UNIVERSIDAD DE CARABOBO
ÁREA DE ESTUDIOS DE POSTGRADO
FACULTAD DE DERECHO
ESPECIALIZACIÓN EN DERECHO PENAL

ESTUDIO DE LAS CONDUCTAS DISVALIOSAS EMERGENTES DEL NUEVO MILENIO: LOS DELITOS INFORMÁTICOS Y SU ACTIVIDAD PROBATORIA SEGÚN EL COPP

Autor: Di Fabio Bentivegna, Giuseppe
Tutora: Marcano De Araujo, Luisa

Trabajo De Especialización Presentado Ante El Área De Estudios De Postgrado De La Universidad De Carabobo Para Optar Al Título De Especialista En Derecho Penal

Valencia, Diciembre de 2002

ESTUDIO DE LAS CONDUCTAS DISVALIOSAS EMERGENTES DEL NUEVO MILENIO: LOS DELITOS INFORMÁTICOS Y SU ACTIVIDAD PROBATORIA SEGÚN EL COPP

RESUMEN

El objetivo de esta investigación fue estudiar las conductas disvaliosas emergentes del nuevo milenio: Los delitos informáticos y su actividad probatoria según el Código Orgánico Procesal Penal. Metodológicamente, el trabajo correspondió a una investigación jurídica de campo y por los objetivos específicos planteados el método fue de tipo analítico-descriptivo. Las fuentes documentales que se utilizaron, exclusivamente primarias, fueron textos jurídicos doctrinales, legales y jurisprudenciales tanto nacionales como internacionales, la Internet y la prensa nacional relacionadas con las variables objeto del estudio para cubrir la primera fase; luego, la aplicación de una encuesta de escala dicotómica, válida por verificación del juicio de expertos y la confiabilidad establecida por la aplicación del coeficiente Alpha de Cronbach; ésta se dirigió a tres estratos poblacionales y la técnica para la selección de la muestra fue intencional quedando constituida por 20 abogados en el libre ejercicio, 15 fiscales del Ministerio Público y 10 Jueces de la Circunscripción Judicial de Carabobo. Analizados e interpretados los resultados, según los métodos de la estadística descriptiva de frecuencia y porcentaje, la investigación concluyó que: Los operadores de justicia no están suficientemente preparados ni informados respecto al contenido y alcance de la Ley especial contra delitos informáticos; también se constató que la obtención y preservación de las pruebas resulta compleja y difícilmente reproducible en juicio. La confianza de los operadores de justicia en los órganos de investigación penales y criminalísticas es muy baja y se deberá propiciar su modernización a los fines de actualizarse en la investigación de este novel tipo de criminalidad.

Basado en estas conclusiones, el investigador recomienda: Actualización de los jueces, fiscales y abogados en la materia de delitos informáticos. La compilación en un solo texto jurídico todas las leyes de carácter penal.

Además de, incentivar a futuros investigadores a profundizar en el tema aquí estudiado.

Descriptotes: Delitos Informáticos, Derecho Penal.

INTRODUCCIÓN

La computación y la informática son un fenómeno plurifacético de la era moderna y postmoderna. Su expansión ha alienado rápida y ampliamente la economía, la cultura, la educación, la política entre otras áreas. Paralelamente, y como consecuencia inmediata de esos avances, la noción de delito fue mutando. Es cierto, y lo tenemos como máxima de experiencia, que el crimen existe desde que surgió el hombre. Sin embargo, este progreso tecnológico ha hecho dificultoso para el derecho su control y penalización.

Para hablar de "delito" en el sentido propio de la dogmática penal como acción típica, antijurídica y culpable es necesario que esté contemplada en textos jurídicos-penales con carácter legal; es decir, se requiere que la expresión "Delitos Informáticos" esté consignada en alguna Ley Penal, como efectivamente acontece en el caso venezolano: Ley especial contra los Delitos Informáticos.

Es imprescindible aclarar que a nivel internacional se considera que no existe una definición propia de delito informático; sin embargo, muchos han sido los esfuerzos de expertos que se ocupan del tema y aun cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales específicas.

Ante esta nueva alternativa que en el tradicional concepto de delito producen los ilícitos informáticos, ellos han obligado al Estado, frente al problema concreto que significa la delincuencia, a ampliar las estrategias y objetivos en materia de política criminal, colapsada ya con los innumerables casos de delincuencia común. La realidad demuestra que las mencionadas conductas ilícitas provienen de esta nueva criminalidad, pueden quedar impunes en algunos casos o ser muy difíciles de calificar en otros, generando incertidumbre jurídica.

Con la puesta en vigencia de esta ley se evita la duda de si determinados hechos punibles resultan aplicables en el caso de intervención de sistemas con tecnología informática. Pese a ello, emana la necesidad de interpretar los elementos que especifican estos supuestos cometidos contra o por intermedio de procesos automatizados de datos o computadoras. Se hace imperioso determinar el alcance y sentido de estos nuevos elementos y supuestos. De hecho, es posible que con los avances propios de la informática ya hayan aparecido nuevas conductas que al

legislador no pudo prever, pese al tan corto tiempo que se tiene de haber sancionado y promulgado dicho instrumento jurídico.

Otro aspecto de gran interés es el de la prueba. La novedad y diferencias fundamentales con los métodos tradicionales de comisión de delitos hacen de la investigación y obtención de la prueba de estos hechos un campo diferenciado. Es de acotar que la persecución de los delitos informáticos resulta compleja y sobre todo la individualización del agente. Igualmente, la reproducción o incorporación material de esa prueba en el proceso oral contemplado en el Código Orgánico Procesal Penal venezolano.

El presente trabajo de investigación se encuentra estructurado de la siguiente manera: Capítulo I: el problema y su planteamiento así como los objetivos general y específicos, la justificación y alcances de la investigación; en el Capítulo II: los antecedentes de la investigación, marco teórico divididos en títulos y subtítulos, y el sistema de hipótesis y variables comprometidas en la investigación; en el Capítulo III: marco metodológico; el Capítulo IV se plasma el análisis de los instrumentos aplicados al caso concreto. Seguidamente, en el Capítulo V se presentan las conclusiones y recomendaciones que son el producto final de la investigación. Por último, se exponen las referencias bibliográficas, legales y anexos.

CAPÍTULO I

EL PROBLEMA

La tradicional rigidez del sistema jurídico penal venezolano, género propio del Estado de Derecho, para adaptarse a las exigencias de la dinámica social y sus constantes cambios, ha encontrado en el mundo informático un elocuente carácter resaltante. La normativa jurídica –específicamente, la penal-, que siempre ha estado rezagada de nuestra realidad, enfrenta ahora no sólo a un mundo extraño y desconocido en sus verdaderas potencialidades que, a su vez, discurre a un vertiginoso ritmo transformativo. De "auténtica conmoción para el Ordenamiento Jurídico" califica Gutiérrez (1991, p. 42) el impacto de las nuevas tecnologías sobre el campo legal.

Es un hecho notorio que la informática nos circunda, haciéndonos cada vez más cyberdependientes, acarreando ésto una realidad incuestionable e inexorablemente irreversible. Se afirma que los sistemas de novel tecnología están en todos los ámbitos del quehacer del hombre. Los medios informáticos traspolaron su funcionalidad como simple herramienta auxiliar de soporte a las distintas actividades humanas y hoy en día se les tiene como un recurso eficaz para obtener, procesar, generar información y conectividad en red; por lo que se convierte en una nueva forma de medio de comunicación e interactuar entre individuos. En virtud de ello, sin dichos sistemas las sociedades actuales estuvieran colapsadas.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento de datos, la constante miniaturización de los chips de las computadoras instaladas en productos industriales, la fusión del proceso de 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. Se convierte así, la informática, en un instrumento difuso de poder, por medio del cual con simples conexiones remotas se logra obtener acceso a computadoras sin necesidad de la presencia física de sus operarios. Las consecuencias de este fenómeno, en prima facie, han redundado en beneficio tanto de entes gubernamentales como privados, por ser aquéllos accesos rápidos e implicando un

ahorro significativo de tiempo y recursos (tanto materiales como humano), facilitando el quehacer diario y la eficacia del trabajo cotidiano.

A la par de esa contribución al desarrollo social, cultural, económico y político que representan sin duda las técnicas y procedimientos informáticos, han surgido prácticas anómalas que van en detrimento de esos mismos sectores causando cuantiosos daños materiales, económicos y morales. Tal como lo reseña el diario El Nacional (26 de agosto de 2000) "PTJ ha recibido más de 1.200 denuncias sobre fraudes electrónicos en el año. Banca sufre pérdida de Bs. 3 millardos", en fecha (20 de septiembre de 2001) "La Policía Técnica Judicial detuvo a un individuo que mediante la clonación de tarjetas de crédito doradas cometió una estafa millonaria, aún no cuantificada" y en el Diario El Universal (del 23 de junio de 2002) se reportó "55% del software usado en el país es ilegal, los productores locales de programas son los más perjudicados"; éstos por citar sólo tres de las innumerables denuncias que cursan por ante los organismos de seguridad nacional competentes.

Imbricados en esa realidad se nota que el desarrollo tan amplio de la tecnología informática ofrece también un aspecto negativo, debido a que se han desarrollado nuevas conductas, en apariencias delictivas, hasta que las tipificó como delitos la Ley especial contra los Delitos Informáticos (LEDI, ver anexo Nº 1), que se manifiestan en la actualidad y fueron imprevistas allí por el legislador penal en un pasado reciente. Los sistemas de computadoras ofrecen oportunidades nuevas y muy complejas de infringir la Ley y han creado la posibilidad de cometer delitos tradicionales en forma no tan tradicionales.

Aparece en escena, lo que muchos autores han denominado, la criminalidad informática sustentada en la burla a los sistemas de dispositivos de seguridad, tanto en cajeros automáticos, como en máquinas tragamonedas, manipulaciones técnicas en el sistema de televisión por cable, invasiones a computadoras, correos electrónicos o sistemas mediante una clave de acceso, fraudes en la telefonía móvil celular, conductas ilícitas de personas que ingresan a sistemas no autorizados, sustracción de información, envío de mensajes falsos, alteración de datos que provocan cada vez más pérdidas dinerarias cuantiosas.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer delitos. Se tiene entonces que no son los grandes sistemas de información los que afectan el desarrollo, in genere, de los individuos y de la sociedad; sino personas o grupos con fines diversos. Originando lo que en la actualidad se conoce como Delitos Informáticos; señalamiento polémico y confuso tanto en la doctrina internacional como en las diversas legislaciones comparadas. Precisamente, porque la protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o mercantil, e incluso de derecho administrativo. Aunque estas medidas de protección no tienen que ser excluyentes unas de otras.

En irrestricta consonancia con lo anterior, la posición asumida por la legislación venezolana para proteger el vertiginoso avance de las diversas formas delictivas informáticas, dadas que las interpretaciones del ordenamiento legal vigente eran insuficientes para detener a los aprovechadores del vacío legal, fue la sanción y consecuente promulgación de la "Ley Especial contra los Delitos Informáticos", publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.313 de fecha treinta (30) de octubre del 2001 y posteriormente la Ley Aprobatoria de la "Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional", en Gaceta Nº 37.357 de fecha 04 de enero de 2002. Teniendo en cuenta, igualmente, que el desarrollo informático en el medio gubernamental nacional, estadal y municipal ha venido creciendo, como se deduce del Decreto 825, que establece la Internet como prioridad nacional, que a juicio de Genatios citado por Tablante (2001, p. 10-11) expresa que, "este decreto exige la creación de estrategias de desarrollo y modernización en cada uno de los ministerios, con la finalidad de mejorar sus capacidades administrativas y la prestación de servicios al ciudadano" y en el ámbito privado con la Promulgación del Decreto con Fuerza de Ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas publicado en Gaceta Oficial Nº 37.148 de fecha 28 de febrero de 2001.

Teniendo en cuenta los argumentos precedentes y visto que la Ley especial contra los Delitos Informáticos está en vigencia, tipificándose así nuevos delitos para la competencia de los tribunales penales venezolanos, abriendo campos para la investigación científica, control, prevención y seguridad en este novel paradigma

social y comercial, recién descrito, que evidentemente nos impulsa a ingresar en ámbitos probatorios no articulados hasta los actuales momentos; evidenciando, de la misma manera, que el desarrollo del cuerpo normativo procesal penal (Código Orgánico Procesal Penal, en adelante COPP) ha sido insatisfactorio, que por decir lo menos ya ha sido modificado en dos oportunidades desde 1998 fecha de su publicación es que surgen las siguientes interrogantes:

- La nueva Ley contra los Delitos Informáticos abarcará todos los supuestos fácticos de este tipo de criminalidad;
- Los recursos con los que cuenta el Estado Venezolano son suficientes para implementar efectivamente esa Ley y propender a la disminución de estos delitos;
- Se presenta una vulneración o menoscabo de los derechos constitucionales de las personas respecto a la privacidad, la libertad individual, de opinión, de comunicación y a la libre circulación, entre otros;
- Están capacitados los operadores de justicia para implementar y operar a cabalidad la Ley especial en comento;
- Podrá reproducirse en juicio las pruebas de delitos informáticos practicadas cuando la mayoría de éstas son intangibles.

Responder a estas interrogantes son los objetivos con lo que se pretende estudiar las conductas disvaliosas emergentes del nuevo milenio: Los Delitos Informáticos y su actividad probatoria según el COPP.

Propósito de la investigación

Es indudable que la informática ha obligado a evolucionar las distintas ramas del Derecho (Constitucional, Civil, Mercantil, Penal). Esta nueva realidad nos pone frente al desafío de encontrar fórmulas eficaces de aplicación del Derecho -en nuestro caso, del Derecho Penal- porque constituye, igualmente, parte esencial indesligable de esa dinámica del desarrollo tecnológico, comercial y jurídico del mundo en su acepción globalizadora.

Atendiendo a ese argumento y producto de todo el avance tecnológico, el Derecho se ve inmerso en nuevas formas de actividades de diversos tipos. Como

consecuencia del surgimiento de diversas conductas delictivas atípicas, es que ha sido necesaria regularlas para garantizar el correcto funcionamiento de nuestra política, economía y sociedad.

El problema del avance incontrolable, impostergable y sostenido que las constante innovaciones tecnológicas han inserto en la sociedad, degeneró una temática que no fue ajena a nuestro órgano legislativo nacional. Y la respuesta de la Asamblea Nacional venezolana, al clamor del cese de la impunidad de los delitos cometidos por medio o a través de sistemas informáticos, no se hizo esperar y su pronunciamiento fue la sancionar la Ley Especial contra los Delitos Informáticos.

En consecuencia, la notable dificultad que presenta indagar sobre la materia respecto a los crímenes informáticos, visto la multiplicidad de factores intervinientes; pero una vez generado el marco legal que regirá y delimitará ciertas situaciones fácticas relativas los delitos informáticos, que tiene por supuesto una directa relación con la naturaleza humana y las normas de convivencia civilizada, se proyecta desde ya, la intervención de variables que ponen en peligro la efectividad del instrumento legal visto desde la perspectiva de conjunto.

Las fallas en la administración de justicia, el colapso funcional del Ministerio Público, la problemática operativa del Cuerpo de Investigaciones Científicas Penales y Criminalísticas, la novedad del instrumento penalizador, el desconocimiento técnico por parte de los operadores de justicia (incluyendo al abogado litigante) de los sistemas informáticos, son sólo algunos de los tópicos que se presentan como introducción para apostar al fracaso de la normativa supra indicada.

Con la presente investigación se estará contribuyendo a enriquecer la doctrina en el campo de las ciencias del Derecho, a la vez que servirá de antecedente para futuras investigaciones o material de guía en la preparación de casos penales relativos al objeto aquí tratado.

Para el logro del presente propósito se plantearon los siguientes objetivos:

OBJETIVO GENERAL:

Estudiar las conductas disvaliosas emergentes del nuevo milenio: Los Delitos Informáticos y su actividad probatoria según el Código Orgánico Procesal Penal.

OBJETIVOS ESPECÍFICOS:

- Revisar el ordenamiento jurídico vigente, constitucional y legal para encuadrar el supuesto planteado en la investigación.

- Sondear el nivel académico-instrumental de los operadores de justicia con respecto a la nueva Ley especial contra Delitos Informáticos y el proceso probatorio penal de los delitos allí contemplados.

- Determinar la eficacia y pertinencia de los medios probatorios de los hechos a debatirse en el proceso.

- Comprobar la existencia de organizaciones no gubernamentales y su rol para la prevención y control de los delitos informáticos.

- Constatar si esta ley asegura efectivamente la protección contra las lesiones sufridas en los bienes jurídicos allí tutelados.

- Verificar si el Estado Venezolano cuenta con recursos suficientes para implementar de manera efectiva la correcta operatividad de la Ley especial contra los Delitos Informáticos.

Justificación de la investigación

El análisis del alcance y delimitación de la Ley especial contra los Delitos Informáticos y su técnica probatoria bajo el imperio del Código Orgánico Procesal Penal es un tema ineludible si se pretende proporcionar una solución que satisfaga un sistema pleno de garantías y preserve ante todo el Estado de Derecho. El tema de la criminalidad informática presenta una complejidad elevada, la necesidad de un estudio profundo y la operacionalidad propia del texto jurídico de reciente data.

Esta investigación se justifica en cuanto trata un tema de actualidad y escasamente estudiado en el foro jurídico venezolano. Se aspira que el enfoque, planteamientos, consideraciones y recomendaciones que se generen de este análisis pudieran contribuir con el fin de lograr una efectiva administración de justicia.

De esta manera, este estudio se justifica dentro del marco jurídico actual, dada la recién sanción y promulgación de la Ley especial contra los Delitos Informáticos; y resulta a la vez relevante, porque al respecto, la doctrina es escasísima y la jurisprudencia local nula.

Alcances y Limitaciones

El alcance de la investigación se puede considerar desde tres dimensiones diferentes como son: en virtud del propósito, desde el punto de vista geográfico y de los resultados de la investigación

En cuanto al propósito, la investigación se concretó a estudiar las conductas disvaliosas emergentes del nuevo milenio contempladas en la Ley especial contra los Delitos Informáticos y su imbricación sistémica en la actividad probatoria jurisdiccional en concordancia con las reglas establecidas en el COPP.

Desde el punto de vista geográfico la investigación involucra a los tribunales penales ordinarios de la circunscripción judicial del Estado Carabobo, a los operadores de justicia y órganos de investigaciones penales, científicas y criminalísticas de la misma circunscripción.

Los alcances considerados en virtud de los resultados arrojados por la investigación, respecto a la temática planteada en el ámbito jurídico penal forense e informático pueden ser considerados de proyección nacional por cuanto la realidad local es representativa del engranaje funcional del país; a la vez que abre nuevas posibilidades para el desarrollo de la disciplina investigativa delictiva informática atendiendo a preceptos de garantías y derechos Constitucionales.

En cuanto a las limitaciones, se observa que el nivel de conocimiento aportado por este tipo de investigación presenta un mayor índice probabilístico de error, por cuanto los datos son obtenidos directamente de la realidad careciendo de patrón comparativo de control. Esta dificultad hace que las múltiples variables intervinientes en el problema investigado limiten las posibilidades de predicción, basándose únicamente en la realidad actual.

Por otra parte, en la recopilación del material bibliográfico, el escollo a superar fue internalizar la multiplicidad de criterios doctrinales contradictorios, documentos, leyes, propuestas que se encuentran en Internet y afrontar la escasa investigación académica venezolana respecto al tema objeto de la investigación.

CAPÍTULO II
MARCO TEÓRICO

Antecedentes de la Investigación

Los antecedentes son considerados para conocer si el tema objeto de la investigación ha sido ya abordado, explorando el grado de conocimiento que sobre éste existe o si brinda algún aporte a la investigación. La relevancia de los antecedentes en esta investigación tiene una finalidad implícita: conocer el alcance de conocimiento, hasta los actuales momentos, sobre el tema de los delitos informáticos y sus medios probatorios, tanto en ámbitos doctrinales como legales.

Al respecto, el autor evidencia que entre los antecedentes legales internacionales, de reciente data, se encuentra la Convención sobre el Cybercrimen (Tratado Nº 185), firmado en Budapest el 23 de noviembre de 2001 por los miembros de Estado del Consejo de Europa y otros Estados firmantes, instrumento jurídico en el cual se fija la ley marco para los países comunitarios europeos teniéndolo como directrices a tomar en su ordenamiento local, tanto sustantivo como procedimentales, a los fines de combatir los delitos informáticos (cyberdelitos); en su preámbulo expresan que "han tenido la convicción de necesidad, como materia de prioridad, las políticas criminales comunes dirigidas a la protección de la sociedad contra los delitos cibernéticos, inter alia, adoptando una legislación apropiada y alentando la cooperación internacional". Reconocen, así mismo, la urgencia de determinar las acciones directas contra la confidencialidad e integridad de los sistemas computacionales, de las redes informáticas y bases de datos, en sus usos indebidos dirigidos a la criminalización. Resalta el instrumento en comento que éste busca dar respuestas comunes al desarrollo de las nuevas tecnologías de la información basadas en los estándares y valores del Consejo Europeo y a los avances del entendimiento y cooperación, combatiendo el cybercrimen en acciones tomadas por las Naciones Unidas, la Unión Europea y el Grupo de los 8 (países más industrializados).

En el mismo plano internacional, ahora enfocado hacia el ordenamiento propio de cada foro soberano, se evidencia que ciertos países contaban ya con una legislación que consideraron apropiada a sus necesidades y que se ha ido

actualizando en la medida que aparecen nuevas conductas con apariencia delictiva. Entre los que se destacan:

a) Estados Unidos, que adoptó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó el Acta de Fraude y Abuso Computacional de 1986, con la finalidad de eliminar los argumentos excesivamente técnicos acerca de los tipos que penaban conductas relativas a mal prácticas informáticas.
b) Alemania sancionó en 1986 la Ley contra la criminalidad económica que contempla los siguientes delitos: espionaje de datos, estafa informática, alteración de datos y sabotaje informático.
c) En Holanda, entró en vigencia en el año 1993 la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el preacking (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.
d) Francia con su Ley relativa al fraude informático, tiene todo un elenco de conductas que tipifican delitos, con una gama de penas que van desde el mes y en aumento hasta varios años, más las pecuniarias en moneda local, dependiendo el daño causado, la intencionalidad, incluso la culpabilidad.
e) España incluyó ciertos delitos informáticos, dentro del catálogo de conductas tipificadas delictivas, en su Código Penal (1995) entre las que se encuentran: Daños contra la propiedad ajena, violación de secretos, espionaje, divulgación de datos y estafas electrónicas.
f) Para Chile, primer país latinoamericano en sancionar una Ley contra delitos informáticos (1993), entre los cuales, del género en estudio, se tienen: la destrucción o inutilización de los datos contenidos dentro de una computadora, la conducta maliciosa tendiente a destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento

Aún hay Estados o Gobiernos del mundo que no han acogido en su ordenamiento jurídico normas de esta naturaleza, bien dentro del Código Penal

o en leyes especiales; es de reconocer que, la temática que se plantea no es fácil y es la propia estructura normativa jurídica la que determinará la opción a escoger. Se tiene que en el ámbito venezolano fue la presión ejercida por grupos económicos la que impulsó al órgano legislativo nacional a adoptar una ley especial que protegiera diversos bienes jurídicos, y, es por ello, que recientemente, la legislación venezolana añadió al acervo jurídico-legal un texto normativo que se publicó en la Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001, que lleva por nombre Ley Nº 48 Ley especial contra los Delitos Informáticos, en la cual con treinta y tres artículos acaba con la especulación interpretativa que se realizó en los casos penales pasados.

De los estudios que pueden citarse por su conexión y aportes a la profundización de este análisis se encuentra la investigación documental de Leotta (1999) intitulada "La aplicación y utilidad de la criminalística en la actividad probatoria establecida en el COPP", trabajo de grado presentado en la Universidad Bicentenaria de Aragua. En dicho trabajo se concluye que "la criminalística permite determinar más clara y precisamente cómo se desarrollaron los hechos objeto de la investigación mediante el uso de sus métodos y técnicas" añadiendo que "permite establecer de una manera más acertada, precisa e inequívoca la inocencia o culpabilidad de un sujeto (imputado); como ciencia auxiliar del proceso penal es indispensable para realizar toda investigación criminal a fin de obtener las pruebas" y afirma categóricamente que "se recomienda a los jueces y abogados que participan en la administración de justicia penal, considerar la criminalística como herramienta indispensable en las distintas fases del nuevo proceso penal".

Otro de los antecedentes considerados por el autor, íntimamente relacionado con el anterior pero específicamente enfocado a la criminalística informática, es el Trabajo de Grado presentado por Toledo (2001) en la que el autor realizó e implementó una metodología técnica en el ámbito de la informática, para el desarrollo de un servicio criminalístico informático forense, aplicable, en sus palabra, "a la investigación y resolución de hechos que revisten caracteres de delitos informáticos, acorde con la legislación y que alteran el orden social causando graves perjuicios económicos al empresariado nacional"

no circunscribiéndolo sólo a ello sino como también -expresa- "considerar hechos que sin encontrarse adscritos a una legislación nacional, causan problemáticas graves en las relaciones sociales, económicas y morales, técnicas que alcanzan los estándares de confiabilidad requeridos por los Tribunales de Justicia".

En ese sentido, las investigaciones llevan a la convicción que mediante el conocimiento de la criminalística y el uso de misma se podría percibir de forma clara los medios empleados en la comisión de un delito y la manera de llevar a adelante una investigación de esta naturaleza, la cual tiene una importancia inmensa para la presentación de las pruebas en juicio penal. Es de resaltar que este conocimiento de la criminalística no debe ser exclusivo del órgano investigativo sino de todos los intervinientes en el proceso judicial penal.

Por su parte, Solange (2001) en su Tesis de Grado realiza una propuesta de Lege Ferenda planteando: a) Mecanismos de control institucional preventivo a priori sería conveniente la creación de una institución que regule y fiscalice la actuación de los sistemas informáticos; b) Afirma que por cuanto existe un número ilimitado de conductas y situaciones que están constantemente sometidas a los adelantos tecnológicos, lo cual conlleva necesariamente a nuevas modalidades delictivas, por ello deben ser reformulados los tipos penales de los delitos informáticos; c) Los ilícitos y abusos informáticos han sorprendido a los penalistas, situación que en parte se debe a que el Derecho penal anterior al desarrollo de la informática no pudo prever sus implicancias criminales y, además, que por lo novedoso el tratamiento de esta temática, se caracteriza por una notable falta de precisión.

En consecuencia, de las investigaciones reseñadas se hace patente que los delitos informáticos son una realidad en la sociedad globalizada y que en el foro jurídico venezolano, la acogida de la Ley especial contra los Delitos Informáticos a poco menos de un año, no ha dado las respuestas doctrinales ni jurisprudenciales para entender o lograr una aproximación a la aplicabilidad de éste.

BASES TEÓRICAS

Génesis de la delincuencia informática y su persecución policial

La manera de delinquir experimenta constantes cambios. La informática, si bien ha coadyuvado a interconectar el acceso masivo a las fuentes directas de información y los avances tecnológicos, trajo aparejado consigo el surgimiento de nuevas modalidades delictivas o el perfeccionamiento de las ya existentes.

A principio de los años ochenta había sonado una alarma para los responsables de aquellos sistemas informáticos en los que se guardan informaciones confidenciales. Un nuevo deporte había surgido en los Estados Unidos: el allanamiento a ordenadores; se trataba de una moda entre aficionados a la informática, generalmente jóvenes estudiantes de las mejores Universidades americanas que se las ingeniaban para conseguir acceso a sistemas ajenos, sin la debida autorización. Ya para ese entonces, en otros países desarrollados europeos venía ocurriendo algo similar. El acceso ilegal a los ordenadores originaba riesgos en materia de defensa, terrorismo, espionaje y robos; además de, afectar, en sentido lato, a la seguridad de todas las actividades dependientes del buen funcionamiento de un sistema computacional. De esta manera, cualquier persona con conocimientos suficientes podría llegar a sustraer, alterar o destruir información para sus propietarios o, sencillamente, sabotear el sistema que maneja los datos.

El jefe de sistemas del Hospital SloanKettering, centro neoyorquino especializado en la lucha contra el cáncer, descubrió a mediados de 1983 que alguien había conseguido introducirse en el computador principal de ese centro médico. Basado en la reseña difundida por la enciclopedia práctica de la informática (1984, p. 499) “En ese ordenador se guardan los datos sobre muchos enfermos y desde él se controlan, incluso, las dosis de radiación que los pacientes deben recibir en su tratamiento. Toda esa información, confidencial, estaba disponible para un escaso número de médicos”. Para ese entonces, unas palabras claves, al parecer muy poco corrientes, protegían el sistema. Lo cual ponía de relieve la vulnerabilidad no sólo de datos sino de la misma raza humana.

En este mismo orden de ideas, la noción de delito informático viene siendo tratada desde el comienzo mismo de la masificación de las computadoras; primeramente en el ámbito científico y luego en el comercial y doméstico, pero cobró especial atención a nivel propiamente social, según comenta Quiñones (1989), cuando se hizo público el tema en cuestión de la forma siguiente:

> **Una fría mañana de marzo de 1985, los telespectadores de Estados Unidos (…) presenciaron por primera vez una discusión revolucionaria (***omissis***) Phil Donahue, el conocido anfitrión de uno de los más famosos programas de opinión, favorito de millones, mirando a la cámara preguntó: ¿Sabe usted si es posible entrar en línea con una computadora para averiguar el saldo de una cuenta bancaria, verificar cuantas veces se ha divorciado un determinado individuo, o si éste recibe publicaciones pornográficas?**
>
> **Sin esperar la respuesta, prosiguió: Les informo que es posible acceder a estos datos, y aún más, es posible alterarlos, inclusive podría tenerse acceso a su tarjeta de crédito.**

Pero este tema, que causó alarma y zozobra en las personas de diversos estratos sociales, ya se venía tratando por ante el Departamento de Defensa de los Estados Unidos desde el año 1950 a través de la Agencia de Proyectos de Investigación Avanzada denominada (ARPA), la cual investigaba los campos de ciencia y tecnología militar. El objetivo de esta agencia era, en opinión de Toledo (2001), "plantear una red que tuviera la máxima resistencia ante cualquier ataque enemigo. Se suponía que la red de comunicaciones, por si misma, no es fiable debido a que parte de ella podría ser destruida durante un ataque bélico". Este proyecto fue evolucionando aunándose la intervención no sólo militar sino universitaria ínter América (ahora llamada ARPANET) para luego globalizarse, específicamente hacia Europa y Asia. La expansión resultó ser fácticamente procedente debido a su estructura descentralizada.

En 1986, la Fundación Nacional de Ciencias (NSF, sus siglas en inglés) inició el desarrollo de la "net" (gran proyecto de interconexión) que se diseño originalmente para conectar cinco superordenadores. Este evento aceleró el

desarrollo tecnológico de “Internet” y brindó a sus usuarios mejores infraestructuras de telecomunicaciones, uniéndose otras agencias de la administración norteamericana con sus inmensos recursos informáticos y de comunicaciones, entre ellos la Nasa y el Departamento de Energía.

Un revés significativo sufrió tan magno proyecto, a decir de Toledo (2001), para “el día 1 de noviembre de 1988 Internet fue 'infectada' con un virus de tipo 'gusano'. Hasta el 10% de los servidores conectados fueron afectados. El acontecimiento subrayó la falta de adecuados mecanismos de seguridad en Internet”. Lo cual degeneró en la inagotable búsqueda de soluciones a este tipo de problemática, pero como se observa no ha sido del todo satisfactoria.

Hechos más recientes, indica Blyde (2002, p. 5/1), entre la diversidad de modalidades de ataque en o por computadoras se tiene que:

> **(*omissis*) han pululado millares de corsarios informáticos, pero quizás uno de los más famosos es el que logró burlarse del propio Bill Gates, a quien osó mandarle viagra con su tarjeta de crédito, y sólo por el placer de jactarse de haber vulnerado sus sistemas informáticos.**
>
> **Se trata de Raphael Gray, un adolescente (*teenager*) de 19 años, quien desde su casa en Gales, en el Reino Unido, obtuvo miles de números de tarjetas de crédito disponibles en la Internet, entre ellas la de Bill Gates, la que utilizó para enviarle la medicina a su domicilio. Gray -quien aparentemente sufre de esquizofrenia- fue detenido por agentes del FBI y de la Policía Montada canadiense, luego de que se escapara a ese país, pero un juez de la Corte de Swansea lo dejó en libertad condicional.**
>
> **Según sus propias palabras, desde pequeño comenzó a interesarse por la Internet y de manera especial por los sitios pornográficos, hasta que comenzó a escuchar sobre hackers. Comenzó a ingresar en todo tipo de páginas digitales, y se le ocurrió perseguir portales y sitios de ventas. (…)**

Así, casi por casualidad, le llegaron 5.500 números de tarjetas de crédito a su computadora personal, decidió abrir una página y publicar los números (…)

Para ver lo que hacen los hacker hoy en día, basta echarle un vistazo al site, indicado por Morris (2001), “http://www.attrition.org”. Este es uno de los lugares en la Internet en los cuales los hackers reciben 'créditos' por sus ataques, en asignaciones encomendadas y efectivamente realizadas, comprobadas por el operador de ese website, a través de una imagen digital de los daños y, posteriormente, es anunciada su vandálica acción en la cartelera del site en cuestión.

De todo lo anteriormente descrito, se evidencia que hay una serie de modalidades delictivas que involucran a organizaciones políticas y económicamente activas, recursos monetarios, sujetos activos y pasivos de delitos y factor tiempo. La gama de conductas disvaliosas se han ido estudiando y clasificando en atención a los bienes jurídicos que se afectan y las tipificaciones son propias de cada ordenamiento jurídico, al igual que su persecución. Este es un paso vital, pero no definitivo, se debe armonizar dichas leyes nacionales con acuerdos o tratados internacionales para convenir en el tratamiento de delitos que involucren a dos o más países o sus connacionales -llamada extraterritorialidad- como sujetos pasivos.

La pregunta obvia partiendo de la lógica estructural de esta problemática es ¿Qué hacer? Es evidente que como punto de partida inicial se presenta el comprender que es necesario generar marcos legales que reglamenten y delimiten el manejo usual de los sistemas informáticos, lo que tiene una estrecha relación con la naturaleza humana y las normas de civilización impuestas por la normativa legal.

Pero sólo ello no es suficiente, se necesita adicionalmente todo un entramado compuesto por personal capacitado, infraestructura y órganos judiciales eficaces, capaces de materializar el ideal pacifista que la sociedad requiere.

Visto desde esta perspectiva, es necesario mencionar, por ejemplo, que Estados Unidos ha decidido invertir más de trescientos millones de dólares en la lucha contra el ciberterrorismo reforzando así las actuales disponibilidades económicas al alcance del Centro de Protección de la Infraestructura Nacional, que reúne los esfuerzos del Federal Bureau of Investigation (FBI) y el Pentágono. En la actualidad el FBI se vale, tan sólo de doscientos cuarenta (240) especialistas

en la investigación de delitos informáticos y pese a ello ha obtenido resultados notorios (datos obtenidos del site mismo de este organismo de investigación).

En el ámbito de la Unión Europea, las iniciativas para una mayor eficacia y coordinación policial en materia de delincuencia cibernética se suceden sin interrupción: Se destaca el denominado Plan Falcone encaminado a una acción común en programas de intercambios, formación y cooperación para responsables de la lucha contra la delincuencia organizada; el Tratado de Amsterdam relativo a la creación de un espacio de libertad, seguridad y justicia; y lo más reciente, el Consejo de Europa ha concluido en Tampere (1999) que entre sus objetivos prioritarios se encuentra la lucha contra la 'delincuencia de alta tecnología', datos recopilados por Marchena (2001, p. 4).

En contraste con esos países desarrollados, la circunscripción del Estado Carabobo ha tenido como punto de referencia, la denuncia efectuada por Mendoza (2002, p. A-8): “Corrupción y desvíos de fondos minan los cuerpos policiales - En Carabobo se combate el crimen con las uñas”. Salta a relucir, como también acae en todo el territorio nacional, las deficiencias que tiene el cuerpo llamado a realizar las investigaciones penales. Resulta inexplicable que el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC, en adelante) con toda una serie de actividades, por imperio legal, pueda llevar a cabo una seria indagación tendente a determinar las personas involucradas en un hecho punible así como la colección y preservación de los elementos de convicción que servirán de pruebas en juicio.

La descripción que se realiza acto seguido, tomado del trabajo periodístico elaborado por Mendoza (op. Cit), resalta la trágica realidad de uno de los pilares que sustenta el endeble entramado judicial penal venezolano:

> **Una casa alquilada desde 1964, funciona como sede de la Comisaría Las Acacias del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas. Esta quinta, de vieja estructura, no ha sufrido cambios ni modificaciones, aunque con la colaboración de la empresa privada, se espera que en las próximas semanas, se inicie una serie de reparaciones y remodelaciones para reforzar las bases y paredes de esta vivienda (…)**

> **Actualmente, en la Comisaría Las Acacias hay unos 50 funcionarios judiciales, pero se necesitan 30 más para cubrir las necesidades de investigación. Aunque en esta sede policial se maneja menor índice delictivo, por tratarse del norte de Valencia, y los municipios Naguanagua y San Diego, es indispensable también, contar con los recursos mínimos para llevar a buen término el trabajo policial (…) Todavía son usadas 15 máquinas de escribir, cuya data es de más de 15 años (…) Tampoco tienen cámaras fotográficas y al momento de hacer las reseñas policiales, deben contar con las que el personal de guardia posee. Éstas fueron adquiridas por ellos, para los recuerdos familiares, pero a la hora de cumplir con el trabajo deben usarlas.**

Con respecto al novedoso texto legal objeto de esta investigación, en el foro jurídico es bien sabido que una ley penal puede considerarse imprescindible bien por lo novedoso del asunto, o porque ha causado alarma pública o debido a que se considera una necesidad inaplazable, pero eso no basta. Para Tablante (2001, p.185) "resulta impostergable capacitar técnicamente a los ciudadanos, funcionarios y trabajadores en torno al uso y aprovechamiento de las tecnologías digitales", enfatizando que, "la idea de que el gobierno pueda efectivamente no sólo regular sino participar activamente en los procesos digitales, es definida hoy como la de un Gobierno Electrónico". Con propiedad se afirma que no hay evidencias documentales o estadísticas de las acciones gubernamentales en torno a esta problemática, para ninguno de los actores de la jurisdicción penal.

Aproximación a una conceptualización sobre Delitos Informáticos

La profusión de la informática es un factor que determina el origen de nuevas formas de delinquir. La sociedad, en general, se ve afectada con la otra cara de la moneda respecto a los beneficios, amplia e indudablemente, reconocidos que los medios informáticos han aportados a la humanidad.

De acuerdo con la definición ensayada por un grupo de expertos de la Organización para la Cooperación Económica (OCDE) reunidos en Paris (mayo 1983), el término delitos relacionados con las computadoras (computer related crime) se definiría como "cualquier comportamiento antijurídico, no ético o no autorizado,

relacionado con el proceso automático de datos y/o transmisiones de datos". Se tiene que en la actualidad la informatización se ha implementado en casi todos los países y, por demás, el espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia para ese entonces impensadas.

La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción o adulteración de programas o datos, la clonación de bandas magnéticas de tarjetas de débito o crédito, el acceso y la utilización indebida de información que puede afectar la esfera de la privacidad, transferencias ilícitas de fondos, captación de menores con fines libidinosos o prostitución o pornográficos, compras no autorizadas de bienes a través de Internet con números de cuentas o tarjetas pertenecientes a terceros, son algunos de los procedimientos relacionados con la amplia gama de delitos mediante los cuales es factible obtener grandes beneficios económicos o causar importantes daños físicos, materiales o morales; que en un principio se pensó combatir encuadrándolos en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafas, sabotajes no sólo en el ámbito penal, sino también con disposiciones normativas del derecho mercantil o civil.

La falta de concretización respecto al tema llevó en 1991 a la Secretaría de la Interpol a individualizar treinta (30) tipos delictivos relacionados con estos medios, destacando Schreiber citado por Mata (2001, p. 21), que esta misma indefinición conlleva a grandes dificultades "a la hora de lograr un intercambio internacional de información para actuar cohesionadamente frente a este tipo de comportamientos desde la perspectiva supranacional". Es evidente, por lo tanto, que la polimórfica realidad de la criminalidad informática, se refleja directamente en los intentos de definición o conceptualización de la misma y a una errónea prosecución penal.

También se observa que se ha querido optar por un cierto criterio restrictivo a la hora de establecer una noción general, donde se incluye exclusivamente los supuestos en los que el computador representa el medio de ejecución, pues sólo en éstos se aprecian las peculiaridades y características de los sistemas informáticos o del procesamiento electrónico de datos que convierte estos hechos en algo novedoso, diverso.

Criterios más avanzados, entre ellos el de Romeo citado por Mata (op. Cit), han establecido que en unos casos el computador y sus aplicaciones constituyen el objeto material del delito (sobre el que recae físicamente la acción) y en otros un mero instrumento para cometer hechos generalmente tipificados en el Código Penal. Por eso la doctrina alemana, dice el autor en comento, define "estos supuestos como el conjunto de actos (punibles o dignos de incriminación) los cuales el ordenador (o el procesamiento automatizado de datos) es el instrumento o el objeto de la comisión".

En concordancia con lo anteriormente descrito, los delitos informáticos serían todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático. Por su parte Tellez, citado por Manson (op. Cit), clasifica a estos delitos de acuerdo a dos criterios:

<u>Como instrumento o medio</u>: En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo de comisión del ilícito, por ejemplo:

a. **Falsificación de documentos vía computarizada (cheques, tarjetas de crédito)**
b. **Variación de los activos y pasivos en la situación contable de las empresas**
c. **Lectura, sustracción o copiado de información confidencial**
d. **Planeamiento y simulación de delitos convencionales (robos, fraudes)**
e. **Modificación de datos tanto en la entrada como en la salida**
f. **Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas**
g. **Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa**
h. **Uso no autorizado de programas de cómputo**
i. **Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas**

j. **Alteración en el funcionamiento de los sistemas, a través de los virus informáticos**
k. **Obtención de información residual impresa en papel luego de la ejecución de trabajos**
l. **Acceso a áreas informatizadas en forma no autorizada**
m. **Intervención en las líneas de comunicación de datos o teleprocesos**

<u>Como fin u objetivo</u>: En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidades físicas, ejemplo:

a. **Programación de instrucciones que producen un bloqueo total o parcial al sistema**
b. **Destrucción de programas por cualquier método**
c. **Daño a la memoria del computador (CPU o cualquier componente lógico)**
d. **Atentado físico contra la máquina o sus accesorios**
e. **Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados**
f. **Secuestros de soportes magnéticos entre los que figure información con fines de chantaje (pago de rescate)**

Es de observar que existen diversos tipos de delitos que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas, estos son: Accesos no autorizados (uso ilegítimo de passwords), destrucción de datos, infracción al derecho de autor y propiedad intelectual de las bases de datos, interceptación de e-mail, estafas electrónicas y transferencias de fondos. Desde no hace mucho tiempo, la Internet permite dar soporte a la comisión de otros delitos, entre los que se encuentran: El espionaje, el terrorismo, narcotráfico, entre otros.

Este tipo de acciones presentan las siguientes características principales, apunta el autor recientemente citado:

a. Son conductas criminales de cuello blanco, en tanto que sólo un determinado grupo de personas con ciertos conocimientos pueden llegar a cometerlas
b. Son acciones de oportunidad

c. Provocan serias pérdidas económicas
d. Ofrecen posibilidades de tiempo y espacio (se puede realizar en segundos y sin necesidad de presencia física del agente)
e. Presentan delitos que incrementan las cifras negra, por cuanto son pocamente denunciados
f. Son muy sofisticados y relativamente frecuentes en el ámbito militar
g. Presentan grandes dificultades para su comprobación
h. Pueden ser cometidos tanto dolosa como culposamente
i. Tiene una alta probabilidad de proyección en cuanto a su comisión
j. Por los momentos siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Sentadas las precedentes consideraciones, se afirma que para plantear una definición sobre esta materia es necesario -primero- tener presente que ello no ha sido tarea fácil y doctrinariamente punto álgidamente controvertido, atendiendo a la razón misma de su especial denominación "Delitos Informáticos"; y -segundo- hablar propiamente de "delitos" en el sentido de la dogmática penal como acciones típicas, ello es, tipificadas o contempladas en textos jurídico-penales con fuerza normativa general, se requiere que la expresión mencionada, "Delitos Informáticos", esté consignada en el Código Penal o en nuestro caso en una ley penal colateral con igual rango, distinguiéndose la definición propiamente típica de otras atípicas (simples actitudes con apariencia delictivas).

Por lo tanto, actualmente no se cuenta con una definición de delitos informáticos, pues cada país de acuerdo a sus realidades ha formulado un concepto en el cual, en principio, se procura incluir nuevas modalidades delictivas o se describen los términos más actuales en comportamientos tradicionales que, en razón al medio de comisión empleado, adquieren la condición de informáticos. El artículo 1º de la Ley especial contra los Delitos Informáticos venezolana no lo define taxativamente, sino que, lo enmarca dentro de términos amplios y aceptados en la doctrina más reconocida, teniendo como objetivo describir, a grosso modo, las conductas que se pretenden prevenir y sancionar.

Determinación espacial de aplicación de la Ley contra los Delitos Informáticos

La persecución de los delitos informáticos tiene que ser entendida en un sentido estricto; debiendo ser analizada, ab initio, las vías que ofrece el ordenamiento jurídico venezolano, al momento de garantizarle a las partes involucradas, la investigación del delito informático y su eventual tratamiento jurisdiccional de la agresión sufrida. El artículo 3 de la LEDI acoge el principio de "Extraterritorialidad" al establecerla en los siguientes términos:

> **Cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.**

La fijación de los límites jurisdiccionales de un Estado es algo más que un mero mandato legislativo. La determinación de la potestad de enjuiciamiento de los órganos judiciales impone una decisión mediante la que se expresa el interés de cada Estado en la protección a ciertos bienes jurídicos.

Se parte de la idea, y es evidente, que las normas penales en esta materia deben estar investidas de cierta elasticidad operacional, permitiendo así la proyección de su validez fuera de los límites del territorio a que cada Estado circunscribe su soberanía. Esto no es sino consecuencia de la necesidad de asegurar la protección natural que ofrecen los límites territoriales y evitar que quede ilusorio su espíritu o la misma intención legislativa.

Resulta ser, como deducción liminar, que el principio de territorialidad general del Código Penal, por si sólo no agota las posibilidades y las exigencias del espíritu de la LEDI al momento de preservar los intereses jurídicos, combinando esta ley de manera tácita, y especialmente la norma citada, ese principio de territorialidad, con otros criterios informadores, como los enseña el criterio más aceptado de la doctrina resumidos por Reyes (2000, p. 72):

a.- el principio de personalidad referido a que el agente sea un venezolano, que cometa un delito en el extranjero y de los tipificados en leyes penales locales; ambas premisas deben ser concurrentes;

b.- principio real o de protección de la soberanía, donde cualquier persona que cometa en el extranjero uno de los delitos que tipifiquen las leyes penales, bien contra la existencia y seguridad del Estado, contra el régimen constitucional, el orden económico social, la salud pública, la administración pública, por ejemplo;
c.- principio de universalidad, aparejando la doctrina, para este principio, el catálogo de premisas siguiente: c.1) que el autor del delito sea un extranjero; c.2) que el ilícito se realice en perjuicio de extranjeros, ello es, que el sujeto pasivo del delito no sea venezolano; c.3) que la infracción se haya consumado en territorio extranjero; c.4) que el agente o sujeto activo del delito se encuentre en Venezuela; c.5) que el delito esté sancionado en la legislación venezolana con pena privativa de libertad; c.6) que no se trate de delitos políticos; c.7) que sea solicitada la extradición del delincuente (para el caso de no ser concedida, no habrá lugar a proceso); y c.8) que el delincuente no haya sido juzgado previamente por los mismos hechos.

A la luz del ordenamiento jurídico vigente venezolano, es necesario identificar y contrastar esta intención persecutoria judicial "extraterritorial" de forma concatenada y razonada a los fines de verificar su procedencia iuris-fáctica, teniendo presente la complejidad del tema y su relevancia. Es plausible la voluntad del legislador al sancionar una norma de esta naturaleza, para perseguir a los transgresores en cualquier lugar en que delinquen. Se debe precisar que hay principios fundamentales en derecho; la jurisdicción y la competencia, en especial en materia penal, son de orden público y no pueden ser violentados por los jueces ni por las partes, pues viene establecida por la Constitución y las leyes en resguardo de la garantía constitucional del derecho a la defensa, al debido proceso, al ser juzgado por el juez natural, entre otros.

La jurisdicción

La evolución de las ideas y su consecuente traducción en los distintos sistemas jurídicos ha permitido perfilar un mecanismo de aplicación espacial de la norma penal que se encamina a la protección de aquellos bienes jurídicos que nuestro legislador considera prevalentes. La combinación entre el forum delicti comisi, la

nacionalidad del autor y la proclamación de determinados bienes jurídicos cuyas exigencias de tutela y protección penal ha considerado el legislador por encima de los límites fronterizos pueda ser perseguido por los tribunales penales ordinarios venezolanos sin mayor obstáculo resulta un hito a salvar con el devenir de la novedosa y revolucionaria LEDI.

Históricamente, dijo Calamandrei citado por Rengel (1994), “la jurisdicción nace paralelamente con el surgimiento del Estado en la civilización humana”. Comúnmente, este vocablo se utiliza para designar la función judicial; propiamente, la función de dirimir litigios dentro de un Estado Soberano moderno, en virtud de la cual el derecho de la persona individualizada o colectiva (derechos difusos) se encuentra protegido y asegurado por el imperium estatal y no por la fuerza privada de su titular en concreto, de manera que, si bien el Estado asumió y tiene efectivamente el monopolio de la justicia (lo que sería jurisdicción), los particulares tienen por su parte el derecho, facultad, prerrogativa o poder de exigir del Estado la protección de su derecho violado o amenazado (la acción).

Como corolario de lo afirmado recientemente, debe tenerse presente que: a) la jurisdicción constituye un presupuesto procesal como condición de legitimidad del proceso; b) tiene carácter público devenido de la soberanía estatal; c) es monopólico del Estado; d) se tiene como función autónoma, en el sentido de que no está sometida al control de los otros poderes u órganos que conforman el Poder Público. Por lo tanto, este sistema de legalidad blindado constitucionalmente ofrece una triple garantía, unidad del Estado, certeza del derecho y libertad del individuo dentro de los límites legales.

Traspolando esos postulados universales y pacíficamente aceptados en el foro venezolano, ha afirmado la Sala Político-Administrativa del Tribunal Supremo de Justicia, en sentencia 663 de fecha 17 de abril de 2001, lo siguiente: "La jurisdicción es presupuesto lógico necesario para la distribución de la competencia. Sin jurisdicción, resulta innecesario hablar de competencia. La falta de jurisdicción puede ocurrir, sólo cuando el conocimiento del asunto está atribuido a la Administración Pública o bien al juez extranjero".

El COPP preceptúa en el artículo 55, a diferencia del cuerpo normativo adjetivo derogado -Código de Enjuiciamiento Criminal- que debía regirse por reenvío supletorio al artículo 59 del Código Procesal Civil, lo que debe entenderse por jurisdicción ordinaria, a decir:

> **Artículo 55. Jurisdicción ordinaria. Corresponde a los tribunales ordinarios el ejercicio de la jurisdicción para la decisión de los asuntos sometidos a su conocimiento, conforme a lo establecido en este Código y leyes especiales, y de los asuntos penales cuyo conocimiento corresponda a los tribunales venezolanos según el Código Penal, los tratados, convenios y acuerdos internacionales suscritos por la República.**
>
> **La falta de jurisdicción de los tribunales venezolanos será declarada, a instancia de parte, por el tribunal que corresponda, según el estado del proceso. La decisión será recurrible para ante el Tribunal Supremo de Justicia en Sala Político-Administrativa.**

De lo anteriormente citado, concatenado con el artículo 3 del Código Penal que consagra "todo el que cometa un delito o una falta en el espacio geográfico de la República, será penado con arreglos a la ley venezolana", se constata que la ley penal, tanto adjetiva como sustantiva, acoge el principio de territorialidad como aquél que determina la competencia para el conocimiento de la causa penal subiudice. En ese orden de ideas, la misma Sala afirmó en dicha sentencia que "el elemento que determina la atribución de competencia en materia penal, para conocer de la causa a que se contrae la comisión de un ilícito penal, es el territorio donde fue cometido el hecho punible a ser sancionado".

Divaga la Sala Político-Administrativa, al pretender dejar abierta la factibilidad de violentar dicho principio, cuando afirma que si la teoría de la territorialidad de la Ley Penal se aplicase con carácter absoluto, resultaría muy fácil la acción de justicia en el lugar de la comisión del delito. Cabe tener presente que el Tribunal Supremo de Justicia venezolano, acogiendo la más calificada doctrina, dictaminó que el problema de la determinación del lugar donde se realizó el

hecho generador del delito exige que se atienda a la principal actividad que lo originó.

Todo ello conlleva a la convicción de que la LEDI trata de no dejar cabos sueltos al momento de perseguir judicialmente a los culpables, acogiéndose al criterio ecléctico de la doctrina consistente en estimar que el delito puede reputarse cometido, tanto en el lugar de la acción como en el del resultado -llamada teoría de la obicuidad- donde las posibilidades de persecución se amplían considerablemente.

En esa tarea encaminada a la fijación del lugar en el que el hecho delictivo ha acaecido o ha desplegado sus efectos, en ciertos delitos informáticos, se exige un matiz complementario, porque entre el lugar de la acción y el lugar del resultado puede haber afectaciones a los límites jurisdiccionales de otros Estados, gracias a la computación e Internet se pueden dar estos saltos territoriales en los que plantea la duda acerca de si en cualquiera de los Estados en que se sitúa uno de los nodos de conexión, podría reputarse como cometido el delito.

Hechas todas estas consideraciones, se colige que la LEDI le da competencia subsidiaria a los tribunales penales venezolanos para conocer en las circunstancias tipificadas en su artículo 3, pero conviene anticipar que si se llegara a la conclusión de que nuestro sistema jurídico no proscribe la teoría de la obicuidad, como en efecto lo es, e incluso ésta no goza de antecedentes jurisprudenciales, buena parte de los problemas que se plantearan en el futuro no encontrarán vías de solución. Relegando una vez más a la literalidad de la Ley y su obligado cumplimiento en letra muerta.

La aceptación de este criterio en el ámbito de la delincuencia cibernética tendría una traducción inmediata en forma de restricción de las posibilidades de investigación y enjuiciamiento. El Manual de las Naciones Unidas para la prevención y control de Delitos Informáticos, recogido por Manson (op. Cit), señala “cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada”.

Se tiene así que cualquier ofensa ejecutada con atención a lo estipulado en el artículo 3 de la LEDI resulta imposible su persecución en los términos simples en que se ha acogido sin imbricarse dentro de convenios ni tratados internacionales pactados para tal fin.

Tratamiento y experiencias internacionales para la determinación de la jurisdicción y competencia judicial: Caso Yahoo! Inc

De acuerdo con el principio de universalidad, cualquier Estado podría intervenir con su poder punitivo en caso de lesión u ofensa a determinados bienes jurídicos, sin tener en cuenta la nacionalidad del sujeto activo ni el lugar de la comisión del hecho punible. Basado en esa doctrina, comenta Bazuro (2002), en noviembre de 2000 el Tribunal de Gran Instancia de Paris, cuyo titular es el Juez Jean-Jacques Gomez, ordenó a la sociedad mercantil norteamericana Yahoo! Inc "bloquear todas las conexiones a los internautas franceses a los contenidos ilícitos contenidos en su websites"; en la motiva de la sentencia definitivamente firme se argumenta que ello es "debido a que se infringía la ley francesa y, además, estaba sujeta a su jurisdicción en cuanto la infracción se había determinado en territorio francés".

Sin otra opción, la empresa en cuestión se vio obligada a retirar de su servicio de subasta todos los contenidos y materiales cuya disponibilidad online había provocado la condena, cumpliendo así con lo establecido por el Tribunal francés. Por cuanto el fallo le pareció a los directores de Yahoo! Inc un exabrupto jurídico decidieron accionar ante una Corte Norteamericana para que evaluase la posibilidad que tal decisión extranjera afectara un derecho previsto por la Constitución de Estados Unidos. El Juez Jeremy Fogel, el 07 noviembre de 2001, dicta una resolución opuesta, negando cualquier autoridad del tribunal francés en el territorio estadounidense y resaltando la máxima protección y tutela a la libertad de expresión, diciendo expresamente "a la luz de estas consideraciones, el tribunal concluye que la aplicación del mandato del juez francés serían inconsistentes con la primera enmienda y ello determinaría una inaceptable restricción de la libertad de opinión".

Esta sentencia marcó un hito en el análisis de una posible regulación del ciberespacio y fija un precedente jurisdiccional respecto a la punibilidad de delitos informáticos. La regulación de las cuestiones jurídicas conectadas a las nuevas tecnologías y a las nuevas redes de comunicación electrónicas, sustentadas en la ausencia de normas específicas; basadas siempre más en el perenne compromiso entre los principios generales del derecho aplicable y las problemáticas técnicas que obstaculizan los mandatos judiciales hacen que surjan ciertas soluciones viables jurídicamente, que permiten paliar el vacío legal.

Hoy en día, la fijación del cuadro de delitos que provocan ese efecto de persecución universal se ha determinado con fundamento en tratados internacionales inspirados en el carácter supranacional del bien jurídico ofendido, en cuya protección habrá de existir un interés común a todos los Estados pactantes. Se desprende claramente de la "Convención sobre el Cybercrimen" realizada en Budapest en noviembre de 2001 el espíritu que llevó a los miembros del Consejo de Europa a considerar la conveniencia de dicho pacto. Entre los postulados inspiradores se tiene:

> (omissis) **Conscientes de los profundos cambios originados por la digitalización, convergencia y continuidad globalizadora de las redes de computación;**
>
> **Preocupados por los riesgos de que las redes de computadoras y la información electrónica puedan ser usadas para cometer ofensas criminales y que las evidencias relacionadas con dichas acciones puedan ser almacenadas y transferidas por dicha red;**
>
> **Reconociendo la necesidad de co-operación entre los Estados miembros y la industria privada en combatir el cybercrimen y la necesidad de proteger legítimos intereses en el uso y desarrollo de las tecnologías de información;**
>
> **Convencidos que la presente Convención es necesaria para implementar las acciones contra la confidencialidad, integridad y disponibilidad de los sistemas de computación, redes y sistemas de datos también como su mal uso o conductas impropias relacionadas y la adopción de poderes suficientemente eficaces para combatir dichas**

ofensas criminales, facilitando su detección, investigación y prosecución tanto en nivel doméstico (nacional) **como internacionalmente y proveyendo arreglos para una pronta solución internacional …**

Retomando la Recomendación del Comité de Ministros Nº R (85) 10 concerniente a la aplicación práctica de la Convención Europea sobre la mutua asistencia en materia criminal con respecto a las rogatorias para la interceptación de telecomunicaciones, Nº R (88) 2 protección de copyrights y derechos inherentes de los ciudadanos, Nº R (87) 15 reguladora del uso de datos personales en el sector policial, Nº R (95) 4 sobre la protección de los datos personales en el área de servicios de telecomunicaciones con especial referencia a los servicios de telefonía, y también Nº R (89) 9 sobre los crímenes relacionados con computadoras proveyendo procedimientos para las legislaturas nacionales respecto a las definiciones de ciertos crímenes informáticos y la Nº R (95) 13 concerniente a los problemas de derecho adjetivo respecto a la tecnología de la información

… para buscar respuestas al desarrollo de nuevas tecnologías basadas en estandares y valores del Consejo de Europa (omissis) subrayado del autor

Admitida la existencia de una convergente voluntad interestatal para proteger sus respectivos sistemas jurídicos frente a agresiones externas y aceptado el compromiso recíproco de activar las jurisdicciones para el enjuiciamiento de determinados delitos cibernéticos, según opinión de Manson (op. Cit) “la solución exigiría algunos matices” y necesariamente habrían que evaluarse los resultados.

De todas formas, afirmando el interés supranacional en dificultar la utilización de los sistemas computarizados e Internet con fines delictivos debe necesariamente descenderse el escalón para acoplar el sistema jurídico local, modificándolo y lograr así la sincronización ideal para su persecución.

Claro está que la intención no es proponer un listado "numerus clausus o apertus" de figuras delictivas posibles o imaginables que pudieran ser tratadas en su persecución, sólo hacer viable el principio de universalidad. Haciendo la salvedad que no todos los bienes jurídicos sean protegido, pero si una buena parte de ellos. Enfatiza Manson (op. Cit) que "el proceso de convergencia normativa e institucional que ha traído consigo la Unión Europea, refuerza la idea de que la delincuencia transfronteriza impone, además de irrenunciables fórmulas de cooperación judicial y policial, soluciones extraterritoriales que eliminen viejos obstáculos de antes" para, concluye, "la eficaz protección que ahora demandan ciertos bienes jurídicos seriamente amenazados".

La esencia del asunto estriba que a toda consta debe alejarse de la discrecionalidad en materia de procedimientos policiales y judiciales, al igual que las interpretaciones casuísticas al momento de realizar o autorizar una investigación, debiendo preservarse la incolumidad de los derechos fundamentales recogidos en la Constitución de cada Nación o Estado. De esta manera se salvarán las actuaciones policiales de vicios procesales y se contribuirá con el progreso económico, social y cultural, así como el bienestar de los individuos.

Problemática actual en la identificación y persecución del agente activo del delito informático

Otro punto álgido a tratar en la sistemática interpretativa de la LEDI es el mecanismo de identificación e individualización de los sujetos que se encuentran atomizados en una red global, teniendo presente que el anonimato o enmascaramiento estatuyen el orden del día, siendo ello la mampara sobre la que se escudan al momento de cometer los ilícitos. Muy bien lo refleja Ablan (2002, p. 1-13) cuando expresa que "Poder, dinero, control, supremacía: el mundo en las manos sin moverse de su silla (…) El universo del crimen virtual no tiene límites". La aparición de la tecnología de la computación ciertamente abrió nuevas posibilidades para transgredir la ley y como se había previamente analizado, los computadores pueden ser blanco de un ataque o servir de herramienta para la ejecución de un delito.

Los computadores han servido como medio para delinquir al usarse para publicar pornografía infantil; para robar, permitiendo la transferencia ilegal de fondos entre cuentas bancarias beneficiando a terceros no autorizados o consentidos; o para planificar asesinatos modificando las proporciones de medicamentos suministrados a una persona hospitalizada. A su vez, los sistemas tecnológicos se convierten en objetivos de un asalto cuando se produce sustracción de información ilícita, acceso al sistema cuando no se está autorizado o saboteando el propio u otros sistemas (modificación o destrucción de datos).

En principio, se tenía la convicción de que las personas que cometían "Delitos Informáticos" eran aquellas que poseían ciertas características que no presentaban el denominador común de los delincuentes; en opinión de Manson (op. Cit) "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".

Es criterio, mayoritariamente, aceptado que los criminólogos lo encuadren en la tipología delictiva de cuello blanco. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre si es la divergencia de los bienes jurídicos vulnerados, o sea, la naturaleza de los delitos cometidos. Un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (números 43 y 44), recogida por el autor en comento, refleja que "el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada". Asimismo, otro estudio realizado en Estados Unidos de América y Europa indica que el 73% de las intrusiones cometidas eran atribuibles a fuentes internas y sólo el 23% a la actividad delictiva externa.

En otro sentido, a nivel internacional los cuerpos policiales se han visto en la necesidad de ampliar extensivamente el entrenamiento de las fuerzas del orden en aras de identificar a aquellos sujetos que se valen de la Internet o medios computacionales online para cometer delitos o actos ilícitos. Publica el Departamento de Justicia Americano (2000) que han tenido la necesidad de proteger cierta clase de ciudadanos, específicamente menores de edad, para evitar

el acceso a ciertos materiales o contenidos nocivos –pornografía infantil o juegos de envite y azar– evidenciando que el problema potencial de identificación es la obtención de la prueba.

Una reseña periodística publicada en el diario El Universal (2002, sección zona, p.7) destaca que "la popularidad de los teléfonos móviles con acceso a la Internet en Japón, especialmente entre los adolescentes, ha desatado un aumento de los delitos sexuales que involucra menores". Sonando nuevas alarmas que pondrán, lamentablemente, en cero los procedimientos investigativos.

Teniendo ello presente, se preguntan los expertos pertenecientes a la organización recién mencionada: "¿Cómo pueden controlarse actividades como apuestas, o ventas de fármacos con prescripción obligatoria o alcohol cuando éstas son limitadas a personas adultas y menores de edad se ocultan o falsean la identificaciones haciéndose pasar por adultos?". Similarmente, ocurre que los adultos se hacen pasar por niños o adolescentes interceptando a verdaderos menores llevándolos a situaciones peligrosas, siendo la pregunta lógica y necesaria: ¿Cómo esas potenciales víctimas pueden ser protegidas? . Eso es materia frecuente en los esfuerzos que hacen tanto el cuerpo legislativo, así como el judicial y el investigativo.

Ha habido propuestas tales como: a) crear mecanismos de identificación utilizando los protocolos de Internet; b) formas para evaluación la identificación por nodos de conexión en accesos públicos; c) asignar códigos individualizados a cada computadora, entre otros. Los conflictos entre las distintas tecnologías y, específicamente, la vulneración a derechos fundamentales es lo que ha frenado toda acción al respecto.

En la actualidad, muchos procedimientos investigativos se han dado a conocer a nivel internacional, coadyuvando a optimizarlos con las críticas y polémica desatada en las distintas mesas de trabajo o simples reuniones para intercambio de ideas. La realidad obliga a la constante producción de ideas. Se afirma que ocurrido cualquier hecho delictivo, de naturaleza informática, los investigadores especializados deben localizar la fuente de comisión; para conseguirlo, deben rastrear la pista electrónica comenzando desde la víctima hacia el perpetrador. La sociedad enfrenta cambios significativos que con el devenir de los años los criminales en línea se han

sofisticados, pudiendo mantener el anonimato más fácilmente. El reto que hoy en día deben enfrentar, tanto la industria informática y las fuerzas de la ley, estriba en superar los siguientes obstáculos, según reseña el Departamento de Justicia Americano (2000):

1) Ambientes Desprotegidos y Diversos: En los ambientes comunicacionales de la actualidad, donde el servicio no es prestado por una empresa de manera monopólica, una transmisión simple puede involucrar distintos operadores nacionales, incluso internacionales. Como resultado, la conexión de un hacker o cualquier otro criminal informático puede pasar por distintos tipos de empresas de comunicación que a su vez funcionan con tecnologías diversas entre si. Este fenómeno hace aún más dificultosa, y a veces imposible, rastrear al criminal; quién está, tecnológica e intelectualmente, mejor preparado para esconder su ubicación e identidad.

2) Comunicación Satelital (inalámbrica): Celulares y redes telefónicas conectadas vía satélite permiten a los usuarios discurrir en diversas locaciones equis distante usando el mismo equipo telefónico. Claro está, que los beneficios sociales y comerciales de este mecanismo son obvios; pero como contrapartida, también proveen de una herramienta comunicacional invalorable para el criminal. Existen ciertos dispositivos que permiten a los policías, bajo ciertas circunstancias,
identificar el área geográfica general en la cual la llamada "inalámbrica" se está generando o quien es su receptor. El problema radica en que la interceptación lesiona el derecho a la privacidad (debería seguirse un procedimiento judicial previo para el control de la prueba) y por ser una tecnología sumamente costosa, ya hay en el mercado teléfonos satelitales desechables de costos reducidos, lo cual viene a complicar la persecución policial en la obtención de las evidencias y relacionar éstas con el criminal.

3) Rastreo en tiempo real: Realizar esta operación, como se dijo recientemente, desde la víctima hasta el perpetrador o atacante puede ser posible sólo cuando el sujeto activo (atacante) está en línea. Criminales sofisticados pueden alterar los datos concernientes con la fuente o el destino de sus comunicaciones, o utilizar las cuentas de Internet de otras personas -sin su autorización-. Debe tenerse en cuenta que la transmisión de la información puede no ser retenida o grabada por el proveedor del servicio o puede no ser capturada en su totalidad o almacenada parcialmente por un

corto período de tiempo. Incluso, si es grabada o retenida, aunque sea de manera parcial existe la posibilidad que pueda ser borrada por un intruso habilidoso en aras de ocultar su identidad.

4) Infraestructura técnica y retención de datos: Dicen los expertos americanos que si las redes de comunicación, las computadoras y su software no estuviesen diseñados y configurados para generar y preservar el tráfico crítico de datos, la información de origen y destino de los cyber-atacantes no existiría. Esto es en el caso de las conexiones hechas a través de un servidor que va realizando las asignaciones al servidor de manera aleatoria y por disponibilidad de puertos. Una red diseñada de esta forma dificulta la obtención del reporte de tráfico crítico de datos en una investigación criminal al no saberse con precisión cual es el delincuente y en que momento se conectó y mediante cual dispositivo.

5) Anonimato: Cuentas de correo electrónicas con la cual los suscriptores se benefician de ellas sin necesidad de verificación de identidad, representan una espada de doble filo. Tales cuentas anónimas pueden proteger en muchos casos la privacidad, pero ello añade una nueva complejidad en la identificación de los delincuentes online; ejemplo, dificultad para identificar los comerciantes de pornografía infantil, las amenazas de muerte, el envío de virus o producción de copias ilícitas de los trabajos amparados por los derechos de autor o copyright. Similar situación acae con los re-enviadores anónimos de correo electrónico que obtienen, bien ilegalmente o comprando los listados sin autorización del titular, direcciones de correo electrónico de un prestador de servicios de mensajería.

Políticas internacionales concernientes al anonimato y gestiones comerciales en línea necesitan ser desarrolladas con el fin de tomar en cuenta la privacidad, la verificación y autenticación del titular para lograr en gran parte disminuir los delitos informáticos y generar un estado de seguridad pública digitalizada. En los actuales momentos parece no haber una solución que sea viable y la producción legislativa de cada Gobierno o Estado, así como los tratados internacionales es excesivamente lenta.

Es importante resaltar otro tópico que se encuentra en la palestra jurídica, referido a los proveedores de Internet y la factibilidad de su imputabilidad; es lógico pensar, a primera vista, que la responsabilidad penal queda excluida cuando la información

ilícita la envíen terceras personas en forma de correo electrónico o adjunto a estos mensajes. La problemática que se plantea es cuando de los contenidos alojados en foros públicos (sitios en Internet dedicados al intercambio de ideas) se evidencia que hay transgresiones a la LEDI. Orts (2002, p. 164) se ha hecho las siguientes preguntas: "¿Es exigible al proveedor algún tipo de control respecto a esos contenidos?, y por ende, ¿Puede atribuírsele responsabilidad penal en comisión por omisión?; ¿Qué ocurre si conoce el carácter delictivo de la información?".

El debate se trae a colación, por el planteamiento hecho por ante los tribunales Alemanes en 1997, acerca de la posible responsabilidad penal de los proveedores de Internet y de los operadores en servicios online, contra la compañía Americana Compuserve por difundir pornografía infantil emitida desde los Estados Unidos de América. El fallo de primera instancia de la jurisdicción germana condenó al proveedor americano, pero fueron absueltos en la apelación; la alzada asumió el criterio citado, por Orts (2002, op. Cit): "la responsabilidad del proveedor basada en la falta de control de la información difundida carecía en absoluto de cobertura legal, toda vez que el Código Penal Alemán no establece la obligación de esos sujetos de supervisar los contenidos divulgados".

Acota el mismo autor que otros países, en cambio, optaron por una regulación más estricta, estableciendo la responsabilidad de tales intermediarios por omitir los controles necesarios para evitar la circulación de contenidos prohibidos (caso: Communications Decency Act de 1996 Estados Unidos). No obstante, la incompatibilidad de esta ley con el derecho fundamental a la libertad de expresión previsto en la enmienda Nº 1 de la Constitución Americana hizo que se declarara inconstitucional. Y, a la vez, es lógico pensar que no es posible estar monitoreando permanentemente la red, visto que se estaría en presencia de la violación de otro Derecho Humano como es la privacidad e intimidad.

La posición asumida por la legislación venezolana resulta ser más definida, al contemplar en el artículo 5 de la LEDI,

> ***Responsabilidad de las personas jurídicas*. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su**

nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

Se desprende del tipo recién citado que los elementos para imputársele a una persona jurídica responsabilidad penal por delitos contemplados en la LEDI, deben de manera concurrente haberse dado todos los supuestos allí expresados, caso contrario, subsecuente ratio, podrá perseguirse judicialmente a las personas naturales en el tipo mencionado pero sólo a título personal. La pena aplicable a las personas jurídicas se aplicará atendiendo al artículo 28 de la LEDI: "La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito" (subrayado del autor).

El bien jurídico tutelado en la Ley especial contra los Delitos Informáticos

Como principio consagrado en la Constitución de la República Bolivariana de Venezuela referente a los Códigos se desprende de su artículo 202 que éstos son leyes sistemáticas que regulan determinadas materias. En este justo sentido, el Código Penal debería ser la ley que regula de forma sistemática todo lo que se denomine delito y esté tipificado como tal por el legislador.

Una de las características más perniciosas de la legislación venezolana en los recientes pasados veinticinco años ha sido, a juicio de Fernández (2002), "la descodificación penal, la cual se ha traducido en casi 60 leyes especiales con delitos que tutelan los bienes jurídicos e instituciones creados en esas leyes". Resaltando que "lo notable de esta situación es que se tratan de leyes penales concebidas de forma aparte y contradictoria con relación a la sistemática del Código Penal".

La multiplicación de leyes penales, como sostiene Zaffaroni citado por Sáez (2001), "se transformaría en una banalización de la legislación penal, con lo que ésta

pierde claridad, precisión y orden, al tiempo que gana en confusión, descodificación, farragosidad, casuismo y pésimo castellano".

Aunque se tenga este fatal precedente, la realidad es que ante nuevas formas alternativas que en el tradicional concepto de delito producen los ilícitos informáticos, ellos obligan al Estado frente al problema concreto que significa la delincuencia, a modificar o reformular todas sus estrategias y objetivos en materia de política criminal, sea desde una perspectiva de carácter preventivo, como también desde un sentido represivo. Lo tradicional en la producción legislativa venezolana ha sido crear leyes penales especiales (que autores han denominado colaterales), y cierto es, comoquiera que sea, el ordenamiento jurídico venezolano dio como salida a las necesidades en la materia aquí en estudio, a la LEDI.

En otro sentido, pese a lo anteriormente indicado, se resalta que la doctrina ha cuestionado el bien jurídico tutelado en los delitos relacionados con la informática, a punto tal que para algunos tratadistas, sólo la información sería lo que la integrase. Pero muy pocos de los delitos escapan a la informática; incluso hoy se puede matar mediante manipulación del programa conectado a un enfermo, comentado supra; blanquear capitales, falsificar, hacer apología de delito en la red, cometer delitos contra el patrimonio, entre otros tantos ejemplos.

Por lo que a juicio de la doctrina, resulta impropio hablar de delitos informáticos; sin perjuicio de que exista una nueva realidad que interesa distintos bienes jurídicos tutelados, como los delitos contra la intimidad, contra el patrimonio, contra la seguridad del Estado. Indica Sáez (2001) "no existe un delito informático, sino una realidad criminal compleja, vinculada a las nuevas técnicas de información, imposible de ser incluidas en un único tipo legal".

Desde su promulgación esta Ley especial (LEDI) ha sido objeto de innumerables críticas practicadas desde distintos puntos de vista, entre los argumentos esgrimidos se pueden mencionar los resumidos por Fernández (2002):

(i) Utiliza términos en idioma inglés, cuando la Constitución sólo autoriza el uso del castellano o lenguas indígenas en documentos oficiales;

(ii) No tipifica delito alguno relativo a la seguridad e integridad de la firma electrónica y a su registro;

(iii) La terminología utilizada es diferente a la de la Ley de Mensajes de Datos y Firmas Electrónicas (*omissis*) con lo que se propicia un desorden conceptual de la legislación en materia electrónica;

(iv) Repite delitos ya existentes en el Código Penal y en otras leyes penales, a los cuales agrega el medio empleado y la naturaleza intangible del bien afectado;

(v) Tutela los sistemas de información sin referirse a su contenido ni sus aplicaciones;

(vi) No tutela el uso indebido de la Internet, y

(vii) Establece principios generales diferentes a los establecidos en el Libro Primero del Código Penal, con lo cual empeora la descodificación.

Teniendo ese marco referencial y no obstante lo recién dicho, la LEDI presenta los siguientes bienes afectados que ostentan el estatus de tutelable en materia judicial penal: a) contra los sistemas que utilizan tecnología de la información; b) contra la propiedad; c) contra la privacidad de las personas y de las comunicaciones; d) contra el indemnidad sexual de sujetos pasivos determinados -niños, niñas y adolescentes- (faltó contemplar a los incapaces); y por último, e) contra el orden económico. Acto seguido se describen brevemente los tipo penales a los fines de comenzar a dar luces de lo que se debe entender por tales.

Delitos contra los Sistemas que utilizan Tecnologías de Información

En el Título II "De los Delitos" en el Capítulo I, de la LEDI, se contempla "De los Delitos Contra los Sistemas que utilizan Tecnologías de Información". En los artículos del 6 al 12 se tipifican ciertas conductas que la ley describe como: acceso indebido, sabotaje o daño a sistemas, protegidos o no, e incluso su favorecimiento culposo, posesión de equipos o prestación de servicios de sabotaje, espionaje informático y la falsificación de documentos informatizados.

Con respecto al acceso indebido, en la descripción del tipo subyace la idea de penar la simple intromisión no autorizada o excediéndose de la que se tenga desplegando las conductas allí indicadas: interceptar, interferir o usar un sistema que utilice tecnologías de información.

Se deduce que esto es producto de las conductas temerarias de los llamados hackers benignos, en su variante inofensiva o simples amedrentadores, que se complacen meramente con irrumpir dentro de los sistemas informáticos, probando sus habilidades y destrezas para romper o violar códigos de accesos o seguridad.

Las dudas abundan cuando se piensa en la comisión imperfecta de éste, o si pudiese ser cometido por más de un sujeto activo o cualquier otra variante que la imaginación permita y, por otro lado, cómo controlarlo y probarlo judicialmente cuando no se ha causado daño propiamente. Tablante (2001, p. 164) indica que el espíritu del artículo 6 se inspira en ciertas "conductas que atentan contra los sistemas que utilizan tecnologías de información (…) se castiga el tipo doloso -sic- de acceso no autorizado a dichos sistemas" aclara que "si bien esa modalidad no produce un daño a los sistemas su acceso a través del uso ilegítimo de password compromete seriamente la seguridad que el propietario quiso resguardar mediante la contraseña" por ello su represión penal.

Una primera apreciación devenida de este análisis concreto del tipo comentado es que se precisa indeterminado y mal ubicado dentro del texto normativo, el cual podría estar mejor imbricado entre las disposiciones contra la privacidad de las personas y de las telecomunicaciones. Se estima que su vaguedad hará que procesalmente sea mínima la probabilidad de su demanda.

En otro orden de ideas, el sentido genérico del clásico delito de daño informático, computadoras como fin u objeto del delito, es la destrucción, inutilización, deterioro o menoscabo de una cosa; específicamente, en palabras de la propia ley los verbos rectores del tipo son: destruir, dañar, modificar, alterar o inutilizar el funcionamiento de sistemas que utilicen tecnologías de información. Con los avances en las tecnologías de la información se planteó esta problemática del encaje en esta figura delictiva de comportamientos recaídos sobre elementos lógicos de los sistemas informáticos (entre los que se encuentran los archivos, programas y

bases de datos) produciéndose la destrucción o deterioro de los mismos. Es lo que generalmente desde el punto de vista criminológico, según Mata (2001, p. 59), se denomina "sabotaje informático".

Estos tipos de conductas tendientes a atacar elementos lógicos de los sistemas informáticos pueden llevarse a cabo a través de procedimientos denominados: programas de destrucción progresiva, rutinas cancerígenas, virus informáticos o bombas lógicas. Como ocurre también mediante, la actuación sobre soportes físicos, golpear o romper disquetes o el computador mismo donde se contienen los datos, programas o documentos, o vertiendo sobre éstos materiales o substancias, ácidos, corrosivos y aun inertes como el agua.

Afirma Orts (2001, p.79) que en estos delitos "el bien jurídico protegido es el patrimonio" y contrariamente Tablante (2001, p. 164) es de la opinión que "el bien jurídico protegido no es la propiedad sino la seguridad de los sistemas que utilizan tecnologías de información" puesto que, concluyendo, prevalecen los daños lógicos sobre los físicos. Si bien en este delito el sujeto activo no lleva aparejada la incorporación de la cosa a su patrimonio ni a la de un tercero, ni que se produzca en absoluto incremento alguno de su patrimonio, los daños reposan en el menoscabo causado a la cosa ajena, bien sea cometido de manera dolosa o culposamente. De las acciones descritas en el tipo se infiere que se está ante un delito de resultado en el que es posible su comisión imperfecta.

El artículo 8 contempla la figura culposa de sabotaje o daños a sistemas en virtud del riesgo que supone el uso negligente, imprudente o imperito de tales acciones o del incumplimiento de las normas pautadas para su uso apropiado. Se observa que la reprochabilidad de las conductas antes referidas es mayor cuando recaen sobre un sistema que esté protegido con mecanismos lógicos de seguridad o su destinación esté asignada a las funciones públicas (artículo 9).

Los delitos descritos pueden cometerse con auxilio de tercero (el conocido cooperador, que la LEDI lo describe como "el prestador de servicios de sabotaje") bien en la perpetración o favoreciendo los medios idóneos, que la ley identifica como: importar, fabricar, distribuir, vender o utilizar equipos, dispositivos o programas para vulnerar los sistemas o prestar sus servicios.

En otro sentido, la obtención indebida de datos incorporados en los sistemas que usan tecnologías de información o cualquiera de sus componentes, constituye el delito de espionaje informático. La intimidad y su tutela jurídica se corresponde con dos grandes bloques: en primer lugar, hace referencia a aquellas facultades jurídicas que le proporcionan al titular la capacidad de excluir a terceros de determinados ámbitos a los que se extiende la intimidad de la persona. Así los supuestos relativos al acceso de data confidencial, documentos secretos, control ilícito de sonidos o imágenes de personas se entienden como violación de esas facultades de exclusión frente a terceros en determinados espacios jurídicos.

Pero hoy, se considera también que la intimidad proporciona en determinados casos, singularmente los que afectan a datos obrantes en sistemas informáticos, poderes de control sobre determinados datos y aspectos relativos a la intimidad de las personas. Mata (2001, p. 126) expresa "La eclosión en la sociedad moderna de los sistemas informáticos y las enormes potencialidades lesivas para la intimidad de las personas (naturales y jurídicas) aconsejan que en este territorio se disponga de mecanismos jurídicos apropiados para conocer y vigilar los datos de las personas", debe incluirse, cualquier información que deba ser procesada automáticamente o deba ser almacenada por el motivo que sea.

De esta forma, en concordancia con el artículo 11, quien indebidamente obtenga, revele o difunda la data o información contenida en un sistema que utilice tecnologías de información será perseguido por la vindicta pública como reo de delito; y entre las agravantes contempla la ley: que se obtenga algún beneficio de carácter lucrativo o pecuniario, que se afecte la seguridad del Estado, la confiabilidad de las instituciones afectadas o se produzca algún daño a personas naturales o jurídicas.

Justifica Tablante (2001, p. 165) a favor de la consagración en ley de este tipo argumentando, a manera de ejemplo, que "con la obtención indebida de bases de datos, además de haberse vulnerado la seguridad del sistema, resulta comprometida la privacidad de las personas aun cuando el propósito haya sido la obtención de la información general para utilizarla comercialmente". Se considera que la intimidad proporciona en determinados casos, singularmente los que afectan a datos obrantes en sistemas informáticos, poderes de control sobre determinados datos y aspectos

relativos inherentes exclusivamente a las personas por ello deben ser protegidos in extremis.

En otro contexto, el artículo 12 describe lo que es el delito de falsificación documental, materializado así: crear, modificar o eliminar documentos o datos incorporados a sistemas que utilicen tecnologías de información; o incorporar documentos inexistentes. Las agravantes del tipo atienden a si el autor del hecho delictivo se procuró para si o para un tercero de algún tipo de beneficio o causó un daño a tercero.

Se debe tener presente que las técnicas informáticas pueden ser un instrumento idóneo para cometer falsedades documentales. En cierta manera, aunque el legislador no lo contempla expresamente, la tutela jurídica está orientada a la intimidad recogidos documentalmente o en efectos personales de carácter electrónico. La definición acogida por la ley enmarca al documento en un "registro, incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o actos capaces de causar efectos jurídicos". Indica la jurisprudencia española, compilada por Orts (2001, p. 149), que el documento, a los efectos penales, pueden cumplir tres funciones: 1) de perpetuación, pues hacen que una declaración, una narración, persistan en el tiempo; 2) de garantía, pues permite deducir de quién procede; y, 3) probatoria cualquier otra con efectos jurídicos.

Este tipo se debe principalmente a la expansión del comercio electrónico, teniendo presente que existe incorporado al ordenamiento jurídico venezolano una Ley de mensajes de datos y firmas electrónicas; pero también, el acceso a un sistema para alterar registros, calificaciones, credenciales, antecedentes como se detectó en ciertas oportunidades. Es obligatorio observar, sine qua non, que dicho documento debe tener efectos jurídicos para completar los requisitos del tipo.

Delitos contra la Propiedad

En el mismo Título II en el Capítulo II de la Ley en estudio, desde los artículos 13 al 19 se contemplan los siguientes delitos: Hurto, Fraude, obtención indebida de bienes o servicios, manejo fraudulento de tarjetas o instrumentos

analógicos, apropiación de los mismos, provisión indebida de bienes o servicios y posesión de equipos para falsificaciones.

Ciertos de los delitos que se tipifican en este capítulo guardan similitud con aquellos que se incluyen en el ámbito de los hechos punibles que tutelan penalmente la propiedad en el Código Penal, pero el legislador con su concepción de lo que abunda no daña, los volvió a consagrar.

El ánimo de lucro es parte integrante de todos los delitos allí contemplados, siendo el factor común necesario para la ejecución del delito. Este ánimo de lucro concebido como la pretensión del autor del hecho de conseguir, para sí o para un tercero, un beneficio patrimonial informa también, a decir de Mata (2001, p. 40), "el hecho punible aunque ahora desde la esfera interna del autor, como elemento que exige también el delito pero desde la vertiente subjetiva, la propia del sujeto activo". Al momento de la imputación del hecho al agente se debe tener presente que la tipicidad de los delitos depende de la afirmación de la relación de causalidad entre el comportamiento del sujeto activo y el resultado patrimonial desfavorable al sujeto pasivo (disminución patrimonial) por una parte, y por la otra, de la imputación objetiva del hecho a su autor.

El artículo 13 contempla el delito de hurto, que para ese caso el perpetrador, valiéndose de accesos, interferencias, interceptaciones o manipulaciones de sistemas informáticos, se apodere sacando de la esfera de disposición de su titular, bienes tangibles (dinero efectivo, principalmente) o intangible (créditos, bonos, cupones electrónicos).

Con respecto al fraude, la sutil diferenciación con el hurto estriba en que el primero de los mencionados, el autor debe insertar instrucciones falsas o fraudulentas que conlleven a la producción del resultado "provecho injusto en perjuicio ajeno". Aquí el legislador castiga la manipulación de datos almacenados en sistemas informáticos para lograr una transferencia no consentida de activos patrimoniales. Esta manipulación puede producirse de cualquier forma, en el mismo programa o en cualquier momento del procesamiento o tratamiento automatizado de datos y, también, desde cualquier lugar. Este tipo penal se conoce en otras latitudes, específicamente España, como estafa informática (vid. Código Penal artículo 284.2).

La obtención indebida de bienes o servicios (artículo 15) apareja la utilización de una tarjeta inteligente ajena o un instrumento destinado a los mismos fines para la obtención de efectos, bienes o servicios con la evasión del pago respectivo o evitando asumir su compromiso. Este tipo es muy parecido al contemplado en el artículo 18, siendo este último de pésima redacción para su inteligencia, cuando perfectamente se podrían haber fusionado en un solo artículo.

En el manejo fraudulento y la apropiación de tarjetas inteligentes o instrumentos análogos se sancionan respectivamente, la creación, grabación, duplicación o eliminación de la data o información contenidas en ellas, con el fin de usarlos o transferirlos a un tercero. En ambos casos, se sanciona a quien sin haber tomado parte en el hecho principal, realice cualquier tipo de intermediación con esas tarjetas, las adquiera o reciba. También es penada la posesión de equipos informáticos, aunque sean de libre tracto mercantil, pero que se usen con fines de delinquir; es decir, no autorizados para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos.

Delitos contra la Privacidad de las Personas y de las Comunicaciones

El Capítulo III desarrolla el mandato constitucional contemplado en el artículo 60, conforme al cual la ley debe limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos, describe ciertos comportamientos en los que se afecta la privacidad de las personas y de las comunicaciones a través de los sistemas de información.

El peligro potencial que entraña la tecnología informática para los derechos de los ciudadanos, inconvenientes que se ponen de relieve en los delitos que vulneran la intimidad, no sólo por la facilidad con la que pueden quebrantar estos derechos sino porque la mecanización de datos permite obtener información relevante sobre las personas registradas en sistemas computacionales a través de la combinación de elementos que individualmente pueden resultar intranscendentes. Ejemplifica lo anteriormente dicho, Orts (2001, p. 17) con lo siguiente:

> **La conjugación de los datos concernientes a la identidad de un sujeto con otros, como los relativos a la profesión, nivel económico,**

tendencias en el consumo, preferencias culturales, etc. (sic), permiten conocer caracteres de su personalidad que podrán utilizarse con muy diversos fines (comerciales, laborales, políticos, etc. -sic-). Información que hay que añadir, cuya obtención no resulta difícil, sobre todo respecto de los usuarios de servicios Web disponibles en Internet, para lo cual basta con combinar los datos requeridos para acceder a los mismos con el tipo de servicios consultados.

El Tribunal Constitucional Español en sentencia 110/1984, de 26 de septiembre, había establecido desde esa fecha "1984" la premisa que a continuación se transcribe: “la llamada privacidad informática no se concibe sólo desde el prisma negativo, como prohibición o injerencias externas en el ámbito de la intimidad, sino también como habeas data o libertad informática”, aclarando que “es el derecho de control sobre los datos personales informatizados; entendidos por tales los que conciernen a la persona, su privacidad, pertenezcan o no al ámbito más estricto de la intimidad”.

Este derecho es hoy un derecho fundamental, que además de un instituto de garantía de otros derechos (honor e intimidad), es también, en sí mismo, un derecho o libertad fundamental. Es más, la doctrina ha llegado a diferenciar claramente el derecho de "control de los datos personales" del "derecho a la intimidad" configurándolos como derechos autónomos. Ello en atención a su contenido, pues, dice Orts (2001, p. 19) “mientras el derecho a la intimidad personal y familiar confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en su esfera íntima y la prohibición de hacer uso de lo así conocido” por otra parte “el derecho a la protección de datos atribuye a su titular un haz de facultades cuyo ejercicio impone a terceros deberes jurídicos; en concreto, el derecho a que se requiera el consentimiento para la recogida, uso de los datos personales” y sobre todo “el derecho a saber y ser informado sobre su destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos”; ello es, en definitiva, el poder de disposición sobre los datos personales.

En esencia, estos son los postulados constitucionales y doctrinarios que ha llevado a establecer el artículo 20 de la ley en comento, referente a la violación de la

privacidad de la data o información de carácter personal; destacando ahora las acciones que intencionalmente debe desplegar el agente, tales como: apoderarse, utilizar, modificar o eliminar la data o información incorporada al sistema, sin el consentimiento de su dueño o sobre quien tenga interés legítimo. Debe tenerse presente que una agravante del tipo es el aparte in fine de dicho artículo que pauta un incremento de la pena establecida si tal acción causa daño a su titular o a un tercero.

La violación de la privacidad de las comunicaciones viene contemplada en artículo contiguo y para lo cual el legislador destacó como acciones tendentes a la comisión de ese delito que debe realizarse bien accediendo, capturando, interceptando, interfiriendo, reproduciendo, modificando, desviando o eliminando: a) cualquier mensaje de datos, b) señal de transmisión, c) comunicación ajena.

De las conductas tipificadas en el artículo 21, recién parafraseado, se evidencia que hay dos modalidades comisivas en concreto: la interceptación (a través de todas sus variantes: captura, interferencia, desvío) de telecomunicaciones, entre las que se encuentra la transmisión electrónica de datos y el apoderamiento de mensajes de datos (cualquiera sea su forma de transmitirlo: vía correo electrónico, satélite, línea muerta, entre otros).

Es evidente que el legislador protege en este caso la intimidad propia de cualquier tipo de comunicación, por lo que no exige que ésta se produzca a través de medios técnicos, ni que el autor realice una acción física dirigida a obtener sólo datos secretos; otra cosa es que si exija que el autor en la conducta de ataque a la intimidad, penalmente relevante, emplee medios técnicos para el acceso al contenido de la comunicación o la captación de imágenes o sonidos. La necesidad de empleo de instrumental técnico o de apoderamiento documental impone un umbral mínimo para las conductas penalmente relevantes, que se corresponde con la misión propia del Derecho Penal.

Por su parte, expresa Tablante (2001, p. 167) que “el artículo 21 resguarda la privacidad de las comunicaciones, garantizada en el artículo 48 de la Constitución, en la medida en que resulte vulnerada por el uso de las tecnologías de información”. Con esta regulación, acota el autor citado, se actualiza el concepto de

correspondencia incluyéndose la intercepción de e-mails (correos electrónicos) o cualquier otro mensaje de datos transmitidos por un sistema de comunicaciones.

Por último, se pena la revelación indebida de datos o información de carácter personal en los términos siguientes: “Quien revele, difunda o ceda en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general la data o información obtenidos por alguno de los medios (…) en los artículos 20 y 21 (omissis)”. Agravándose la pena si dicha revelación implica alguna percepción pecuniaria o gratificación material o si resultare algún perjuicio para otro.

Es fácil deducir que la comisión de alguno de los delitos hasta ahora estudiados pueda implicar el concurso material de otros delitos relacionados, con lo cual se elevaría significativamente la pena a imponer. Razonamiento basado en la lógica de que quien comete una acción de esta naturaleza generalmente lo hace motivado por gratificación personal, obtención de incremento patrimonial o fines lucrativo para si o un tercero y el ánimo de causar daños a terceros y alarma social.

Delitos contra (la libertad e indemnidad sexual) Niños, Niñas o Adolescente

El Derecho Penal relativo a las conductas humanas con significación sexual ha experimentado simples cambios relativos en la última década a raíz de la declaratoria de inconstitucionalidad de varios de sus artículos y por la introducción de dos nuevas normativas referentes a: la Difusión o exhibición de material pornográfico (artículo 23) y la Exhibición pornográfica de niños y adolescentes (artículo 24), ambos de la Ley especial contra los Delitos Informáticos.

Sin embargo, la justicia penal en el campo informático, recién referenciado, presenta otros aspectos donde la satisfacción no puede sino ser mucho menor, especialmente en lo referente a la criminalidad sexual violenta y cuyo principal escollo es el de la dificultad para la imputación o capacidad de culpabilidad de los autores de delitos sexuales, a los cuales la ley especial (contra la violencia doméstica y la mujer) no ha podido poner coto. No menos dificultosa es la novel tipología.

En el tapete subyace una controversia que ha llevado a ingentes abogados americanos a las Cortes Penales para dilucidar los límites entre la libertad de expresión, considerada como uno de los derechos fundamentales de la sociedad

moderna que incluye no sólo el derecho de transmitir y difundir ideas e información, sino que también incluye el derecho a recibirlas. Este derecho no debe ser limitado, pronunciamiento del Tribunal, por las fronteras nacionales ni por la forma o medio de comunicación que se utilice para transmitir dichas ideas e informaciones.

Por otra parte, los padres, los institutos de educación y la sociedad en su conjunto tienen la obligación de velar por la educación de los niños y adolescentes, así como protegerlos en su integridad física, psíquica y moral. El objetivo final debería ser la formación integral del menor para su adecuada inserción en el medio social; objetivo que en definitiva apunta a la protección de la dignidad humana, otro de los bienes jurídicos fundamentales cuya tutela también ha sido recogida por la Constitución de la República Bolivariana de Venezuela y en Tratados Internacionales reconocidos por el Estado venezolano.

Es este el marco referencial en el que se encuentra la cuestión en cuanto al control de los contenidos, dos posturas antagónicas con argumentos que involucran en si tres Derechos Humanos Fundamentales: el Derecho a la Intimidad, el Derecho a la libertad de expresión y el Derecho de libre acceso a la información. Hay tres escenarios dentro de los cuales se están manejado ciertos países para sobrellevar la situación: 1) Libertad total, sin control ni restricciones de ninguna naturaleza; 2) Libertad de expresión sin restricciones pero con obligación de los padres a supervisar los contenidos dentro de los cuales sus hijos se desenvuelven; 3) Es el Estado quien a través de órganos que este designe haga la selección de la información a la que el menor puede acceder, censurando o inhibiendo el acceso a los contenidos prohibidos. La solución que plantea la normativa especial venezolana en la materia es muy conciliadora al tipificar:

> **Artículo 23. Difusión o exhibición de material pornográfico. Todo aquél que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.**

Quizá la extensión con la que fue redactada esta norma el legislador pretendió establecer el mecanismo de control suficiente para que la situación de riesgo a la que están expuestos los niños, niñas y adolescentes al acceder a cualquier medio que involucre el uso de tecnologías de información queden incólumes cuando se tropiecen con materiales pornográficos, siendo la obligación del emisor de poner en aviso a los usuarios del material al cual se expondrán y, por el otro, los usuarios quedan facultados para restringir su acceso a los menores. De esta manera, los derechos constitucionales de los involucrados no se ve afectado, la libertad, absoluta, pero se implanta la duda de las personas inescrupulosas que difunden material, no sólo pornográfico, sino racista, xenofóbico o inherentes a cultos satánicos en general y que no tienen su sede comercial en el territorio de Venezuela. Por los momentos no hay forma de controlarlos o simplemente van alternando o rotando sus posiciones.

Con referencia a la utilización de niños, adolescentes (faltó contemplar los incapaces) con la finalidad de utilizarlos con fines exhibicionistas o pornográficos se encuentra penado en el artículo 24 de la LEDI.

La acción que se debe efectuar por cualquier medio que involucre el uso de tecnología de información es: utilizar a la persona o imagen, de los sujetos pasivos determinados “niños, niñas o adolescentes”, con fines exhibicionistas o pornográficos. El legislador pretendió enmarcar todas las posibilidades de formas comitivas que envuelve a personas menores de dieciocho años de edad, en un tipo tan escueto y con una pena muy alta; faltando entre otros aspectos, contemplar también como sujeto pasivo a los incapaces o entredichos, declarados o no por la vía que establece la ley y el castigar a quien ejerce la conducta de mero usuario del contenido o material pornográfico, que dicho por Martín (2001) “no dejará de plantear problemas en la lucha contra este tipo de criminalidad”.

Sin embargo, esta consagración delictual en el ámbito penal ha de considerarse un avance importante en la lucha contra estas transgresiones a personas que no han alcanzado la madurez suficiente para obrar con plena libertad. Se estima que con tal cláusula no se reducirá el ámbito de impunidad de las conductas típicamente constitutivas de delito de pornografía infantil en los casos cuando haya desconocimiento del origen de la actividad o por ubicarse en país extranjero.

Delitos contra el Orden Económico

Con carácter general la tutela penal de la propiedad intelectual protege, frente a los constantes ataques, el conjunto de facultades que el creador tiene sobre su obra literaria, artística o científica. La regulación penal se refiere a las conductas de:obtener algún provecho económico, reproducir, modificar, copiar distribuir o divulgar, sin autorización de su propietario, software o cualquier otra obra del intelecto que haya obtenido el agente por medio del acceso a cualquier sistema que utilice tecnologías de información. Es lo que desde un punto de vista genérico y extrajurídico se conoce piratería y contra la cual grandes empresas trasnacionales habían estado exigiendo para continuar sus operaciones en el país. En el artículo 26 se pena la oferta engañosa así:

> **Artículo 26. Oferta engañosa. Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.**

Visto así, estas ofertas engañosas se convierten en una variante de las estafas informática y se viene a castigar la causación de un perjuicio patrimonial cometido por engaño o artilugios capaces de sorprender la buena fe de las personas. Muchos autores opinan, entre ellos Mata (2001, p. 37), “hay que tener en cuenta la importancia de este hecho punible –la estafa electrónica o informática– que puede catalogarse acertadamente como el centro del Derecho Penal informático”.

Analizados, a grosso modo, los distintos tipos penales de la LEDI se puede destacar que ahora es cuando viene lo difícil del asunto; el legislador soltó un instrumento incompleto, vago y difícil de sortear en estos momentos de crisis.

La criminalidad informática y la dificultad de la prueba judicial

La prueba, referida a la terminología empleada en el proceso judicial, se presenta como un estado de cosas objetivamente verificables y susceptibles de contradecirse en sede jurisdiccional conforme a la ley para producir convencimiento

en los juzgadores (esto en principio, aunque se incluye también a la sociedad) sobre la veracidad o falsedad de los hechos objeto del proceso. Se presenta así que la certeza en el proceso se aproximará más a la verdad objetiva cuanto más amplios, igualitarios, libres, lícitos y flexibles sean los métodos de investigación y cuanto más equilibrado sea la carga de ella en las partes intervinientes.

Por lo tanto, toda cuestión judicial se sustenta, casi siempre, en un hecho o serie de hechos respecto de los cuales existen divergencias entre las partes; lo que genera, indefectiblemente, realizar una exhaustiva investigación y, para el caso informático, delicadas operaciones dirigidas a establecer con exactitud la existencia de hechos constitutivos de delitos. La prueba es un método de averiguación y comprobación, que su libre apreciación hará, según Borrego (1998, p. 74), que "el juez y las partes se sientan más comprometidos por la labor que van a desempeñar (…) en los límites de la rigorosa observancia del deber de comprobación de los hechos, eso sí guiado por la sensatez que brinda el mundo de las garantías procesales y humanas".

Dentro del marco de esta investigación, en lo que se refiere a este punto en concreto, se constata que los países de la comunidad internacional han verificado tres aspectos del fenómeno de la criminalidad informática: su complejidad técnica, el carácter fugaz de sus acciones y su condición predominantemente internacional. Es obvio que la investigación de este tipo de hechos delictivos se aparta en gran medida de los procedimientos investigativos judiciales habituales. Para el cumplimiento de estas misiones se requiere presentar una respuesta por parte del Estado de Derecho rápida, tecnológicamente capaz y coordinada interestatalmente.

Si antes el hecho criminal requería la presencia física de su autor -lo que favorecería su posible localización- hoy día el delito puede cometerse a distancia, amparado en el largo alcance de las redes de comunicación y en sus facilidades de ocultación de identidad. Además, las alteraciones de datos y programas y los accesos a sistemas informáticos no dejan huellas semejantes a la delincuencia tradicional, de forma que las "huellas digitales", según Mata (2001, p. 155), introducen una gran novedad y complejidad.

La afirmación anterior es ratificación de lo expresado por Tiedemann, citado por Sáez (2001), quien plasmó que "la acción y efecto en este tipo de delito, se encuentran generalmente alejadas una de otra y su descubrimiento es difícil

(…) Este es un problema que afecta la investigación y a la prueba que hay que tener en cuenta". La Administración de Justicia y las fuerzas del orden confrontan grandes inconvenientes para detectar la comisión de delitos a través de los medios informáticos y encontrar pruebas jurídicamente relevantes, de que efectivamente, se han perpetrado por un sujeto identificado o identificable conocido como el presunto agente activo del delito. Tales dificultades existen, pero sería exagerado deducir de ahí que se trata de barreras insalvables.

Visto de esta manera, el principal reto a vencer es el cambio de paradigma que involucra una transformación radical de las tradiciones indagatorias (investigativas) con el fin de obtener la verdad bajo este novedoso esquema delictual. Orts (2001, p.169) plantea algunas de las principales dificultades probatorias a las que deben enfrentarse los operadores de justicia hoy en día, resumidamente son:

> a) Una presumible -con bastante fundamento- diferencia tecnológica cuantitativa y cualitativa, en cuanto a los medios, a favor de quienes realizan conductas supuestamente delictivas…
>
> b) La posible tardanza en la concesión de los mandamientos judiciales autorizando la intervención de las comunicaciones electrónicas…
>
> c) Las oportunidades que proporciona la informática para realizar programas que pueden ir seguidos de una inmediata activación o de una activación retardada, que deja sentir sus efectos tiempo después de dada la orden, tal vez incluso, de forma ya no controlada por quien la ordenó. Lo que de modo patente, puede obstaculizar seriamente el rastreo y detección del autor, máxime cuando es factible que al tiempo de la exteriorización del delito, se encuentre realizando una actividad incompatible con la determinante de aquella.
>
> d) Como lo obstaculiza la posibilidad de encubrir el hecho, por ejemplo modificando un programa, para que realice una actividad ilícita en beneficio del autor y establezca una rutina software que vuelva a modificar el programa, en forma automática, una vez realizado el hecho, dejándolo tal y como se encontraba al principio.

e) La facilidad para borrar las pruebas es otro de los impedimentos para la probanza de los hechos. Facilidad que puede estar originada por la pertenencia del autor a la plantilla profesional de la empresa en
la que se encuentra el ordenador, con el que se ha realizado la acción delictiva; por la flexibilidad y dinámica del procedimiento informático, que impide detectar una determinada actividad con posterioridad a su realización, o permite lograr la desaparición de las operaciones efectuadas (omissis)

Pese a todo lo recién reseñado, los operadores de justicia y, especialmente, los cuerpos de investigaciones penales no deben decaer; en muchos casos, será viable afrontar una investigación criminal de naturaleza informática o electrónica que tenga visos de éxito siempre y cuando se disponga de personal especializado y de los medios materiales adecuados.

Principios rectores en materia probatoria para los distintos tipos penales contemplados en la LEDI

El Estado de Derecho es el estamento fundamental de los principios y garantías constitucionales, conjuntamente con la democracia, la igualdad social y la tutela de la condición humana. Cabe destacar que esos postulados conceptuales están materializados en preceptos constitucionales positivo y vigente que sirven de sustento a todo el ordenamiento jurídico venezolano. La ley procesal penal, como expresa Lösing (1998, p. 211), "es la ley operativa de la fiscalía (y su cuerpo de investigaciones científicas, penales y criminalísticas adscrito funcionalmente) para investigar y acusar y del tribunal para procesar a un sospechoso". Pero al mismo tiempo es la “Magna Carta del imputado”, porque por medio del ordenamiento del proceso le brinda protección de sus derechos garantizados en la Constitución. Todo Estado o Nación donde imperen a plenitud los principios informadores del Estado de Derecho tiene la obligación de propiciar y mantener de manera cierta y positiva la igualdad de los individuos y suprimir los impedimentos, que eventualmente surgieran, para el logro de esos fines. Es decir, todas las actividades del Estado, actuando a través de los órganos del Poder Público están sujetas a normas

jurídicas; lo cual se conoce como principio de legalidad. Este principio atribuye potestades, facultades de actuación definiendo cuidadosamente sus límites.

Se puede afirmar, en consecuencia, que el elemento sustancial del Estado de Derecho radica en ser fundamento jurídico de la organización estatal y, subsecuentemente, el establecimiento del principio de legalidad. Bajo esta concepción el Estado no puede subsistir sin Derecho y no podría haber Derecho sin Estado.

Para Marienhoff, citado por Gómez (1995, p. 7), el Estado de Derecho "presupone una autolimitación de sus propios poderes por parte del estado (sic) que permite frente a él un ensanchamiento de la esfera jurídica del administrado (…) que incluye responsabilidad estatal por actos o hechos que le sean jurídicamente imputables".

Sustentados en principios universalmente aceptados, la doctrina ha establecido que las leyes procesales penales domésticas (las propias de cada país) deben prever la adecuada protección de los Derechos Humanos y las libertades. Razón por la cual el Tribunal Constitucional Español en sentencia 21/1998 de fecha 15 de junio de 1998, ratificada en el fallo 49/1999 citadas por Mata (2001, p. 159), señaló que en las investigaciones judiciales donde deba inmiscuirse el Estado en la privacidad de los individuos deben observarse los siguientes principios básicos, sin lo cual se produce vulneración de derechos fundamentales, el criterio mantenido es:

a) La exclusividad jurisdiccional en el sentido que únicamente por la autoridad judicial pueden establecerse restricciones y suspensiones temporales de derechos constitucionales; ejemplo, el secreto de las comunicaciones telefónicas.
b) La finalidad exclusivamente probatoria de las interceptaciones, allanamientos, rastreos electrónicos, entre otros, para establecer la existencia de delito y descubrimiento de las personas responsables del mismo.
c) La excepcionalidad de los medios, que sólo deberá de adoptarse cuando no existan otros medios de investigación del delito, que sea de menor incidencia y causación de daños sobre los derechos y libertades fundamentales del individuo que los que inciden sobre la intimidad personal.
d) Fundamentación de la medida, en el doble sentido de la proporcionalidad y motivación; ello es, balance entre la necesidad de satisfacción social imperiosa y

proporcionalidad a la finalidad legítima perseguida, y en cuanto a la motivación se entiende que el acto es tan grave que necesita encontrar una causa especial suficientemente explicada, para que los destinatarios conozcan las razones del sacrificio de su derecho.

e) Especialidad, principio que significa que no cabe, obviamente decretar una medida de esa naturaleza para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos.
f) Control judicial por cuanto el afectado no conoce la medida y por lo tanto no la puede impugnar ha de garantizarse sus derechos futuros, por lo que aquél debe ser riguroso.
g) Limitación temporal de la utilización de la medida, por cuanto la intervención de manera indefinida o excesiva se convertiría en desproporcional e ilegal.
h) La existencia previa de un procedimiento de investigación penal relacionado con la prueba que se solicita.

Algunos instrumentos jurídicos, entre ellos la Convención sobre Cybercrimen en artículo 16, se lee que "deben existir mecanismos legales expeditos para la habilitación de la competencia de las autoridades con el fin de preservar una la data específica de un computador, especialmente cuando se presuma que dicha información es susceptible de perderse o ser modificada con facilidad". En cuanto a la preservación, almacenamiento o custodia de la data almacenada en la computadora secuestrada judicialmente, y que esté bajo la posesión de su dueño o un tercero que detente su control, debe obligarse a mantener la integridad de la data objeto de investigación por todo el tiempo que dure la investigación o proceso.

Para afrontar la tarea que implica la comprobación del hecho en materia penal conforme a las exigencias constitucionales, es necesario establecer, ab initio, que el Estado establece reglas claras por medio de las cuales deben probarse dichos hechos punibles y las formas como los jueces deben valorarlas pues constituye la base fundamental del debido proceso.

La jurisprudencia nacional (sentencia Nº 00-142, Tribunal Supremo de Justicia en Sala Casación Penal, Ponente Magistrado Jorge Rosell Senhenn) y la doctrina patria ya han aclarado en forma muy amplia que toda prueba a fin de

obtener carácter de tal tiene que cumplir con una serie de requisitos; entendido así, en el caso que nos ocupa, debe tenerse presente que el sistema penal acusatorio venezolano se sustenta sobre estos cimientos: La libertad de la prueba, la dicotomía de la prueba, la distribución cero por ciento (0%) de la carga de la prueba para el imputado o acusado y la libre valoración de la prueba. Gravitándose siempre entorno al principio de legalidad.

Lo dicho anteriormente, alude a que la actividad probatoria debe conducirse en un ambiente de garantías, por lo que la conducta de los operadores de justicia ha de enmarcarse dentro de este propósito; vale decir, que el medio probatorio estará rodeado de condiciones que procuren darle el piso de legitimidad suficiente para ser adquirido por el proceso. La norma rectora de rango constitucional que establece este postulado es el artículo 49, donde se lee:

> **El debido proceso se aplicará a todas y cada una de las actuaciones judiciales y administrativas y, en consecuencia:**
>
> **1.- La defensa y la asistencia jurídica son derechos inviolables en todo estado y grado del proceso. Toda persona tiene derecho a ser notificada de los cargos por los cuales se le investiga, de acceder a las pruebas y de disponer de tiempo y de los medios adecuados para ejercer su defensa. Serán nulas las pruebas obtenidas mediante la violación del debido proceso (…)**
>
> **2.- Toda persona se presume inocente mientras no se prueba lo contrario (omissis)** -subrayado del autor-

Dicho en otras palabras, la prueba no puede ser producto de actos contrarios al Estado de Derecho, democrático y respetuoso de los Derechos Humanos, quebrando así las prácticas perniciosas que se gestaban en los órganos de investigaciones penales y que aún, pese a ello, hoy en día, dichos vicios subsisten.

Otra carga que lleva a sus espaldas el Ministerio Público, conjuntamente con los principios de legalidad y debido proceso, es el desvirtuar la presunción de inocencia; mandato constitucional que impone a todos los ciudadanos y, especialmente, a los operadores de justicia consistente en que nadie puede ser considerado culpable de un delito sin una sentencia obtenida en un juicio. Este principio de inocencia fue reconocido a nivel internacional en muchas declaraciones

y tratados que sobre Derechos Humanos se han efectuado; la Constitución de la República Bolivariana de Venezuela reconoce taxativamente dicho principio, de manera formal, leyéndose en el artículo 49 numeral 2 “Toda persona se presume inocente mientras no se pruebe lo contrario”.

Apunta acertadamente Binder (1999, p. 132) “la vigencia real de esos pilares es lo que diferencia a las sociedades democráticas de los Estados autoritarios o de aquellas democracias que no son más que meras fachadas de un poder arbitrario”. Dicho de esta manera, los instrumentos Constitucionales y legales existentes en Venezuela otorgan a todos sus ciudadanos dichos derechos, lo que queda por hacer es hacerlo valer efectivamente.

A todo lo anteriormente dicho, debe agregarse que el respeto a la dignidad e integridad de la persona (artículo 3 de la Constitución de la República Bolivariana de Venezuela) en materia de pruebas, visto desde el ámbito legal -propiamente en el COPP- se materializa en su artículo 197 primer aparte “los elementos de convicción sólo tendrán valor si han sido obtenidos por un medio lícito e incorporado al proceso conforme a las disposiciones de este Código”. En otras palabras, la prueba no se puede obtener mediante tortura, maltrato, incomunicación, amenaza, engaño, indebida intromisión en la privacidad personal, domicilio o comunicaciones íntimas de cualquier naturaleza, ni archivos privados sin la debida autorización judicial y siguiendo todas las pautas que para ello son requeridas, tal como se comentó ut supra.

Es muy conocida la teoría en la que se apoyan muchos juristas para impugnar medios probatorios obtenido en contravención a las pautas ya comentada y es la llamada “fruta del árbol envenenado”. Ello significa que no se puede asumir ni dar valor probatorio a aquellas pruebas que fueren obtenidas sacrificando derechos y garantías constitucionales e, incluso, violando los Derechos Humanos; la concepción también se extiende a aquellos medios probatorios que aunque lícitos, provienen de una fuente viciada y contraria al debido proceso, refleja Borrego (1998, p. 82).

La necesidad de la prueba es entendida por algunos autores como sinónimo de objeto de la prueba, siendo éste último como el tema de la prueba (thema probandum), en tanto hay otros que suponen que el objeto de la prueba es una noción genérica e indeterminada que expresa todo lo que en general puede probarse,

considerando que la necesidad de prueba es una noción concreta lo que indica efectivamente debe probarse en un proceso determinado. Resumiendo, para estos últimos el thema probandum es lo mismo que la necesidad de la prueba, lo que debe ser probado.

Esa necesidad de probar lo alegado se contempla en el COPP en el artículo 198, donde las partes pueden hacer de manera libre, pero en los términos siguientes:

> **Salvo previsión expresa en contrario de la ley, se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso y por cualquier medio de prueba, incorporado conforme a las disposiciones de este Código y que no estén expresamente prohibidos por la ley (…)**
>
> **Un medio de prueba para ser admitido, debe referirse, directa o indirectamente, al objeto de la investigación y ser útil para el descubrimiento de la verdad (omissis)**

A propósito de la libertad probatoria contenida en dicho artículo y regulada en todo el Título VII artículos desde el 197 al 236 inclusive, el artículo recién citado sirve de orientador para conducir la actividad probatoria y en este sentido, los medios probatorios tienen que disponerse para satisfacer el objeto de prueba, por lo que cualquier prueba que no cumpla con este cometido, será una prueba descartada.

Por todo esto, debe necesariamente concluirse que las pruebas que se aporten a un juicio donde se ventile la comisión de un delito informático deben atenerse inexorablemente a estos postulados; por lo tanto, los órganos de investigaciones penales y el Ministerio Público deben ser exacerbadamente cuidadosos de no incurrir en violaciones flagrantes a estos principios por muy urgentes que sea la práctica de cualquier actuación para obtenerla y poder atrapar al sujeto activo.

Principios metodológicos propuestos para las investigaciones criminalísticas en materia informática

La criminalística es definida por Del Giudice (2000, p.49) como “la ciencia que aplica los procedimientos técnicos y científicos empleados en las diferentes áreas de las ciencias naturales (…) a los objetos involucrados en la comisión de un hecho punible, previstos, contemplados y sancionados en el Código Penal”. Al respecto,

concuerda López (2000, p. 148), al interpretar varias definiciones que la criminalísitica, que ésta es “la ciencia auxiliar del derecho que utiliza o emplea los recursos técnicos-científicos en la búsqueda y análisis de los elementos materiales de pruebas, a fin de establecer si hubo un delito (…) y determinar las posibles causas o móviles de lo sucedido”.

Los elementos de convicción son analizados y evaluados en las diferentes áreas de la criminalística y los resultados obtenidos, concatenados entre sí, serán determinantes para sustentar los argumentos y alegatos de las partes -inculpatorios o exculpatorios- durante el proceso. La criminalística es una especialidad científica que aporta y explica los procedimientos técnicos a los elementos probatorios, involucrados en la comisión de un hecho punible en materia penal. El conocimiento del modus operandi de los transgresores y los métodos para su aprehensión; la habilidad, la paciencia, el tacto, la laboriosidad y la minuciosidad, aunados a una disposición peculiar del investigador criminal eficiente, serán siempre los recursos primordiales en la labor investigativa, según afirma López (2000, p. 149).

En este contexto, el objetivo formal de la criminalística es auxiliar con los resultados basados en análisis técnicos-científicos, metodología y tecnología, a los fiscales del Ministerio Público, con el fin de darles suficiente material probatorio identificadores y reconstructores conducentes a restablecer la verdad de los hechos que se investigan e incorporarlos pertinentemente al juicio. La estructura procedimental de esta ciencia en estudio consiste en la aplicación de conocimientos técnicos que se desprenden, informa Del Giudice (2000, p. 50), a partir de “la observación y recolección de los objetos hasta el desarrollo del análisis cualitativo y cuantitativo empleados en los laboratorio científicos, los cuales utilizan principios, leyes, causas y efectos de la naturaleza en el campo penal”.

Punto previo, a los fines de armonizar todo lo anteriormente dicho, se debe establecer la denominada cadena de custodia que preservará la evidencia hasta su evacuación en el proceso penal respectivo; entendida ésta por López (2000, p. 139) “como un procedimiento que tiene el propósito de garantizar la integridad, conservación e inalterabilidad de elementos materiales de prueba (omissis) entregados a los laboratorios criminalísticos o forenses por la autoridad competente a fin de analizar y obtener, por parte de los expertos, técnicos o científicos un concepto

pericial". Como nota a resaltar de esto, la cadena de custodia permite conocer en cualquier estado del proceso dónde se encuentra el elemento de prueba, quién lo tiene, nombre del perito; lo cual, lógicamente, garantiza la seriedad y transparencia del dictamen efectuado por expertos de los distintos laboratorios, debiéndose entregar los resultados en forma oportuna y con la calidad exigida en la investigación.

Del Giudice (2000, p. 51) describe en líneas generales, refiriéndose a los procedimientos técnicos preliminares, las fases de los métodos practicados en la recolección de los medios de prueba en el sitio del suceso o en áreas correlacionadas con el hecho, a saber: Protección y resguardo; búsqueda y hallazgos; fijación, fotografía o videografía; metodología para el levantamiento de rastro, huella o muestras; constancia en acta; traslado al laboratorio y entrega de los resultados al solicitante.

Del razonamiento anterior en confrontación con el problema objeto de esta investigación se colige, por lo tanto, que surge una nueva rama de esta ciencia denominada por Toledo (2001) como "criminalísitica informática", donde la evidencia, por tratarse de delitos informáticos, debe analizarse desde el punto de vista físico como lógico. Esta novel modalidad delictiva abrie nuevas áreas que deben vigilarse, desarrollando un adecuado control, mecanismo de seguridad e investigación en atención al emergente paradigma criminal digitalizado.

Se pasa así a un sitio del suceso informático "físico" si las experticias deben realizarse sobre el hardware o sistemas que utilicen tecnología de información o "virtual" en los términos contemplados en la LEDI (ejemplo, rastreo de comunicaciones en línea). Ello para establecer fehacientemente: el qué, cómo, dónde, cuándo, por qué y quienes; o también, causas, motivos, formas o maneras, ubicación en el tiempo y en el espacio e identidades en general.

En relación con la investigación de los entes físicos, propone Toledo (2001) la técnica que a continuación se detalla:

- La protección: Tiene por objetivo primordial conservar el sitio informático de irrupción en las mismas condiciones físicas de hardware y software y del entorno físico en que fue encontrado;

- Inspección ocular: Acto de verificación personal en el mismo lugar de ocurrencias de los hechos, practicados para describir, recoger elementos o materiales de la perpetración del hecho y los objetos relacionados con la existencia y naturaleza del hecho presuntamente delictivo. Debe ser realizado por el funcionario que tenga a cargo la investigación, de forma excluyente, y cuente con la respectiva orden de allanamiento, procurando mantener el lugar sin alteraciones de ningún tipo;
- Aislamiento: Consistente en delimitar el sitio del suceso para impedir se contamine o altere, bien evitando la circulación de data o el acceso a terceros a los equipos propiamente;
- Clausura del establecimiento o comiso de los bienes incautados para su posterior análisis.

Advierte dicho autor que antes de proceder a la fijación, levantamiento, custodia y envío de las evidencias colectadas, es preciso que el personal investigador considere las siguientes recomendaciones, para su trabajo en el sitio del suceso:

- Establecer los tipos de evidencias que serán más probables que se encuentren;
- Concentrarse en las evidencias más transitorias o perecederas;
- Asegurarse que todo el personal considere la gran variedad de evidencias posibles existentes;
- Asegurarse que se tenga a mano suficiente material para empacar (para practicar el denominado embalaje);
- Enfocarse en las áreas de fácil acceso que se encuentren a simple vista y luego en lugares menos accesibles;
- Verificar si la evidencia a sido desplazada, movida, se encuentra en un sitio de liberación o deliberadamente preparadas simulando un hecho punible;

Una vez procesada y analizada la evidencia física este autor citado sugiere que se evacuen las resultas en un formato diseñado exclusivamente para tal fin, como los que se presentan en los anexos Nº 4 y 5; en atención si el análisis correspondió a componentes lógicos o físicos de los sistemas de tecnología de información.

Las investigaciones de los delitos virtuales o en línea se torna más compleja porque ellas son sui generis, esto es, dependerá del medio comisivo o forma de

conculcación de los derechos jurídicamente tutelados. El autor de este trabajo no encontró documentación alguna que describiera experiencias sobre esos aspectos. Sobre la base del contenido de este capítulo puede deducirse que esas investigaciones deben contar con una orden judicial previa y deben documentarse de manera idónea (bitácora, grabaciones, registros, entre otros) de forma tal que puedan ser reproducidas en juicio.

Sistema de Hipótesis

Ya planteado el problema, revisada la literatura especializada tanto nacional como internacional y contextualizado los antecedentes y el marco teórico de esta investigación, por cuanto el estudio es exploratorio, analítico-descriptivo, el siguiente paso es establecer las guías precisas del problema éstas son las hipótesis.

Las hipótesis indican lo que se está buscando o tratando de probar y la define la Universidad Nacional Abierta -UNA- (1998, p. 175) como "la explicación tentativa a un problema de estudio de una manera amplia"; esto es, son las explicaciones tentativas acerca de las relaciones entre dos o mas variables y se apoyan en conocimientos organizados y sistematizados, del fenómeno investigado formulado a manera de proposiciones.

Siendo la hipótesis el supuesto que se enuncia para indicar la manera en que ocurre un determinado hecho, en relación a los factores involucrados en ellos, tenemos que la hipótesis planteada por el autor del presente Trabajo de Grado es:

H1: La incorporación formal al ordenamiento jurídico venezolano de la Ley especial contra los Delitos Informáticos soluciona la problemática inherente a este tipo de criminalidad, probarlo judicialmente es fáctico y materializable contando con la preparación intelectual y académica de los cuerpos de investigaciones penales y los operadores de justicia.

H0: La incorporación formal al ordenamiento jurídico venezolano de la Ley especial contra los Delitos Informáticos no soluciona la problemática inherente a este tipo de criminalidad, probarlo judicialmente no es fáctico porque no se cuenta con una idónea preparación intelectual y académica de los cuerpos de investigaciones penales y los operadores de justicia.

Sistema de Variables

Variable es definida por la UNA (1998, p. 203) como “una característica de un objeto de investigación que puede ser medida”. Por lo tanto, un sistema de variables, según Arias (1999, p. 43) es aquel que “consiste, por lo tanto, en una serie de características por estudiar, definidas de manera operacional, es decir, en funciones de sus indicadores o unidades de medida”.

MAPA DE VARIABLES

Objetivo Sondeo Opinión	Variables	Dimensiones	Indicador
2,3		Tipificación	Conducta Penada
4			Regulación
1,4	Legislación	Procedimiento	Prohibida
1,3,4,6		Regulación	Violación de Ppios
Estudio de las Conductas Disvaliosas Emergentes Del nuevo Milenio: Los Delitos Informáticos Y su actividad Probatoria Según el COPP 1,3,6,9 1,6,8,10	Área de Derecho	Conocimiento	Opinión
		Capacitación	Información
3,4,6,7,9		Acuerdo/Desacuerdo	Práctica Judicial
1,5,6,8,10	Ejercicio o Praxis Judicial	Ejercicio Profesional	Preparación Técnica
		Aceptación/Rechazo	Tipos penales /

Las variables comprometidas en la presente investigación corresponden:

- Regulación Penal especial/colateral
- Ámbito probatorio Penal
- Recursos materiales y humanos para una idónea operatividad.

CAPÍTULO III
MARCO METODOLÓGICO

Tipo de Investigación

La investigación de campo es entendida como "el análisis sistemático de problemas de la realidad con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos, o predecir su ocurrencia", resaltando que se hace "uso de métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo" (Universidad Pedagógica Experimental Libertador, 2001).

En atención a ello, el diseño escogido por el investigador para la presente investigación es de campo con carácter exploratorio-descriptivo orientada al estudio de las conductas disvaliosas del nuevo milenio: Los Delitos Informáticos y su actividad probatoria según el Código Orgánico Procesal Penal venezolano vigente; consistente en la recolección de datos directamente de la realidad donde ocurren los hechos; es decir, a partir de datos originales o primarios sin manipular o controlar variable alguna.

Según los objetivos del estudio propuesto y la disciplina en la cual se enmarca la temática se dice que éste es de tipo exploratorio por cuanto se efectúa sobre un tema e instrumento legal poco conocido o estudiado dentro de lo que corresponde al ordenamiento jurídico venezolano, por lo que sus resultados constituyen una visión aproximada de dicho objeto.

Desde el punto de vista de los objetivos, general y específicos, de la investigación y al tipo de conocimiento que se quiso obtener, es de carácter analítico-descriptivo, que según Sabino (1987, p. 89), "se proponen conocer grupos homogéneos de fenómenos utilizando criterios sistemáticos que permitan poner de manifiesto su estructura o comportamiento".

En consecuencia, el estudio de las conductas disvaliosas del nuevo milenio: Los Delitos Informáticos y su actividad probatoria según el COPP fue realizado de manera analítico-descriptiva lo cual deviene de la novedad del tema en el ámbito legislativo y se trata de un área del conocimiento precaria de investigación a nivel nacional y todas las obvias consecuencias implícitas que en el área del Derecho Penal tiene ese instrumento legal.

Población y Muestra

Población

Una población está determinada por sus características definitorias. Se define como “todas las unidades de investigación que seleccionamos de acuerdo a la naturaleza de un problema, para generalizar hasta ella los datos recolectados” (UNA 1998, p. 272).

Por lo tanto, el conjunto de elementos que posea estas características se denomina población o universo. La población es la totalidad del fenómeno a estudiar, donde las unidades de población poseen una característica común, la que se estudia y da origen a los datos de la investigación.

Para el estudio propuesto, la población considerada estuvo enmarcada dentro de los siguientes estratos: abogados en el libre ejercicio de la profesión, fiscales del Ministerio Público y Jueces con competencia Penal, todos éstos pertenecientes al Circuito Judicial Penal del Estado Carabobo o ejerciendo en dicha circunscripción.

Muestra

Cuando se selecciona algunos elementos con la intención de averiguar algo sobre una población determinada, se infiere a este grupo como muestra. Por supuesto, se espera que lo obtenido o averiguado en la muestra sea cierto para la población en su conjunto. Sería, entonces, la muestra un subconjunto de elementos de la población; soliéndose tomar muestras cuando es difícil o costosa la observación de todos los elementos de la población estadística.

La exactitud de la información recolectada depende en gran medida de la forma en que se selecciona la muestra. La muestra descansa en el principio de que las partes representan al todo y, por tal motivo, refleja las características que definen la población de la que extraída, lo cual indica que es representativa.

En la presente investigación el tipo de muestreo fue no probabilísticas y para su conformación se seleccionó una muestra intencional debido a la magnitud de la

población, lo cual permitió la selección de profesionales en derecho escogidos por los siguientes criterios:

- Asentimiento libre de coacción para formar parte integrante de la investigación;
- Ser profesional en Derecho y estar ejerciendo de manera activa bien en el libre ejercicio, ser fiscales del Ministerio Público o Jueces con competencia en lo Penal;
- Que desarrollasen su actividad jurídica profesional en el ámbito de la Circunscripción Judicial del Estado Carabobo.

Muestreo Intencional

Estrato	Muestra
Abogados en el libre ejercicio de la profesión	20
Fiscales del Ministerio Público	15
Jueces con competencia en lo Penal	10
TOTAL	45

Todos ellos proporcionaron información inherente al tema objeto de la investigación por medio de un instrumento-cuestionario especialmente elaborado para tal fin y ajustado a la característica propia de este estrato.

Instrumentos y Técnicas de recolección de datos

Uno de los tantos escollos que se le presenta al investigador durante su trabajo investigativo es la recolección de datos o información que necesita para comprobar la hipótesis que se ha formulado. Para ello, se tiene que elaborar lo que se conoce como instrumento de recolección de datos y que le permitirá registrar y tabular la información que interesa, para luego ser procesada y extraer las conclusiones comprobando o rechazando, finalmente, dichas hipótesis.

El instrumento es definido como el consistente “en un formulario diseñado para registrar la información que se obtiene durante el proceso de recolección” (Universidad Nacional Abierta 1998, p. 307). Es decir, son los medios materiales que se emplean para recopilar la información requerida. Concuerdan expertos en metodología que un instrumento de medición adecuado es aquel que registra datos observables que representan verdaderamente a los conceptos o variables que el investigador tiene en mente.

Las técnicas que se utilizaron en esta investigación fueron: el análisis documental, de contenido y la encuesta.

Es evidente que los datos y la información adquieren la significación en función de la interpretación del investigador. El análisis documental y de contenido permitió la revisión bibliográfica así como la normativa nacional e internacional para configurar el marco teórico. En la realización del presente análisis se utilizaron las diversas formas de interpretación del material revisado, dado que la interpretación de las fuentes formales del derecho, aun las indirectas, se explican a través del lenguaje que es el elemento simbólico cuyo contenido se desentraña en la medida que se aproxima a lo que él significa. Para analizar las normas legales se empleó el método de interpretación exegética, sistemática y gramatical, también se recurrió a la analogía y a los principios generales del derecho; pero, en última instancia se empleó la hermenéutica para fijar el verdadero contenido de la problemática sujeta a análisis.

La aplicación del instrumento cuestionario permitió pulsar la opinión en la muestra seleccionada, que en función de la operacionalización de las variables del estudio constan de dos partes:

I. Identificación de la muestra: Abogados en el libre ejercicio de la profesión, fiscales del Ministerio Público y Jueces con competencia en lo Penal.

II. Comprendida por los diversos ítems del cuestionario que versan sobre la opinión del tema objeto de estudio. La escala utilizada para las respuestas es la denominadas “Dicotómica, limitadas o de alternativa fija” que sólo pueden ser contestadas por un “si”, “no” y en último caso “no sé/no contesta”.

Validez y Confiabilidad

Validez

La cualidad de un buen instrumento de recolección de datos se expresa por medio de su validez: bien sea, de contenido, de criterio o de costructo. Para el estudio de marras, la validez de contenido representa el grado con el cual un instrumento examina, contiene o es representativo de los distintos aspectos que se pretenden ubicar. La UNA (1998, p. 311) establece ciertas características para que un instrumento tenga validez, entre las cuales destaca que debe: "medir lo que se pretende que mida y no otra cosa, hacerlo en forma correcta, adecuado al problema de estudio, seguro para facilitar la comparación, discriminar bien los datos y omitir datos no significativos".

Para dar cumplimiento a estas recomendaciones, al instrumento-cuestionario se le aplicó validez de contenido por medio del procedimiento de juicio de expertos, consistente en presentarlo (conjuntamente con un anexo que indicaba los objetivos de la investigación y el cuadro de variables) a especialistas en las siguientes áreas: metodología, gramática y literatura y abogado especialista en el área penal. La labor desempeñada por estos profesionales se centró en determinar la congruencia los aspectos de redacción con la pertinencia de los ítems con los objetivos.

Los resultados de este proceso conllevó a la subsanación de errores en varios ítems, considerados confusos o ambiguos para las posibles respuestas.

Confiabilidad

La confiabilidad viene dada por la seguridad que tiene un investigador de la exactitud y estabilidad de los resultados obtenidos al aplicar un instrumento; dicha medición se refiere a que su aplicación repetida a la misma muestra produce iguales resultados.

Hay distintos métodos para determinar la confiabilidad de un instrumento dado, entre las cuales se tiene: medida de estabilidad (test-retest), método de formas alternativas (versiones similares), método de mitades partidas (división y comparación de los items) y el alpha de Cronbach. Estos coeficientes oscilan entre

los valores de cero (0) y uno (1), donde la tendencia hacia cero significa "nula" confiabilidad y hacia el uno, confiabilidad total.

La confiabilidad fue realizada a través de una prueba piloto, consistente en aplicar el instrumento a manera de prueba a un grupo de personas similares a la muestra pero no pertenecientes a la misma y luego examinar los resultados, aplicando luego la fórmula de alpha de Cronbach, que arrojó como resultado un índice de alta confiabilidad (0,91). Hay que acotar que este coeficiente alpha se utiliza para describir la confiabilidad de los factores extraídos de cuestionarios o escalas ajustadas a formato dicotómico, y que mide especialmente variables unidimensionales puesto que para datos multidimensionalmente estructurados el coeficiente alpha siempre será bajo.

Fases de la investigación

De acuerdo al tipo de diseño investigativo, ya mencionado, y para lograr alcanzar los objetivos propuestos, se procedió de la siguiente manera:

a) Se acopió de manera sistemática los textos (incluidos la prensa nacional y documentos de la Internet), leyes y jurisprudencias pertinentes con el tema investigado atendiendo al criterio de autenticidad e integridad de fuentes primarias; tratando de cubrir el universo cognoscitivo transitado hasta la fecha. Realizando, a posteriori, una organización de las mismas, indicando las respectivas referencias bibliográficas de los documentos consultados.
b) Seguidamente, se procedió a una clasificación detallada para extraer de ellas todos los datos indispensables, acumulándolos para la cabal sustentación teórica del planteamiento del tema y que tendría incidencia directa en las conclusiones. Realizando, para ello, una lectura comprensiva, analítica y discriminatoria que permitió organizar los distintos títulos y subtítulos planteados.
c) Se elaboraron fichas de contenido que luego fueron vertidas en las matrices de análisis de relevancia del contenido (ver anexos Nº 2 y 3), para realizar luego una referencia cruzada de la información, inferencias y análisis crítico, enfatizando los aspectos coincidentes y discordantes que hay entre ellas.

d) Seguidamente, correspondió el análisis de los resultados obtenidos en el sondeo de opinión, el cual fue aplicado, previamente, a la muestra intencional reseñada ut supra.
e) Todo lo anterior conllevó a los resultados explanados en la conclusión de la investigación y permitió hacer las recomendaciones subsecuentes.

CAPÍTULO IV

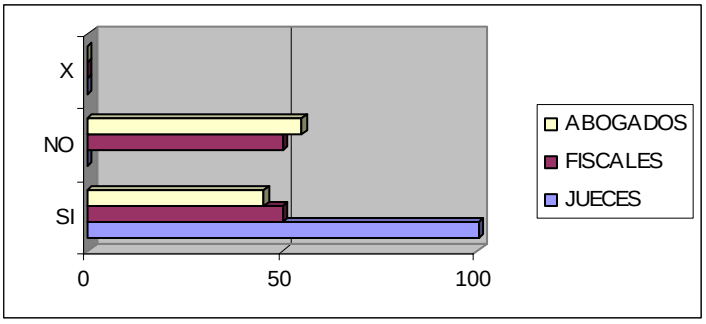
ANÁLISIS DE DATOS

Para dar cumplimiento a los objetivos propuestos en la investigación, como técnica de análisis de resultados obtenidos se utilizó la estadística descriptiva mediante el uso de "distribución de frecuencias y porcentajes". Del instrumento aplicado a la muestra establecida en el capítulo anteriormente indicada, se extrajo la siguiente información:

Preguntas del instrumento de recolección de datos:

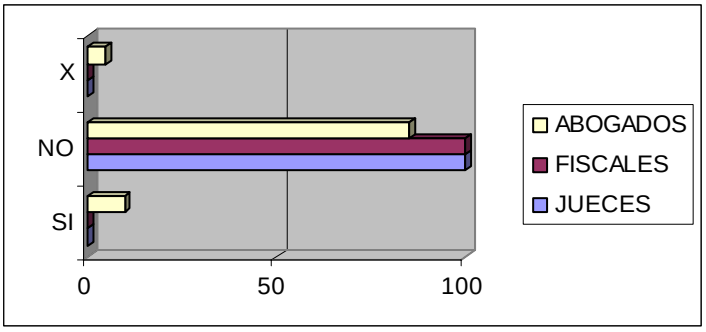
1.- ¿ Está familiarizado(a) con los tipos penales contemplados en la Ley especial contra Delitos Informáticos ?

	SI	NO	no contesta
JUECES	100	0	0
FISCALES	50	50	0
ABOGADOS	45	55	0



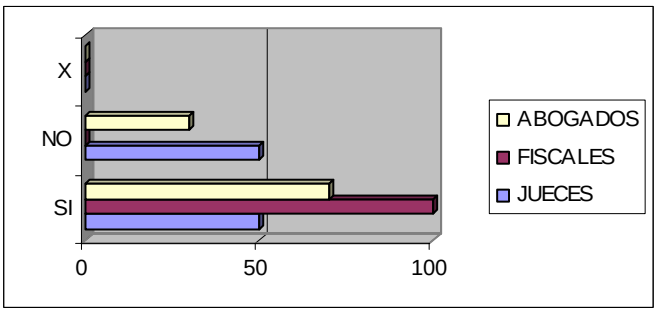
2.- ¿ Este instrumento legal (Ley especial contra Delitos Informáticos) será suficiente para prevenir o minimizar el auge delictivo empleando nuevas tecnologías ?

	SI	NO	no contesta
JUECES	0	100	0
FISCALES	0	100	0
ABOGADOS	10	85	5



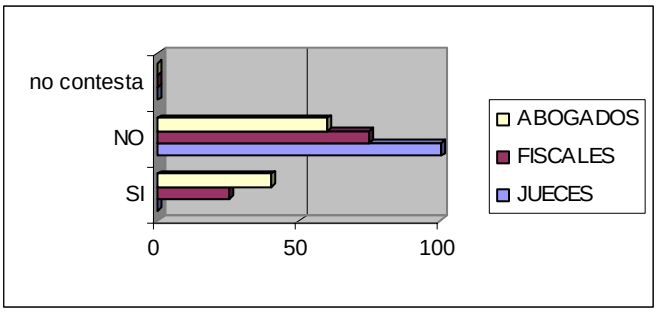
3.- ¿ Considera que es pertinente este nuevo texto legislativo como regulación penal especial colateral al Código Penal Venezolano vigente ?

	SI	NO	no contesta
JUECES	50	50	0
FISCALES	100	0	0
ABOGADOS	70	30	0



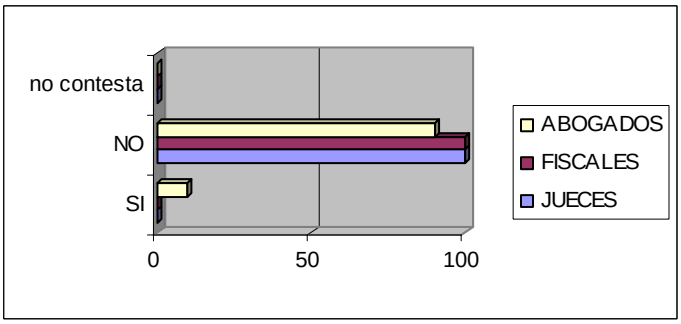
4.- Al ser una materia novedosa este tipo de criminalidad, ¿ opina Usted favorablemente de tramitarlo por otra jurisdicción distinta a la penal ordinaria ?

	SI	NO	no contesta
JUECES	0	100	0
FISCALES	25	75	0
ABOGADOS	40	60	0



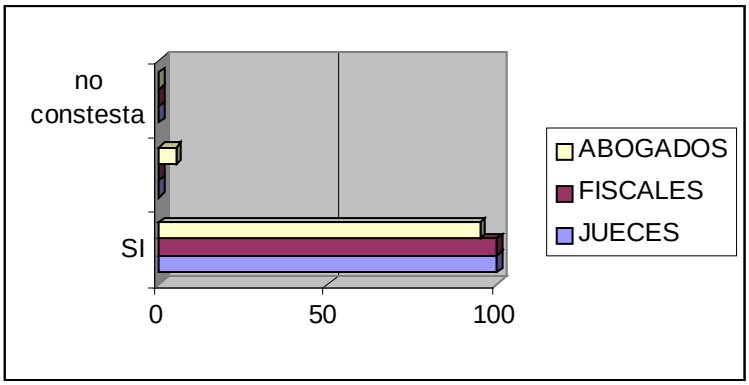
5.- ¿ Está Usted suficientemente preparado(a), técnica y jurídicamente, para llevar a cabo un proceso judicial penal en esta materia ?

	SI	NO	no contesta
JUECES	0	100	0
FISCALES	0	100	0
ABOGADOS	10	90	0



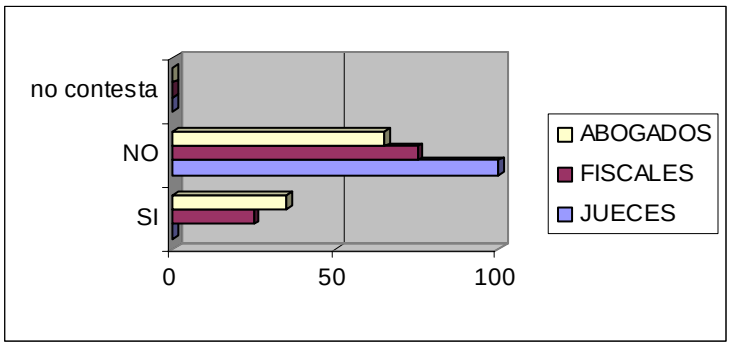
6.- ¿ Cree Usted que habrá dificultad probatoria para demostrar el hecho punible al momento de realizarse el juicio ?

	SI	NO	no contesta
JUECES	100	0	0
FISCALES	100	0	0
ABOGADOS	95	5	0



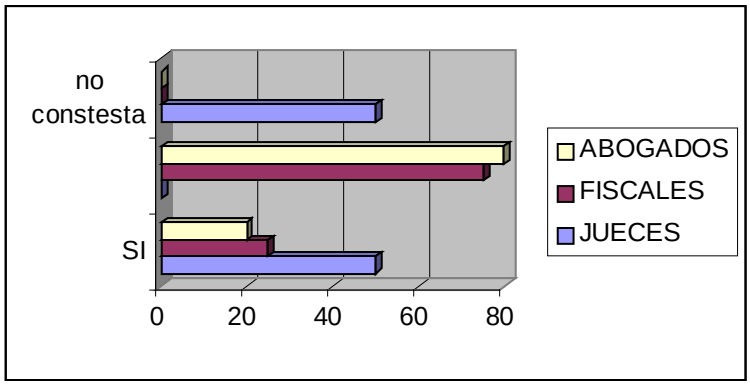
7.- ¿ Existen recursos técnicos suficientes para establecer y reproducir en juicio de manera indubitable la prueba de la comisión del delito ?

	SI	NO	no contesta
JUECES	0	100	0
FISCALES	25	75	0
ABOGADOS	35	65	0



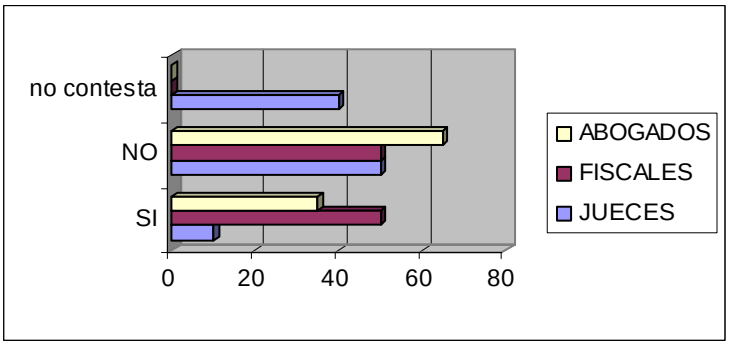
8.- ¿ Maneja Usted las definiciones técnico-jurídicas de orden informático empleada en la mencionada Ley especial ?

	SI	NO	no contesta
JUECES	50	0	50
FISCALES	25	75	0
ABOGADOS	20	80	0



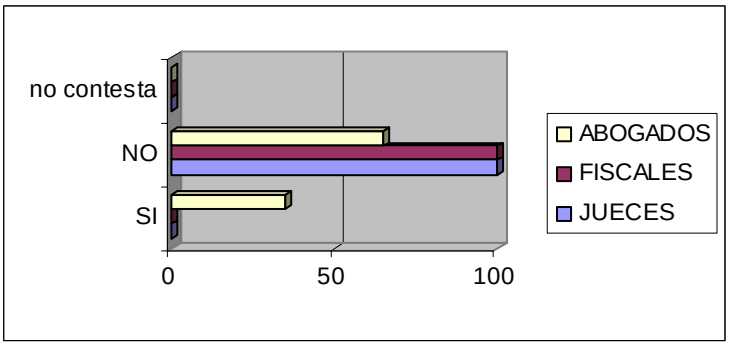
9.- ¿ Confía en la prueba pericial que efectúa el cuerpo de investigaciones científicas, penales y criminalísticas (CICPC) en la materia informática ?

	SI	NO	no contesta
JUECES	10	50	40
FISCALES	50	50	0
ABOGADOS	35	65	0



10.- ¿ Tiene conocimiento de algún centro especializado o perito que puedan realizar verificaciones o corroboraciones a las pruebas obtenidas por el (CICPC) a los fines de desvirtuarlas o no ?

	SI	NO	no contesta
JUECES	0	100	0
FISCALES	0	100	0
ABOGADOS	35	65	0



Fuente: Di Fabio (2002)

De la información recopilada y que se muestra ut supra gráficamente se desprende lo siguiente:

1.- El texto legal que recoge los tipos penales que el legislador venezolano consideró debían ser considerados delitos informáticos no es conocido por la totalidad de los operadores de justicia. Sólo los jueces expresan conocer la ley en su totalidad, no así los fiscales y abogados en el libre ejercicio de la profesión que contestaron afirmativamente un 50 y 45 por ciento respectivamente.

2.- Con respecto al freno delictivo que supondría la ley, creando así la intimidación necesaria para evitar esas conductas, los encuestados contestaron mayoritariamente de manera negativa, salvo un 10% de los abogados en el libre ejercicio que consideran que este instrumento legal frenará la comisión de esos delitos. Por lo que se deduce que la impresión en los operadores de justicia es que ha sido un esfuerzo vano y sin repercusiones favorables para la sociedad que pretende proteger.

3.- La implementación de leyes penales fuera del contexto unificador que debe representar el Código Penal sigue siendo una constante dentro de nuestro ámbito jurídico y los encuestados manifiestan sentirse cómodos con esta práctica. Según se desprende de la información los jueces en partes iguales; es decir, 50% a favor y 50% en contra;los fiscales en su totalidad y los abogados en un 70% favorablemente.

4.- Cuando se les preguntó al respecto de crear una jurisdicción especial o tramitarlo por ante tribunales con competencia especial en la materia el criterio mantenido se inclina al ámbito negativo; ello es, la convicción de los operadores de justicia es a mantener la jurisdicción penal ordinaria para encausar los procedimientos judiciales en la materia. Sólo un 25% de los fiscales y un 40% de los abogados en el libre

ejercicio son de la opinión de que se cree un tribunal especial en la materia de delitos informáticos.

5.- Al inquirirse respecto al fondo o contenido propiamente de la ley y sus particularidades, la casi totalidad de los encuestados afirma no sentirse preparado técnica o jurídicamente para llevar a cabo un proceso judicial en materia penal tan específico como es el referente a delitos informáticos. Sólo un 10% de los encuestados pertenecientes a renglón de abogados en el libre ejercicio dicen sentirse preparados para llevar adelante un juicio de esta naturaleza.

6.- La materia probatoria de los delitos informáticos es un aspecto que se presenta preocupante para los involucrados en el proceso penal. Casi en su totalidad (salvo un 5% de los abogados en el libre ejercicio) manifiestan que probar delitos informáticos en un juicio penal resulta prácticamente imposible.

7.- Manteniendo una concordancia sincrónica con la pregunta anterior, es preocupación evidente la ausencia de recursos suficientes para establecer y reproducir en juicio la prueba de la comisión del delito. Por lo tanto, el 100% de los jueces, el 75% de los fiscales y el 65% de los abogados en el libre ejercicio encuestados mantienen que los recursos y técnicas para la obtención de la prueba y así su posterior preservación para la reproducción de ella en juicio no es del todo cónsona con los mínimos establecidos para crear la certeza o convicción suficiente a los fines de imputar la comisión de un delito de esta naturaleza a un imputado.

8.- Respecto al manejo instrumental de los términos no sólo jurídicos sino técnicos contemplados en la ley la opinión está dividida. Sólo un 50% de los jueces, 25% de los fiscales y el 20% de los abogados en el libre ejercicio manejan las definiciones propias de la ley. Lo cual es preocupante porque si el instrumento legal no es bien operativizado no podrá haber una buena administración de justicia.

9.- Cuando se indaga por el órgano encargado de practicar todas las experticias necesarias para la obtención de la prueba la opinión está también dividida. Tienen la convicción de que el cuerpo de investigaciones científicas, penales y criminalísticas (CICPC) realiza propiamente su trabajo el 10% de los jueces, el 50% de los fiscales y el 35% de los abogados en el libre ejercicio.

10.- El sondeo de opinión, por último, arrojó que de entrevistados mayoritariamente no conocen de otros centros o cuerpos alternos al CICPC para la realización o

prácticas de experticias a los fines de ratificar o contratar las investigaciones practicadas por el ente público de investigaciones. De ello, tanto el 100% de los jueces y fiscales, como el 65% de los abogados en el libre ejercicio de la profesión declaran no conocer otros centros especializados en la práctica de pruebas específicas en la materia.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

De la investigación realizada con la finalidad de estudiar las conductas disvaliosas emergentes del nuevo milenio: Los delitos informáticos y su actividad probatoria según el Código Orgánico Procesal Penal vigente en Venezuela se concluye que:

- La presunción consagrada en el ordenamiento jurídico el cual estipula que la ley es conocida por todos una vez cumplidas todas las formalidades de la Carta Magna para la formación de las leyes, no es suficiente. Máxime cuando son los llamados a aplicarla quienes requieren de una precisa consolidación conceptual. Para una correcta administración de justicia es imperioso conocer a plenitud el texto legal su alcance y limitaciones no sólo desde el punto de vista formal sino material. La judicatura y la fiscalía general deberían preocuparse aún más en la preparación de sus funcionarios cuando se está en presencia de creaciones o actualizaciones legislativas, la preservación del Estado de Derecho requiere de una correcta administración de justicia.

- La simple sanción, promulgación y posterior publicación de textos legislativos que estipulen tipos penales no es suficiente para que se detenga el auge delictivo. Las políticas deben ser integrales y multidisciplinarias, potenciadas para este novedoso medio de comisión de delitos como lo es empleando tecnologías avanzadas que obstaculizan o minimizan la individualización del agente activo. La concepción de que la ley penal detendrá la comisión de delitos es algo superado que tendría que internalizarlo el ente productor de leyes (la Asamblea Nacional) y evitar continuar sancionando leyes que a la postre serán letra muerta.

- La atomización de leyes penales en Venezuela es una constante perniciosa que va en detrimento de la seguridad jurídica. La concepción de recoger en un solo Código Penal todas las leyes de carácter penal dispersas en el ordenamiento jurídico venezolano es el desideratum de los operadores de justicia y sabiendo que está en curso una compilación de esta naturaleza; es, a entender del investigador, una labor que no se verá materializada ni incluso de manera mediata.

- La concentración de la competencia penal en tribunales penales ordinarios es un buen síntoma en la administración de justicia y esa es la tendencia en opinión de todos los operadores de justicia penal entrevistados.
- Esta investigación ha arrojado que los administradores de justicia, los fiscales y abogados en su mayoría desconocen los alcances de la ley y la persecución judicial se obstaculiza: por la ausencia de conocimiento de los términos técnicos y particulares de la ley, la poca profusión del instrumento legal y la poca credibilidad o confianza (más que credibilidad institucional –que aquí no se cuestiona) que le dan al cuerpo de investigaciones penales y criminalísticas encargados de hacer todas las investigaciones periciales a los fines de determinar con exactitud las pruebas respectivas de la comisión del delito y su fijación para luego ser evacuadas en el juicio oral y público que exige el Código Orgánico Procesal Penal.
- La persecución de los delitos informáticos tiene muchos obstáculos y esa es la convicción mayoritaria de los entrevistados. Los recursos mínimos requeridos para la obtención de la prueba no son suficientes y los medios alternativos también son desconocidos. Cuando no se cuenta ni con la preparación suficiente ni con los medios materiales necesarios para determinar indubitablemente al sujeto activo de la comisión de unos de los delitos tipo establecidos en la ley especial como tampoco una correcta manera de fijación de las pruebas necesarias, por lo que se deduce que al final esta ley permanecerá en los anaqueles del acervo legal hasta tanto haya voluntad de potenciarla correctamente o el desbordamiento de este tipo de criminalidad se haga insostenible y la sociedad exija el perfeccionamiento del instrumento legal a los fines de hacerlo efectivo y operativo.

Recomendaciones

El sistema procesal penal venezolano es extremadamente exigente al momento de la reproducción de las pruebas en el juicio respectivo a los fines de mantener integras las garantías constitucionales y procesales en el juicio penal. La veracidad y precisión con la que se deben mover los operadores de justicia exige que se perfeccione el mecanismo de recolección y fijación de los medios probatorios, el cual se evidencia como muy débil; se potencien los recursos materiales y financieros para

que el cuerpo de investigaciones penales y criminalísticos funcione de manera correcta.

Por otro lado, la judicatura y la fiscalía del Ministerio Público deberían, respectivamente, incrementar los cursos de capacitación de todo su personal dando esta preparación académica e intelectual, es un esfuerzo imperioso que no se podrá postergar por mucho tiempo, ello repercutiría negativamente en la administración de justicia pudiendo acarrear consecuencias negativas desastrosas para la sociedad.

Para subsanar la deficiencia académica (evidenciadas en esta investigación) de los abogados en el libre ejercicio los colegios de abogados están en la obligación de gestionar cursos, talleres y cualquier evento de promulgación cognoscitiva que coadyuve a la potencialización de los profesionales del derecho, para que se pueda cumplir con el requisito de asistencia letrada al momento de que el Estado decida llevar adelante una investigación y juicio en la materia aquí referida.

Por último, el Estado debería tomar la decisión de una vez por todas de integrar en un solo cuerpo legal (Código Penal) todas las leyes de carácter penal para reducir así la incertidumbre jurídica que suscita esa atomización de leyes dispersas en distintas leyes penales especiales.

REFERENCIAS BIBLIOGRÁFICAS

ARIAS, Galicia. (1999). **Introducción a la técnica de investigación en ciencias de la administración y del comportamiento**. México.

ABLAN, Edymar. (2002, septiembre 01). **Hackers al ataque**. Caracas. Diario El Universal. Sección Internacional. p. 1/13.

BAZURO, Andrea. (2002). **Italia: Internet, la soberanía y las jurisdicciones nacionales: orientaciones después de la sentencia sobre el affaire Yahoo!Inc (Parte I)**. España. Revista electrónica de Derecho Informático # 42. Disponible en Internet, consultado el 2002, mayo 04. Site Noticias vLex (http://v2.vlex.com/global/redi/detalle_doctrina-redi.asp?articulo=122883)

BINDER, Alberto (1999). **Introducción al Derecho Procesal Penal**. Argentina. Editorial Ad-Hoc. Segunda edición actualizada y ampliada.

BLYDE, Aurora. (2002, julio 17). **Corsarios del siglo XXI**. Caracas. Diario El Universal. P. 5/1.

BORREGO, Carmelo y otros. (1998). Código Orgánico Procesal Penal. Caracas. Serie Jurídica. Editorial McGraw Hill.

CHIAPPE, Giuliana. (2002). **55% del software usado en el país es ilegal**. Caracas. Diario El Universal. Sección TEC+NET 2-3. de fecha 23 de junio de 2002.

COLINA, Aisa. (1997). **Cómo recopilar y procesar la información en la investigación documental**. Maracay. Universidad Experimental Libertador. Ponencia Inédita.

CONSEJ DE EUROPA. (2001) **Convención sobre el Cybercrimen**. Budapest. European Treaty Series Nº 185. Disponible en Internet, consultado el 2002, mayo 04. Site Council of Europe (http://conventions.coe.int/treaty/EN/cadreprincipal.htm)

DEL GIUDICE, Mario. (2000). **La criminalísitica, la lógica y la prueba en el Código Orgánico Procesal Penal**. Caracas. Editorial Vadell Hermanos.

DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS. (2000). **Retos en la persecución de las conductas ilícitas donde se involucra el uso de Internet**. Estados Unidos de América. Site del Departamento de Justicia Americano. Disponible en Internet, consultado el 2002, mayo

23.(http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#CHALLENGES)

DIARIO EL NACIONAL. **PTJ ha recibido más de 1.200 denuncias sobre fraudes electrónicos en el año**. Caracas. Diario El Nacional. Sucesos. Site del Diario El Nacional. Disponible en Internet, consultado el 2002, mayo 23. (http://www.el-nacional.com/L&F/result.asp?file=c%3A%5Cnacional%5Cnacionalfront%5Cl%26f%5Carchive%5C2000%5C08%5C26%5Cpe1s1%2Ehtm&rest=delincuencia+organizada)

DIARIO EL UNIVERSAL (01 de septiembre de 2002). **Internet y los delitos**. Caracas. Diario El Universal. Sección Zona. Cultura Binaria.

ENCICLOPEDIA PRÁCTICA DE LA INFORMÁTICA. (1984). **Delitos Informáticos**. España. Ediciones Nueva Lente + Ingelek. Fascículos coleccionables.

FERNÁNDEZ, Fernando. (2002). **La firma electrónica y los delitos en la red**. Caracas. Inédito. Disponible en Internet, consultado el 2002, abril 04.(http://www.delitos informaticos .com/estafas/firmaelectronica.shtml)

---------- (2002). **Resumen de la Ley de Delitos Informáticos de Venezuela**. Caracas. Foro de Opinión: Los Delitos informáticos en Venezuela. Disponible en Internet, consultado el 2002, septiembre 06.(http://www.analitica.com/cyberanalitica/maquilla/5319791.asp)

GÓMEZ C., E. (1995). **La Responsabilidad del Estado en la Constitución del '91**. Colombia. Biblioteca Jurídica DIKE. Primera Edición.

GÓMEZ, Leopoldo.(2000). **Marco normativo para el desarrollo de pericias informáticas.** Argentina. Inédito. Revista electrónica de Derecho Informático. Número 42. Disponible en Internet, consultado el 2002, mayo 02 (http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=122758)

GUERRERO, Sandra. (2001). **PTJ apresó a individuo que clonaba tarjetas de crédito.** Caracas. Diario El Nacional. Sucesos. Site del Diario El Nacional. Disponible en Internet, consultado el 2002, mayo 23. (http://www.el-nacional.com/L&F/result.asp?file=c%3A%5Cnacional%5Cnacionalfront%5C

l%26f%5Carchive%5C2001%5C09%5C20%5Cpd8s3%2Ehtm&rest=delincuencia+organizada)

GUTIÉRREZ F., María. (1991). **Fraude informático y estafa**. Madrid. Publicaciones de Ministerio de Justicia Español.

LEOTTA, Audry. (1999). **La aplicación y utilidad de la criminalística en la actividad probatoria establecida en el COPP**. Maracay. Trabajo especial de Grado para optar al Título de Abogado. Inédita. Universidad Bicentenaria de Aragua.

LÓPEZ, Pedro y Gómez. (2000). **Investigación criminal y criminalística**. Bogotá. Editorial Temis S.A.

LÖSING, Norbert. (1998). **Estado de Derecho y Proceso Penal**. Barquisimeto. Ponencia presentada en las XXIII Jornadas "J. M. Domínguez Escovar". Tipografía Litografía Horizonte C.A.

MANSON, Marcelo. (s/f). **Legislación sobre delitos informáticos**. México. Disponible en Internet, consultado el 2001, noviembre 15. Site monografias.com (http://www.monografias.com/legislacionsobredelitosinformaticos.htm)

MARCHENA, Manuel. (2001). **Aspectos procesales de Internet**. Madrid. Disponible en Internet, consultado el 2002, mayo 23. Site fiscalía española (http://www.fiscalia.org/doctdocu/doct/interneterritorialidad.pdf)

MARTÍN, Juan. (2001). **Internet y pornografía infantil**. España. Disponible en Internet, consultado el 2002, mayo 23. Site fiscalía española (http://www.fiscalia.org/doctdocu/doct/interponograf.pdf)

MATA, Ricardo. (2001). **Delincuencia Informática y Derecho Penal**. Madrid. Edisofer S.L. Libros Jurídicos.

MENDOZA, Mariela. (2002, julio 18). **En Carabobo se combate el crimen con las uñas**. Valencia. Diario El Carabobeño. P. A-8)

MORRIS, Daniel. (2001). **Tracking a Computer Hacker**. Nebraska-USA. Disponible en Internet, consultado el 2002, julio 17. Site del FBI en Estados Unidos (http://www.cybercrime.gov/usamay2001_2.htm)

ORTS, ENRIQUE. (2001). **Delitos informáticos y delitos comunes cometidos a través de la informática**. España. Tirant lo blanch "colección los delitos" 41.

QUIÑONES, Gregorio. (1989). **Cibernética Penal, el delito computarizado**. Caracas. Gráficas Capitolio C.A.

RENGEL, Aristides. (1994). **Tratado de Derecho Procesal Civil Venezolano (según el nuevo Código de 1987)**. Caracas. Volumen I. Editorial Arte.

REPÚBLICA BOLIVARIANA DE VENEZUELA. (2000). **Reforma Parcial del Código Penal**. Caracas. Gaceta Oficial Nº 5.494 Extraordinario de fecha 20 de octubre de 2000.

REPÚBLICA BOLIVARIANA DE VENEZUELA. (2000). **Constitución de la República Bolivariana de Venezuela**. Caracas. Gaceta Oficial Nº 5.453 Extraordinario de fecha 24 de marzo de 2000.

REPÚBLICA BOLIVARIANA DE VENEZUELA. (2002). **Sentencia que declarada Sin Lugar el recurso interpuesto ante la Corte de Apelaciones del Circuito Judicial Penal del Estado Cojedes.** Caracas. Site de Tribunal Supremo de Justicia. Disponible en Internet, expediente Nº 00-1142, sentencia de fecha 07 de noviembre de 2000. Consultada el 2002, septiembre 18. (http:/www.tsj.gov.ve/Decisiones/spa/Abril/1401-071100-C001142.htm)

REPÚBLICA BOLIVARIANA DE VENEZUELA. (2001). **Decreto con Fuerza de Ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas.** Caracas. Gaceta Oficial Nº 37.148 de fecha 28 de febrero de 2001.

REPÚBLICA BOLIVARIANA DE VENEZUELA. (2001). **Ley especial contra los Delitos Informáticos.** Caracas. Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001.

REPÚBLICA BOLIVARIANA DE VENEZUELA. (2001). **Código Orgánico Procesal Penal.** Caracas. Gaceta Oficial Nº 5.558 Extraordinario de fecha 14 de noviembre de 2001.

REPÚBLICA BOLIVARIANA DE VENEZUELA. (2002). **Ley Aprobatoria de la «Convención de las Naciones Unidas contra la Delincuencia Organizada**

Trasnacional». Caracas. Gaceta Oficial Nº 37.357 de fecha 04 de enero de 2002.

REPÚBLICA BOLIVARIANA DE VENEZUELA. (2002). **Sentencia que anula la decisión emanada del Juzgado Décimo Octavo de Primera Instancia en lo Penal y de Salvaguarda del Patrimonio Público de la Circunscripción Judicial del Área Metropolitana de Caracas y declara que si tienen Jurisdicción los tribunales venezolanos para conocer y decidir del caso de autos.** Caracas. Site de Tribunal Supremo de Justicia. Disponible en Internet, expediente Nº 11.832, sentencia 00663 de fecha 17 de abril de 2001. Consultada el 2002, julio 30. (http:/www.tsj.gov.ve/Decisiones/spa/Abril/00663-170401-11832.htm)

REYES, Alfonso. (2000). **Derecho Penal**. Santa Fe de Bogotá. Editorial Temis. Séptima impresión de la undécima edición.

SABINO, Carlos. (1987). **Metodología de Investigación. Una Introducción teórico-práctica**. Buenos Aires. Editorial El Cid.

SÁEZ, José. (2001). **Delitos Informáticos o cometidos por medios informáticos. El bien jurídico tutelado**. Argentina. Inédito. Revista electrónica de Derecho Informático. Número 45. Disponible en Internet, consultado el 2002, mayo 02.

(http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=146295)

SOLANGE, Grettel. (2001). **Delimitación del Delito Informático: Bien Jurídico Protegido y Análisis de la Legislación vigente"**. Lima. Tesis para obtener el Título de Abogado. Disponible en Internet, consultado el 2002, abril 04. (http://www.delitosinformaticos.com/tesis2.htm)

TABLANTE, Carlos. (2001). **Delitos informáticos – Delincuentes sin rostro: Una propuesta legal para enfrentar las amenazas del ciberespacio**. Caracas. Fundación En cambio. Primera Edición.

TOLEDO, José. (2001). **Criminalística Forense Informática.** Chile. Trabajo de Grado para optar al Título de Ingeniero en Investigación Policial. Inédita

UNIVERSIDAD DE CARABOBO. (1994). **Normas para la elaboración y presentación de trabajo de grado para optar al Título de Especialista**.

Valencia. Aprobado por el Consejo General de Postgrado, en su reunión ordinaria celebrada el día 15-12-94.

UNIVERSIDAD NACIONAL ABIERTA. (1998). **Técnicas de Investigación y Documentación II**. Caracas. Fondo Editorial UNA.

UNIVERSIDAD PEDAGÓGICA EXPERIMENTAL LIBERTADOR. (2001). **Manual de Trabajos de Grado de Especialización y Maestrías y Tesis Doctorales**. Maracay. Impresión FEDUPEL.

ANEXOS

ANEXO Nº 1
LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS

Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001

LA ASAMBLEA NACIONAL
DE LA REPUBLICA BOLIVARIANA DE VENEZUELA
DECRETA

la siguiente,

LEY ESPECIAL CONTRA DELITOS INFORMATICOS

Título I

Disposiciones Generales

Artículo 1. Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo 2. Definiciones. A los efectos de la presente ley y cumpliendo con lo previsto en el artículo 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a. **Tecnología de Información:** rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del “hardware”, “firmware”, “software”, cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

b. **Sistema:** cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un

paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c. **Data:** hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.

d. **Información:** significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e. **Documento:** registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f. **Computador:** dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g. **Hardware:** equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h. **Firmware:** programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

i. **Software:** información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

j. **Programa:** plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

k. **Procesamiento de data o de información:** realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

l. **Seguridad:** Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos

hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

m. **Virus:** programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

n. **Tarjeta inteligente:** rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

o. **Contraseña (password):** secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

p. **Mensaje de datos:** cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3. Extraterritorialidad. Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4. Sanciones. Las sanciones por los delitos previstos en esta ley serán principales y accesorias.

Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley

Artículo 5. Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente

Título II

De los delitos

Capítulo I

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Artículo 6. Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias

Artículo 7. Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Artículo 8. Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9. Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de

seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Artículo 10. Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11. Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12. Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad.

El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Capítulo II

De los Delitos Contra la Propiedad

Artículo 13. Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho

económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14. Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15. Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18. Provisión indebida de bienes o servicios. El que a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado, alterado, provea a quien los presente de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19. Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Capítulo III

De los delitos contra la privacidad de las personas y de las comunicaciones

Artículo 20. Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21. Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22. Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV

De los delitos contra niños, niñas o adolescentes

Artículo 23. Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24. Exhibición pornográfica de niños o adolescentes. El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Capítulo V

De los delitos contra el orden económico

Artículo 25. Apropiación de propiedad intelectual. El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26. Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Título III

Disposiciones comunes

Artículo 27. Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:

1º Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.

2º Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.

Artículo 28. Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Artículo 29. Penas accesorias. Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las accesorias siguientes:

1º El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la presente ley.

2º El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.

3º La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión, arte o industria, o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas o al conocimiento privilegiado de contraseñas

en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente.

4º La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30. Divulgación de la sentencia condenatoria. El Tribunal podrá disponer, además, la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31. Indemnización Civil. En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado.

Para la determinación del monto de la indemnización acordada, el Juez requerirá del auxilio de expertos.

Título IV

Disposiciones Finales

Artículo 32.Vigencia. La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Artículo 33. Derogatoria. Se deroga cualquier disposición que colida con la presente Ley.

Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los seis días del mes de septiembre de dos mil uno. Año 191° de la Independencia y 142° de la Federación.

ANEXO Nº 2

MATRIZ DE ANÁLISIS POR CATEGORÍA

MATRIZ DE ANÁLISIS POR CATEGORÍAS

AUTOR (ES)	ANO	TÍTULO DE LA REFERENCIA	CATEGORÍA	ANÁLISIS CRÍTICO

FUENTE: COLINA (1997)

ANEXO Nº 3
MATRIZ DE ANÁLISIS DE RELEVANCIA DEL CONTENIDO

MATRIZ DE ANÁLISIS DE RELEVANCIA DEL CONTENIDO

CATEGORÍA	INFERENCIAS E INTERPRETACIONES	CONCLUSIONES

FUENTE: COLINA (1997)

ANEXO Nº 4
ACTA LEVANTAMIENTO DE FIJACIÓN Y RESPALDO ARCHIVOS

ACTA DE LEVANTAMIENTO DE FIJACIÓN Y RESPALDO ARCHIVOS

En la ciudad de_____ , a los ____ días del mes de _____ del año _____, quien abajo firma, procede a levantar acta por la custodia y traslado de la Fijación en Sistema de Respaldo Disco Compacto, correspondiente al proceso de Trabajo Informático Forense en _____, bajo la responsabilidad de _____, Cédula de Identidad Nro. _____, conforme al siguiente detalle:

Nro. CD. Lugar de Respaldo Archivo OBSERVACIÓN

1.- _____
2.- _____
3.- _____
4.- _____
5.- _____
6.- _____
7.- _____
8.- _____

TESTIGOS:
Ø _____ _____
Ø _____ _____

FIRMA RESPONSABLE

_____

Nota: Tarjar espacios en blanco/firmas completas/

ANEXO Nº 5

ACTA LEVANTAMIENTO DE ESPECIES

ACTA LEVANTAMIENTO DE ESPECIES

En la ciudad de _____, a los _____ días del mes de _____ del año _____, quien abajo firma, procede a levantar acta por la custodia y traslado de las especies, correspondiente al proceso de Trabajo Informático Forense en _____, bajo la responsabilidad de _____, Cédula de Identidad Nro. _____, conforme al siguiente detalle:

Nro. _____ Orden ESPECIE OBSERVACIÓN

1.- _____

2.- _____

3.- _____

4.- _____

5.- _____

6.- _____

7.- _____

8.- _____

TESTIGOS:

Ø _____ _____

Ø _____ _____

FIRMA RESPONSABLE

_____

ANEXO Nº 6

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

Faudes cometidos mediante manipulación de computadoras.

- Manipulación de los datos de entrada: Este tipo de fraude informático conocido también como sustracción de datos, representa informático más común ya que es fácil de cometer y difícil de descubrir. Este delito conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga funciones normales de procesamiento de datos en la fase de adquisición de los mismo
- La manipulación de programas: Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente conocimientos técnicos concretos de informática. Este delito cinsiste en modificar existentes en el sistema computadoras o en nuevos programas o nuevas método común utilizado por las personas que tienen conocimientos especializados e programación informática es el denominado Caballo de Troya, que consiste en inserir instrucciones de computadora de forma encubierta en un programa informático para realizar una función no autorizada al mismo tiempo que su función normal.
- Manipulación de los datos salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraude base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamientos programas de computadora especializados para codificar información electrónica fal bandas magnéticas de las tarjetas de crédito.
- Fraude efectuado por manipulación informática: Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perce transacciones financieras, se van sacando repetidamente de una cuenta y se transfier.

Falsificaciones informáticas.

- Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documento comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en colores rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulenta fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos pueden crear documentos falsos sin tener que

recurrir a un original, y los documentos producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

- Sabotaje informático: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de com intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que per sabotajes informáticos son:
- Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos a otros programas informáticos. Un virus puede ingresar en un sistema por conduct legítima de soporte lógico que ha quedado infectada, así como utilizando el método Troya.
- Gusanos: Se fabrica de forma análogica 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 que 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 pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gu subsiguientemente se destuirá puede dar instrucciones a un sistema informático de que transfiera continuamente dinero a una cuenta ilícita.
- Bomba lógica o cronológica: Exige conocimientos especializados ya que requiere la programación de la destrucción modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo daño. Su detonación puede programarse para que cause el máximo de daño y para que mucho tiempo después de que se haya marchado el delincuente. La bomba lógica también como instrumento de extorsión y se puede pedir un rescate a cambio de dar lugar en donde se halla la bomba.
- Acceso no autorizado a servicios y sistemas informáticos: Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas (hackers) hasta el sabotaje o espionaje informático.
- Piratas informáticos o hackers: El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones recurriendo a uno de los diversos medios que se mencionan a continuación. El delin aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema de los piratas informáticos se hacen

pasar por usuarios legítimos del sistema; esto suele frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes contraseñas de mantenimiento que están en el propio sistema.

- Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propretarios legítimos jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a penales. El problema ha alcanzado dimenciones transnacionales con el tráfico de esa reproducciones no autorizadas a través de las redes de telecomunicaciones moderna consideramos, que la reproducción no autorizada de programas informáticos no es u *informático* debido a que el bien jurídico a tutelar es la propiedad intelectual.

Otras definiciones complementarias.

HACKER. Persona a la que le gusta explorar, en detalle, un sistema programable y exceder sus posibilidades. Comúnemente se les confunde con los crackers.

CRACKER. Individuo que usa su destreza computacional para irrumpir en redes ilegalmente. Coloquialmente se le llama hacker.

PHREAKER. Persona que irrumpe en redes telefónicas.

CIBERESPACIO. Mundo artificial formado por el despliegue virtual de datos, a través del cual se puede navegar. Se le conoce como World Wide Web (WWW).

CIBERTERRORISMO. Uso ilegal de recursos de computación para intimidar o hacer daño a otros.

INTERNAUTA. Individuo que navega por internet.

WWW. Ciberespacio. Red mundial de comunicación.

INTRUSIÓN. Ingreso desautorizado de una persona en un sistema.

ESPIONAJE. Intrusión en una red u ordenador para recopilar información.

FRAUDE. Robo de números de tarjetas de crédito o de dinero en cuentas.

SNIFFERS. Programa que permite grabar el nombre y clave de una persona que se conecta a una página, pudiendo luego ganar acceso a ella usando su identidad.

DOS. Ataque de servicio denegado. Envío de peticiones múltiples a un servidor, causando su colapso y evitando que los usuarios de Internet tengan acceso a él.

MAIL BOMBA. Envío de muchos mensajes electrónicos a una cuenta de correo, causando su bloqueo.

SPOOFING. Es el acto de "disfrazar" una computadora, para que electrónicamente parezca otra, de modo de ganar acceso a un sistema restringido.

DNS SPOOFING. Ocurre cuando es alterada la dirección de entrada a una página, causando que el usuario sea redireccionado a otra.

CABALLO DE TROYA. Programa que no es lo que parece, pues esconde una función perjudicial.

VIRUS. Programa que puede reproducirse, infectar a otros y transmitirse a otro ordenador al copiar una información afectada.

GUSANOS. Virus que se transmite por sí solo a través de la red.

PHREAKING. Piratería de líneas telefónicas.

ANEXO Nº 7

INSTRUMENTO - CUESTIONARIO

UNIVERSIDAD DE CARABOBO
ÁREA DE ESTUDIOS DE POSTGRADO
FACULTAD DE DERECHO

ESPECIALIZACIÓN EN DERECHO PENAL

Estimado Señor / Señora / Colega,

El siguiente es un instrumento de recolección de datos dirigido a profesionales del derecho (jueces, fiscales y abogados en el libre ejercicio de la abogacía) con el objetivo de probar una hipótesis de trabajo investigativo referente a la Ley especial contra Delitos Informáticos.

No tiene otra utilidad que fines académicos.

Se le solicita, por favor, marque con una equis (X) el ítem que Usted considere oportuno para cada una de las preguntas. Una sola marca para cada pregunta.

Este instrumento es anónimo y sólo le tomará pocos minutos en contestarlo.

Agradeciendo su gentileza u atención.

Atentamente,

Giuseppe Di Fabio Bentivegna

Abogado

INSTRUMENTO

Profesión / Cargo

(__) Juez con Competencia en lo Penal

(__) Fiscal del Ministerio Público

(__) Abogado en el Libre Ejercicio

Preguntas:

1.- ¿Está familiarizado (a) con los tipos penales contemplados en la Ley especial contra Delitos Informáticos?

(__) SI / (__) NO / (__) No contesta

2.- ¿Este instrumento legal (Ley especial contra Delitos Informáticos) será suficiente para prevenir o minimizar el auge delictivo empleando nuevas tecnologías?

(__) SI / (__) NO / (__) No contesta

3.- ¿Considera que es pertinente este nuevo texto legislativo como regulación penal especial colateral al Código Penal Venezolano vigente?

(__) SI / (__) NO / (__) No contesta

4.- Al una materia novedosa este tipo de criminalidad, ¿Opina Usted favorablemente de tramitarlo por otra jurisdicción distinta a la penal ordinaria?

(__) SI / (__) NO / (__) No contesta

5.- ¿Está Usted suficientemente preparado (a), técnica y jurídicamente, para llevar a cabo un proceso judicial penal en esta materia?

(__) SI / (__) NO / (__) No contesta

6.- ¿Cree Usted que habrá dificultad probatoria para demostrar el hecho punible al momento de realizarse el juicio?

(__) SI / (__) NO / (__) No contesta

7.- ¿Existen recursos técnicos suficiente para establecer y reproducir en juicio de manera indubitable la prueba de la comisión del delito?

(__) SI / (__) NO / (__) No contesta

8.- ¿Maneja Usted las definiciones técnico-jurídicas de orden informático empleada en la mencionada Ley especial?

(__) SI / (__) NO / (__) No contesta

9.- ¿Confía en la prueba pericial que efectúa el cuerpo de investigaciones científicas, penales y criminalísticas (CICPC) en la materia informática?

(__) SI / (__) NO / (__) No contesta

10.- ¿Tiene conocimiento de algún centro especializado o perito que puedan realizar verificaciones o corroboraciones a las pruebas obtenidas por el (CPCPC) a los fines de desvirtuarlas o no?

(__) SI / (__) NO / (__) No contesta

Gracias por su colaboración.