 700 mensuales por un enlace de 128 KBps, dependiendo del proveedor.
- El precio de instalación depende de la factibilidad técnica de cada cliente.

La cobertura de servicio provista se halla concentrada típicamente en San Salvador y probablemente algunas otras pocas localidades específicas del interior del país.

El servicio de acceso conmutado es ofrecido en forma gratuita por varios proveedores, quienes generan beneficios a partir del cobro de impulsos telefónicos y por medio de la venta de publicidad. También se presenta la modalidad de cobro por acceso conmutado, normalmente sin límite de uso. Algunas de las tasas que se emplean en los proveedores locales de acceso conmutado son de 6 líneas telefónicas por módem y 25 a 45 usuarios por módem. Hay enlaces “peer to peer” en forma bilateral entre algunos de los proveedores para intercambiar el tráfico que fluye entre ambos, con anchos de banda que van desde los 64 KBps hasta los 1024 KBps, dependiendo del tráfico observado.

Estos arreglos bilaterales, si bien solucionan el problema del intercambio de tráfico entre los proveedores involucrados sin utilizar el ancho de banda internacional contratado, resultan una alternativa ineficiente en el largo plazo. De ser extendido este esquema, cada proveedor debería contar con un enlace dedicado a cada uno de los demás proveedores, lo que haría incosteable la operación. De aquí que la mejor alternativa sea la instalación de un NAP, a lo que prácticamente la totalidad de proveedores se halla anuente.

Algunos de los servicios ofrecidos por las empresas consideradas Proveedores de Servicios Internet (ISPs) en el país son:

- Accesos conmutados
- Accesos dedicados
- Alojamiento de sitios Web (Web Hosting)
- Web TV
- Videoconferencia a través de IP
- Diseño de paginas Web
- Servicios de soporte a servidores de Internet
- Diseño, Instalación y configuración de redes LAN y WAN
- Asesoría en adquisición de sistemas de comunicación de datos
- Capacitación a empresas
- Desarrollo de aplicaciones orientadas o basadas en tecnología Internet, tales como Intranet y sistemas bancarios
- Telefonía Computarizada
- Servicios de acceso satelital

A diferencia de la telefonía, la provisión de servicios relacionados con Internet, como tales, no requieren de una autorización por parte de la Superintendencia General de Electricidad y Telecomunicaciones (SIGET). Esto ha propiciado que aun empresas de relativo pequeño tamaño, hayan visualizado éste como un negocio productivo, y se hallen decididos a perseverar y obtener una cuota importante de un mercado en continuo crecimiento, en El Salvador como en el resto del mundo.

En lo que tiene El Salvador de estar permanentemente conectado a Internet, como se dijo anteriormente, desde Febrero de 1996, y considerando la fecha presente, han llegado a existir más de veinte empresas proveedoras de servicios de conectividad a Internet. Algunas de estas empresas han sido absorbidas por otras, nacionales o internacionales, otras más han surgido en distintos años, y muchas de las empresas tienen entre sus actividades la provisión de otros servicios, desde el alojamiento de páginas Web hasta la telefonía tradicional (fija, móvil, internacional, o todas).

Algunas Empresas dedicadas a la provisión de servicios de conectividad a Internet, ordenadas según la fecha de surgimiento en el mercado nacional, como proveedores de Internet (Como es evidente al leer algunos nombres, algunas de estas empresas ya existían en el mercado nacional, ofreciendo algún otro tipo de servicios y/o productos. La fecha consignada es, en algunos casos aproximadamente, cuando iniciaron la oferta del servicio de conectividad a Internet) son:

Proveedor	Inicio de operaciones
CTE-ANTEL-Telecom	Enero 1996
NetCom S.A.	Marzo 1996
Insatelsa	Junio 1996
GBM	Junio 1996
EJJE	Febrero 1997

Vianet – IFX	Octubre 1997
CyTec	Diciembre 1997
SalNet	Diciembre 1997
SalTel	Abril 1998
Telecam	Junio 1998
QuickInternet	Julio 1998
CBNet	Agosto 1998
Telemóvil	Diciembre 1998
Telefónica El Salvador	Desconocido
Convergence	Desconocido
Cybernet	Desconocido
AmNet	Desconocido
Integra	Desconocido
Americatel	Desconocido
El Salvador On Line	Desconocido
Tutopía	Desconocido
Internet Gratis	Desconocido
NewCom	Desconocido
Intercom	Octubre 2001

TITULO II

ANTECEDENTES DE LOS DELITOS INFORMÁTICOS

1. SURGIMIENTO A NIVEL INTERNACIONAL

(1977) La primer propuesta de legislar el delito informático fue la introducida por el Senador Ribicoff en 1977 en el Congreso Federal de Estados Unidos. Años después, en 1983, la OECD (Acrónimo en inglés de Organization for Economic Co-operation and Development, es decir, Organización de Cooperación y Desarrollo Económico u OCDE) en París, designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los Códigos Penales. Como resultado de las propuestas de este comité, la OCDE recomendó a sus países miembros la modificación de su legislación penal, a los efectos de que la misma pueda aplicarse a ciertas categorías de delitos informáticos. La propuesta incluía una lista de actas que podían constituir un común denominador.

(1983) La Organización de Cooperación y Desarrollo Económico (OCDE u OECD, en su acrónimo en inglés) con el fin de proteger el uso indebido de programas de computación, inició un estudio sobre la posibilidad de armonizar las leyes penales en el plano internacional. Como consecuencia de dicho estudio en 1986 publicó un informe, llamado "Delitos de Informática: análisis

de la normativa jurídica" con las recomendaciones sobre cuales serian los usos indebidos que los distintos países podrían prohibir y sancionar a través de sus leyes penales.

(1989) El Consejo de Europa convocó a otro comité de expertos, que en la Recomendación número (89) 9 adoptada el 13 de septiembre de 1989, presenta una lista mínima de los delitos sobre los que debía necesariamente legislarse en cada país miembro, y una lista opcional.

(1990) El tema fue también discutido en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado en Montreal en 1990, en el octavo Congreso Criminal de las Naciones Unidas celebrado en La Habana el mismo año y en la Conferencia de Wurzburgo, Alemania, en 1992.

(1995) El Consejo de Europa adopta en Septiembre de 1995, otra recomendación concerniente a los problemas de derecho procesal conectados con la Información Tecnológica.

(1996) El Comité Europeo para los Problemas Criminales (CDPC, acrónimo en francés de Comité Européen pour les Problèmes Criminels) decidió en noviembre de 1996 establecer un nuevo comité de expertos para que se abordaran el tema de los delitos informáticos. Con relación a la decisión del CDPC, el Comité de Ministros estableció el nuevo comité denominado: "Comité

Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras (PC-CY)" por decisión nº CM/Del/Dec(97)583, tomada en la 583ª reunión de los Representantes de los Ministros (celebrada el 4 de febrero de 1997).

(1997- 2000) El Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras (PC-CY), inició su labor en abril de 1997 y efectuó negociaciones con respecto al borrador de un convenio internacional en materia de delitos informáticos. Entre abril de 1997 y diciembre de 2000, el Comité PC-CY celebró 10 reuniones plenarias y 15 reuniones de su Grupo de Redacción. Se levantó el secreto a una primer versión del borrador del Convenio y se la publicó en abril de 2000, seguida por borradores que fueron publicados después de cada reunión plenaria, con el fin de posibilitar que los Estados negociadores la realización de consultas con todas las partes interesadas. Este proceso de consulta resultó muy útil.

El borrador del Convenio revisado y finalizado y su Memorando Explicativo fue sometido para su aprobación al CDPC en su 50ª sesión plenaria en junio de 2001, después de lo cual el texto del borrador del Convenio fue sometido a consideración del Comité de Ministros para su aprobación y quedó abierto para su firma.

(1990's – Actualidad) Prácticamente desde la década de los años noventa distintos países del mundo comenzaron a regular en sus respectivos ordenamientos jurídicos lo concerniente a los delitos informáticos, con el fin de crear o establecer seguridad y prevenir esta nueva forma de criminalidad.

2. DIFERENTES DEFINICIONES DE DELITOS INFORMÁTICOS.

Para la comisión de las conductas delictivas denominadas "Delitos Informáticos", es indispensable el uso de la computadora y del manejo del Internet, sin embargo, aún en la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe una concepto propio de los llamados delitos informáticos. Aún cuando no existe dicha definición con carácter universal, se han formulado conceptos funcionales atendiendo a las realidades concretas de cada país.

Pero hay que hacer notar que dar un concepto de delitos informáticos no es tarea fácil, ya que su denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas, o sea contempladas en textos jurídico-penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país,

al igual que otros muchos, no ha sido objeto de tipificación aún; sin embargo, y habida cuenta de la necesidad de esto, emplearemos dicha alusión.

Asimismo, para lo que llamamos delitos informáticos, existen diversas acepciones, encontrando entre ellas las siguientes: Delitos electrónicos, Cibercrímenes, Ciberdelitos, Crímenes informáticos, etc., las cuales doctrinariamente son empleadas como sinónimos, por lo que puede emplearse cualquiera de estas acepciones.

Establecido lo anterior, algunas de las definiciones más comunes de delitos informáticos son las que se detallan a continuación:

El **Departamento de Investigación de la Universidad de México**, entiende que "delitos informáticos" son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático[23].

La **Organización para la Cooperación Económica y el Desarrollo (OCED)** lo define como: "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos"[24].

[23] Dirección Electrónica: http://www.aaba.org.ar/bi180p43.htm
[24] Dirección Electrónica: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Renato Javier Jijena Leiva lo define como: "... toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma"[25].

Julio Téllez Valdés, define el delito informático, en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"[26].

Maria de la Luz Lima define a los delitos electrónicos o informáticos "en un sentido amplio como cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[27] .

[25] JIJENA LEIVA, Renato Javier. Chile, la protección penal de la intimidad y el delito informático. Editorial Jurídica de Chile. Santiago de Chile. Pág. 88
[26] TÉLLEZ Valdés, Julio. Op. Cit., Pág. 82
[27] DE LA LUZ LIMA, María. "Delitos Electrónicos". Academia Mexicana de Ciencias Penales. Editorial Porrúa. No. 1-6. Año L. Enero-Junio 1984. Pág. 100

Nidia Callegari: define a los "delitos informáticos" como "aquellos que se dan con la ayuda de la informática o de técnicas anexas"[28].

Rafael Fernández Calvo: define a los "delitos informáticos" como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el titulo 1 de la Constitución Española"[29].

Carlo Sarzana, en su obra "Criminalitá e tecnología", dice que los crímenes por computadoras comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo"[30].

Teniendo en cuenta que delito, tal como lo establece Francisco Muñoz Conde, es *"toda acción u omisión típica, antijurídica, culpable y punible"*[31], desde nuestra perspectiva, podemos conceptualizar el delito informático como ***"toda***

---

[28] CALLEGARI, Nidia. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985. Pág. 115.

[29] FERNÁNDEZ CALVO, Rafael. "El tratamiento de llamado delito informático en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática)" en Informática y Derecho. Pág. 1150.

[30] SARZANA, Carlo. "Criminalità e tecnología", Computers Crime, Rassagna Penitenziaria e Criminologia. Nos. 1-2. Anno 1. Roma, Italia. Gennaio-Giugno, 1979. Pág. 59

[31] MUÑOZ CONDE, Francisco. Teoría General del Delito, 2ª edición, Editorial Temis S. A., 2001, pág. 4.

acción u omisión que se encuentra tipificada en la ley, y que mediante la aplicación de la tecnología informática afecta la información contenida en un sistema computarizado o el sistema como tal, y que origina la aplicación de una sanción o pena".

2.1. CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

En forma general, las principales características que revisten los Delitos informáticos son:

"a) Son Conductas criminógenas de cuello blanco.

b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

c) Son acciones de oportunidad, en cuanto a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.

e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i) Ofrecen facilidades para su comisión a los menores de edad.

j) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

k) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley"[32].

Por lo anterior, se puede apreciar que los que cometen este tipo de ilícitos (de cuello blanco), son personas con conocimientos sobre la informática y cibernética, los cuales, se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, como puede ser a instituciones crediticias o del gobierno, empresas o personas en lo particular, dañando en la mayoría de los casos el patrimonio de la víctima, así como su intimidad y dignidad, conductas que por la falta de una ley aplicable al caso concreto, no son denunciadas, quedando impunes estos tipos de conductas antisociales; siendo esto alarmante, pues como se mencionó en líneas precedentes este tipo de acciones tienden a proliferar y ser más comunes, por lo que se pretende en la presente investigación, es crear una conciencia sobre la necesidad urgente de regular estas conductas, ya que debe ser legislado de

[32] TÉLLEZ Valdés, Julio. Op. Cit., Págs. 82 y 83

una manera seria y honesta, recurriendo a las diferentes personalidades del conocimiento, tanto técnico en materia de computación, como en lo legal, ya que si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular.-

2.2. CLASIFICACIÓN DE DELITOS INFORMÁTICOS.

Los delitos informáticos han sido objeto de variadísimas clasificaciones, y se han tenido en cuenta a estos efectos:

· El perjuicio causado

· El papel que la computadora desempeña en la realización del mismo

· El modo de actuar del sujeto

· El tipo penal en que se encuadren los delitos

· Clase de actividad que implique según los datos involucrados.

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios:

· "Como instrumento o medio: referido a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

· Como fin u objetivo: se enmarcan a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física"[33].

María de la Luz Lima clasifica los delitos electrónicos en tres categorías, de acuerdo a como utilizan la tecnología electrónica:

· "Como método: cuando los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

· Como medio: en donde para realizar un delito utilizan una computadora como medio o símbolo.

· Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla"[34].

[33] TÉLLEZ Valdés, Julio. Op. Cit., Págs. 83 y 84
[34] DE LA LUZ LIMA, María. Op. Cit. Pág. 100

CAPÍTULO II

ANÁLISIS DE LOS TIPOS PENALES EN EL DERECHO COMPARADO

TÍTULO I

ANÁLISIS DE TIPOS PENALES

1. LA TIPICIDAD Y EL TIPO.

La Tipicidad es "la adecuación de un hecho cometido a la descripción que de ese hecho se hace en la ley penal. Ningún hecho por antijurídico y culpable que sea, puede llegar a la categoría de delito si, al mismo tiempo, no es típico, es decir, no corresponde a la descripción contenida en una norma penal"[35].

La Tipicidad o Infracción de una norma, por otra parte, puede tener lugar en forma Voluntaria, es decir, cuando el autor quiere realizar el hecho que infringe la norma, o no Voluntaria, pero expresando el desprecio del autor por los bienes que las normas protegen, es decir, el autor no se comporta con el cuidado exigido para evitar la lesión de bienes jurídicos. En el primer supuesto se habla de delitos dolosos, mientras que en el segundo se habla de delitos culposos.

---

[35] MUÑOZ CONDE, Francisco. Teoría General del Delito, segunda edición, Editorial Temis S. A., 2001, pág. 31.

Tipo es la descripción de la conducta prohibida que lleva a cabo el legislador en el supuesto de hecho de una norma penal[36].

El Tipo tiene en Derecho penal una triple función[37]:

Una función seleccionadora de los comportamientos humanos penalmente relevantes.

Una función de garantía, en la medida que sólo los comportamientos subsumibles en él pueden ser sancionados penalmente.

Una función motivadora general, por cuanto con la descripción de los comportamientos en el tipo Penal el legislador indica a los ciudadanos que comportamientos están prohibidos y espera que con la conminación penal contenida en los tipos, los ciudadanos se abstengan de realizar la conducta prohibida, la materia de prohibición.

Se puede entender por Tipo Penal la descripción objetiva y material de la conducta prohibida.

Estructura y Composición de los Tipos Penales.

El Tipo se formula en expresiones lingüísticas que, con mayor o menor acierto, intentan describir, con las debidas notas de abstracción y generalidad, la conducta prohibida.

[36] Ídem., pág. 32
[37] Ídem.

Para cumplir con su función de garantía, el Tipo tiene que estar redactado de tal modo que de su texto se pueda deducir con claridad la conducta prohibida. Para ello hay que utilizar un lenguaje claro y preciso asequible al nivel cultural medio. Hay que ser moderado en la utilización de Elementos Normativos (acreedor, insolvencia, ajenidad, etc.), que implican siempre una valorización y, por eso, un cierto grado de subjetivismo y emplear sobre todo Elementos Lingüísticos Descriptivos que cualquiera pueda apreciar o conocer en su significado sin mayor esfuerzo (matar, daños, lesiones, etc.); Debe evitarse en lo posible el Casuismo en la descripción de conductas prohibidas; Es preferible utilizar Cláusulas Generales, definiciones y descripciones genéricas que reúnan los caracteres comunes esenciales a cada grupo de delitos; Deben evitarse los Conceptos Indeterminados (moral, buenas costumbres) por el peligro que representan para la seguridad jurídica de los ciudadanos, al dejar sin precisar claramente la conducta prohibida[38].

Los elementos que siempre están presentes en la Composición de todos los Tipos son:

Sujeto Activo. El delito como obra humana siempre tiene un autor, aquel que precisamente realiza la acción prohibida. Normalmente en el Tipo se alude a dicho sujeto con expresiones impersonales como “el que”, “quien” o “los que”.

Acción. En todo Tipo hay una acción, entendida como comportamiento humano (acción u omisión), que constituye el núcleo del Tipo, su elemento

[38] MUÑOZ CONDE, Francisco; García Arán, Mercedes: “Derecho Penal” (Parte General), 2ª Edición, Temis, 1995, págs. 274 y 275

más importante. La acción viene descrita generalmente por un verbo (matare, maltratare, mutilare, etc.), que puede indicar una acción positiva o una omisión.

Bien Jurídico. La Norma Penal tiene una función protectora de bienes jurídicos. Para cumplir esta función protectora eleva a la categoría de delitos, por medio de su tipificación legal, aquellos comportamientos que más gravemente lesionan o ponen en peligro los bienes jurídicos protegidos. El bien jurídico, es por tanto, la clave que permite descubrir la naturaleza del Tipo, dándole sentido y fundamento. Todo tipo de delito debe incluir un comportamiento humano capaz de provocar la puesta en peligro o la lesión de un bien jurídico.

Diferencia entre Tipo y Tipicidad

Tipo es la descripción de la conducta prohibida que lleva a cabo el legislador en el supuesto de hecho de una norma penal.

Tipicidad es la cualidad que se atribuye a un comportamiento cuando es subsumible en el supuesto de hecho de una norma penal.

El concepto de Tipicidad no es exclusivo del Derecho Penal – aunque dentro de este campo sea más conocido – ya que el Estado, como regulador de la convivencia humana, provee por medio de sus ordenamientos jurídicos una

serie de disposiciones con impacto sobre la de los individuos en el seno de la sociedad. Ocurre que, a pesar de ese afán por alcanzar la armonía jurídico social, hay conductas que rompen con ese equilibrio pretendido. Si estas conductas desviadas de los lineamientos normativos traen como consecuencia una perturbación del orden social, habrá que clasificarlas según la "naturaleza" de la relación y del orden que menoscaben (ya se trate de interese particulares o públicos)[39].

Si la perturbación rompe con el orden social entre particulares, o lesiona levemente bienes que no son relevantes para el Derecho Penal tendrá por respuesta una regulación normativa privada. En sentido contrario, si la perturbación de ese orden social es grave o pone en peligro bienes jurídicos vitales, tal hecho trasciende al derecho privado y entra en el campo del Derecho Penal[40].

Se concluye para el caso que la naturaleza jurídica de la tipicidad va a estar dada en relación a la naturaleza del propio ordenamiento jurídico, por ello, cuando una conducta típica pertenece a la esfera del Derecho Penal, no puede sino admitirse que la naturaleza jurídica de la Tipicidad es de orden Público[41].

---

[39] TREJO ESCOBAR, Miguel Alberto; Serrano, Armando Antonio, y Otros: "Manual de Derecho Penal" (Parte General), 2ª edición, Centro de Información Jurídica, Ministerio de Justicia, S.S., El Salvador, 1996, pág. 226

[40] Ídem.

[41] Ídem., pág. 227

2. TIPOS SURGIDOS DEL DERECHO COMPARADO.

Los tipos o clases de Cibercrímenes o Delitos Informáticos reconocidos por la Organización de las Naciones Unidas (ONU)[42] son los siguientes:

A. Fraudes cometidos mediante manipulación de computadoras.

a) Manipulación de los datos de entrada[43]: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Podemos decir o aclarar que este delito consiste en la manipulación que se hace en la transferencia de entrada o en los datos de entrada con el fin de introducir datos falsos, o sustrayendo la entrada de datos reales que debieron haber sido ingresados. El procesamiento de los datos es el correcto, lo que es incorrecto o erróneo son los datos, lo cual produce un resultado inexacto. Un ejemplo de este ilícito es el hecho de crear o ingresar una cartera ficticia de proveedores en el sistema informático, a los cuales se les realizan los abonos o pagos correspondientes, obteniendo el autor de esa cartera ficticia un beneficio económico.

---

[42] Dirección Electrónica: http://www.seguridad-la.com/e_delitos_un.htm

[43] Por Datos de Entrada se entiende todo lo que es ingresado a la Computadora u Ordenador

b) La manipulación de programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c) Manipulación de los datos de salida[44]: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

d) Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salchichón o de salami, en la que "rodajas muy finas"

[44] Salida o Datos de Salida son datos que ya han sido procesados y convertidos en una forma más util que ahora se llama Información.

apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

B. Falsificaciones informáticas.

a) Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.

b) Como instrumentos: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

C. Daños o modificaciones de programas o datos computarizados.

a) Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar

el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

i) Virus: es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

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

iii) Bomba lógica o cronológica: exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su

"detonación" puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

b) Acceso no autorizado a servicios y sistemas informáticos: se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

i) Piratas informáticos o hackers: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

c) Reproducción no autorizada de programas informáticos de protección legal: ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado

dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

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

a) Acceso no autorizado: uso ilegitimo de contraseñas y la entrada de un sistema informático sin la autorización del propietario.

b) Destrucción de datos: los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

c) Infracción al copyright de bases de datos: uso no autorizado de información almacenada en una base de datos.

d) Interceptación de correo electrónico: lectura de un mensaje electrónico ajeno.

e) Estafas electrónicas: a través de compras realizadas haciendo uso de la red.

f) Transferencias de fondos: engaños en la realización de actividades bancarias electrónicas.

Asimismo, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

a) Espionaje: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

b) Terrorismo: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

c) Narcotráfico: transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

d) Otros delitos: las mismas ventajas que encuentran en el Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa.

2.1. BIENES JURÍDICOS PROTEGIDOS.

El bien jurídico, en sentido general, es aquel bien que el derecho ampara o protege. Su carácter jurídico deviene de la creación de una norma jurídica que prescribe una pena o sanción para toda conducta que pueda lesionar dicho bien. Sin la existencia de esa norma, que tiene que estar vigente y ser eficaz, el bien pierde su carácter jurídico.

Con una intención puramente didáctica, puede decirse que el concepto preanunciado adquiere mayor relieve y claridad dentro del derecho penal, puesto que la represión de cada uno de los delitos tipificados en la ley penal protege de una manera inmediata y directa a los bienes jurídicamente tutelados por todo el ordenamiento; así por ejemplo, por medio del delito de homicidio se protege la vida; por medio de las injurias, el honor; por medio de la violación, la libertad sexual; etcétera.

Sin perjuicio de lo expuesto, no debe olvidarse que sea cual fuere la identidad de una norma, esta protege el bien jurídico determinado por el legislador. Esta protección es brindada por todo el ordenamiento jurídico, puesto que sería contradictorio el supuesto de que por un lado se proteja la vida y por el otro se tolere el asesinato.

Una distinción es necesaria. Cuando hablamos de "bienes jurídicos" conculcados por un delito aludimos a valores esenciales para la sociedad que, por su importancia, el derecho penal los protege mediante la tipificación o consagración de hipótesis, casos o conductas que atentan en su contra. Es diferente en ciencia jurídica cuando hablamos de "objeto material", porque nos referimos a la cosa o persona sobre la cual recae la conducta típica, al llamado "cuerpo del delito", a la casa destruida, al auto robado, a la persona injuriada, etcétera.

Como hemos mencionado anteriormente, la informática nos rodea y se encuentra inmersa en todos los aspectos de la vida del hombre, generándose lo que se conoce como computer dependency o dependencia computacional. La informática se presenta como una nueva forma de poder, que puede estar concentrado o difuminado en una sociedad, confiado a la iniciativa privada o reservado al monopolio estatal. Es instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva forma de energía, si se quiere intelectual, de valor inconmensurable, que potencia y multiplica de manera insospechada las posibilidades de desarrollo científico y social, erigiéndose en patrimonio universal de la humanidad.

No es ninguna revelación señalar que gran parte de los sistemas -algunos de ellos vitales- que se utilizan en la vida cotidiana funcionan basándose en sistemas de tratamiento automatizado de la información (sistemas de control de potabilización del agua, bases militares, controladores de vuelo, televisión, mercados financieros, gestión gubernamental, control de tránsito, bases de datos personales, industria, educación, democracia digital, redes de comunicación, etcétera. Siguiendo al sociólogo español Manuel Castells[45], podemos afirmar que este fenómeno ha derivado en un nuevo entramado social. Podemos citar, asimismo, el cambio que producen las tecnologías de información, respecto al funcionamiento del capital. Y aquí también, muy esquemáticamente, destacamos que el centro de la economía global son los

[45] "Globalización, sociedad y política en la era de la información", Ponencia presentada por el autor en el Auditorio León de Greiff de la Universidad Nacional de Colombia el 7 de mayo de 1999

mercados financieros globalizados que funcionan mediante conexiones entre ordenadores. Esta red es lo que subyace en la articulación, la interdependencia y también en la volatilidad del mercado global financiero y en el desarrollo vertiginoso de la transacción financiera electrónica.

El citado sociólogo nos dice que también la sociedad se ha transformado, constituyéndose en lo que se conoce como Sociedad Red, en donde el fenómeno de las nuevas tecnologías de la comunicación (en especial Internet) conforma la base material y tecnológica que la sustenta. Debemos señalar que, si bien es el comportamiento social e individual el que moldea a Internet, ésta termina identificándose con la sociedad misma, con el "tejido de nuestras vidas", en un nuevo y potentísimo vehículo de la interacción social, que objetiva nuestra realidad pese a su virtualidad. En conclusión, para Castells, Internet es la sociedad, y es, a la vez, la infraestructura tecnológica y el medio organizativo que permite el desarrollo de una serie de nuevas formas de relación social que no tienen su origen Internet, sino que son fruto de una serie de cambios históricos, pero que no podrían desarrollarse sin Internet, puesto que suponen una construcción social en torno a las redes de información, como bien de altísimo valor para el tráfico jurídico y económico. Ahora bien, esta evolución, naturalmente, tiene su aspecto negativo. En efecto, la informática ha abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional.

En consonancia con lo expuesto en el punto anterior, consideramos que el bien jurídico tutelado en los delitos informáticos, es la Información en sí misma, en toda su amplitud (titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad), sin perjuicio de que con su ataque, subsidiariamente y tratándose de un interés colectivo, afecte otros bienes jurídicos como la intimidad o la propiedad.

Debemos señalar que a los efectos de no violentar los principios constitucionales de legalidad y reserva tipificando como delitos conductas que no implican una real afectación o un concreto peligro sobre un interés social, deberá tenerse presente que el derecho penal es la última "ratio" del orden normativo, el último instrumento de control social, a disposición del Estado para la prevención de la criminalidad, por lo que su utilización debe limitarse a la intervención necesaria, mínima, para preservar la convivencia humana en la comunidad. La norma penal tiene una función protectora de bienes jurídicos y para cumplir dicha función, eleva a la categoría de delito, por medio de la tipificación legal, aquellos comportamientos que más gravemente los lesionan o ponen en peligro.

En cuanto al bien jurídico en sí, compartimos los alcances de las concepciones trascendentes, en cuanto a que la realidad social es la que le otorga su contenido. Los bienes jurídicos son intereses vitales del individuo o la comunidad, el orden no puede crearlo, lo crea la vida, pero la protección del

Derecho eleva el interés vital a bien jurídico. En definitiva, entendemos que el bien jurídico en los delitos informáticos es la información en sí misma, en todos sus aspectos, como interés macro-social o colectivo, porque su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos. Disentimos, acorde con la postura sustentada en torno al bien jurídico tutelado en los delitos informáticos, con las tradicionales distinciones doctrinales de estas conductas ilícitas en delitos informáticos de carácter económico y aquellos que atentan contra la privacidad.

En primer lugar, porque toda la información -aún la privada- posee un valor apreciable económicamente y en segundo, porque los intereses vulnerados superan el marco meramente patrimonial, verificándose un verdadero carácter pluriofensivo de las conductas disvaliosas, por implicar afectación de cuestiones que atañen a la seguridad y a la confianza en el correcto funcionamiento de los sistemas informáticos que repercuten en la vida social colectiva. Por otra parte, tal reduccionismo haría innecesaria la creación de la categoría de los delitos informáticos, puesto que no serían más que delitos contra la propiedad, o bien, contra la intimidad o privacidad. Con el mismo criterio equívoco para nosotros, Klaus Tiedemann señala que, “con la expresión criminalidad mediante computadoras (adviértase que en el ámbito tecnológico actual las computadoras u ordenadores tal como los conocemos se encuentran casi obsoletos), se alude a todos los actos, antijurídicos según la ley penal

vigente (lo cual no significa más que decir que los delitos informáticos no son otros que los que la ley define como tal), realizados con el empleo de un equipo automático de procesamiento de datos"[46].

Esta definición lleva al absurdo de calificar como delito informático o "criminalidad mediante computadoras" (término por demás deficiente para abarcar el fenómeno en estudio) a la acción de matar a una persona aplicándole un golpe con un equipo de computación (un CPU por ejemplo). Los delitos informáticos se realizan necesariamente con la ayuda de sistemas informáticos o tecnologías similares, pero tienen como objeto del injusto la información en sí misma, la cual, como expresamos, posee múltiples características que trascienden lo meramente económico o confidencial.

En el Primer Congreso Andino de Derecho e Informática, celebrado en marzo de 2001 en Venezuela, el Director de la Revista Electrónica de Derecho Penal, el profesor peruano Luís Miguel Reyna Alfaro, propuso en su ponencia que se incorporara como bien jurídico objeto de tutela la "información", tratándose de conductas cometidas valiéndose de medios informáticos. Algunos de los argumentos expuestos en su escrito fueron los siguientes[47]: "el punto de partida y también de más difícil resolución es el de la identificación del bien jurídico penalmente tutelado, lo que nos lleva a escudriñar si el delito informático en realidad protege algún nuevo interés social, todas estas

[46] TIEDEMANN, Klaus, "Poder Económico y Delito", Editorial Ariel, Barcelona, 1985, pág. 122.
[47] Dirección Electrónica: http://dragonjar.nolimites.net/HTM/DragoN.php?subaction=showfull&id=1088639499&archive=&start_from=&ucat=3&Abrir=Portada

cuestiones son planteadas en el presente trabajo apostando por la idea, ya expuesta por la profesora española Gutiérrez Francés, de entender que el bien jurídico que pone en peligro el delito informático es la información: (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos). Los constantes avances tecnológicos en materia informática han propiciado la aparición de nuevos conceptos, generando así mismo la modificación de otros tantos, enriqueciéndolos la mayoría de ocasiones, así el contenido del término 'información', que según la definición de la Real Academia de la Lengua Española significa: 'enterar, dar noticia de algo' y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose como advierte Gutiérrez Francés: 'en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico'. Hoy en día no resulta suficiente poseer la información, es necesario además tener la capacidad de almacenarla, tratarla y transmitirla eficientemente, de allí que 'la información' deba ser entendida como un proceso en el cual se englobe los tres supuestos (almacenamiento, tratamiento y transmisión). Así podemos decir que el interés social digno de tutela penal sería: la información (almacenada, tratada y transmitida a través de sistemas informáticos)".

Podemos concluir que los delitos informáticos recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro-social (abarcativo de otros intereses,

como por ejemplo la propiedad común, intimidad, etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas. Es decir, que la Información es un Bien Jurídico que puede considerarse como de interés colectivo tutelado penalmente de forma conjunta con bienes de los particulares, siendo ambos de carácter homogéneo o estando situados en la misma línea de ataque, por lo que hay una relación medial entre el derecho a la información como bien colectivo y los derechos individuales que pueden verse afectados. El primero es medio o paso previo necesario para la lesión o puesta en peligro de los segundos.

2.2. SUJETOS DE LOS DELITOS INFORMÁTICOS.

2.2.1. EL SUJETO ACTIVO.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter

sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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

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

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943. En aquella etapa también se le clasificaba así porque se requería de un determinado conocimiento y posición ocupacional para poder llevar acabo este

actuar, y con ello un cierto status socio-económico; en cambio actualmente cualquier persona con medianos conocimientos de informática puede llegar a ser un delincuente informático. Mas, actualmente se ha llegado a denominar como "Delito de Cuello Dorado" por la gran vistosidad con que se maneja esta figura delictiva, y la gran relevancia que tiene su proceder en comparación con las restantes figuras delictivas que son manejadas por los ordenamientos penales, por sus dañinas consecuencias.

A estos comisores hubo de llamarles de alguna forma, por ello se les denominó, en círculos profanos, Hackers. Es un término ingles con el que se define a las personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, y apenas constituyen una muestra de la nueva faceta de la criminalidad: El delincuente silencioso o tecnológico. Producto de la falta de información se les nombra así a todos sin tener en cuenta las diferencias implícitas que lleva su actuar y las consecuencias del mismo. Por otro lado no tienen ni punto de comparación con lo que este término significa, y que deshonra a los verdaderos Hackers, "cortador".

A pesar de esto las incursiones de estos piratas y corsarios son diferentes y responden a distintas motivaciones y momentos en el desarrollo computacional. A comienzos de los '90, Internet era todavía un fenómeno lejano, al que pocos tenían acceso, mas la información restringida y

confidencial atrajo a los primeros criminales informáticos. En aquel tiempo eran catalogados como:

-Sombrero Negro: calificados como terroristas y mercenarios, usaban sus conocimientos para acceder a bases de datos que luego vendían.

-Sombrero Gris: este tipo de piratas se dedicaba a demostrar cuanto sabía y cual era su capacidad para vulnerar sistemas. Su acción nunca fue con la intención de causar daño.

-Sombrero Blanco: detectaban errores y fallas en los sistemas de seguridad y advertían como remediar el problema.

Con Internet el pirateo se simplificó porque los programas fueron puestos a disposición del público en la misma red. Desde entonces, la distinción se hace por los grados de conocimiento y la esfera de su actuar. Así nos encontramos con los Hackers, los Crackers y los Phreakers, quienes son los tres grupos originarios de los que se subdividen otros tantos. A continuación distinguiremos cada uno de ellos.

A) HACKER: Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas. El término de hacker en castellano significa "cortador". Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión. Los "Hackers", son

fanáticos de la informática, generalmente jóvenes, que tan sólo con un ordenador personal, un módem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer información, copiarla, modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla. Se pueden considerar que hay dos tipos; 1) los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad; 2) los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

Un hacker es un Apasionado de la tecnología, de todo tipo, quiere investigar cuanta cosa sale en el mercado. Experto en SO, sistemas de seguridad, programación avanzada, criptología, conocimiento de phreaking

El hacker puede actuar solo o en grupo, pero generalmente si se reúnen es para intercambiar información, no para que los demás miembros le enseñen a hackear.

La rutina para ellos es bajar todo lo que puedan de Internet sobre vulnerabilidad, sistemas operativos, ingeniería social, phreaking, programación), Inventan un nick (sobrenombre), para que los demás los reconozcan, y generalmente no transmiten desde su casa

B) CRACKER: Para las acciones nocivas existe la más contundente expresión, "Cracker" o "rompedor", sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se infiltra en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware[48] para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia.

Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofia de los Hackers.

En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado más adelante.

[48] Significado en ingles que es equivalente a Programa de Prueba o Temporal.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

Como su nombre indica se dedican a romper, por supuesto las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos del mercado negro. Estos crean códigos para utilizarlos en la copia de archivos. Sus acciones pueden ir desde la destrucción de información ya sea a través de virus u otros medios, hasta el robo de datos y venta de ellos. Ejemplo de su actuar ilegal son los millones de CD's con software pirata que circulan por el mundo entero y de hecho, muchas personas no llegan a sospechar que parte del soft que tienen en sus máquinas, incluso con certificados de garantía de procedencia, es craqueado. Esto sucede sobre todo en los países del tercer mundo; se agrupan en pequeñas compañías y contratan especialistas de alto nivel.

Aunque tratan de cubrirse con el ropaje de la aventura y el desafío tecnológico, los miles y millones de perdidas y los cientos de casos que conocen anualmente la policía y fiscales de todo el mundo, hablan más de un interés pecuniario y delictivo que científico. Las herramientas de este espécimen suelen ser potentes editores hexadecimales y debuger's mediante los cuales "desmontonan" los programas, lo que se conoce como ingeniería inversa hasta

llegar a las protecciones que son generalmente utilidades de tiempo que se representan en el reloj interno de la máquina o en el sistema operativo para desencadenar una cuenta regresiva que descontará los días posibles a usar el software hasta que el mismo caduque y el usuario este obligado a pagarlo o renunciar a él.

Claro que la prensa, e incluso autoridades del mundo entero, diferencian al estudiante sin recursos que "craquea" un programa para su uso, de los que hacen de ello un negocio, aunque insisten que nadie debe actuar así. Lo cierto es que la principal condición para que florezca el negocio del cracking es el precio, siempre en ascenso y en algunos casos exorbitantes, de los programas de mayor utilidad en contraposición con el del hardware que ha mantenido una tendencia decreciente, por lo que no es de extrañar que con frecuencia el costo del software que soporta una máquina, aun una de última generación, sea superior al de ésta.

C) PHREAKER: Es el especialista en telefonía (Cracker de teléfono). Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el

control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

Estos buscan burlar la protección de las redes públicas y corporativas de telefonía, con el declarado fin de poner a prueba conocimientos y habilidades(en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación), pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de "Hacking" a sus servidores.

Estos tipos con conocimientos de telefonía insuperables conocen a fondo los sistemas telefónicos incluso más que los propios técnicos de las compañías telefónicas. Ellos han sabido crear todo tipo de cajas de colores con una función determinada. Por ejemplo la caja azul permite realizar llamadas gratuitas, ya que emula el tono de 2600 hz. para desactivar el contador de la centralita.

Actualmente se preocupan más de las tarjetas prepago, que de estas cajas, ya que suelen operar desde cabinas telefónicas o móviles. Un sistema de retos, es capaz de captar los números de abonado en el aire. De esta forma es posible crear clones de tarjetas telefónicas a distancia.

Dentro de las actuales manifestaciones de phreaking podríamos distinguir:

a) Shoulder-surfing: esta conducta se realiza por el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, el cual lo obtiene al momento en que ella lo utiliza, sin que la víctima pueda percatarse de que está siendo observada por este sujeto quien, posteriormente, aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno.

b) Call-sell operations: el accionar del sujeto activo consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima. Esta acción aprovecha la especial vulnerabilidad de los teléfonos celulares y principalmente ha sido aprovechada a nivel internacional por los traficantes de drogas.

c) Diverting: consiste en la penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan posteriormente al dueño de la central a la que se ingresó clandestinamente. La conducta se realiza atacando a empresas que registren un alto volumen de tráfico de llamadas telefónicas, con el fin de hacer más difícil su detección.

d) Acceso no autorizado a sistemas de correos de voz: el agente ataca por esta vía las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los usuarios suscriptores del servicio. A través de esta conducta el sujeto activo puede perseguir diversos objetivos:

d.1) Utilizar los códigos de transferencia de mensajería automática manejados por el sistema.

d.2) Lograr el conocimiento ilícito de la información recibida y grabada por el sistema.

e) Monitoreo pasivo: por medio de esta conducta el agente intercepta ondas radiales para tener acceso a información transmitida por las frecuencias utilizadas por los teléfonos inalámbricos y los celulares.

D) VIRUCKER: Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

E) PIRATA INFORMÁTICO: Es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor.; hay que considerar también la piratería como descargar música de internet y grabarla en un CD para escucharla; resulta pues que estamos inmersos entre una juventud de

"corsarios negros" y cada día hay programas donde se puede descargar gratuitamente el software para descargar la música gratuitamente

F) LAMMERS: Aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar más allá. Generalmente, son despreciados por los verdaderos hackers que los miran en menos por su falta de conocimientos y herramientas propias. Muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría.

G) GURUS: Son los maestros y enseñan a los futuros Hackers. Normalmente se trata se personas adultas, me refiero a adultas, porque la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma hay, para enseñar a o sacar de cualquier duda al joven iniciativo al tema. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El guru no esta activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimientos propios y solo enseña las técnicas más básicas.

H) BUCANEROS: En realidad se trata de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, los bucaneros no existen en la Red. Solo se dedican a explotar

este tipo de tarjetas para canales de pago que los Hardware Crackers, crean. Suelen ser personas sin ningún tipo de conocimientos ni de electrónica ni de informática, pero si de negocios. El bucanero compra al CopyHacker y revende el producto bajo un nombre comercial. En realidad es un empresario con mucha afición a ganar dinero rápido y de forma sucia.

I) NEWBIE: Traducción literal de novato. Es alguien que empieza a partir de una WEB basada en Hacking. Inicial-mente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la pagina WEB para seguir las instrucciones de nuevo. Es el típico tipo, simple y nada peligroso. Está apartado en un rincón y no es considerado.

J) TRASHING: Esta conducta tiene la particularidad de haber sido considerada recientemente en relación con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas acciones corresponden a una desviación del procedimiento conocido como reingeniería social.

Entre los métodos preferidos por estos delincuentes para desarrollar su actuar son:

a) Cazadores de contraseñas

Un cazador de contraseñas es un programa que desencripta[49] las contraseñas o elimina su protección. Aunque estos programas no han de desencriptar nada, y además con determinados sistemas de encriptación[50] es imposible invertir el proceso, si no es de forma autorizada.

b) Caballos de Troya o troyanos

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto, p. ej. Formatear el disco duro, modificar un fichero, sacar un mensaje, obtener información privilegiada del sistema, etc. Los troyanos los crean los programadores, ya sea creando ellos un programa original, e introduciendo el código maligno, o cogiendo el código fuente de otro programa e introduciendo el código maligno, y luego distribuirlo como el original.

[49] Desencriptar es descodificar la información de un fichero, archivo o correo electrónico para que pueda ser leída la información que contiene.

[50] Encriptar es una manera de codificar la información de un fichero o de un correo electrónico de manera que no pueda ser leído en caso de ser interceptado por una tercera persona mientras viaja por la red. Sólo la persona o personas que tienen el tipo de de software de descodificación adecuado pueden descifrar el mensaje.

c) Superzapping

Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador.

d) Puertas falsas

Es una practica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

e) Herramientas de destrucción

Este suele ser el procedimiento de sabotaje mas utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificara la información, o provocará el cuelgue del sistema. Podemos distinguir cuatro métodos de destrucción: mailbombing, flash bombs, aplicaciones especiales de negación de servicio, y virus, de los cuales mencionaremos los primeros tres:

e1) Mailbombing

Este método se basa en enviar muchos mensajes de correo electrónico, al mismo usuario, lo cual provoca una gran molestia a dicho usuario. Las herramientas que existen para estos ataques son: Up Yours, KaBoom, Avalanche, Unabomber, extreme mail, Homicide, etc.

e2) Flash bombs

Son herramientas que se utilizan en el IRC[51]. Cuando nos conectamos a un IRC, hay varios canales o chats[52], y cada canal tiene su operador que es la autoridad, y decide la persona que ha de marcharse del chat. Las personas expulsadas del chat toman represalias, y apareció el flash bombs. Las aplicaciones de flahs bombs que existen atacan en el IRC de una forma diferente, pero básicamente lo que hacen puede ser es expulsar a otros usuarios del chat, dejar colgado el chat, o llenar de basura (flooding) un canal. Las herramientas que tenemos a nuestra disposición son: crash.irc, botkill2.irc, ACME, Saga, THUGS, o The 7th Sphere.

e3) Aplicaciones de negación de servicio

Este tipo de ataques trata de dejar colgado o desactivar un servicio de la red saturándolo de información y dejándolo bloqueado, e incluso se obligará a reiniciar la máquina. Las utilidades que podemos encontrar

[51] IRC significa Internet Relay Chat. La red de IRC es un lugar de reunión virtual donde personas de todo el mundo pueden encontrarse y pueden hablar. En IRC te encuentras otras personas en "canales" (salas, lugares virtuales, normalmente con un tema de conversación) para hablar en grupo, o privadamente.
[52] Chat es una charla en directo a través de Internet.

para realizar este tipo de ataques son: Syn_floder, DNSKiller, arnudp100.c, cbcb.c, o win95ping.c.

f) Ataques asincrónicos

Este es quizá el procedimiento más complicado y del que menos casos se han tenido conocimiento. Se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc. de una forma periódica; Si alguien consiguiera hacer caer el sistema y modificar dichos ficheros en el momento en que se ponga de nuevo en funcionamiento el sistema éste continuará con la información facilitada y por tanto la información podría ser modificada o cuando menos provocar errores.

g) Ingeniera social

Básicamente es convencer a la gente de que haga lo que en realidad no debería, por ejemplo, llamar a un usuario haciéndose pasar por administrador del sistema y requerirle el password o contraseña con alguna excusa convincente.

h) Simulación de identidad

Básicamente es usar un terminal de un sistema en nombre de otro usuario, bien porque se conoce su clave, o bien porque abandonó el terminal pero no lo

desconectó y ocupamos su lugar. El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona.

i) Spoofing

Mediante este sistema se utiliza una máquina con la identidad de otra persona, es decir, se puede acceder a un servidor remoto sin utilizar ninguna contraseña. ¿Cómo se hace esto? Pues utilizando la dirección IP de otro usuario, y así hacemos creer al servidor que somos un usuario autorizado.

k) Sniffer

Un sniffer es un dispositivo que captura la información que viaja a través de una red, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico. Este tráfico se compone de paquetes de datos, que se intercambian entre ordenadores, y estos paquetes a veces contienen información muy importante, y el sniffer está diseñado para capturar y guardar esos datos, y poder analizarlos con posterioridad. Un ataque mediante un sniffer se considera un riesgo muy alto, ¿por qué?, pues porque se pueden utilizar los sniffers para algo más que para capturar contraseñas, también pueden obtener números de tarjetas de crédito, información confidencial y privada, etc. Actualmente existen sniffers para todas las plataformas, ya que los sniffers se dedican a capturar datos, no computadoras, y por ello es igual la plataforma que se utilice. Algunos sniffers son los siguientes: Gobbler,

ETHLOAD, Netman, Esniff.c (se distribuye en código fuente), Sunsniff, linux_sniffer.c, etc.

2.2.2. EL SUJETO PASIVO.

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

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la

falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

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

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

conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

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

3. PENAS APLICADAS A LOS DELITOS INFORMÁTICOS EN EL DERECHO COMPARADO.

La Pena no es la única, pero sí es la más importante consecuencia jurídica que se deriva de la comisión de un hecho delictivo. No es la única porque el arsenal punitivo, del que hace uso el Estado para la protección de los delitos, no se limita exclusivamente a esa sanción, pues incorpora otras consecuencias, como las medidas de seguridad.

La Pena es la privación de bienes jurídicos prevista por la Ley, que se impone por los órganos jurisdiccionales competentes al responsable de un hecho

delictivo[53]. Es decir, que al tratarse de la sanción más severa que puede imponer el Estado, algo muy negativo para el condenado, es su presupuesto indispensable la comisión de un hecho delictivo. En cualquier caso, la pena supone una consecuencia jurídica grave, que se impone en atención a la violación de un interés considerado vital para la comunidad, esto es, por la afección a un bien jurídico.

Existe un gran número de países que poco a poco han ido regulando los delitos informáticos en sus ordenamientos jurídicos, y dentro de los países latinoamericanos que cuentan con regulación expresa sobre delitos informáticos encontramos a: España, Chile, Costa Rica y el Estado de Sinaloa en México, Venezuela y Perú. De ellos analizaremos brevemente las penas aplicadas a estos delitos, aunque también estudiaremos las penas establecidas en el anteproyecto de ley sobre delitos informáticos de Argentina.

❖ España

Los delitos informáticos en España se encuentran regulados en su Código Penal [Ley-Orgánica 10/1995, de 23 de Noviembre/ BOE número 281, de 24 de Noviembre de 1995]. Aunque en la mayoría de los artículos referentes a delitos informáticos, la tecnología de la información aparece como un medio

[53] BERDUGO GÓMEZ DE LA TORRE, I, ARROYO ZAPATERO, L, GARCÍA RIVAS, N. FERRÉ OLIVÉ, J. SERRANO PIEDECASAS, J. Lecciones de Derecho Penal, segunda edición, Barcelona, 1999, pág. 22

para la realización de delitos tradicionales, existen algunos novedosos e importantes.

Las penas impuestas para la mayoría de las conductas tipificadas como delitos informáticos en el código penal español, son la pena de privación de libertad y la multa. El tiempo mínimo establecido para la pena de prisión, es de un año y una máxima de cinco.

❖ Chile

A diferencia de España, los delitos informáticos en Chile se encuentran regulados en una ley especial, denominada ley relativa a delitos informáticos [Ley No.:19223], la cual fe aprobada en 1993, lo cual muestra el alto grado de desarrollo jurídico de Chile y su capacidad de anticipación.

La pena establecida para los delitos informáticos es la de privación de libertad, llamada en dicha ley como pena de presidio. El tiempo de duración de esta pena se encuentra establecido bajo las reglas específicas del código penal de Chile, cuyo cómputo varía con respecto a nuestra legislación penal.

❖ Costa Rica

En Costa Rica, los delitos informáticos fueron incluidos al Código Penal. Se adhirieron los artículos 196 bis, 217 bis y 229 bis al respectivo código penal, bajo la denominación de Ley N. 8148 para reprimir y sancionar los delitos informáticos.

La pena aplicada a los delitos informáticos en Costa Rica es la de privación de libertad, con un mínimo de seis meses y como máximo diez años de prisión.

❖ México

El Código Penal del Estado de Sinaloa, de los Estados Unidos Mexicanos, incorpora a los delitos informáticos, penándolos con pena de privación de libertad y la multa. La pena de prisión establece como mínimo de seis meses hasta un máximo de dos años.

El Estado de Sinaloa optó por la regulación dentro del Código, para evitar la dispersión y el fraccionamiento, y favorecer la generalidad y abstracción de la norma penal.

❖ Venezuela

La Ley especial contra los delitos informáticos de Venezuela, es una ley especial que precisa bastante cada tipo, pudiendo a veces carecer de abstracción y generalidad, ya que incluso establece definiciones legales de algunos términos de la informática.

Las penas establecidas en esta ley especial son la multa y la privación de libertad. Esta última con un mínimo de un año y un máximo de ocho años.

❖ Perú

Las reformas para la inclusión de delitos informáticos en el código penal peruano, aplicaron la prestación de servicios comunitarios, para sustituir a la

pena de privación de libertad. En caso de aplicarse esta última no podrá superar los dos años.

❖ Argentina

El anteproyecto de Ley de delitos informáticos, que sometido a consulta pública por la secretaria de comunicaciones por resolución no. 476/2001 del 21.11.2001, es junto con la legislación de Costa Rica, una de las más precisas en cuanto a tipificar al delito informático, situando a esta tecnología ya no sólo como un medio para la comisión de otro delito.

La pena que se establece en este anteproyecto de ley es la de privación de libertad, con un mínimo de un mes y máximo de veinticinco años. Los veinticinco años de prisión sólo pueden darse en caso de agravación en unas figuras.

Como se puede apreciar, la tendencia general de la legislación comentada, es la de aplicar la Pena de Prisión y la Multa para sancionar los delitos informáticos. La Prisión es una auténtica pena privativa de libertad, la cual supone el internamiento del reo en un centro penitenciario, y puede tener diversa duración según lo que establezca la ley para cada delito. A menudo los sistemas dan a estas penas diferentes denominaciones, dada su distinta duración. Se habla así, por ejemplo, de reclusión, prisión, arresto y presidio.

La Multa consiste en la detracción de una parte de la capacidad económica del sujeto en beneficio de la colectividad ofendida por el delito, representada a través del Estado. La multa se ha convertido en una sanción muy importante dentro del sistema penal, pues funciona perfectamente como una alternativa a la prisión, y al mismo tiempo posee un importante efecto intimidatorio, si sus cuantías se determinan adecuadamente. Es una alternativa a la prisión en la medida que el sujeto no sufre los efectos negativos de la cárcel respecto a la desocialización, pérdida del trabajo, etc. Pero es una auténtica pena, pues nuestra sociedad actual, que da enorme trascendencia a los medios materiales y al dinero, la posibilidad de perder esos bienes o una parte de ellos puede inhibir a los sujetos, conducirlos a evitar conductas delictivas. El principal problema con la Multa es su aplicación desigual. Se adopte el sistema que se adopte, una persona con medios económicos suficientes podrá hacer frente a esta pena. Quien no tenga dinero tendrá muchos problemas para cumplir con la sanción impuesta.

3.1 JUSTIFICACIÓN DE LAS PENAS

Las penas aplicadas a los delitos informáticos en el derecho comparado tienen una razón de ser, y por eso es importante que definamos el objetivo de las penas en general. La pena se justifica como medio de represión indispensable

para mantener las condiciones de vida fundamentales para la convivencia de personas de una comunidad[54].

Sin la pena, la convivencia humana en la sociedad actual sería imposible. Se trata de un elemental recurso al que debe acudir el Estado para posibilitar la convivencia entre los hombres. Su justificación no es, por consiguiente, una cuestión religiosa ni filosófica, sino una amarga necesidad en una sociedad seres imperfectos como los son los hombres[55].

El establecimiento de la pena dentro de la norma jurídico-penal no debe ser una tarea menor, ni tampoco una potestad antojadiza del legislador, sino que debe cumplir con los parámetros y análisis jurídico-penales respectivos. La pena debe establecerse en relación de, al menos, tres criterios básicos, los cuales son:

El nivel jerárquico del bien jurídico afectado;

El grado o nivel de ofensa que se ha ejercido sobre éste; y,

El cumplimiento los fines de la pena, establecidos en la Constitución de la República[56].

---

[54] Dirección Electrónica: http://www.bahaidream.com/lapluma/derecho/revista002/pena.htm.
[55] Ídem.
[56] La pena de privación de libertad, según nuestra Constitución, en el artículo 27, establece como objeto *"corregir a los delincuentes, educarlos y formarles hábitos de trabajo, procurando su readaptación y la prevención de los delitos".*

La justificación para las penas de privación de libertad en el derecho comparado, viene a raíz de la importancia de la informática en nuestros días, ya que ésta nos rodea y es un fenómeno irreversible. Se encuentra involucrada en todos los ámbitos de la interacción humana, desde los más importantes a los más triviales, generándose lo que, en la doctrina norteamericana, se denomina computer dependency o dependencia computacional. Sin la informática las sociedades actuales colapsarían. Es instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva de forma de energía, e inclusive, de poder intelectual"[57].

Así también, "las tecnologías de la información han abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional. A ello contribuye la facilidad para la comisión y encubrimiento de estas conductas disvaliosas y la dificultad para su descubrimiento, prueba y persecución"[58].

La información, como valor o bien jurídico a proteger, ya ha sido considerada por el Derecho Penal en otras ocasiones. Sin embargo, se ha hecho desde la óptica de la confidencialidad, pero no como un nuevo bien jurídico tutelado que abarca varios intereses dignos de protección penal. Es debido a esa relevancia que la información ha ganado con la tecnología informática, y por todos los ámbitos que puede afectar un ataque a este bien jurídico es que la

[57] Dirección Electrónica: http//:www.delitosinformáticos.com
[58] Idem.

pena de privación de libertad, es aplicada en el derecho comparado, pues se considera que el bien atacado es de suma importancia y por tanto debe de ser protegido y reprimido de la manera más contundente y enérgica, como es la de privar al delincuente de su libertad, ya que la libertad ambulatoria se ha convertido en un valor extraordinariamente codiciado lo que supone que la amenaza de su privación a través de la prisión debería surtir efectos sustanciales, de cara a los fines preventivos generales de la pena. Es por ello que la mayoría de legislaciones sobre delitos informáticos sancionan dichos ilícitos con la pena de prisión, variando el tiempo de aplicación de la misma desde un mes hasta veinticinco años. No obstante ello, doctrinariamente se crítica la aplicación de penas cortas, pues como dijo Fran Von Liszt, "ni corrigen, ni intimidan, ni inocuizan; pero, en cambio, arrojan frecuentemente al delincuente primario en el camino definitivo del crimen", es decir, que trae consecuencias negativas para la reinserción social del interno, y al ejecutarse una pena tan breve no puede llevarse a la práctica ningún tratamiento resocializador. En cuanto al limite máximo de la pena de prisión, un importante sector científico sostiene que, con base en investigaciones criminológicas, el limite máximo de la privación de libertad no debería superar los quince años de prisión efectiva, pues con penas demasiado elevadas no se puede reinsertar socialmente a nadie, sino que por el contrario, aleja al individuo de la sociedad, convirtiéndolo en una especie de muerto en vida, pues destruye su personalidad.

TÍTULO II

LEGISLACIÓN, NORMAS INTERNACIONALES, JURISPRUDENCIA Y CASOS EMBLEMÁTICOS SOBRE DELITOS INFORMÁTICOS

1. PAÍSES QUE ACTUALMENTE CUENTAN CON LEGISLACIÓN SOBRE DELITOS INFORMÁTICOS

En lo que atañe al derecho comparado, hemos analizado la legislación relacionada con nuestra materia de estudio y podemos distinguir cuatro situaciones bien diferenciadas en el mundo:

a) Legislación en el continente Europeo

b) Legislación en el Continente Asiático

c) Leyes de Estados Unidos de América

d) Legislación de algunos países de América Latina.

❖ Europa

En general, la legislación comparada imperante en el derecho europeo es insuficiente. Pero se está trabajando ampliamente, tanto a nivel estadual, como a nivel bloque comunitario. Para formarnos una breve idea de lo avanzado que esta el tema, entraremos en detalles respecto de ciertos países que por su trascendencia, estimamos nos brindaran una comparación generosa en consideraciones.

España: Si bien su Código Penal es el más actualizado de ese continente, las distintas figuras convencionales no alcanzan para perseguir la amplia gama de delitos informáticos que se pueden presentar, como por ejemplo distintas conductas de hacking[59], accesos ilegítimos a sistemas informáticos y distribución de virus, bombas lógicas, etc. El 26 de octubre de 1995 se aprobó la nueva Ley Orgánica 1071995 del nuevo Código penal español, el cual entró en vigor el 24 de mayo de 1996. Este nuevo código intenta solucionar el problema de conductas delictivas que surgen a raíz del incremento de las nuevas tecnologías. Introduce tipos penales nuevos y modifica algunos de los existentes con el fin de adaptar la norma positiva al uso delictivo de los ordenadores, sistemas lógicos y tecnologías de la información aunque no alcanzan para perseguir la amplia gama de delitos informáticos que se pueden presentar, como por ejemplo distintas conductas de hacking, accesos ilegítimos a sistemas informáticos y distribución de virus, bombas lógicas, etc. La reforma aborda temas, desde la delincuencia clásica con medios tecnológicos a los delitos cometidos a través de redes informáticas, como Internet. Podemos extraer los siguientes principios, receptados en el texto legal mencionado: 1. Se

[59] El término puede significar la libre exploración intelectual del potencial más profundo y más grande de los sistemas informáticos. El hacking se puede escribir como la determinación para hacer el acceso a la información, y los ordenadores, tan libre y abierta como sea posible. El hacking puede implicar la convicción más sincera de que la belleza puede ser hallada en los ordenadores, que la elegante estética de un programa perfecto puede liberar la mente y el espíritu. Esto es el "hacking" tal y como fue definido en la muy elogiada historia de Steven Levy sobre los pioneros en el mundo del ordenador, Hackers, publicado en 1984. "Hacking" en su definición actual más común, es la intromisión en un sistema informático a escondidas y sin permiso. El término "hacking" se ha usado rutinariamente hoy en día por casi todos los policías con algún interés profesional en el abuso y el fraude informático. La policía americana describe casi cualquier crimen cometido con, por, a través, o contra un ordenador como hacking.

equiparan los mensajes de correo electrónico a las cartas y papeles privados (artículo 197) (11). 2. Se castiga a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de terceros, datos personales de otro que se hallen registrados, entre otros, en soportes informáticos (artículo 197) 3. Se reprime el delito de amenazas hechas "por cualquier medio de comunicación" (artículo 169) 4. Se castigan las calumnias e injurias difundidas por cualquier medio (artículo 211) 5. A los efectos de tipificar el delito de robo con fuerza en las cosas, se incluye el uso de llaves falsas, entendiendo que son llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia. (art 238- 239) (12) Se modifica el artículo 248 que tipifica el delito de estafa incluyendo a los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. 6. Penaliza la conducta de quien hiciera uso de cualquier equipo terminal de telecomunicación sin consentimiento de su titular, ocasionando a este un perjuicio de más de cincuenta mil pesetas. 7. Se protege el software, al castigarse a quien dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos (artículo 264) (13), así como la fabricación, puesta en circulación y tenencia de cualquier medio destinado a facilitar la supresión no autorizada de cualquier dispositivo utilizado para proteger programas de ordenador (artículo 270) (14) 8. Se sanciona la fabricación o tenencia de programas de ordenador, entre otros,

específicamente destinados a la falsificación de todo tipo de documento (artículo 400) (15)

Alemania: El modelo alemán seguido por la legislación penal alemana respecto a la lucha contra la criminalidad informática, se construye sobre la base de identificar dos supuestos de acciones atentatorias para determinados bienes jurídicos. Se tipifica al fraude informático y al delito de sabotaje informático. El bien jurídico protegido primordialmente es el patrimonio. En cuanto a conductas atentatorias a la vida personal y la privacidad, el Código penal alemán sanciona el espionaje de datos pero excluye la información que se encuentre almacenada o que pueda ser transmitida electrónica o magnéticamente o transmitida de forma inmediatamente accesible. Con ello, prácticamente no se regula ningún tipo penal que pudiera estar referido a un espionaje de datos informatizados. No se quiso punir la mera intrusión informática, sino sólo en aquellos casos de conductas que signifiquen la manipulación de las computadoras y persigan un ánimo de lucro. A partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos: Espionaje de datos (202 a); Estafa informática (263 a); Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273) Ø 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) En lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal, tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita. Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada, fue también adoptada en los Países Escandinavos y en Austria. En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada. En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el

gobierno, tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados. Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos. Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas. En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, especialmente en la medida en que el objeto de la acción sean datos almacenados o transmitidos o se trate del daño a sistemas informáticos. Podemos concluir que la violación al derecho a la intimidad u otras acciones que no tengan consecuencias patrimoniales, como por ejemplo accesos ilegítimos realizados por hackers en los que el móvil es el desafío de acceder ilegítimamente a un sistema y curiosear la información

contenida en él, la interceptación de un correo electrónico, etc. no se encuentran previstas en la Legislación alemana.

Austria: La reforma del Código Penal Austríaco del 22 de diciembre de 1987 contempla dos figuras relacionadas con nuestra materia: la destrucción de datos, personales, no personales y programas (artículo 126) y la estafa informática (artículo 148). 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.
Establece una pena de multa para aquel que acceda ilegalmente a datos no autorizados o para quien intencionalmente los borre.

Francia: La ley número 88-19 de 5 de enero de 1988 sobre el fraude informático Contempla los siguientes delitos informáticos: 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.

Italia: El Código Penal Italiano tipifica los siguientes delitos: Art 615 ter: Acceso no autorizado a un sistema de computadoras o telecomunicaciones; Art 615 quater: Posesión y disponibilidad de códigos de acceso a sistemas de computadoras o telecomunicaciones; Art 615 quinter: Difusión de Programas que puedan causar daños o interrumpir sistemas de computación.

Inglaterra: La Computer Misuse Act (Ley de Abusos Informáticos) comenzó a regir en el año 1991.- Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Contiene además la ley un apartado que específica la modificación de datos sin

autorización. Los virus están incluidos en esa categoría. Asimismo dispone que liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.-

Otros países Europeos que contienen normativa sobre delitos informáticos, aunque incompleta y solo relacionada a algunos aspectos generales son:

Bélgica: El Parlamento Belga incorporó en su Código Penal nuevos delitos informáticos, vigentes desde febrero de 2001. Los cuatro principales problemas relacionados con los delitos informáticos que son tratados por esta reforma son: el robo por computadora, el fraude por computadora, el hacking y el sabotaje informático.

Estonia: El Código Penal de Estonia prevé en los artículos 269 a 273 los delitos de: Destrucción de programas y datos en una computadora; Sabotaje informático; Uso no autorizado de computadoras o sistemas de computación; Daños o interferencias ocasionados con conexiones de computadoras; Transmisión de virus informáticos.

Holanda: El 1 de mayo de 1993 entró en vigencia la ley de Delitos Informáticos, en la cual se penaliza: El hacking, El phreacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), La ingeniería social (arte de convencer a la gente de entregar

información que en circunstancias normales no entregaría), y La distribución de virus.

Dinamarca: Código Penal sección 263. Considera conducta punible al acceso no autorizado a información o programas instalados en un sistema de procesamiento de datos. Agrava las penas según las intenciones o circunstancias.

Finlandia: Código Penal Capitulo 38 sección 8, considera punible el acceso no autorizado a un sistema de computadoras para robar o transmitir parte del sistema. La tentativa es punible

Hungría: Código Penal. Sección 300 C, contempla el fraude informático.
Luxemburgo Acta del 15 de julio de 1993 sobre la lucha contra el crimen financiero y computacional. Prevé: Acceso ilegítimo a un sistema de procesamiento de datos. Agrava la pena cuando dicho acceso produce la supresión, modificación o alteración de los datos o parte del sistema.

❖ **Asia**

Algunos de los países del continente Asiático que han legislado sobre delitos informáticos son:

India: Acta de Información Tecnológica n° 21 año 2000, Pena y define al hacking.

Israel: The Computer Law de 1995. Sección 4, condena el acceso ilegítimo a una computadora.

Japón: Ley n° 128 de 1999 (Con efecto desde el 3 de febrero de 2000) Prohíbe el acceso no autorizado a sistemas de computadoras y los actos que faciliten dicho acceso no autorizado. Establece penas de multa o prisión para los infractores.

China: Decreto n° 147 de Febrero de 1994 "Regulación del Pueblo de la Republica de China en protección de la seguridad de Datos Informáticos" y la Ordenanza de Telecomunicaciones, Sección 27 A : Tipifica el delito de acceso ilegal a la información o programas de un sistema de computadora, estableciendo una pena de multa o prisión no mayor a seis meses, pena ésta que se eleva hasta dos años según las circunstancias o intenciones del sujeto.

Malasia: Acta de Crimen Computacional de 1997, condena el acceso ilegítimo a sistemas de computación

Filipinas: Republic Act n° 8792, sobre "Reconocimiento y uso de transacciones electrónicas, penalidades y otros propósitos", en su Par. V, denominada

Provisiones Finales, penaliza: Hacking y craking, entendido como acceso no autorizado o interferencia en un sistema de computadoras o telecomunicaciones para alterar, robar o destruir, usando para ello un computador o sistema de telecomunicaciones, incluyendo la introducción de virus.

Singapur: Computer Misuse Act prevé la penalización: Acceso no autorizado a una computadora; Acceso con la intención de cometer o facilitar la comisión de un delito.

❖ **Estados Unidos**

En los Estados Unidos, existen leyes federales que protegen contra el ataque a ordenadores, uso ilegítimo de passwords, invasiones electrónicas en la privacidad, y otras transgresiones.

Las dos leyes Federales de EEUU mas importantes utilizadas por los jueces Federales de USA para perseguir a los delincuentes informáticos son: USC (Acrónimo en inglés de United States Code, que significa Código de los Estados Unidos) TITULO 18, CAPÍTULO 47, SECCIÓN 1029 Y SECCIÓN 1030, de 1994 que modificó al Acta de Fraude y el Acta Federal de Abuso Computacional de 1986.

El Pronunciamiento sobre Abuso y Fraude Informático de 1986, es la principal pieza legislativa aplicable a la mayoría de los delitos informáticos, aunque

muchas otras leyes pueden ser usadas para perseguir diferentes tipos de delitos informáticos.

El pronunciamiento fue modificado con el Título 18 del Código de los Estados Unidos Sección 1030. También complementó a la Ley de Privacidad de las Comunicaciones Electrónicas de 1986, que dejó fuera de la ley el interceptar comunicaciones digitales. Las Modificaciones de la Ley de Abusos Informáticos de 1994 amplió la Ley de 1986 al acto de transmitir virus y otra clase de código dañino.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etcétera y en que difieren de los virus, el acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, a la información, los datos o programas.

La nueva ley representa un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento de aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus un castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera negligente la sanción fluctúa entre una multa y un año en prisión.

En virtud del Acta de 1994, el creador de un virus no podría escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos. No se define a los virus, sino que se los describe, para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

En general, un delito informático quebranta las leyes federales cuando entra en alguna de las siguientes categorías:

Implica el compromiso o el robo de información de defensa nacional, asuntos exteriores, energía atómica u otra información restringida.

Involucra a un ordenador perteneciente a departamentos o agencias del gobierno de los Estados Unidos.

Involucra a un banco o cualquier otra clase de institución financiera.

Involucra comunicaciones interestatales o con el extranjero.

Afecta a gente u ordenadores en otros países o estados.

"**La Sección 1029**" La Sección 1029 prohíbe el fraude y cualquier actividad relacionada que pueda realizarse mediante el acceso o uso de dispositivos falsificados como PINs, tarjetas de crédito, números de cuentas, y algunos tipos más de identificadores electrónicos. Las nueve áreas de actividad criminal

que se cubren en la Sección 1029 están listadas abajo. Todas *requieren* que el delito implique comercio interestatal o con el extranjero.

1. Producción, uso o tráfico de dispositivos de acceso falsificados. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $50,000 o dos veces el valor del crimen cometido y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

2. Uso u obtención sin autorización de dispositivos de acceso para obtener algo de valor totalizando $1000 o más, durante un periodo de un año. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $10,000 o dos veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

3. Posesión de 15 o más dispositivos de acceso no autorizados o falsificados. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $10,000 o dos veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

4. Fabricación, tráfico o posesión de equipo de fabricación de dispositivos de acceso ilegales. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $50,000 o dos veces el valor del crimen cometido y/o hasta 15 años de cárcel, $1,000,000 y/o 20 años de cárcel si se reincide.

5. Realización de transacciones con dispositivos de acceso pertenecientes a otra persona con el objetivo de obtener dinero o algo de valor totalizando $1000 o más durante un periodo de un año. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa de $10,000 o dos

veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

6. Solicitar a una persona con el objetivo de ofrecerle algún dispositivo de acceso o venderle información que pueda ser usada para conseguir acceso a algún sistema. (El delito debe ser cometido conscientemente y con intención de estafar, y sin la autorización del propietario del sistema de acceso.) Pena: Multa de $50,000 o dos veces el valor del crimen y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

7. Uso, producción, tráfico o posesión de instrumentos de telecomunicación que hayan sido alterados o modificados para obtener un uso no autorizado de un servicio de telecomunicaciones. (El delito debe ser cometido conscientemente y con ánimo de estafar.) Esto incluiría el uso de "Red Boxes", "Blue Boxes" (sí, todavía funcionan en algunas redes telefónicas) y teléfonos celulares reprogramados, cuando el usuario legítimo del teléfono que se haya reprogramado no esté de acuerdo con esa acción. Pena: Multa de $50,000 o el doble del valor del crimen cometido y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

8. Uso, fabricación, tráfico o posesión de receptores-escaneadores o hardware o software usado para alterar o modificar instrumentos de telecomunicaciones para obtener acceso no autorizado a servicios de telecomunicaciones. Esto también incluye los scanners que mucha gente usa para interceptar llamadas de teléfonos celulares. Se suscitó un gran escándalo cuando los medios de comunicación tuvieron noticia de una llamada de un celular interceptada (la

llamada correspondía al Portavoz de los Representantes de la Casa Blanca, Newt Gingrinch.) Pena: Multa de $50,000 o dos veces el valor del crimen y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

9. Hacer creer a una persona el delincuente es un miembro de su compañía de tarjeta de crédito o su agente para obtener dinero o realización de transacciones hechas con un dispositivo de acceso Y viceversa (tratar de hacer creer a la compañía de crédito que se trata de la persona legítima). El delito debe ser cometido conscientemente y con objetivo de estafar, y sin permiso. Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

"**La Sección 1030**", como parte de la Ley sobre Abuso y Fraude Informático de 1986, prohíbe el acceso no autorizado o fraudulento a ordenadores gubernamentales, y establece diversas condenas para esa clase de accesos. Esta ley es una de las pocas piezas de legislación federal únicamente referidas a ordenadores. Bajo la Ley de Abuso y Fraude Informático, el Servicio Secreto americano y el F.B.I. tienen jurisprudencia para investigar los delitos definidos en este decreto. Las seis áreas de actividad criminal cubiertas por la Sección 1030 son:

1. Adquisición de información restringida relacionada con defensa nacional, asuntos exteriores o sobre energía nuclear con el objetivo o posibilidad de que sean usados para dañar a los Estados Unidos o para aventajar a cualquier otra nación extranjera. (El delito debe ser cometido consciente-mente accediendo a un ordenador sin autorización o exceder el acceso autorizado.)

2. Obtención de información en un registro financiero de una institución fiscal o de un propietario de tarjeta de crédito; o de información de un cliente en un archivo de una agencia de información de clientes. (El delito debe ser cometido conscientemente intencionadamente accediendo a un ordenador sin autorización o excediendo el acceso autorizado.) Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

3. Atacar un ordenador que sólo corresponda ser usado por algún departamento o agencia del gobierno de los EEUU, para el caso de que no sólo puede ser usada por esta agencia, atacar un ordenador usado por el gobierno en el que la intrusión producida afecte el uso que el gobierno hace de él. (El delito debe ser cometido intencionadamente accediendo a un ordenador sin autorización.)

4. Promover un fraude accediendo a un ordenador de interés federal y obtener algo de valor, a menos que el fraude y la cosa obtenida consistan solamente en el uso de dicho ordenador. (El delito debe ser cometido conscientemente, con intención de cometer dicho fraude, y sin autorización o excediéndose de la autorización obtenida) [La visión que tiene el gobierno de "ordenador de interés federal" está definida abajo] Pena: Multa y/o hasta 5 años de cárcel, hasta 10 años si se reincide.

5. A través del uso de un ordenador utilizado en comercio interestatal, transmitir intencionadamente programas, información, códigos o comandos a otro sistema informático. Existen dos situaciones diferentes:

A.- En esta situación (I) la persona que realiza la transmisión está intentando dañar el otro ordenador o provocar que no se permita a otras personas acceder a él; y (II) la transmisión se produce sin la autorización de los propietarios u operadores de los ordenadores, y causa $1000 o más de pérdidas, o modifica o perjudica, o potencialmente modifica o altera un examen o tratamiento médico. Pena con intento de dañar: Multa y/o hasta 5 años de cárcel, hasta 10 años si se reincide.

B.- En esta situación, (I) la persona que realiza la transmisión no intenta hacer ningún daño, pero actúa imprudentemente despreciando el riesgo que existe de que la transmisión causara daño a los propietarios u operadores de los ordenadores y provoca $1000 o más de pérdidas, modifica o potencialmente modifica un examen o tratamiento médico. Pena por actuación temeraria: Multa y/o hasta 1 año de cárcel.

6. Promover el fraude traficando con passwords o información similar que haga que se pueda acceder a un ordenador sin la debida autorización. Todo esto si ese tráfico afecta al comercio estatal o internacional o si el ordenador afectado es utilizado por o para el Gobierno. (El delito debe ser cometido conscientemente y con voluntad de estafar.) Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

Para la Sección 1030, un ordenador de interés federal tiene las siguientes características:

1. Un ordenador que es exclusivamente para el uso de una institución financiera o del Gobierno de los EEUU o, si su uso no está restringido a lo

anterior, uno usado por una institución financiera o el gobierno de los EEUU en el que el ataque afecte negativamente al servicio que está desarrollando en esas instituciones. 2. Un ordenador de los dos o más que hayan sido usados para cometer el ataque, no estando todos ellos en el mismo estado. Las disposiciones citadas se complementan con los siguientes instrumentos: 18.U.S.C. 875 Interstate Communication Including Threats, kidnapping, Ransom, extortion 18 U.S.C. 1343 Fraud by wire, radio or television 18 U.S.C. 1361 Injury to Goverment Property 18 U.S.C. 1362 Government Communication systems 18 U.S.C. 1831 Economic Espionage Act 18 U.S.C. 1832 Trade Secrets Act

Asimismo, se debe destacar que existe una abundante legislación dentro de cada uno de los más de cincuenta estados. Estos suelen avanzar, tanto en lo que hace a la tipificación de los delitos u ofensas (spam, etc), como respecto de materias procesales. Algunos ejemplos son: i. Arizona Computer Crimes Laws, Section 13-2316 ii. Iowa Computer Crime Law, Chapter 716A.9 iii. Kansas Computer Crimes Law, Kansas, Section 1-3755 iv. Louisiana evised Status 14:73.4 (Computer Fraud) v. Michigan Compiled Laws Section 752.794 (Acces to computers for devising or excecuting scheme to defraud or obtain money, property, or services).

❖ **América Latina**

Chile: Este país es el primero de América del Sur que ha actualizado su legislación en la materia. Mediante la ley 19.223 (28 de mayo de 1993) se han tipificado figuras penales relativas a la informática:

1. Destrucción o inutilización maliciosa de hardware y software, así como alteración de su funcionamiento por cualquier medio 2. Acceso a información "contenida en un sistema de tratamiento de la misma" con ánimo de "apoderarse, usar o conocerla indebidamente" 3. Difusión maliciosa de datos contenidos en un sistema de información Asimismo, este país reconoce al software como obra intelectual (ley 17.336).

Perú: El Código Penal de Perú incluyó, a fines de año 2000, un capítulo específico para el tratamiento de los delitos informáticos (Capítulo X) que incorporó los artículos 207°-A, 207°-B y 207°-C. Allí se reprime: 1. Utilizar o ingresar indebidamente a una base de datos o red de computadoras para alterar un esquema, interceptar o copiar información en tránsito o contenida en una base de datos. Se agrava la pena si se actúa con propósito de beneficio económico. 2. Utilizar, ingresar o interferir indebidamente una base de datos o red de computadoras con el fin de dañarlos o alterarlos. Las conductas anteriores se agravan cuando el agente hace uso de información privilegiada obtenida en función de su cargo o pone en peligro la seguridad nacional.

México: El Código Penal mejicano se reformó en 1999, incorporando los artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7. Se sanciona al que, Sin autorización: a) Modifique, destruya o provoque pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad; b) Conozca o copie dicha información. Se agravan las conductas anteriores si se tratare de sistemas de informática del Estado o de instituciones que integran el sistema financiero y más aún si el agente estuviere autorizado para acceder a los mismos o cuando la información obtenida se utilice en provecho propio o ajeno. El software es considerado obra intelectual y, consecuentemente, recibe protección legal. Sin perjuicio de advertirse preocupación por el impacto de la alta tecnología en la comisión de delitos, ninguna de las legislaciones analizadas contempla íntegramente la problemática que la materia ofrece. No se prevé expresamente el fraude informático, aunque todas condenan el acceso ilegítimo a datos ajenos informatizados (hacking). La corta vigencia de las normas peruanas (2000) y mexicanas (1999) impiden hacer una evaluación precisa de la efectividad de las mismas. En este punto corresponde destacar las recomendaciones dadas en dos congresos internacionales. Estos son los de Río de Janeiro del año 1994, y del de Montevideo de 1998. En el primero se distinguen distintos delitos que deben ser tipificados, como el fraude en la introducción alteración, o supresión de datos; las falsificaciones informáticas; los daños causados a datos o programas; el sabotaje informático; los accesos ilegítimos; la interceptación, reproducción no autorizada de un programa informático; etc. En el segundo, se

analizó profundamente la cuestión de la responsabilidad penal emergente de estos delitos, el respeto por el principio de legalidad y la protección de la propiedad intelectual.

Costa Rica: En el 2001 se adicionaron al Código Penal (Ley No. 4573), los artículos 196 bis, 217 bis y 229 bis, los cuales corresponden a Violación de Comunicaciones Electrónicas, Fraude Informático, y, Alteración de Datos y Sabotaje Informático, respectivamente.

Venezuela: La Ley sobre Delitos Informáticos (Gaceta Oficial N° 37.313 del 30 de octubre de 2001), define los términos tecnología de la información, sistema, data, documento, computadora, hardware, firmware, software, programa, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña y mensaje de datos. Elabora cinco clases de delitos: 1) Contra los sistemas que utilizan tecnologías de información (Acceso indebido a un sistema, el Sabotaje o daño a sistemas, el Espionaje informático, etc.); 2) Contra la propiedad (El Hurto, El Fraude realizado mediante el uso indebido de tecnologías de la información, etc.); 3) Contra la privacidad de las personas y de las comunicaciones (La violación de la privacidad de las comunicaciones, etc.); 4) Contra niños y adolescentes (La exhibición pornográfica de niños y adolescentes, etc.), y; 5) Contra el orden económico (La apropiación indebida de propiedad intelectual mediante la reproducción, divulgación, modificación o copia de un software, etc.).

2. REGULACIÓN EN EL DERECHO INTERNACIONAL SOBRE DELITOS INFORMÁTICOS.

El Derecho Internacional es el conjunto de normas, convenios y protocolos que regulan las relaciones entre los distintos estados y que son instrumentados por su Servicio Diplomático[60].

El Derecho Internacional está integrado, en el ámbito bilateral, por acuerdos firmados entre Estados – denominados tratados, convenios, memorandos, intercambio de Notas Diplomáticas, enmienda, anexo, protocolo, etc. –, por el derecho consuetudinario internacional que se compone a su vez de la práctica de los Estados que éstos reconocen como obligatoria, así como por principios generales del derecho. En el ámbito multilateral, el derecho internacional se nutre de los acuerdos a los que lleguen los estados en el marco de algún organismo internacional, y dentro de éste, de aquel mecanismo bajo el cual se comprometen los estados a aplicar[61].

En ambos casos, bilateral o multilateral, el nivel adquirido al comprometerse un país, es el de poner en vigor la norma acordada en su propio territorio y pasa a ser automáticamente aplicada internamente y por encima de las normas nacionales[62].

---

[60] Dirección Electrónica: http://es.wikipedia.org/wiki/Derecho_internacional
[61] Ídem.
[62] Ídem.

El 23 de Noviembre del año 2001, el Consejo de Ministros de Europa, compuesto por los Ministros del Interior de los Estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón, firmaron en Budapest la *Convención sobre Delitos Informáticos*.

Esta Convención, cuya elaboración tomó más de cuatro años, tiene como objetivos fundamentales los siguientes: (1) Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático; (2) Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y (3) Establecer un régimen dinámico y efectivo de cooperación internacional.

La estructura normativa de este novedoso instrumento jurídico internacional consta de 4 capítulos. El capítulo I define algunos conceptos básicos, tales como "sistema de cómputo", "datos informáticos", "proveedor de servicios de interconexión o almacenamiento de datos informáticos" e "intercambio electrónico de datos". El capítulo II establece las medidas que deben adoptar los Estados signatarios dentro del marco de sus legislaciones penales sustantivas (sección 1) y adjetivas (sección 2). El capítulo III recoge los principios generales de cooperación internacional, incluyendo aspectos tales como extradición, asistencia legal mutua e intercambio de información. Por último, el capítulo IV recoge lo que se refiere a las Disposiciones Finales.

La sección 1 del Capítulo II está dividida, a su vez, en cinco títulos que establecen nuevas categorías penales sobre conductas asociadas con el almacenamiento, tratamiento y transmisión ilegítima e intencional de datos a través sistemas de cómputo (hardware) y programas informáticos (software).

El título 1 describe dentro de los "Delitos contra la Confidencialidad, Integridad y Disponibilidad de los Datos y Sistemas Informáticos" a los siguientes actos: "Acceso ilícito", "Interceptación ilícita", "Interferencia en los datos", "Interferencia en el sistema", y "Abuso de los dispositivos".

Por su parte, el título 2 contempla los "Delitos Informáticos", estableciendo como los siguientes actos o conductas: "Falsificación Informática" y "Fraude Informático".

El título 3 establece los "Delitos relacionados con el contenido". Dentro de esta categoría se encuentran las siguientes formas de comportamiento antisocial: "Delitos relacionados con la pornografía infantil": y dentro de estos: Producción, ofrecimiento, difusión, adquisición y posesión de Pornografía Infantil.

El título 4 regula los "Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines", reconociendo la necesidad de dar validez a los acuerdos internacionales sobre esta materia, entre otros, la Convención de Berna para la Protección de Trabajos Literarios y Artísticos, y el Tratado sobre Derechos de Autor de la Organización Mundial de la Propiedad Intelectual (OMPI).

Por último, el título 5 establece un régimen de responsabilidad penal para las personas jurídicas que estén involucradas en alguna de las conductas descritas en los primeros cuatro títulos. Señalando la "tentativa y complicidad", la "responsabilidad de las personas jurídicas" y "Sanciones y medidas".

Por otra parte, la sección 2 del capítulo II contiene las condiciones y principios que han de orientar las normas de procedimiento en materia de delitos informáticos.

Adicionalmente, en esta misma sección están contempladas algunas medidas judiciales concretas, a saber: (1) Medidas cautelares tendientes a la preservación de la integridad y custodia de datos informáticos; (2) Medidas tendientes a obtener la divulgación total o parcial de datos informáticos; y (3) Órdenes de búsqueda y allanamiento de datos informáticos almacenados en sistemas de cómputo; (4) Órdenes para la recolección e interceptación de datos informáticos en tiempo real. Estas medidas u órdenes, emitidas por autoridad competente, de conformidad con las disposiciones normativas internas que adopten los Estados signatarios, podrán ser dirigidas tanto a individuos como a proveedores de servicios de interconexión informática (ISP, Internet Service Providers) que estén domiciliados o establecidos, respectivamente, dentro del territorio nacional de cada Estado.

Finalmente, la sección 3 reconoce los distintos ámbitos de competencia en los que es viable ejercer la acción penal sobre aquellos delitos descritos en la sección 1. En este contexto, queda establecido, salvo reserva hecha por el Estado, que tendrán competencia las autoridades nacionales en cualquiera de las siguientes circunstancias: (1) Cuando el delito sea cometido dentro del territorio del Estado; (2) Cuando el delito sea cometido a bordo de un buque con la bandera del Estado; (3) Cuando el delito sea cometido a borde de una aeronave con la bandera del Estado; y (4) Cuando el delito sea cometido por alguno de sus nacionales, si éste es punible de acuerdo con las leyes del lugar en que fue cometido, o si fue perpetrado fuera de la jurisdicción territorial del Estado.

La Convención sobre Delitos Informáticos constituye sin duda el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos. La misma tiene lugar en momentos en que el Internet ha dejado de ser tan solo el vehículo más idóneo para la propagación y perfeccionamiento de actos criminales bajo condiciones de anonimato, sino que además representa el entorno más frecuentemente utilizado para la financiación de este tipo de actividades. Como una muestra evidente de la aplicación efectiva de sus normas sobre cooperación internacional, la actividad conjunta de autoridades policiales en países como Inglaterra y España ha permitido desmantelar un número considerable de células criminales dedicadas a la producción y comercialización de pornografía

infantil a través del Internet. Corresponde ahora a los países latinoamericanos, y al nuestro en particular, la responsabilidad de reconocer la importancia de establecer sanciones y mecanismos de investigación adecuados, que sean lo suficientemente avanzados y dinámicos como para hacer frente a este tipo de actividades delincuenciales que afectan a la raíz misma de nuestra sociedad, una sociedad que ha llegado a ser denominada por algunos como "sociedad de la información o sociedad red".

3. JURISPRUDENCIA Y CASOS EMBLEMÁTICOS SOBRE DELITOS INFORMÁTICOS.

Jurisprudencia, en algunos países este término designa la ciencia del Derecho en un sentido global. Así, en Italia las facultades de Derecho se denominan Facoltà de Giurisprudenza. En el mundo hispánico, en cambio, jurisprudencia posee un significado distinto: es el criterio constante y uniforme de aplicar el Derecho por parte del Tribunal Supremo.

No puede equipararse su sentido en los ordenamientos hispanoamericanos respecto al que tiene en el Derecho anglosajón, donde al precedente judicial (la respuesta que los tribunales hayan dado en casos análogos enjuiciados con anterioridad) le asiste verdadera fuerza de ley, y hasta superior a la ley si se

considera que multitud de cuestiones no se encuentran reguladas de forma legal, dejándose al criterio del juez la auténtica creación del Derecho. No tiene la jurisprudencia en el mundo hispánico carácter de fuente de Derecho en el sentido técnico, pero sí una importancia decisiva. Un abogado cuenta con una enorme probabilidad de éxito si lo que alega en favor de su cliente o representado ha sido decidido de esa misma manera en resoluciones judiciales anteriores. No cabe duda que el Derecho vivo se encuentra antes en la jurisprudencia que en la ley, pues si el ordenamiento jurídico consiste en una norma jurídica abstracta y general, lo relevante en la práctica consiste en cómo se adapta, aplicando esa norma general al caso concreto.

Ocurre en numerosas oportunidades que las resoluciones constantes y uniformes emitidas por el Tribunal Supremo en un determinado sentido acaban consolidando un criterio firme que, en lenguaje jurídico, sienta jurisprudencia y a menudo modifica los propios términos en que se expresa la ley vigente. Por ejemplo, es habitual encontrar en los códigos civiles que para que una persona deba reparar el daño que ha causado a otra, ha de haber existido culpa o negligencia por su parte, es decir, descuido, ligereza, en suma. Sin embargo, la forma de asimilarse este requisito por parte de los tribunales ha llevado a considerar a la culpa como una exigencia innecesaria en la práctica: el imperativo de proteger a las víctimas, por ejemplo, de un atropello por un vehículo de motor, hizo que los tribunales desde mediados del siglo XX entendieran que lo importante es que el daño quedase reparado, mediara o no

culpa del conductor, incluso aunque éste haya sido cuidadoso y precavido al conducir su automóvil.

Es fácil observar que un criterio mantenido de forma constante por la jurisprudencia de espaldas a lo que la ley determina, acaba propiciando que el propio ordenamiento jurídico se reforme y autorregule para adecuarse a la cambiante realidad de las cosas. Se dice entonces que, aunque la jurisprudencia no sea una fuente de Derecho en sentido formal, termina siéndolo en sentido material, al asignar a la ley su sentido y alcance práctico y concreto.

En otro orden de cosas, se denomina jurisprudencia constitucional a la que emana del Tribunal Constitucional o de Garantías Constitucionales, al que compete como finalidad básica y esencial procurar y garantizar que la Constitución, como norma suprema del ordenamiento jurídico, cumpla también una función rectora en la aplicación cotidiana del Derecho. Este tribunal se erige de esta manera en intérprete supremo de la Constitución.

Por último, tienen algún interés las declaraciones de tribunales inferiores (la denominada pequeña jurisprudencia) aunque en propiedad sólo es jurisprudencia la que emana del Tribunal Supremo y del Constitucional; los jueces y tribunales de rango inferior no dejan de ser órganos encargados de aplicar las leyes. Además, existen y surgen cuestiones que no pueden ser

tratadas por el Tribunal Supremo porque la ley establece que el proceso concluya en tribunales de inferior categoría.

En lo que respecta a los delitos informáticos podemos mencionar, muy brevemente, cierta Jurisprudencia que ha sentado un importante precedente en lo que respecta a este tipo de criminalidad:

❖ CHILE

Análisis de la Ley N°19.223: El bien jurídico protegido, según la historia fidedigna de esta ley, es: La calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan.

Sin embargo, importante doctrina sostiene que los Delitos Informáticos son «pluriofensivos, por lo que atentan contra diversos bienes jurídicos, a saber, la propiedad, la intimidad, etc.».
La doctrina suele clasificar los tipos penales de esta ley en: a) delitos de espionaje informático y b) delitos de sabotaje informático.

Esta ley consta de tan solo cuatro artículos, de los cuales los artículos 1, 3 y 4 exigen un dolo específico o directo en la comisión del delito, al exigir el tipo un actuar «malicioso».

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

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

Parte de la doctrina sostiene que no se tarta de un Delito Informático propiamente tal, sino más bien de un «delito de daños convencional». Además, en esta disposición se mezcla erróneamente el daño producido al «software» con el «hardware».

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

Se trata de un delito de espionaje informático, requiriendo el sujeto activo actuar con una determinada motivación, precisamente aquellas que el mismo tipo penal describe: «con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en él».

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

Nos encontramos frente a una especie de sabotaje informático, requiriendo el elemento subjetivo la concurrencia de un dolo específico o directo.

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

Nuevamente se trata de una especie de espionaje informático, requiriendo el tipo un dolo específico. Además, se contempla una figura agravada, cuando quien incurre en este delito es el responsable del sistema.

Un ex empleado de la empresa ATI Chile, entre los días 28 de diciembre de 2001 y 8 de enero de 2002, realizó diversas intromisiones ilegales al servidor de ésta, alterando, dañando y conociendo indebidamente información contenida en éste. Los sitios Web afectados fueron: http://www.guestbook.cl/ y http://www.metabuscador.cl/

El imputado era un joven de 19 años, conocido en el Chat IRC con el seudónimo «P0key», el cual habría actuado por «venganza» en contra de la empresa, pues había sido despedido de ésta.

El «cracker» al ingresar ilegalmente a estos sitios, alteró el contenido de éstos, creando una nueva página Web (index.html) en reemplazo de la existente, que mostraba mensajes ofensivos («Sí, soy un criminal …, mi crimen es ser mejor que todos ustedes, algo que jamás me perdonarán …») hacia la empresa e indicaba que el sitio había sido hackeado.

El administrador del sistema informático procedió a efectuar una inmediata auditoria de todos los archivos «LOG» del servidor y pudo comprobar que dichos sitios habían sido víctima de una serie de ataques e intromisiones, además, la eliminación de algunos archivos de auditoria de transacciones de cuentas de FTP, para borrar rastros desde dónde se efectuaban los ataques. Incluso, mientras se realizaban las auditorias, se pudo comprobar que el «cracker» intentaba ingresar al correo electrónico del gerente general de la empresa, hecho que pudo ser controlado a tiempo.

Se pudo comprobar que el 90% de los ataques provenía desde una IP fija, que correspondía a un Cibercafé en el cual el imputado trabajaba como administrador. El resto de los ataques provenía desde cuentas conmutadas de acceso a Internet, fundamentalmente desde el domicilio del imputado.

Una vez iniciada la investigación y presentada la querella criminal por delitos informáticos, el caso tomó especial importancia en la prensa de la ciudad de Talca y entre los usuarios del Chat IRC. Aprovechando este momento, el

imputado concurrió en forma voluntaria al diario El Centro de Talca y entregó una entrevista, siendo portada, bajo el título: «Yo soy el ciber pirata». De esta manera lograba la fama y reconocimiento por sus pares, hecho buscado comúnmente entre los «crackers». Incluso ofrecía sus servicios para reparar las fallas de seguridad del sistema.

El día fijado para la audiencia de preparación del juicio oral, los intervinientes: Ministerio Público, Defensor Penal Público y Querellante, acordaron proceder conforme al Procedimiento Abreviado. Para ello el querellante tuvo que desistirse de otros dos delitos a fin de cumplir con los requisitos establecidos en el Código Procesal Penal. Una vez realizadas las preguntas de rigor al acusado, la Juez de Garantía señora Marta Asiaín Madariaga, autoriza la realización del juicio abreviado y da la palabra al fiscal para que exponga el caso.

El fiscal jefe de la ciudad de Talca don Carlos Olivos Muñoz, realizó una clara exposición respecto de los hechos, la investigación realizada, todos los medios de prueba reunidos durante ocho meses de investigación y solicitó la aplicación de una pena de 3 años y un día de presidio, por tres delitos informáticos: artículos 1, 2 y 3 de la Ley 19.223.

El querellante, abogado Alberto Contreras Clunes, ratifica todo lo señalado por el fiscal y recalca la gravedad de los delitos imputados, los perjuicios ocasionados a la empresa y el actuar malicioso del acusado. También resalta el

hecho que el acusado confiesa su participación en su declaración policial y el jactarse de ello en la entrevista del diario El Centro.

Importante resulta la inclusión de un peritaje informático realizado por la Brigada del Ciber Crimen de la Policía de Investigaciones de Chile. En efecto, se realizó un peritaje a la computadora que ocupaba el acusado en el Ciber Café, como a su computadora personal. Por medio de un sofisticado programa, inaugurado en esta ocasión, se logra recuperar diversos archivos borrados del disco duro de la CPU del Ciber Café. Merece especial atención uno, consistente en un correo electrónico enviado por el acusado a su pareja en el cual le cuenta: «estoy borrando unas («weas») que me pueden comprometer en los asuntos judiciales…», enviado precisamente en la tarde del día anterior al que prestó declaración policial.

En sus conclusiones el peritaje señala que: «El computador en cuestión cuenta con las capacidades técnicas necesarias y los programas adecuados tanto para navegar por Internet como para efectuar daños a sistemas informáticos». En efecto, se pudo determinar que el disco duro contenía 24 programas: «… de uso frecuente por los Hackers, Crackers o Criminales Informáticos».

Finaliza el querellante señalando la importancia que tiene la informática en la actualidad, las potenciales víctimas de este tipo de delitos y los graves perjuicios que se causan a las empresas, pudiendo éstas llegar a quebrar

económicamente por el desprestigio que estos delitos le provocan, solicitando la imposición de una pena de cinco años de presidio, en atención a tratarse de reiteración de delitos, contemplados en los artículos 1, 2 y 3 de la Ley 19.223.
Por su parte el defensor penal público don Joaquín Lagos León, alegó indicando que no se encontraba acreditada la participación de su defendido en los hechos, negándole valor a la declaración policial.

Introdujo una novedosa jurisprudencia del derecho norte americano, en la cual se penaliza a las empresas que ofrecen servicios de seguridad informática y son víctimas de «hackers», puesto que no dan cumplimiento a los servicios ofrecidos (La empresa víctima se dedica sólo a «Web hosting», es decir, alberga páginas Web, las diseña y mantiene).

Trata en detalle las circunstancias personales del acusado, indicando que se trata de un joven autodidacta en computación, de esfuerzo, padre de familia, casado. Solicita la absolución de su representado y en caso de condena, se aplique el mínimo de la escala, esto es, la pena de 541 días de presidio, con el beneficio de libertad vigilada, al no registrar antecedentes penales.

Al finalizar la audiencia, la Juez de Garantía dicta su veredicto: Culpable por los delitos N°1, 2 y 3 de la Ley 19.223, fijando la fecha de la lectura del fallo para el día 11 de abril de 2003.

El fallo consta de 13 fojas en las que pormenorizadamente se analizan todos los medios de prueba, describiendo en forma precisa el actuar delictivo y la forma en que éste se encontraba acreditado.

Al fijar la pena, la Juez advierte que tratándose de reiteración de delitos resulta más beneficioso aplicar una pena única conforme al artículo 351 del Código Procesal Penal. Señala también que lo dispuesto en el inciso cuarto de dicho artículo, es: «una facultad para el Tribunal» en consideración a que el querellante solicitó una pena superior a la del fiscal.

Por otra parte, afirma que: «la entidad de las atenuantes no nos convence, teniendo presente que según quedó establecido se trata de delitos reiterados, por lo que la pena que se impondrá en el grado señalado se considera más condigna con el actuar ilícito del acusado».

En atención a ello aplica la pena de tres años y un día de presidio, que es el mínimo de la escala penal de presidio menor en su grado máximo.

COMENTARIOS

Tratar los Delitos Informáticos es en sí un tema complejo. Sin embargo, el fallo da la pauta que se ha comprendido en toda su dimensión el tipo penal y las consecuencias que de él derivan.

Siendo muchas veces la prueba pericial esencial en el esclarecimiento de los hechos y la participación del autor de estos ilícitos, ella fue cabalmente

comprendida y acreditó, más allá de toda duda razonable, la participación culpable del acusado.

La oportuna incautación de la CPU del acusado y del servidor del Ciber Café, además, del análisis exhaustivo dichos equipos; logró precisar con fecha, hora, minuto y segundo cuando se cometieron los ataques, como también el lugar de origen de éstos y el usuario que los realizó.

La oportuna detección de los ataques y las rigurosas medidas de seguridad aplicadas por la empresa, evitaron que los daños y perjuicios fuesen mayores.
La adecuada colaboración entre el fiscal jefe del Misterio Público de la ciudad de Talca señor Carlos Olivos con el abogado querellante y la víctima, lograron diseñar una investigación que a lo largo de ocho meses obtuvo abundantes medios probatorios que incriminaron al imputado.

Siendo éste el primer caso sobre Delito Informático dentro de la reforma procesal penal chilena y la meridiana claridad de los fundamentos en la sentencia condenatoria, la ha convertido necesariamente en un obligado precedente.

Es necesario destacar que, más allá del éxito en la resolución del caso, existió una empresa que se atrevió a denunciar el delito, con todas las consecuencias

que trajo para con sus clientes y prestigio, algo que por lo general no hacen las víctimas de estos delitos.

Como conclusión final simplemente cabe señalar que en la actualidad existe suficiente tecnología para investigar este tipo de delitos y, mejor aún, es posible sancionar a los autores de éstos, erróneamente denominados «hackers», siendo en rigor, simples delincuentes informáticos.

❖ ARGENTINA

Sentencia Del Juez Del Juzgado Federal en lo Criminal y Correccional Nº 12 de Buenas Aires, Argentina de fecha 20 Marzo del 2002 sobre supuesto Delito De Hackeo.

"…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 ------ - el cual habría sido enviado a través del servidor Startel, cuyo usuario emisor habría sido la firma ------.

… 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 5º 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 5º 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:

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. 3º del C.P.P.N.)…"

COMENTARIOS

El objeto de la acción, es decir alterar el sitio Web de la Corte Suprema de Justicia Argentina, cual no se encuentra protegido por el Código Penal

Argentino, dado que si bien la información puede integrar el patrimonio de una persona, no es cosa a los fines del derecho penal, salvo vulnerando la proscripción de analogía que dimana del principio de legalidad. Nos encontramos frente a una situación análoga a la ya esbozada de los derechos y los documentos que los prueban. El valor intrínseco de la información poco tiene que ver con la energía que permite su manifestación material (su flujo, intercambio, etc.), dado que, como se ha sostenido, en la Sociedad actual reviste la naturaleza de interés colectivo sustancial (al igual que el medio ambiente, su ataque supone la vulneración de un complejo entramado de relaciones socio-económico-culturales, sin posibilidad de establecer "a priori", como acontece con otros bienes jurídicos, aún con provisoriedad, el grado y la extensión del daño causado). Señalar que la información es cosa porque es detectable materialmente, dado que se trata de energía y, por ende, es susceptible de ser objeto del delito, es un reduccionismo inaceptable.

Si la información pudiera identificarse con la sustancia que le permite ser expresada, tampoco se advierte en el caso examinado de qué manera se vió disminuída o eliminada esta energía, teniendo presente que la alteración no es típica -salvo aquella que recaiga sobre su sustancia y que permanezca de una manera indeleble o considerablemente fija-. La conclusión a la que arriba el fallo (atipicidad de la conducta del sabotaje informático), si bien no profundiza en el concepto de información como interés social que amerita especial protección penal, mediante su elevación a la categoría de bien jurídico, ni aclara la naturaleza que el Magistrado le asigna a un sitio web, en modo

alguno implica que las conductas de "hackear" o de "crackear" sean legales. El ordenamiento jurídico argentino (vgr.: el derecho civil, el administrativo) puede brindar una respuesta reparatoria para el daño causado (por ejemplo, a través de la obtención de una indemnización por daños y perjuicios), pero no será posible hacerlo, atento al estado legislativo actual, sin vulnerar garantías de raigambre constitucional, mediante la última herramienta de control social: el derecho penal.

La necesidad de una legislación específica en la materia ha quedado de manifiesto, con meridiana claridad, con este fallo que comentamos y ha sido el despertar para muchos a la realidad de un anacronismo y una desactualización del ordenamiento penal positivo argentino en materia de conductas disvaliosas que recaen sobre las nuevas tecnologías de la información y que, en muy poco tiempo, también constituirán un grave problema social.

CASOS EMBLEMÁTICOS

A) INTERNACIONALES

❖ La página oficial de Bush atacada con éxito.

La seguridad de la página oficial que promociona la campaña de reelección de George Bush fue comprometida el día 26 de Octubre del 2004. Ayer miércoles

aparecía un mensaje de error cuando se intentaba acceder a ella. Fuentes oficiales han confirmado que la página se encuentra inoperativa por haber sufrido una intrusión.

El mensaje en la página web oficial con la que George Bush promociona su reelección a presidente de los Estados Unidos: www.georgebush.com, prohibía el acceso a la web y era el siguiente:

Access Denied, You don't have permission to access "http://www.georgewbush.com/" on this server. (Acceso Negado, no tienes permiso para accesar a *http://www.georgebush.com/* en este servidor)

Organizadores de la campaña han confirmado a Reuters que se trata de una medida de prevención ante los ataques sufridos durante el día de ayer, que apuntan a que podrían tratarse a un intento de denegación de servicio, aunque no queda claro si los delincuentes llegaron a tomar posesión de la máquina. Ya a finales de junio el experto en seguridad Richard Smith avisó de los posibles problemas de seguridad que sufrían tanto la página oficial de Bush como la de su principal rival John Kerry. Ambas cometían "descuidos" de seguridad comunes a otras webs. Pero fue un usuario anónimo quien facilitó a una página de noticias un informe detallado de todos los problemas de seguridad que sufría el servidor de George Bush, demostrando lo vulnerable del sitio. Sin duda han sido estas vulnerabilidades las que han facilitado el ataque exitoso a la página web.

❖ Primer cracker condenado a cárcel en España

La sentencia 312/04 del Juzgado de lo Penal número 7 de Valencia ha condenado a dos años de pena de carcel a Óscar L.H., creador del virus "Cabronator", según informa La Vanguardia.

Este virus afectó cerca de 100.000 usuarios, de los cuales el condenado pudo acceder a sus datos personales de sus discos duros una vez los usuarios visitaban la página que había creado y que instalaba dicho software. Añadido a la pena de cárcel, el condenado deberá indemnizar a la red de chat IRC-Hispano y a particulares perjudicados que presentaron acusación en la vista.

La detención fue llevada a cabo por la Guardia Civil en abril del 2003. Además se registro el domicilio de Óscar L.H., donde se encontraron documentos y fotografías de los usuarios afectados.

❖ Descubierto fraude utilizando banco en Internet falso

El Servicio Nacional de Inteligencia Criminal (NCIS), perteneciente a la policía británica, ha informado de la detección de un banco falso en Internet que ha sido usado para estafar al menos a dos personas con al menos 100.000 dólares.

El supuesto ciberbanco usaba un nombre de dominio muy similar al de un gran banco británico, según ha informado Europa Press.

Las dos únicas víctimas que por el momento han denunciado, son canadienses y habían sido atraídas a la web por presuntos ciudadanos nigerianos que les habían dado acceso a cuentas ficticias.

Tras comprobar el funcionamiento del servicio bancario fueron convencidos para que entregaran su dinero con la promesa de que se multiplicaría en un plan fraudulento y que sería reintegrado a las cuentas ficticias.

❖ Un universitario detenido en Boston por espiar computadoras

Un joven estudiante universitario ha sido acusado de instalar un programa informático en decenas de computadoras para capturar las teclas que los usuarios tecleaban. Una vez almacenada esa información la utilizó para robar 2.000 dólares.

Este caso pone de manifiesto las vulnerabilidades que existen en computadoras destinadas al acceso público, como cibercafés, bibliotecas públicas, salas estudiantiles, etc...

El acusado, Douglas Boudreau, instaló el programa espía en más de 100 computadoras del Boston College. La información que logró capturar iba desde claves para el acceso a cuentas de correo a información para realizar operaciones bancarias online. Así, el universitario se hizo con una base de datos de unas 4.800 personas entre profesores, personal administrativo y alumnos del Boston College.

Boudreau se puede enfrentar a una sentencia de 20 años de prisión, si se le encuentra culpable.

❖ El Juez Garzón pide a EE.UU. la investigación de una web, por insultos contra el Rey de España

El Juez Baltasar Garzón, titular del Juzgado Número 5 de la Audiencia Nacional, ha enviado una comisión rogatoria internacional a las autoridades estadounidenses para que investiguen una página web en la que se profieren insultos al Rey y a otros miembros de la familia real, según han informado a Europa Press fuentes judiciales.

La página en cuestión se encuentra alojada por la empresa "Yahoo Inc." y se presume que sus autores son de nacionalidad española.

Al parecer, casi todos los miembros de la familia real son insultados de alguna u otra forma en los contenidos del sitio en Internet.

En una de las páginas se encuentra una foto de baja calidad, pero que se puede distinguir que es la familia real y que bajo la misma reza la siguiente frase "No, kiero makakos", como una opción a seleccionar.

El artículo 491 del Código Penal, perteneciente al capítulo II de Delitos contra la Corona, establece que "las calumnias e injurias" contra algún miembro de la familia real "serán castigadas con la pena de multa de cuatro a veinte meses". En su apartado segundo, el mismo artículo añade que "se impondrá la pena de multa de seis a veinticuatro meses al que utilizare la imagen del Rey o de cualquiera de sus ascendientes o descendientes, o de la Reina consorte o del consorte de la Reina, o del Regente o de algún miembro de la Regencia, o del Príncipe heredero, de cualquier forma que pueda dañar el prestigio de la Corona".

❖ Detenido un joven por estafar a 39 personas a través de la Red

J.C.G., de 23 años de edad, ha sido detenido en San Antonio de Benagéber (Castellón) por la Guardia Civil por haber estafado presuntamente a 39 personas en el territorio nacional la cantidad de 18.300 euros realizando supuestas ventas a través de la Red.

Parece ser que el detenido utilizaba una identidad falsa de una persona de Meliana (Valencia), a quien parece ser había sustraido la documentación para poder abrir una cuenta bancaria en la que solicitaba le fueran ingresadas las cantidades de los productos ofertados.

Uno de los perjudicados denunció los hechos en abril del 2004, fecha desde la que la investigación ha estado abierta.

Las investigaciones llevadas a cabo por el Equipo de Delitos Telemáticos de la Comandancia de Castellón dieron con el punto de origen desde el que se estaban realizando las conexiones y demás, y descubrió que había más perjudicados, un total de 39.

El vecino de Meliana al que le fue suplantada la identidad para llevar a cabo dichas acciones le ha supuesto tener que acudir a diversas citaciones judiciales como autor de las estafas, y su puesto de trabajo se ha visto afectado por los continuos permisos a los que se ha visto obligado a solicitar para poder hacer acto de presencia en las mismas.

B) NACIONALES

❖ Sistema para escrutinio electoral fue alterado en segundo simulacro

A solo dos semanas de celebrarse las elecciones presidenciales, la Junta de Vigilancia Electoral demostró la vulnerabilidad del sistema de transmisión de resultados al lograr ingresar al mismo y alterar la información sobre los votos obtenidos por cada partido. Los integrantes de la JVE piden ahora la destitución del Gerente de Tecnología e Información del TSE.

La vulnerabilidad del sistema para escrutar los votos el próximo 21 de marzo quedó en evidencia tras el segundo simulacro de transmisión de resultados realizado el día de ayer. Los miembros de la Junta de Vigilancia Electoral (JVE) lograron entrar al módulo de auditoría y control de resultados, introdujeron actas falsas de 6 juntas receptoras de votos y dejaron con cero votos a tres partidos y con 400 al restante.

"No tenemos una aplicación informática para el proceso de transmisión de resultados. El sistema no provee mecanismos de alerta y, por lo tanto, cualquier intruso puede entrar sin que lo detectemos", se lamentó esta tarde el magistrado por el CDU, Juan José Martell.

A las 11:40 p.m. de ayer, mientras el TSE continuaba con la segunda prueba del sistema, la JVE, en colaboración con los magistrados del Tribunal, hizo un corte al sistema para verificar la información que había sido alterada.

"Se puso a cero toda la base de datos y se necesitaron 30 minutos para volver a recuperar la información perdida. Sin embargo, los datos de los últimos siete

minutos que se habían trabajado, los perdimos y tuvimos que volver a ingresarla", relató Martell.

Al poner los resultados en pantalla, el error era más que evidente: ningún voto para tres partidos y 400 votos para el cuarto.

El objetivo era claro: tanto los magistrados como la JVE querían demostrarle a los técnicos de la Gerencia Técnica e Informática (GTI) que el sistema "sí era violable", según Martell

"La JVE lo que quería era probar la vulnerabilidad del sistema. No haberlo hecho implicaba la vulnerabilidad en el día de las elecciones. La credibilidad para la ciudadanía debe de basarse en darle a conocer toda la información, no ocultársela", dijo.

Él asegura que incluso minutos antes de poner a cero el sistema, se acercaba al gerente de la GTI, Ramón Díaz, para preguntarle si había detectado intrusos en el sistema y si éste no había sido violado. Díaz aseguró en todo momento que todo marchaba con normalidad.

"El sistema no es confiable y lo hemos demostrado. Nuestro trabajo es ser fiscalizadores del proceso y creímos oportuno y saludable hacérselo saber al país. Es complicado decírselo, pero lo es más ocultárselo", dijo Sigfredo Campos, del PDC.

El error que presenta el sistema es "de gravedad" para los miembros de la JVE. Que "cualquier intruso" pueda acceder a los diferentes niveles del sistema y llegar hasta el nivel de auditoría y conteo de votos implica, según dijeron, una fuerte deficiencia.

Ciro Cruz hijo, representante del PCN en la JVE, criticó las fallas y le puso un "0" de calificación al segundo simulacro. El pecenista fue más allá y pidió la cabeza del gerente de la GTI.

"Si al primer simulacro le dimos 4 de calificación, éste definitivamente tiene 0. Que destituyan al Gerente (Ramón Díaz), él falló", sentenció.

Elecciones2004.com.sv intentó en dos ocasiones obtener las declaraciones de Díaz al respecto, pero éste se excusó diciendo que "no tenía nada que comentar".

El afamado sistema informático que se utiliza para el escrutinio de los votos fue donado el año pasado por la Organización de Estados Americanos (OEA). Según explicó Martell, éste estaba diseñado para procesar la información de las pasadas elecciones municipales legislativas. El TSE hizo adaptaciones para utilizarlo en estas elecciones presidenciales y fue probablemente en este proceso que la seguridad del sistema quedó alterada.

TSE aún no da respuestas

"Vamos a esperar a que llegue el técnico de la OEA para conocer el trasfondo de por qué sucedió esto. La GTI ya presentó sus opiniones pero esperamos recabar más información para presentar a su debido tiempo un análisis más completo del problema", dijo esta noche el magistrado por el FMLN, Julio Hernández, tras reunirse con el organismo colegiado y las autoridades de la GTI.

Martell y el presidente de la institución, Sergio Mena Méndez, también declararon que la institución esperará a que la OEA les ayude a detectar "qué

fue lo que pasó". De acuerdo con los magistrados, se tiene previsto que durante esta semana venga el técnico de la OEA Stanley Cardona para solventar el problema.

"Todavía no podemos dar aseveraciones de si fue negligencia de la GTI o si fueron las modificaciones al software las que originaron el problema. Son detalles técnicos que los vamos a terminar de detectar con la gente de la OEA", sentenció Martell.

En relación con la destitución de Díaz, Martell, Mena y Hernández opinaron que "lo más importante en estos momentos es solucionar los problemas con el sistema".

"Vamos a hacer la valoración de responsabilidades, pero hasta el momento no hemos tomado ninguna decisión al respecto. Lo importante es que todavía tenemos un margen de tiempo que permite la corrección de esas medidas de seguridad", dijeron.

Díaz, tras la reunión de esta noche con el organismo colegiado para presentar su informe sobre lo ocurrido, se negó a dar declaraciones a la prensa.

Aunque faltan solo 13 días para los comicios, las autoridades del TSE aseguran que "técnicamente es posible solucionar el error". Para ello, dijeron, prevén realizar más simulacros de transmisión de resultados en estas dos semanas, pero focalizados únicamente en la superación del problema de seguridad en el sistema.

En todos los casos anteriormente mencionados, sean internacionales o nacionales, podemos observar que han sido cometidos mediante conductas ilícitas denominadas delitos informáticos, como lo son el hacking, el fraude informático, intrusiones no autorizadas, espionaje informático, etc., las cuales en ciertos países, como el nuestro no son penalizadas lo cual genera mayor impunidad para quienes cometen tales conductas, e inseguridad jurídica para todas las personas que se pueden ver afectadas por dichas infracciones, existiendo países que si tipifican esas conductas con el fin de prevenir la comisión en masa de los delitos informáticos en esta era de grandes avances tecnológicos, y en la cual los medios electrónicos juegan un papel importante en el mejor desarrollo de vida de las personas en todos sus ámbitos de aplicación.

CAPITULO III

ANÁLISIS DE DERECHO COMPARADO SOBRE DELITOS INFORMÁTICOS.

TÍTULO I

NECESIDAD DE LA TIPIFICACIÓN EN LA LEGISLACIÓN SALVADOREÑA

1. ANÁLISIS SOBRE LA NECESIDAD DE LA TIPIFICACIÓN DE DELITOS INFORMÁTICOS.

La sociedad es titular de variados intereses y utiliza diversos sistemas para la protección de los mismos; El Derecho Penal constituye todo un sistema de protección de la sociedad frente al ataque de determinados bienes jurídicos; cada sociedad escoge en cada momento histórico cuáles son los bienes jurídicos que va a proteger a través del Derecho Penal y en qué modo va a hacerlo, por lo que el Derecho Penal de cada Estado acaba siendo un retrato de él mismo, de sus valores e intereses.

En un país como el nuestro, en donde nos convertimos en eminentes receptores de tecnología informática, y cuya introducción es siempre más lenta que en los países del primer mundo, debemos reaccionar ante las nuevas realidades sociales, culturales y, por supuesto, jurídicas, que esta penetración de tecnología provoca.

Desde el derecho penal se deben estudiar todas aquellas posibilidades de acciones dañosas a los derechos de las personas y nuevas formas de afectación de bienes jurídicos, que por lo complejo y nuevo de esta tecnología, ya no pueden ser tratados adecuadamente desde los tipos penales tradicionales.

La necesidad de tipificar algunas acciones propias de la informática en nuestra legislación deviene de su novedad, capacidad de transformación y afectación directa de bienes jurídicos macro-sociales, como la información. Por su alto grado de complejidad, la tecnología de la informática ya no es sólo un medio para la realización de delitos tradicionales que afectan bienes jurídicos como el patrimonio, la intimidad, la vida, etc.

En virtud del Principio de Lesividad (Art. 3 del Código Penal), según el cual ningún derecho puede legitimar una intervención punitiva cuando no media por lo menos un conflicto jurídico, entendido como la afectación de un bien jurídico total o parcialmente ajeno, individual o colectivo, sólo deben ser sancionadas penalmente aquellas conductas que supongan un daño o un peligro para un determinado bien jurídico al que el legislador reputa merecedor de la especial y máxima protección que supone su instrumentación a través del Derecho Penal, el cual sólo interviene cuando el propósito criminal ya se ha manifestado al exterior y existe al menos un peligro para el bien jurídico de que se trate, lo que sucede cuando ya ha empezado la acción que puede desembocar en la realización del correspondiente tipo delictivo, lo que se

valorará conforme al modo en que ordinariamente se desarrollan los acontecimientos.

Como hemos mencionado anteriormente, el bien jurídico ha proteger en este tipo de delitos es la Información, por lo cual nuestro legislador debe de reconocer a la Información como un bien jurídico digno de la tutela penal o de relevancia penal, porque sólo de esa manera la construcción de conductas delictivas o tipos penales sería legítima.

El fundamento constitucional del Principio de Lesividad, es posible desentrañarlo a partir del Art. 2 de la Constitución, que garantiza protección a determinados bienes vitales – vida, integridad física, integridad moral, libertad, seguridad, trabajo, propiedad y posesión, honor, intimidad personal y familiar – que no forma un catálogo cerrado, sino sólo enunciativo; pues bien, respecto de esos bienes vitales – y de otros- se erige una doble función de tutela, una respecto de las personas, en cuanto a las ofensas que hagan a dichos bienes jurídicos, mediante la conminación de normas penales, que elevan esos intereses a la categoría de bienes jurídico – penales; y otra respecto de las instituciones de poder del Estado, que también quedan obligadas, a respetar y preservar esos derechos, lo cual se hace mediante la confección de normas penales, que no sean irrazonables ni excesivas, de ahí que las restricciones que se formulen como tipos penales, deben estar dirigidas también a la

conservación y defensa de los derechos fundamentales, ahí donde haya exceso, se vulnera la garantía de lesividad por parte del Estado.

Como es tradicional en la relación derecho versus realidad, ésta última cambia a velocidades mucho más altas que el derecho, y éste debe acoplarse a esos nuevos cambios. La sabiduría del legislador, a la hora de incorporar cambios y de legislar sobre nuevas realidades radica en su capacidad de crear figuras, tipos e instituciones jurídicas que no se desfasen rápidamente, lo cual pasa necesariamente por no ser minuciosamente específicos, sino por manejar un grado de generalidad que deje al aplicador de justicia el respectivo margen de interpretación y fundamentación, es decir, que el juez no se convierta en un mero aplicador matemático, sino en lo que realmente es, un conocedor del derecho, que evalúa y sopesa cada realidad específica a la luz de la norma jurídica[63].

Asimismo, una de las manifestaciones del Principio de Mínima Intervención es que la coherencia del sistema exige que el derecho penal intervenga solo en los casos más graves de ataques contra los bienes jurídicos más importantes, ya que las perturbaciones más leves de los bienes jurídicos o contra los bienes jurídicos menos relevantes son objeto de otras ramas del derecho. En otras

[63] "De ello se sigue que la interpretación judicial de la ley es también siempre un juicio sobre la ley misma, que corresponde al juez, junto con la responsabilidad de elegir los únicos significados válidos, o sea, compatibles con las normas constitucionales sustanciales y con los derechos fundamentales establecidos por los mismos(...)"; Luigi Ferrajoli; *El derecho como sistema de garantías,* Ponencia expuesta en Madrid, 1992.

palabras, existen conductas que perturban bienes jurídicos que no son penalizados o instituidos como delictivos sino que son objeto de solución por las otras ramas del derecho. Una de las finalidades de la política criminal es decidir sobre como las instituciones del Estado responden al problema denominado criminalidad, implicando además decisiones respecto ¿Qué tipos de comportamientos deben ser criminalizados?, es acá donde cobra importancia el principio de mínima intervención.

Es por ello que, encontrándonos en una época en donde el avance tecnológico es cada vez mayor y su empleo se encuentra relacionado en casi todas las actividades y desarrollo humano, es que el legislador debe de considerar y analizar que nos encontramos en un momento histórico en el que se debe de tener a la Información como un bien jurídico importante, el cual es susceptible de ser vulnerado y poner en riesgo otros bienes jurídicos también importantes, como lo sin la intimidad, el patrimonio, etc.

La necesidad de crear nuevos tipos penales para acciones propias de la informática, debe enfocarse desde una perspectiva de futuro, no de corto plazo, y desde una compresión más o menos integral de la realidad informática. Una visión de corto plazo puede hacernos caer en la tentación de tipificar conductas profundamente específicas, que por el grado de complejidad y potencialidad de la informática, con toda seguridad, serán superadas rápidamente.

Es debido a esa rapidez con que la tecnología informática avanza, que se deben tipificar acciones que pueden resultar dañosas a ciertos bienes jurídicos, con la debida claridad técnica como para evitar la constante creación de nuevos tipos, sumamente específicos, que sean superados constantemente por los avances de dicha tecnología. Lo importante es que la tipificación que se haga permita que, a través de la debida interpretación judicial —basada en jurisprudencia, doctrina y la Constitución—, pueda superarse la situación de inseguridad jurídica que genera la constante creatividad y los repentinos cambios de la informática.

1.1. ¿SON SUFICIENTES LOS TIPOS TRADICIONALES DEL CÓDIGO PENAL PARA CASTIGAR ACCIONES INFORMÁTICAS QUE DAÑAN BIENES JURÍDICOS?

Al crear un mundo novedoso y formas nuevas de relación dentro de éste, la informática comienza a crear espacios de interacción entre las personas que ya no pueden ser protegidos por los tipos penales tradicionales, lo cual propicia espacios “libres”, en donde no hay regulación ni protección de los derechos de las personas, y por lo tanto generan inseguridad jurídica para todos aquellos que hacen uso de ella, y, más aún, para quienes esta forma de tecnología se convierte en nueva forma de trabajo, comunicación y cultura, etc.

La Seguridad es un concepto que podemos estudiar desde distintos puntos de vista, en primer lugar como Seguridad del Estado, que se traduce en la capacidad que un Estado posee para afirmar su identidad en el tiempo y en el espacio, es decir, que un Estado es seguro cuando cuenta con un ordenamiento jurídico capaz de afrontar cualquier amenaza para cada uno de sus elementos constitutivos; Se habla también de Seguridad por el Derecho o Seguridad Material, está consiste en el derecho que tiene cualquier persona a encontrarse a salvo de cualquier situación de peligro o de daño, que pueda atentar contra los derechos que legítimamente le corresponden.

Nuestra Constitución Política apunta en su Artículo 1 que el Estado está organizado para la consecución de la justicia, de la seguridad y del bien común y que en consecuencia, es su obligación asegurar a los habitantes de la República el goce de la libertad, la salud, la cultura, el bienestar económico y la justicia social. Es obvio que cualquier persona espera del Estado que éste le brinde los bienes antes mencionados, no todos, sino aquéllos que más necesita. Nada es más desalentador que buscar el auxilio de Estado cuando se teme un mal inminente y no recibir una respuesta adecuada y sobre todo oportuna. Son muchos factores los que inciden para generar un ambiente de inseguridad jurídica y que a su vez repercute negativamente en nuestro desarrollo. En un país en el que las normas se cambian constantemente sin atender a criterios verdaderamente técnicos, o donde las leyes imponen trámites engorrosos e injustificadamente complicados, de tal manera que se

dificulte su cumplimiento, no podemos decir que existe seguridad. En una sociedad donde los límites de la delincuencia se vuelven incontrolables, donde los homicidios, secuestros, robos, estafas, violaciones, etc., son la constante de cada día, obviamente que no podemos hablar de seguridad. Tampoco podemos hablar de seguridad en un sistema donde el funcionario o el servidor público no cumple con capacidad y con ética a toda prueba con las obligaciones que sus respectivos cargos les imponen.

La necesidad de Seguridad Jurídica trasciende a todas las áreas, en materia de Derecho Punitivo, se traduce en la configuración de las conductas consideradas antijurídicas y en el respeto del debido proceso.

Los delitos que hasta ahora contemplan de alguna manera la intervención de la tecnología informática en nuestro código penal, no pasan de tomarla como una agravante o como un medio para la realización de tal o cual acción delictiva. Es decir, que los delitos informáticos, como tales, como aquellos que protegen el bien jurídico de la información, no se encuentran regulados en nuestra legislación penal.

Nuestro código penal, hasta este momento, no deja de ver a la tecnología informática como un “medio” para la comisión de delitos, y no ve todavía en la informática riesgos en sí mismos, es decir, la creación de situaciones y

acciones propias, completamente novedosas, que ya son difícilmente protegidas por los tipos tradicionales.

La necesidad de regular estas conductas ilícitas ha llevado a varios países, especialmente a las grandes potencias a contemplar en sus legislaciones al respecto. Así, podemos encontrar países como Alemania, donde se enfoca principalmente a la protección de datos personales contemplados en un soporte magnético, o Estados Unidos (siendo el más avanzado en cuanto a la regulación de los delitos Informáticos), el cual menciona el problema real de los virus informáticos así como también y de manera especial le da un enfoque a dichos delitos en su Ley de Privacidad; sin pasar por alto a Italia con una importante tradición criminalista, país que nos brinda una amplia gama sobre los Delitos Informáticos.

Todo lo anterior es de gran ayuda a países como el nuestro que aún no comienzan a legislar al respecto, así pues, los delitos informáticos constituyen una gran laguna en nuestras leyes penales, y el Derecho Comparado nos permite hacer una lista de los delitos que no están contemplados en nuestro Códigos Penales y que requieren análisis urgente por parte de nuestros académicos, penalistas y legisladores.

TÍTULO II

REGULACIÓN SOBRE DELITOS INFORMÁTICOS EN EL SALVADOR

1. ANÁLISIS SOBRE LA REGULACIÓN EXISTENTE SOBRE DELITOS INFORMÁTICOS EN EL SALVADOR

El Código Penal vigente de El Salvador, se aprobó por Decreto Legislativo No. 1030, 26 de Abril del 1997, fue publicado en el Diario Oficial No. 85, Tomo No. 335 del 13 de Mayo de 1997, y entró en vigencia el día 20 de Enero de 1998.

Dicho Código regula algunas conductas en ciertos tipos penales en los que la informática aparece como un medio para la comisión de tipos autónomos y distintos a los delitos informáticos. Es decir, que no se encuentran reguladas conductas autónomas de delitos informáticos en nuestra legislación, ya que el bien jurídico que se protege es cualquier otro, menos la información. En los tipos del Código Penal que a continuación mencionamos, la informática ya aparece como un medio para la comisión de éstos, pero no podemos definirlos como delitos informáticos, a saber:

❖ PORNOGRAFÍA

Art. 172.- "El que por cualquier medio directo, inclusive a través de medios electrónicos, fabricare, transfiriere, difundiere, distribuyere, alquilare, vendiere, ofreciere, produjere, ejecutare, exhibiere o mostrare, películas, revistas, pasquines o cualquier otro material pornográfico entre menores de

dieciocho años de edad o deficientes mentales, será sancionado con prisión de tres a cinco años.

En la misma sanción incurrirá el que no advirtiere, de forma visible, sobre el contenido de las películas, revistas, pasquines o cualquier otro material, inclusive el que se pueda transmitir a través de medios electrónicos, cuando éste fuere inadecuado para menores de dieciocho años de edad o deficientes mentales."[64]

El Bien Jurídico protegido es la indemnidad sexual de los menores, así como de la intangibilidad en esta esfera de los deficientes mentales, en aras, en los primeros, de lograr su adecuada educación sexual y su socialización correcta y, en los segundos, el respeto a su dignidad en este campo.

En este tipo penal la conducta típica trata de Difundir, Vender o Exhibir el objeto material por una vía directa; Por lo cual, como Objeto Material, es necesaria la existencia de alguna clase de soporte que fije los actos pornográficos. Es indiferente que se trate de libros, papeles, escritos, revistas, fotografías, dibujos, grabaciones de imagen o sonido o cualquier otro, debiendo incluirse las cada vez más extendidas actividades a través de la red informática, como Internet.

[64] Dirección Electrónica: http://216.184.102.84/

❖ VIOLACIÓN DE COMUNICACIONES PRIVADAS

Art. 184.- "El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa.

El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa"[65].

El Bien Jurídico protegido en este tipo penal es, con carácter general, la Intimidad.

La Conducta típica en el tipo básico consiste en Apoderarse, bien de las comunicaciones escritas, soportes informáticos, documentos o efectos en los que consta el secreto, o, bien, de los propios datos reservados personales o familiares, que consten en ficheros, soportes informáticos, archivos o registros, siempre que, en uno u otro caso, se realice para descubrir los secretos, sin que se exija la difusión o revelación a otro, que sí es elemento del tipo agravado del inciso segundo.

[65] Ídem.

El Objeto Material en el primer inciso son las comunicaciones escritas, soportes informáticos, documentos o efectos personales. En el segundo inciso se trata de de cualquier sistema por el que el dato reservado ha quedado incorporado al fichero, archivo, etc., existentes en este momento o que se puedan inventar en un futuro.

❖ VIOLACIÓN AGRAVADA DE COMUNICACIONES

Art. 185.- "Si los hechos descritos en el artículo anterior se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo público de seis meses a dos años"[66].

Son los mismos elementos contenidos en el Art. 184 Pn., anteriormente comentado, y cuya agravante es en razón de la característica personal del sujeto activo.

❖ ESTAFA AGRAVADA

Art. 216.- "El delito de estafa será sancionado con prisión de cinco a ocho años, en los casos siguientes: (…)

5) Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos"[67].

[66] Ídem.
[67] Ídem.

En este caso se castiga como conducta típica la realización de alguna manipulación informática, con lo que se engloban todos los casos en los que se realiza una transferencia no consentida de activos patrimoniales en perjuicio de tercero.

La Manipulación tiene que ir dirigida a lograr inferir, en el sentido de alterar, el resultado de un procesamiento o transmisión informática de datos, de tal modo que se atribuyan indebidamente ingresos o bienes o servicios o se le anulen incorrectamente débitos o gastos.

❖ DAÑOS AGRAVADOS

Art. 222.- "Se impondrá prisión de dos a cuatro años: (…)

2) Si el daño se realizare mediante manipulación informática"[68].

Con este tipo penal agravado se pretende abarcar tanto los casos en los que se produce una alteración de los datos contenidos en archivos o programas informáticos, como todos otros en los que se suprimen completamente esos datos, así como cualquier comportamiento en el que se ataque soportes físicos de los mismos, destruyendo o inutilizando los propios equipos o elementos informáticos.

[68] Ídem

❖ INFIDELIDAD COMERCIAL

Art. 230.- "El que se apoderare de documentos, soporte informático u otros objetos, para descubrir o revelar un secreto evaluable económicamente, perteneciente a una empresa y que implique ventajas económicas, será castigado con prisión de seis meses a dos años"[69].

El Bien Jurídico protegido es la capacidad competitiva de la empresa en el mercado, entendida como el interés económico en el mantenimiento de la situación de mercado.

El Objeto Material es el secreto de empresa, que ha de ser evaluable económicamente e implicar ventajas económicas.

La Conducta Típica exige un acto de apoderamiento de objetos corporales, por lo que deja sin sanción actos de alta lesividad para la empresa, como las escuchas, sirviéndose o no de aparatos o artefactos, la interceptación de telecomunicaciones y, en general, todos los comportamientos realizados por medios electrónicos que no signifiquen un apoderamiento de soportes informáticos, como puede ser el acceso no autorizado a los datos contenidos en un sistema informático.

Como podemos ver en los delitos anteriormente citados, los bienes jurídicos que se protegen son la intimidad, el patrimonio, la libertad sexual y la

[69] Ídem.

capacidad competitiva de la empresa en el mercado, pero no la información. En ese sentido, nuestro código penal es claro al establecer por cada Título, el bien jurídico que se protege. La información no es un bien jurídico tutelado en la actualidad por nuestro Código Penal, pero que para la sociedad salvadoreña y mundial es cada vez más importante. Por ejemplo, quien atenta contra la base informática de una empresa que presta servicios de correo electrónico, no sólo afecta al patrimonio de la empresa, sino que afecta el medio de comunicación e información utilizado por millones de personas en la actualidad.

La información ya no es un valor menor para esta sociedad, es un pilar fundamental que le permite mantener el ritmo y normalidad de sus actividades, y que en caso de trastocarse o atacarse puede afectar desde el normal desenvolvimiento de las actividades hasta ser la causa de un caos familiar, empresarial, nacional, regional e, incluso, mundial.

Asimismo, existe en nuestro país una Ley con carácter de especialidad, que establece ciertas conductas como delitos informáticos dentro de su competencia; cual es la LEY ESPECIAL PARA SANCIONAR INFRACCIONES ADUANERAS, Decreto Legislativo No. 521 del 20 de Septiembre de 2001, Diario Oficial No. 204, Tomo 353, del 29 de Octubre de 2001, y la cual establece en su Art. 24 lo siguiente:

❖ DELITOS INFORMÁTICOS

"Será sancionado con prisión de tres a cinco años, quien:

Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por la Dirección General;

Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación diseñado por o para tal autoridad o sus bases de datos, que de manera exclusiva y en el ejercicio de sus controles y servicios utilizare la Dirección General;

Dañe los componentes materiales o físicos de los aparatos, las maquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos o de comunicaciones, diseñados para las operaciones de la Dirección General, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra personal;

Facilite el uso del código y la clave de acceso, asignados para ingresar en los sistemas informáticos. La pena será de uno a tres años si el empleo se facilita culposamente; y,

Manipule el sistema informático o de comunicaciones a fin de imposibilitar cualquier control que con base en dicho sistema exista la posibilidad de realizar"[70].

La ley en comento, y como su nombre lo establece, es exclusiva y especial para sancionar las Infracciones Aduaneras, y del artículo citado con anterioridad

[70] Constitución y Leyes Penales de El Salvador. Editor Luis Vásquez López, Editorial LIS, 2004, pág. 451

podemos determinar que todas las conductas ilícitas o verbos rectores del tipo se realizan, directa o indirectamente, en contra de la Dirección General, la cual, según el Art. 4 de la misma ley, se refiere a la Dirección General de la Renta de Aduanas.

La aplicación del tipo penal de delitos informáticos tiene lugar debido a que la ley que se encontraba vigente adolecía de deficiencias que habían permitido el aumento de conductas irregulares dentro de la actividad aduanera, por lo que se estableció un nuevo cuerpo normativo que contemplara sanciones ejemplarizantes y contribuyera a reprimir efectivamente tales conductas.

Es por ello, que el Art. 24 de la L.E.S.I.A., constituye una de las Infracciones Aduaneras Penales, las cuales, según el inciso 4º del Artículo 3 de la LE.S.I.A., son aquellas "acciones u omisiones dolosas o culposas tipificadas como delito por la presente ley que trasgreden o violan la normativa aduanera o de comercio exterior, que provocan o puedan provocar un perjuicio fiscal o que puedan evitar, eludir, alterar, impedir o imposibilitar el efectivo control aduanero o causar daño a los medios utilizados en el ejercicio de dicha función"[71]

No podemos decir que esta ley regula genuinos delitos informáticos, ya que se limita a las infracciones aduaneras, como si fuera éste el único ámbito que pudiera afectarse. Una tipificación más genuina, general y abstracta de delitos

[71] Ibid., pág. 441

informáticos, pudiera tal vez de manera más efectiva proteger el tráfico aduanero de acciones que afectan la información directamente y que permiten cometer infracciones en las aduanas, y además evitaría la dispersión al crear una ley especial.

2. JERARQUÍA DE LA LEGISLACIÓN QUE LOS REGULAN

Debemos ser claros que los delitos informáticos, tal como los hemos definido y entendido en esta tesis, es decir, como protectores del bien jurídico de la información, no se encuentran regulados en nuestra legislación. Lo que existe en nuestra legislación es una regulación de delitos tradicionales en los que la informática aparece como un medio para la comisión del delito.

Teniendo claro ese punto podemos decir que la jerarquía de la legislación penal salvadoreña que contempla a la informática como medio de comisión de delitos tradicionales, es de carácter secundario, por tratarse del Código Penal y de la Ley Especial Para Sancionar Infracciones Aduaneras. La jerarquía de la regulación nos parece la correcta, pues es a través de la normativa secundaria que se intentará hacer efectiva la seguridad jurídica que contempla nuestra Constitución. Sin embargo, somos partidarios de no dispersar la normativa y de mantener su generalidad y abstracción, por lo que creemos que se debe

intentar mantener la codificación y evitar en la medida de lo posible la legislación especial, que tiene como consecuencia la dispersión e inflación legislativa, que desemboca finalmente en inseguridad jurídica para la población.

Tal como es presupuesto de nuestra hipótesis, la no regulación de los delitos informáticos trae como consecuencia una situación de inseguridad jurídica, por lo que no debemos plantear una solución que de manera indirecta conlleve también una situación de inseguridad jurídica, como podría ser la creación de una ley especial para regular los delitos informáticos. Muchas leyes no es sinónimo de buenas leyes. El abuso, la poca calidad del debate y de la libre expresión, no son el ejercicio legítimo de los derechos que garantiza el Estado moderno y democrático.

3. ASPECTOS NO REGULADOS CON RESPECTO AL DERECHO COMPARADO

En el derecho comparado que hemos analizado, hemos encontrado gran cantidad de regulación sobre delitos informáticos, en la cual ésta solo es un medio para la comisión de delitos tradicionales. Pocas son aquellas

legislaciones que contemplan a los delitos informáticos como tipos nuevos, con un bien jurídico específico, como es la informática.

Dentro de las legislaciones más avanzadas podemos encontrar la Argentina, con la claridad suficiente del bien jurídico a proteger. Es este punto en el que nuestra legislación no tiene claridad, al ver a la informática como un medio para la comisión de delitos tradicionales. Nuestra legislación se encuentra aún muy atrasada al entender el fenómeno jurídico provocado por la informática, y no ha detectado la trascendencia de ésta en las relaciones intersubjetivas ni en la creación de nuevas realidades y posibilidades de relacionarse, y por lo tanto la creación de un nuevo campo libre o fuera de regulación alguna, lo cual genera inseguridad jurídica, incluso para las personas que no están en relación directa con la informática.

Más que de aspectos no regulados, podemos decir que nuestra legislación aún no ha logrado proteger el bien jurídico de la información, que es el valor que con la informática ha logrado gran relevancia, al depender de ella prácticamente todo el qué hacer de la sociedad actual, no siendo fortuita la denominación de la sociedad de la información.

CAPÍTULO IV

PROPUESTA PARA LA TIPIFICACIÓN DE DELITOS INFORMÁTICOS EN EL SALVADOR

TÍTULO I

FUNDAMENTACIÓN Y PROPUESTA DE LOS TIPOS PENALES

1. HECHOS HISTÓRICOS Y PERSPECTIVAS DE FUTURO QUE JUSTIFICAN LA NECESIDAD DE SU TIPIFICACIÓN

En la actualidad existe un creciente acceso a la tecnología y a una globalización social de la información y de la economía. El desarrollo tecnológico y el mayor uso de redes abiertas, como Internet, tanto ahora como en los próximos años, proporcionarán oportunidades nuevas e importantes y plantearán nuevos desafíos. La infraestructura de la información se ha convertido en una parte vital del eje de nuestra sociedad. Los usuarios deberían poder confiar en la disponibilidad de los servicios informativos y tener la seguridad de que sus comunicaciones y sus datos están protegidos frente al acceso o la modificación no autorizados. El desarrollo del comercio electrónico y la realización completa de la sociedad de la información dependen de ello.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del

proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información"[72].

El uso de las nuevas tecnologías digitales y de la telefonía inalámbrica ya se ha generalizado. Estas tecnologías nos brindan la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios construidos sobre redes de redes. Nos dan la posibilidad de participar; de enseñar y aprender, de jugar y trabajar juntos, y de intervenir en el proceso político. A medida que las sociedades dependen cada vez más de estas tecnologías, es necesario utilizar medios jurídicos y prácticos eficaces para prevenir los riesgos asociados. Las tecnologías de la sociedad de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas. En manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público.

La delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador del mundo. Se necesita una acción eficaz, tanto en el ámbito nacional como internacional,

[72] Dirección Electrónica: http://www.e-libro.net/E-libro-viejo/gratis/delitoinf.pdf

para luchar contra la delincuencia informática. A escala nacional, no hay respuestas globales y con vocación internacional frente a los nuevos retos de la seguridad de la red y la delincuencia informática. En los países, las reacciones frente a la delincuencia informática se centran en el derecho nacional, descuidando medidas alternativas de prevención. A pesar de los esfuerzos de las organizaciones internacionales y supranacionales, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias, especialmente en las disposiciones del derecho penal sobre piratería informática, protección del secreto comercial y contenidos ilícitos. También existen considerables diferencias en cuanto al poder coercitivo de los organismos investigadores (especialmente por lo que respecta a los datos cifrados y a las investigaciones en redes internacionales), la jurisdicción en materia penal, y con respecto a la responsabilidad de los proveedores de servicios intermediarios por una parte y los proveedores de contenidos por otra.

A escala internacional y supranacional, se ha reconocido ampliamente la necesidad de luchar eficazmente contra la delincuencia informática, y diversas organizaciones han coordinado o han intentado armonizar actividades al respecto.

Todas estas acciones internacionales no han logrado calar en nuestra realidad y lograr cambiar la nula percepción de inseguridad que sentimos frente a estos

nuevos hechos, que anualmente pueden causar daños económicos millonarios. Por tanto, nuestra investigación se enfoca en la penalización de estos delitos; ya que es importante que dentro de nuestro marco legal penal se tipifiquen tales hechos, con el objetivo de brindar seguridad jurídica al usuario.

2. FUNDAMENTACIÓN CONSTITUCIONAL PARA LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS

La Constitución de la República en su artículo uno, inciso primero, establece que el Estado está organizado para la consecución de la seguridad jurídica. Y tal como lo establecimos en nuestra hipótesis: Las actividades delincuenciales que pueden cometerse a través de la tecnología informática, no se encuentran suficientemente reguladas en el derecho penal salvadoreño, generando inseguridad jurídica para las personas naturales y jurídicas que la utilizan en su desempeño, e impunidad para quienes los cometen.

La seguridad jurídica es "la certeza de la vigencia y la aplicación de la ley, tanto en los gobernantes como en los gobernados, sin discriminación ni parcialidad[73]". Si el Estado está organizado para la consecución de la seguridad jurídica, y ésta es la certeza de la vigencia y la aplicación de la ley

[73] CONSTITUCIÓN EXPLICADA. Fundación de Estudios para la Aplicación del Derecho (FESPAD). FESPAD ediciones, 1998. San Salvador

que tiene la población, podemos afirmar que no puede haber tal si en el diario vivir de las personas se dan cierto tipo de relaciones que estén fuera de cualquier control jurídico, tal como es el caso de los delitos informáticos en el país.

Según la Constitución, la persona humana debe tener seguridad jurídica, y para lograr la consecución de ésta, el Estado debe tomar las acciones necesarias y precisas. En este caso, debe tomar una acción desde el marco jurídico-penal, para cubrir aquellos espacios generados por el desarrollo de la informática que han quedado fuera de toda regulación y que por lo tanto generan inseguridad jurídica para toda una población que cada vez depende más de dicha tecnología.

Es así pues, que al demostrar que en la realidad social se han desarrollado nuevas formas de relación y ha generado nuevos valores, que no se encuentran regulados ni protegidos por nuestro derecho penal, la Constitución de la República nos manda a tomar las acciones necesarias para solventar esta situación de inseguridad, ya que ha diseñado el mismo Estado para la consecución de ésta.

La Seguridad Jurídica, la que dignifica y enaltece al hombre, es parte esencial de lo que está en juego y esto, con todos sus elementos, es demasiado importante para permitir su destrucción.

El hombre moderno busca, a través de complejos mecanismos, particularmente jurídicos, mínimos de seguridad. El Estado, se concibe para ello, para lograr seguridad sin sacrificar otros bienes o valores. El Derecho trata de eso, de satisfacer esa necesidad humana básica, el logro de la seguridad.

3. INCONVENIENCIA DE LA DISPERSIÓN E INFLACIÓN JURÍDICA: INCLUSIÓN EN EL CÓDIGO PENAL.

En la actualidad, en nuestro país "la abundancia de leyes, además de afectar la seguridad jurídica, no ha revertido la desconfianza ciudadana en las instituciones que elaboran y aplican las leyes, así como en las leyes mismas; esta desconfianza, sin mayor duda, se encuentra relacionada directamente con un marcado irrespeto a la legalidad de parte de los funcionarios públicos (...), con la falta de igualdad ante la ley y la administración de justicia, y con la dificultad para acceder a ésta; no obstante esta ineficacia y falta de congruencia de la norma con la realidad, la propaganda oficial insiste en presentar tal formalización de la vida social como sinónimo de Estado de Derecho"[74].

[74] Instituto de Estudios Jurídicos de El Salvador (IEJES); *El inicio de la administración Saca y el Estado de Derecho ¿signos de avance o retroceso?*; artículo publicado en la Revista Ciudadana, de Iniciativa Ciudadana (IC): http//www.libros.com.sv/ic/arevista.htm

Esta crisis de confianza e ineficacia de la administración de justicia esta relacionada con el fenómeno de "inflación legislativa provocada por la presión de intereses sectoriales y corporativos, la pérdida de generalidad y abstracción de las leyes, la creciente producción de leyes-acto, el proceso de descodificación y el desarrollo de una legislación fragmentaria, incluso en materia penal, habitualmente bajo el signo de emergencia y la excepción"[75].

El fenómeno de la inflación legislativa y de la fragmentación no es sólo un fenómeno que se de en nuestro país, sino que países del occidente europeo también han experimentado este fenómeno, siendo éste una de las características del deterioro del Estado Constitucional de Derecho. Para Luigi Ferrajoli, el deterioro de la forma de la ley, la falta de certeza generalizada a causa de la incoherencia y la inflación normativa representan no sólo un factor de ineficacia de los derechos de las personas, sino también el terreno más fecundo para la corrupción y el arbitrio.

Tal como lo hemos establecido anteriormente, la intención de proponer la tipificación de delitos informáticos, es evitar la inseguridad jurídica en la que pueden estar las personas en relación con ella. En ese sentido, no creemos conveniente la creación de una ley especial de delitos informáticos, pues no sólo colaboraríamos a aumentar la inseguridad jurídica en general, sino que podríamos caer en una tipificación excesivamente específica, carente de

[75] Dirección Electrónica: http://64.233.161.104/search?q=cache:g0ovrh4d4ewJ:www.trife.gob.mx/eventos_especiales/material/m2_04.pdf+Luigi+Ferrajoli,+el+deterioro+de+la+forma+de+la+ley,+la+falta+de+certeza+generalizada+a+causa+de+la+incoherencia+y+la+inflaci%C3%B3n+normativa+representan+no+s%C3%B3lo+un+factor+de+ineficacia+de+los+derechos+de+las+personas,+sino+tambi%C3%A9n+el+terreno+m%C3%A1s+fecundo+para+la+corrupci%C3%B3n+y+el+arbitrio.&hl=es

generalidad y abstracción, y por tanto inefectiva para la tutela real de los bienes jurídicos y los derechos de las personas.

Es por ello, que en concordancia con la necesidad de generar seguridad jurídica para las personas que hacen uso de la informática, creemos que los nuevos tipos deben formar parte del código penal, y que además deben gozar de la generalidad y abstracción suficiente como para adaptarse a los cambios vertiginosos de esta tecnología.

4. PROPUESTAS DE TIPOS PENALES A ADOPTARSE EN EL DERECHO PENAL SALVADOREÑO

Las características que deben tener los tipos que propondremos pueden resumirse en dos: generalidad y abstracción[76], aunque no sean éstas las únicas, pero sí las principales, sobre las que basaremos nuestras propuestas. La generalidad ligada con el margen de interpretación judicial que debe tener cada norma, la cual no debe ser una formula para aplicar matemáticamente por parte del juez, pues la ausencia de generalidad desemboca en la excesiva

[76] Dirección Electrónica: http://64.233.161.104/search?q=cache:g0ovrh4d4ewJ:www.trife.gob.mx/eventos_especiales/material/m2_04.pdf+Luigi+Ferrajoli,+el+deterioro+de+la+forma+de+la+ley,+la+falta+de+certeza+generalizada+a+causa+de+la+incoherencia+y+la+inflaci%C3%B3n+normativa+representan+no+s%C3%B3lo+un+factor+de+ineficacia+de+los+derechos+de+las+personas,+sino+tambi%C3%A9n+el+terreno+m%C3%A1s+fecundo+para+la+corrupci%C3%B3n+y+el+arbitrio.&hl=es

particularización, fragmentación y una creciente incoherencia, falta de plenitud, imposibilidad de conocimiento e ineficacia del sistema jurídico.

La abstracción, ligada al planteamiento de un tipo con la posibilidad de no agotarse rápidamente, es decir, de no ser fácilmente superado por la realidad, ya que cuando se tipifican conductas demasiado específicas, pueden ser fácilmente superables por los constantes cambios de la realidad, sobre todo cuando nos enfrentamos a la informática, que se encuentra en constante revolución.

En el desarrollo de nuestra tesis, hemos identificado a la información, como el bien jurídico ha proteger, ya que éste "ha adquirido un valor altísimo desde el punto de vista económico [social y político], constituyéndose en un bien sustrato del tráfico jurídico, con relevancia jurídico-penal por ser posible objeto de conductas delictivas y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales".

Es así que para dar nuestras propuestas, hemos entendido por delitos informáticos "*toda acción u omisión que se encuentra tipificada en la ley, y que mediante la aplicación de la tecnología informática afecta la información contenida en un sistema computarizado o el sistema como tal, y que origina la aplicación de una sanción o pena*".

Retomando la legislación y doctrina argentina sobre delitos informáticos, por parecernos la más acertada, por apegarse a los principios de generalidad y abstracción del tipo penal, así como por su claridad en el manejo dogmático-penal del tipo, podemos proponer las siguientes modalidades de afectación del bien jurídico tutelado, y por tanto la creación de tres tipos de delitos básicos, a saber:

a) El acceso ilegítimo informático (hacking) que supone vulnerar la confidencialidad de la información en sus dos aspectos: exclusividad e intimidad.

Se ha optado por incorporar esta figura básica, en la que por acceso se entiende todo ingreso no consentido, ilegítimo y a sabiendas, a un sistema o dato informático. Es una figura básica toda vez que su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido, y del cual no se posee autorización. Así se concluye que están excluidos de la figura aquellos accesos permitidos por el propietario u otro tenedor legítimo del sistema.

El delito de hacking puede clasificarse en: a) delito de hacking directo, hacking propiamente dicho o acceso indebido, y, b) Delito de hacking indirecto o hacking como medio de comisión de otros delitos. Claudio Líbano sostiene, que

el acceso no autorizado o hacking directo "es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor". Agrega, que este ilícito tiene como elementos: la existencia de un acceso no autorizado a un sistema de tratamiento de información; su finalidad es lograr una satisfacción de carácter intelectual; el "hacker" (sujeto que comete el delito de hacking) no busca causar un daño con su actuar y, es un delito de resultado que se consuma al ser descifrados los códigos de acceso secretos y sin que, necesariamente, los usuarios tomen conocimiento del hecho. Por otra parte, el delito de hacking indirecto sería aquel en que el acceso indebido se utiliza como medio de comisión de otros delitos.

b) El sabotaje informático, conducta ésta que va dirigida esencialmente a menoscabar la integridad y disponibilidad de la información.

El termino Sabotaje proviene del francés "sabots", que corresponde al nombre que se le entregaba a los zapatos de madera usados por lo obreros hacia el siglo XVIII en Francia. Algunos obreros textiles - a modo de protesta por los constantes despidos y malas condiciones laborales - utilizaban los "sabots" con el propósito de trabar las máquinas en esas fábricas.

Sin perjuicio de lo anterior, podemos señalar que para alguna parte de la doctrina el sabotaje informático, es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Para Marcelo Huerta, el delito de sabotaje informático "Es toda conducta típica, antijurídica y culpable que atenta contra la integridad de un sistema automatizado de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en él"[77]. A su turno, Rodolfo Herrera Bravo, sostiene que el sabotaje informático es "toda acción típica, antijurídica y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional, empleando medios computacionales"[78]. A nuestro juicio, este último concepto sería más acertado, puesto que deja de lado la destrucción del hardware o soporte fisico, lo que sería lógico si se considera que este ilícito corresponde a los llamados Delitos Computacionales, es decir, La noción de "sabotaje informático" alude a los atentados que causan daños, destruyen o inutilizan un sistema computacional. Para ser exactos, la expresión debe reservarse para los atentados ilícitos que se cometan contra el software o soporte lógico -datos y programas- de un sistema informático, ya que el daño o la destrucción del hardware es una conducta de muy poca ocurrencia y comprendida en los delitos tradicionales. Los ejemplos más clásicos -en

[77] Dirección Electrónica: http://iteso.mx/~soniai/lecturas/delitosinformaticos7.pdf
[78] Ídem.

consideración a sus efectos- son las bombas lógicas, las conductas de los “crakers” y los virus computacionales.

Por otra parte, podemos señalar que dentro del elemento objetivo del delito de sabotaje informático, se encuentran dos clases de acciones:
a) acciones contra el funcionamiento del sistema de tratamiento de información, y, b) acciones que afectan los datos contenidos en un sistema de tratamiento de Información. Por otra parte, podemos agregar que algunas de las modalidades más conocidas de sabotaje informático están representada por los denominados Virus Informáticos, los que pueden ser objeto de diversas clasificaciones y que podemos conceptualizar, siguiendo la legislación Venezolana, como "aquel programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema"; El Gusano, el que se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse; La Bomba lógica o cronológica, que exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro, ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten, por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su "detonación" puede programarse para que cause

el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente.

El daño sufrido por los sistemas o programas informáticos normalmente será un destrozo funcional, un menoscabo en la correcta operatividad del sistema, incorrección que puede, al propio tiempo, proyectar sus efectos sobre otros bienes jurídicos cuya incolumidad puede depender del preciso y adecuado funcionamiento del ordenador. El resultado así entendido encierra una capacidad pluriofensiva tan variada como variadas sean las posibles utilidades que reporta el tratamiento informático y, lo que es más importante, relativiza el significado económico – no descartable en su totalidad – que es propio de la acción.

c) El fraude informático. Para el autor español Carlos Romeo Casabona, el fraude informático es "la incorrecta utilización del resultado de un procesamiento automatizado de datos, mediante la alteración en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de tercero"[79].

El ilícito de Fraude Informático no cumple con los supuestos del delito de estafa, puesto que no se aprecia la existencia de un ardid o engaño que induzca a error a una persona y que la motive para la realización de una determinada conducta ocasionándole un perjuicio. En este mismo sentido,

[79] Dirección Electrónica: http://www.alfa-redi.org/revista/data/53-8.asp

Santiago Acurio Del Pino sostiene que "al verse el tipo penal de la estafa desbordado por los nuevos avances tecnológicos aplicados por los delincuentes para efectuar sus defraudaciones, llevaron a que naciera un nuevo tipo delictivo, el fraude informático, que vendría a absorber todas aquellas conductas defraudatorias que, por tener incorporada la informática como herramienta de comisión, no podían ser subsumidas en el tipo clásico de la estafa"[80]. Al mismo tiempo, Noelia García sostiene que "los principales elementos que constituyen el delito de Fraude Informático son: el ánimo de lucro que se obtendría de la Información contenida en el sistema informático; la acción de valerse de una manipulación informática; la transferencia no consentida del patrimonio de otra persona sin utilizar violencia y la existencia de perjuicio a tercero. Como se advierte, desaparece el engaño y el error"[81].

La actuación sobre una máquina y no sobre una persona humana impide apreciar los clásicos elementos definitorios de la estafa. No se puede engañar a una máquina, pues el error que padece el engañado es sólo concebible si se refiere a una persona humana. Además, la transferencia de fondos en perjuicio de su titular puede tener lugar por la sola relación del sujeto activo y el ordenador sin intervención de otro sujeto que en función de la alteración de los datos informáticos realice la disposición patrimonial. Sólo en los casos en que con carácter previo a la transferencia se produce la concurrencia de una persona humana encargada de verificar la regularidad de los datos

[80] Ídem.
[81] Ídem.

informáticos, podrá considerarse producida la estafa si el ordenador ha sido el medio para el engaño. La inidoneidad del tipo de estafa, ha sido destacada por sentencias españolas, como la Sentencia Tribunal Supremo Español del 19 de Abril de 1991, la cual declara que "mal puede concluirse la perpetración de un delito de estafa por parte del procesado, al impedirlo la concepción legal y jurisprudencial del engaño, ardid que se produce e incide por y sobre personas… La inducción a un acto de disposición patrimonial sólo es realizable frente a una persona y no frente a una máquina… Con razón se ha destacado que a las máquinas no se las puede engañar, a los ordenadores tampoco, por lo que los casos en que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se produce ni el engaño ni el error necesarios para el delito de estafa".

Asimismo, podríamos aclarar en este momento que "Manipular", según el Diccionario de la Real Academia de la Lengua Española, significa "operar con las manos o cualquier otro instrumento", de forma que así concebido, el termino tiene tal amplitud que puede llenar los requisitos de la acción típica establecida en el Art. 216 num. 5 Pn., toda intervención – autorizada o no – en el sistema informático. Por ello se hace preciso atribuir a la expresión un sentido más restringido. Por manipulación informática puede entenderse, a tales efectos, toda acción que suponga intervenir en el sistema informático alterando, modificando u ocultando los datos que deban ser tratados

automáticamente o modificando las instrucciones del programa, con el fin de alterar el resultado debido de un tratamiento informático y con el ánimo de obtener una ventaja patrimonial, mediante la afectación de la información contenida en el sistema. La manipulación puede tener lugar actuando sobre la introducción de datos, sobre su tratamiento o sobre su salida, esto es una intervención sobre el software. Ahora bien, la manipulación no requiere un contacto inmediato con el ordenador que contiene la información o datos. Son cada vez más frecuentes los sistemas para el procesamiento de datos operados a distancia, de modo que puede accederse a una computadora, por ejemplo, a través de la red telefónica, mediante un terminal que opera a distancia. El autor puede efectuar la manipulación desde su casa, con su propia terminal y sin necesidad de introducirse personalmente en la empresa perjudicada.

En cualquier caso los problemas se plantean por la deficiente técnica empleada por el legislador, empeñado en construir figuras paralelas a las tradicionales que recogen en cada tipo el equivalente de la acción por medio de la informática, en lugar de abordar correctamente el problema del delito informático en una perspectiva globalizadora y autónoma.

La única divergencia que tendríamos con la propuesta Argentina, es que se inclina por la creación de una ley especial para delitos informáticos, lo cual no se encuentra dentro de nuestra visión de mantener la codificación y evitar la dispersión e inflación jurídica. Nos parece que no hay razón para romper con la descodificación, pues no se trata siquiera de una cantidad considerable de

nuevos tipos, sino que, por nuestra misma postura de conservar la generalidad y abstracción de la norma penal, se proponen solo tres tipos penales básicos, ya nuestro criterio, suficientes para evitar la actual situación de inseguridad jurídica que genera el despliegue de la informática.

La pena que se impone en toda la legislación comparada sobre delitos informáticos es la privación de libertad, a veces acompañada una pena accesoria, como la multa. De manera unánime en todo el derecho comparado se pena a los delitos informáticos con privación de libertad.

Tal como hemos mencionado anteriormente, la pena debe establecerse en relación de, al menos, tres criterios básicos, los cuales son:

a) El nivel jerárquico del bien jurídico afectado;

b) El grado o nivel de ofensa que se ha ejercido sobre éste; y,

c) El cumplimiento los fines de la pena, establecidos en la Constitución de la República.

El nivel jerárquico de la información, como bien jurídico, en una sociedad cuya actividad depende cada vez más de ella y sus diversas formas de utilización, debe tener un carácter relevante. La información como un valor fundamental, pues depende de ella la realización de casi todas las actividades del ser humano en sociedad de la actualidad. En la era de la información, ésta debe ser protegida por el derecho penal y la actividad que la menoscabe debe ser reprimida por éste.

No se trata nuestra tesis de proponer cantidad de años de privación de libertad que deben imponerse, pero si de hacer hincapié que el ataque al bien jurídico de la información debe ser reprimido con la mayor fuerza, que traducido a nuestro derecho penal, es la privación de libertad del delincuente, y no con un fin exclusivamente retributivo, sino para lograr su readaptación y la prevención de más ataques a dicho bien, tal como lo establece nuestra Constitución.

Creemos que nuestro derecho penal, a través de su inclusión en el Código Penal, debe reconocer a la información como un bien jurídico que debe ser protegido, pues es determinante para la actividad de la sociedad salvadoreña de la actualidad, y con toda seguridad, dicha relevancia irá en aumento con el paso del tiempo y la incursión de una tecnología de la informática cada vez más sofisticada.

CAPITULO V

CONCLUSIONES

- Debido a la relevancia que la información para el desarrollo de casi cualquier actividad humana en la actualidad, tanto a nivel internacional como nacional, nuestro derecho penal debe protegerla, pues un ataque a la información en nuestros tiempos significa atacar un pilar fundamental de las actividades humanas más diversas, que van desde el ámbito económico, cultural, social hasta el político.

- La no tipificación de delitos informáticos, provoca una situación de inseguridad jurídica, al no dar certeza de la vigencia y la aplicación de una ley en aquellos espacios novedosos, generados por el desarrollo de la informática que han quedado fuera de toda regulación y que por lo tanto generan inseguridad jurídica para toda una población que cada vez depende más de dicha tecnología.

- La penalización de los delitos informáticos, pasa necesariamente por el reconocimiento de un nuevo bien jurídico: la información.

- La creación de una ley especial de delitos informáticos contribuiría a la larga a aumentar la inseguridad jurídica, pues la creación de leyes especiales para cada aspecto de la realidad que surge o toma relevancia en cierto momento,

genera inflación legislativa, pérdida de generalidad y abstracción de las leyes, una creciente producción de leyes-acto, un proceso de descodificación y el desarrollo de una legislación fragmentaria, que a la larga, colabora con el aumento de la inseguridad jurídica, y por tanto una inefectiva tutela de los bienes jurídicos y los derechos de las personas.

- El sujeto activo del delito informático es un sujeto especial debido al grado de formación y conocimiento que se requiere para la comisión de este delito, y posee características que deben ser estudiadas por la criminología, para ahondar en la motivación de estos y vislumbrar algunos aspectos como el dolo o la culpa en la comisión de delitos informáticos.

- Las penas aplicadas a los delitos informáticos debe establecerse en relación de tres criterios básicos, como: a) El nivel jerárquico del bien jurídico afectado; b) el grado o nivel de ofensa que se ha ejercido sobre éste; y, c) el cumplimiento los fines de la pena, establecidos en la Constitución de la República.

BIBLIOGRAFÍA

LIBROS

BERDUGO GÓMEZ DE LA TORRE, I, ARROYO ZAPATERO, L, GARCÍA RIVAS, N. FERRÉ OLIVÉ, J. SERRANO PIEDECASAS, J. “Lecciones de Derecho Penal”, segunda edición, Barcelona, 1999.

CALLEGARI, NIDIA. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985.

DE LA LUZ LIMA, MARÍA. “Delitos Electrónicos”. Academia Mexicana de Ciencias Penales. Editorial Porrúa. No. 1-6. Año L. Enero-Junio 1984.

ENCICLOPEDIA OCÉANO MENTOR, grupo editorial océano, Barcelona, España, 1998.

FERNÁNDEZ CALVO, RAFAEL. El Tratamiento del Llamado "Delito Informático" En el Proyecto de Ley Orgánico del Código Penal: Reflexiones y Propuestas de la Cli (Comisión de Libertades e Informática) En Informática y Derecho.

JIJENA LEIVA, RENATO JAVIER. Chile, “La Protección Penal de la Intimidad y el Delito Informático”. Editorial Jurídica de Chile. Santiago de Chile.

LOSANO, Mario G., “Curso de Informática Jurídica”, Tecnos. Madrid 1984.

MUÑOZ CONDE, Francisco. “Teoría General del Delito”, 2ª edición, Editorial Temis S. A., 2001

MUÑOZ CONDE, Francisco; García Arán, Mercedes: “Derecho Penal” (Parte General), 2ª Edición, Temis, 1995

RÍOS ESTAVILLO, JUAN JOSÉ. “Derecho e Informática en México. Informática Jurídica y Derecho a la Informática”, Universidad Nacional Autónoma de México, 1ª Edición, México, 1997.

SARZANA, CARLO. “Criminalità e tecnología”, Computers Crime, Rassagna Penitenziaria e Criminologia. Nos. 1-2. Anno 1. Roma, Italia. Gennaio-Giugno, 1979.

TÉLLEZ Valdés, JULIO. “Derecho Informático”. Universidad Autónoma de México. 1ª Edición. México. 1991.

TIEDEMANN, Klaus, “Poder Económico y Delito”, Editorial Ariel, Barcelona, 1985

TREJO ESCOBAR, Miguel Alberto; Serrano, Armando Antonio, y Otros: “Manual de Derecho Penal” (Parte General), 2ª edición, Centro de Información Jurídica, Ministerio de Justicia, S.S., El Salvador, 1996.

LEGISLACIÓN

CONSTITUCIÓN EXPLICADA. Fundación de Estudios para la Aplicación del Derecho (FESPAD). FESPAD ediciones, 1998. San Salvador

CONSTITUCIÓN Y LEYES PENALES DE EL SALVADOR. Editor Luis Vásquez López, Editorial LIS, 2004

CIBERBIBLIOGRAFÍA

CÓDIGO PENAL COLOMBIANO CONTRA DELITOS INFORMÁTICOS: http://dragonjar.nolimites.net/HTM/DragoN.php?subaction=showfull&id=1088639499&archive=&start_from=&ucat=3&Abrir=Portada

DELITOS INFORMÁTICOS, Año 2000: http://www.e-libro.net/E-libro-viejo/gratis/ delitoinf.pdf

DELITOS INFORMÁTICOS, PERFFIL CRIMINOLÓGICO DEL HACKER Y NORMATIVA APLICABLE, Año 2001: http://www.aaba.org.ar/bi180p43.htm

DELITOS INFORMÁTICOS Y NUEVAS FORMAS DE RESOLUCIÓN DEL CONFLICTO PENAL: http://iteso.mx/~soniai/lecturas/delitosinformaticos7.pdf ; http://www.alfa-redi.org/revista/data/53-8.asp

DERECHO INTERNACIONAL: http://es.wikipedia.org/wiki/Derecho_internacional

EL DERECHO COMO SISTEMA DE GARANTÍAS: http://64.233.161.104/search?q=cache:g0ovrh4d4ewJ:www.trife.gob.mx/eventos_especiales/material/m2_04.pdf+Luigi+Ferrajoli,+el+deterioro+de+la+forma+de+la+ley,+la+falta+de+certeza+generalizada+a+causa+de+la+incoherencia+y+

la+inflaci%C3%B3n+normativa+representan+no+s%C3%B3lo+un+factor+de+ineficacia+de+los+derechos+de+las+personas,+sino+tambi%C3%A9n+el+terreno+m%C3%A1s+fecundo+para+la+corrupci%C3%B3n+y+el+arbitrio.&hl=es

EL INICIO DE LA ADMINISTRACIÓN SACA Y EL ESTADO DE DERECHO ¿SIGNOS DE AVANCE O RETROCESO?: http//www.libros.com.sv/ic/arevista.htm

ÍNDICE LEGISLATIVO DE LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR: http://216.184.102.84/

LAS TEORÍAS DE LA PENA Y SU APLICACIÓN EN EL CÓDIGO PENAL: http://www.bahaidream.com/lapluma/derecho/revista002/pena.htm

LOS TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR NACIONES UNIDAS: http://www.seguridad-la.com/e_delitos_un.htm

OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html