



LA TELEMÁTICA Y LOS DELITOS INFORMÁTICOS EN VENEZUELA

Eugenio E. Mendoza Vera
Eugenio E. Urdaneta
Universidad Rafael Belloso Chacín.Venezuela

RESUMEN

La presente investigación se desarrolló con el propósito de analizar los principales factores telemáticos que limitan la persecución y penalización de los delitos Informáticos en Venezuela. La metodología utilizada en la investigación fue de campo, el diseño fue no experimental descriptivo. La población estuvo conformada por especialistas en las áreas Jurídico Informática y Telemática que laboran en Venezuela, la muestra fue seleccionada mediante el criterio de muestra de expertos y estuvo conformada por veinte especialistas. Como técnicas de recolección de datos se utilizaron: la observación documental y dos instrumentos del tipo encuestas cerradas que fueron validadas por expertos en la materia. Los resultados obtenidos en las encuestas fueron analizados mediante los estadísticos descriptivos; distribución de frecuencias y técnica nominal de la pregunta. Los resultados obtenidos permitieron llegar a las siguientes conclusiones: la nueva Ley especial contra los delitos informáticos (LECDI) presenta deficiencias al tipificar los delitos; el carácter abierto de las redes, el continuo avance en el software y hardware; el carácter virtual de la informática; la necesidad de adiestramiento continuo, y la falta de adecuación del régimen probatorio con las características técnicas de estos nuevos delitos, constituyen los principales factores que limitan su persecución y penalización.

Palabras Claves: telemática, delitos informáticos, persecución, penalización

ABSTRACT

The present investigation was developed for the purpose to analyze the main telematics factors that limit the pursuit and penalty of the data processing crimes in Venezuela. The methodology utilized in the investigation was of field, the design was not experimental descriptive. The population was conformed by specialists in the areas of Legal-DATA PROCESSING and telematics that working in Venezuela. The sample was selected by means the criterion of experts sample and was conformed by twenty specialists. The documentary observation and two instruments type



close surveys, validated by experts in the matter, were the techniques of harvesting data used. The results obtained in the surveys were analyzed by means of the descriptive statistics; frequency distributions and nominal technical of the question. The results obtained, permitted to get the following conclusions: the new LECDI presents deficiencies to typify the crimes; the open character of the networks, the continuous advance in the software and hardware; the virtual character of the data processing; the necessary continuous training and the lack of adaptation of the probatory regime with the characteristic techniques of these new crimes, all constitute the main factors that limit its pursuit and penalty.

Key words: telematics, data processing crimes, pursuit, penalty

INTRODUCCIÓN

El crecimiento de la red de redes "Internet", y la progresiva necesidad de las personas naturales y jurídicas de conectarse a ella, como el carácter abierto de estos sistemas de información, y los bajos costos asociados con su utilización, impulsado la aparición de nuevas formas de materialización de negocios jurídicos (virtuales). Por otra parte, la facilidad con la cual puede ser accedida cualquier red, ha hecho posible la aparición de comportamientos antijurídicos, no éticos o no autorizados, relacionados con el procesamiento y la transmisión de datos.

Uno de los problemas más complejos que las nuevas tecnologías plantean al derecho, lo constituye la regulación de aquellos actos antijurídicos que utilizan la tecnología telemática como medio o fin en la comisión de delitos. Factores como la naturaleza técnica de estos delitos, su extraterritorialidad, la necesidad de adiestramiento constante, la falta de convenios y acuerdos internacionales en esta materia, lo complejo y costoso de las herramientas necesarias para perseguirlos, la continua actualización de la tecnología telemática y la falta de cultura de seguridad informática, son elementos a considerar al momento de realizar cualquier análisis sobre esta materia, sobre todo al momento de elaborar leyes que los penalicen.

Enmarcado dentro del planteamiento anterior y dada la necesidad de adecuar tanto el ordenamiento jurídico vigente, como las prácticas judiciales y penales en materia de delitos informáticos con su carácter telemático, que permita una eficaz persecución y penalización de los responsables, surge la inquietud de hacer un estudio minucioso acerca del modo como la naturaleza telemática de estos delitos afecta la eficacia de la norma sustantiva (Ley especial contra los delitos informáticos) al no disponer de una plataforma Jurídica que asimile dichas características.



Dado lo anterior, el presente trabajo se traz  como objetivo general, analizar los factores telem ticos que limitan la persecuci n y penalizaci n de los delitos contemplados en la Ley especial contra los delitos inform ticos (LECDI) en Venezuela; y como objetivos espec ficos: (a) establecer los factores principales que afectan la vulnerabilidad de los sistemas telem ticos en Venezuela, (b) identificar los factores telem ticos que limitan la persecuci n de los delitos inform ticos en Venezuela, (c) determinar los factores telem ticos que limitan la penalizaci n de los delitos inform ticos en Venezuela; y, (d) analizar la Ley especial contra los delitos inform ticos en funci n de la tipicidad como factor que limita su eficacia Jur dica.

M TODOS

Dada la naturaleza del tema de estudio, y los objetivos espec ficos propuestos, con los cuales se pretende describir y especificar caracter sticas y rasgos del fen meno objeto de an lisis, se seleccion  una investigaci n del tipo descriptivo explicada por Hern ndez, Fern ndez, y Baptista (2003,p:117).

El presente trabajo fue organizado desde un punto de vista metodol gico en atenci n a los modelos epistemol gicos-positivistas.

El fundamento esencial de esta corriente filos fica consiste en hacer tangible la realidad que se pretende estudiar, sin que por esta raz n, se experimenten modificaciones en el objeto que se estudia. Lo que es posible, ya que el positivismo sostiene como concepto te rico, que fuera de un individuo no existe una realidad social externa y objetiva de forma preconcebida.

Por otra parte, en lo que respecta al dise o de la investigaci n, se opt  por el no experimental, definido por Hern ndez et al. (2003) como "...la investigaci n que se realiza sin manipular deliberadamente variables." (p.267). Lo que se hace en este tipo de investigaci n es observar el fen meno tal y como se presentan en su contexto natural, para luego analizarlos. En este tipo de estudio no se construye ninguna situaci n, s lo se observan situaciones ya existentes, no provocadas intencionalmente por el investigador.

En lo que respecta a la modalidad de estudio se seleccion  la denominada de campo, la cual seg n Arias (1999), "consiste en la recolecci n de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna". (p. 48). Bajo este esquema de



trabajo se materializaron los objetivos específicos de la investigación, mediante la realización de las actividades que permitieron recolectar los datos requeridos, directamente de la fuente primaria: especialistas en sistemas telemáticos y jurídicos informáticos del estado Zulia.

En el caso concreto de la presente investigación, la población de estudio estuvo constituida por los profesionales en derecho, informática, redes y telemática relacionados con los delitos informáticos y la protección de los sistemas telemáticos contra las intrusiones prohibidas de cualquier tipo, dentro de la jurisdicción del Estado Zulia

Dado los objetivos planteados en la investigación, fue necesario dividir la población en dos grupos en función de su especialización, y en consecuencia, aplicar dos instrumentos encuestas diferentes de conformidad con estos niveles de especialización; todo con el propósito de optimizar la data recolectada. Las dos muestras fueron seleccionadas de la población siguiendo el criterio de Hernández et al. (2003). Según este criterio y dado el alcance la investigación, se utilizaron muestras no probabilística, y el criterio de muestra de expertos, por ser el que mejor se adaptó a los objetivos del estudio.

En la presente investigación se utilizaron dos técnicas para la recolección de datos; la revisión documental y la encuesta en su modalidad cuestionario.

Se elaboraron dos cuestionarios los cuales se denominaron CUS1 y CUS2, y se aplicaron a las muestras MUS1 y MUS2 seleccionadas según los criterios antes señalados.

Para la validación de los instrumentos utilizados en la presente investigación se elaboró un modelo a ser evaluado y se tomó en cuenta el juicio de varios expertos. Las opiniones y recomendaciones aportadas por los estos mostraron que el instrumento media adecuadamente la variable de estudio, y que las preguntas eran pertinentes con los objetivos e indicadores; por lo que coincidieron que era válido para su aplicación ya que cumplía con las exigencias y necesidades de la investigación.

Con el propósito de medir la confiabilidad de los mismos se realizó una prueba piloto, aplicando cada cuestionario a cinco personas con las mismas características señaladas para la población. La técnica seleccionada para medir la confiabilidad fue la del Coeficiente Cronbach. Los valores calculados fueron de 0.93 y 0.90 respectivamente; lo cual indica que ambos instrumentos resultaron confiables en términos científicos.



El procesamiento y el an lisis de los datos obtenidos en el desarrollo de la presente investigaci n se llev  a cabo mediante dos actividades fundamentales; la primera, referida a la tabulaci n de los datos; y la segunda, inherente al tratamiento estad stico al que ser n sometidos los datos arrojados por la investigaci n.

El tratamiento estad stico seleccionado para el an lisis de los resultados obtenidos en presente estudio fue del tipo descriptivo; selecci n que obedeci  a las cualidades que el mismo posee.

El estad stico descriptivo seleccionado se adecu  al tipo de  tem procesado. Para las preguntas dicot micas y de selecci n  nica de entre varias opciones, se calcul  la frecuencia absoluta (Fa) y la frecuencia relativa (Fr). Para  tems con varias alternativas se emple  el tratamiento estad stico t cnica nominal de la pregunta.

RESULTADOS Y DISCUSI N

A continuaci n se presentan los resultados obtenidos en funci n del objetivo espec fico evaluado:

Objetivo espec fico # 1: Establecer los factores principales que afectan la vulnerabilidad de los sistemas Telem ticos en Venezuela.

La dimensi n vulnerabilidad estuvo integrada por los indicadores: car cter abierto de la tecnolog a de redes, avance de la tecnolog a telem tica, extraterritorialidad, capacitaci n t cnica, herramientas de seguridad y pol ticas de seguridad.

Car cter abierto de la tecnolog a de redes

Para 90% de la poblaci n encuestada, las redes se hacen en mayor o menor grado vulnerables a cualquier tipo de ataque por su car cter abierto. El 90% de los encuestados considera que efectivamente la tarea de determinar el responsable por la perpetraci n de alg n ataque se hace m s compleja dado el car cter abierto de las redes de comunicaciones. En opini n de la totalidad de los encuestados el desarrollo actual de la tecnolog a telem tica se debe a su compatibilidad e interoperatividad.

Seg n Cisco Networking Academy Program (2002), el car cter abierto de las redes telem ticas significa el libre uso de la tecnolog a por el gran p blico, lo que facilita el acceso e interconexi n, y la disponibilidad de



informaci n t cnica sobre el modo como operan las redes e incluso como causarles da o.

Luego de analizar los resultados obtenidos se puede afirmar que efectivamente las redes poseen un grado de vulnerabilidad intr nseca asociado con su car cter abierto, y que el mismo, si bien puede ser minimizado, no podr  ser eliminado ya que hacerlo ser a limitar su desarrollo y evoluci n.

Avance de la tecnolog a telem tica

Para el 90% de los encuestados, los fabricantes dan prioridad a la funcionalidad, y no prestan mucha atenci n por la vulnerabilidad. Respecto al impacto que la incorporaci n de facilidades y servicios en los sistemas telem ticos producen sobre la vulnerabilidad, el 50% de los encuestados respondi  afirmativamente, esto es que incrementa la vulnerabilidad de los sistemas. Por  ltimo, el 90% de los encuestados consider  que el desarrollo de las herramientas de seguridad no est a a la par con los avances de la tecnolog a.

Este resultado coincide con lo se alado por Kargieman (2001) quien afirma, que para los fabricantes, cuando se desarrolla una nueva tecnolog a, y se quiere llevar al mercado lo m s importante es su funcionalidad y no su vulnerabilidad.

El avance de la tecnolog a telem tica obedece a factores de diversa  ndole, tales como: econ micos, sociales, pol ticos, militares y cient ficos; los cuales siempre ser n m s importantes para los productores, que los aspectos relativos a la vulnerabilidad, sea que esta se derive de la propia tecnolog a u obedezca a alguna estrategia de dominaci n cient fica, econ mica, pol tica o cultural.

En raz n de la discusi n anterior se puede afirmar que los avances en materia de tecnolog a telem tica, constituyen un factor a considerar al momento de hablar de la vulnerabilidad de cualquier sistema telem tico.

Extraterritorialidad

Para el 70% de los encuestados, la ausencia de fronteras geogr ficas de Internet incrementa la vulnerabilidad de los sistemas telem ticos conectados a la red. Respecto a la identificaci n de los responsables por la comisi n de alg n hecho, el 70% de los encuestados considera la ausencia



de fronteras geogr ficas de la red de redes Internet, como un factor que dificulta la identificaci n de los responsables

Este resultado se relaciona con el hecho que Internet es por naturaleza vulnerable, y su car cter global es uno de los elementos con mayor aporte sobre esa vulnerabilidad. Seg n Scambray, McClure, y Kurtz (2001) seis de las catorce principales vulnerabilidades de seguridad est n directamente relacionadas con Internet.

Seg n Cross (2003), el rastreo de un simple ataque puede requerir la cooperaci n de m ltiples organizaciones y jurisdicciones, la mayor a de las cuales no se ven directamente afectadas por el ataque y pueden tener poco incentivo para invertir tiempo y recursos en el esfuerzo, lo cual dificulta la persecuci n en la red y por supuesto la identificaci n del autor del hecho.

Como se desprende del an lisis anterior y de los resultados de la investigaci n de campo, la extraterritorialidad constituye un factor que viene a incrementar la vulnerabilidad de las redes o sistemas inform ticos conectados a Internet, tanto en Venezuela como en el resto del mundo.

Capacitaci n T cnica

El 70% de los encuestados respondi  no haber recibido adiestramiento t cnico en la utilizaci n de herramientas de seguridad de nueva tecnolog a. La totalidad de los encuestados opin  que el adiestramiento en nuevas tecnolog as y estrategias de seguridad es fundamental para un  ptimo desempe o de los administradores de redes. El 100% de los encuestados consider  la falta de adiestramiento de los administradores de sistemas en materia de seguridad, incide sobre la vulnerabilidad y con ello se reducen los niveles de seguridad de los sistemas que administran.

Los resultados obtenidos podr amos atribuirlos a la falta de cultura de seguridad que existe en Venezuela. Para Kargieman (2001) este es un problema com n en toda Latinoam rica, donde la preocupaci n por la seguridad llega despu s que alg n ataque ha sido perpetrado.

Respecto el tipo de adiestramiento recomendado en opini n de los encuestados, el adiestramiento en los sistemas de prevenci n de intrusos o IPS result  ser la opci n m s importante para la poblaci n encuestada, seguida con una diferencia notable por los sistemas IDS.

El resultado obtenido est  conforme con lo se alado por Grafinkel y Spafford (1999) quienes comentan que es prudente incluir est ndares para la



capacitación inicial y continua de todos los usuarios. Cada consumidor debe tener capacitación básica sobre seguridad y recibir concientización, la cual debe ser actualizada periódicamente.

Como puede verse en el análisis anterior, los resultados de la investigación de campo indican lo importante del adiestramiento en materia telemática, no solo por la rapidez con la cual evoluciona, sino también por la necesidad de contar con personal capacitado que pueda implementar, y mantener una política de seguridad que proteja los sistemas telemáticos.

Igualmente se tiene para el caso venezolano, que los administradores de sistemas y especialistas en redes telemáticas no cuentan con el adiestramiento necesario para realizar su trabajo, lo cual aunado a lo anteriormente expuesto, muestra la capacitación técnica como uno de los factores que vienen a incrementar la vulnerabilidad de los sistemas telemáticos que operan en Venezuela.

Herramientas de Seguridad

El 90% de los encuestados considera que los costos de las herramientas de seguridad son realmente elevados

Lo costoso de las herramientas de seguridad, hacen su utilización un privilegio casi exclusivo de las grandes empresas, especialmente las de seguridad nacional de las grandes potencias.

Se puede afirmar para el caso venezolano, que el costo de las herramientas de seguridad constituye una barrera para la implementación de políticas de seguridad eficaces. Y por ello, constituye un factor que de modo indirecto incrementa la vulnerabilidad de los sistemas telemáticos que operan en Venezuela.

Políticas de seguridad

La totalidad de los encuestados reconocieron la importancia de la implementación de políticas de seguridad para fortalecer la seguridad de cualquier sistema. Igualmente, el 100% de los encuestados opinó, que las auditorías de seguridad son parte fundamental de cualquier política de seguridad.

Respecto a si los empresarios venezolanos se toman o no en serio la implantación de políticas de seguridad, sólo el 10% respondió afirmativamente, apoyando mayoritariamente la tesis que sólo las empresas



grandes como los bancos y los proveedores de servicios de Internet implementan este tipo de medidas.

Los encuestados se pronunciaron en favor de realizar auditorias de seguridad en todo tipo de empresa. Este resultado esta conforme a lo sealado por Gardinkel y Spafford (1999), quienes consideran la realizaci n de este tipo de auditorias como un elemento fundamental para la seguridad de cualquier sistema telem tico

Seg n Garfinkel y Spafford (1999), las pol ticas de seguridad sirven para definir qu  se considera valioso y establecer las medidas de seguridad que se deben implementar para proteger los activos. Ahora bien, dada la doble naturaleza administrativo-t cnica de las pol ticas de seguridad es quiz s el elemento m s importante a considerar cuando se piensa en seguridad inform tica.

Los programas de revisi n de vulnerabilidades y la implementaci n de parches para corregirlas, es parte de una buena pol tica de seguridad. De hecho, cualquier sistema que no cuente con una pol tica de seguridad, aunque sea m nima, no solo expondr  sus vulnerabilidades intr secas, sino que la convertir  en un sistema inseguro y de f cil acceso por parte de los delincuentes inform ticos.

Los resultados obtenidos de la investigaci n de campo, sugieren que uno de los factores que inciden de modo negativo sobre la vulnerabilidad de cualquier sistema es precisamente la ausencia de pol ticas de seguridad, lo cual incluye la realizaci n de auditorias que permitan evaluar las vulnerabilidades y aspectos de seguridad de los sistemas telem ticos.

Objetivo espec fico # 2: Identificar los factores telem ticos que limitan la persecuci n de los delitos inform ticos en Venezuela.

La dimensi n persecuci n estuvo integrada por los indicadores: tipicidad, capacitaci n t cnica del personal responsable de investigar los delitos inform ticos, disponibilidad de herramientas t cnicas, extraterritorialidad de la tecnolog a, convenios y acuerdos internacionales, y tecnolog a.

Tipicidad

La totalidad de los encuestados consider  que los actos antijur dicos telem ticos constituyen una nueva especie de delito. Respecto a la nueva Ley especial contra los delitos inform ticos, el 70% de los encuestados



consideró que efectivamente la nueva ley presenta deficiencias, y la más notable fue el hecho de no contemplar los delitos relativos a la seguridad e integridad de la firma electrónica. Cuando se preguntó si los continuos avances de la tecnología representan algún obstáculo al momento de tipificar los delitos informáticos, el 80% de los encuestados respondió afirmativamente, señalando que su efecto era significativo.

Estos resultados, conjuntamente con la tipicidad como elemento del delito; y el principio legalista por el cual se rige el derecho penal en Venezuela, obligan al legislador venezolano a producir leyes que contemplen los cada vez más complejos y numerosos actos antijurídicos derivados del mal uso de la tecnología. Por otra parte, debido a las deficiencias presentes en la LECDI, se puede afirmar que la tipicidad en el caso venezolano es un factor que viene a limitar la persecución de este tipo de actos antijurídicos.

Capacitación técnica del personal responsable de investigar los delitos informáticos

El 100% de los encuestados consideró el adiestramiento del personal responsable por la investigación y persecución de los delitos, como una pieza fundamental para lograr los objetivos que se persiguen con la nueva ley. El 60% de los encuestados señaló no haber recibido adiestramiento tecnología telemática que le permitiese realizar su trabajo de modo más eficiente.

Por otra parte, el 80% de los encuestados coincidió en indicar, que el ministerio público no cuenta con los peritos necesarios o debidamente capacitados para descubrir los elementos de convicción propios de este tipo de delito y señalaron como la principal razón de ello lo nuevo de los delitos. Respecto a una doble especialización jurídica y telemática, el 70% de los encuestados lo consideró como una buena alternativa para una eficaz y productiva persecución de los delitos.

Los resultados obtenidos indican la importancia del adiestramiento para confrontar este nuevo tipo de delito.

La importancia que tienen el adiestramiento para la realización de cualquier tarea, principalmente en un área de tan alta especialización como la telemática, llevan a afirmar, que la falta de capacitación técnica del personal responsable de investigar los delitos informáticos constituye en Venezuela un factor que viene a limitar la persecución de los delitos informáticos.



Disponibilidad de herramientas técnicas

El 70% de los encuestados opinaron que los organismos de investigaciones penales venezolanas no cuentan con las herramientas tecnológicas necesarias para perseguir este tipo de delitos. Este resultado ratifica lo señalado por López et al. (2001) respecto a la disponibilidad de herramientas adecuadas por parte del investigador forense.

Cuando se consultó sobre las razones, del porqué los órganos de investigaciones no disponen de las herramientas tecnológicas necesarias, la respuesta de mayor impacto fue la afirmación de que los cuerpos de investigación sólo cuentan con herramientas o equipos obsoletos.

De lo anterior, se podría afirmar, que la falta de herramientas técnicas; tanto de hardware como de software por parte del personal responsable de la investigación de este tipo de actos antijurídicos en Venezuela, constituye un factor que viene a limitar la persecución de los delitos informáticos. Ya que se reduce la posibilidad de obtener evidencia confiable que permita establecer responsabilidades.

Extraterritorialidad de la tecnología

El 60% de los encuestados consideró la extraterritorialidad de la tecnología como una barrera al momento de perseguir gran parte de los delitos informáticos. Los encuestados consideraron como la principal razón de este hecho, las limitaciones jurídicas que presenta la persecución en caliente en la red de redes de Internet, dado su carácter global y extraterritorial.

Este resultado está conforme con lo señalado por Ortiz (2001), para quien algunos de los tipos penales muestran cierto grado de inadecuación respecto de las nuevas modalidades delictivas; y por otra parte, es frecuente la presencia del caso internacional ya que las redes telemáticas permiten el flujo de información fuera de las fronteras del Estado, lo cual plantea complejidades que juristas y legisladores tienen que resolver

Esto lleva a aseverar que, la extraterritorialidad de la tecnología constituye una barrera en la persecución de gran parte de los delitos informáticos en la red.



Convenios y Acuerdos internacionales

El 100% de los encuestados indic  no conocer la existencia de tratados o convenios celebrados por Venezuela con otros estados en materia espec fica de delitos inform ticos. Por otro lado, el 70% de los encuestados consider  la falta de acuerdos y tratados internacionales en materia de delitos inform ticos, como una barrera para su persecuci n.

Al consultar el porque de la importancia de los tratados o convenios internacionales, la mayor a de los encuestados se inclin  por la opci n que se ala que un gran n mero de los ataques son remotos, esto es, que se realizan a trav s de Internet, y tiene su origen en otros Estados, lo que hace necesario la implementaci n de este tipo de herramientas jur dicas.

La afirmaci n anterior obedece al hecho que precisamente el elemento extraterritorialidad es el que crea la necesidad de que existan instrumentos internacionales que sumen los esfuerzos de las naciones en la persecuci n de este tipo de delitos que tiene como una de sus caracter sticas principales la ausencia de barreras geogr ficas.

Igualmente, otros autores como Romero (2003), se alan como un elemento primordial para mejorar la persecuci n de estos delitos, hacer convenios internacionales que permitieran a los distintos pa ses establecer cu l es la jurisdicci n aplicable cuando se cometa un delito de este tipo, y por supuesto, la cooperaci n en materia probatoria.

Todo lo anterior viene a avalar la aseveraci n que sostiene que la falta de tratados o convenios internacionales en materia de delitos inform ticos, constituye un factor que viene a limitar la persecuci n y posterior penalizaci n de aquellos delitos que se valgan de la extraterritorialidad de la tecnolog a para su comisi n.

Tecnolog a

El 100% de los encuestados considera, que efectivamente la facilidad con la cual pueden ser eliminados los rastros del delito y su car cter furtivo pueden hacer que la investigaci n resulte insuficiente para acusar, o no pueda atribuirsele al imputado el hecho objeto del proceso. Los mismos, seleccionaron como la principal raz n de ello; la falta de rastros como factor que limita la obtenci n de evidencias del delito cometido, resultando en



archivo fiscal de las actuaciones de conformidad con el art culo No. 315, del C digo org nico procesal penal (COPP).

Luego de analizar los resultados obtenidos con la investigaci n de campo, y considerar la opini n de los expertos citados, se puede afirmar; que la tecnolog a telem tica por su interconectividad, interoperabilidad, disponibilidad de informaci n t cnica y naturaleza abierta, pueden hacer que la investigaci n de algunos tipos de delitos resulte insuficiente para acusar, o no pueda atribuirsele al imputado el hecho objeto del proceso.

Lo se alado anteriormente, ratifica que la tecnolog a, dada sus caracter sticas muy particulares e intr secas, al no ser considerado en conjunto con otros aspectos como la extraterritorialidad, la necesidad de tratados o convenios internacionales, entre otros, constituye un factor que tambi n viene a limitar la persecuci n de los delitos inform ticos.

Objetivo espec fico # 3: Determinar los factores telem ticos que limitan la penalizaci n de los delitos inform ticos en Venezuela.

La dimensi n penalizaci n estuvo integrada por los indicadores: capacitaci n t cnica de jueces, r gimen probatorio, y por  ltimo convenios y acuerdos internacionales.

Capacitaci n t cnica de jueces

El 70% de los encuestados se al  que los jueces penales venezolanos no han recibido la capacitaci n necesaria en tecnolog a telem tica para de esta manera enfrentar esta nueva clase de delito.

Por otra parte, el 70% de los encuestados considera que no es una buena alternativa conformar un grupo de jueces penales con una doble especializaci n jur dica y telem tica, para una eficaz y productiva penalizaci n de los delitos inform ticos. La principal raz n de ello es la dificultad de implementar un equipo con estas caracter sticas, debido a la actual estructura del poder judicial.

Como se coment  con anterioridad, el adiestramiento constituye una necesidad fundamental en ciertas tareas, sobre todo en aquellas que requieren un cierto nivel de especializaci n.

El an lisis de los resultados de la investigaci n de campo llevan a afirmar; que el poder judicial no dispone de jueces capacitados en materia telem tica para enfrentar de modo eficiente este nuevo tipo de delitos, y que



además, la actual estructura del poder judicial no esta adecuada para realizar cambios orientados a la formación de jueces con un manejo apropiado de la materia telemática.

Se concluye de este punto que en el caso venezolano la capacitación de los jueces en materia telemática prácticamente no existe, en razón de lo cual se convierte en un factor que viene a limitar la penalización de este tipo de delitos, sobre todo cuando se toma en consideración que el juez conoce el derecho: y que además debe apreciar las pruebas según la sana crítica observando las reglas de la lógica, los conocimientos científicos y las máximas experiencias.

Régimen probatorio

El 60% de los encuestados considera la falta de adecuación de régimen probatorio venezolano con las características técnicas de los delitos informáticos tipificados en la nueva Ley, como un elemento que dificulta su persecución y penalización. Señalando como principales razones de ello; (a) que son conductas realizadas en tiempos muy cortos, y en algunos casos, en un momento único del tiempo, lo que se hacen prácticamente ineficaces los artículos del 218 al 221 del COPP; y, (b) las limitaciones impuestas por los artículos 197 y 219 del COPP, que hacen casi imposible que la información capturada en caliente por parte del administrador del sistema, ante la comisión de un delito, pueda ser considerada como prueba.

El análisis de la investigación de campo, confirma que el actual régimen probatorio venezolano presenta ciertas deficiencias al tratarse de los delitos informáticos, lo cual dificulta y hace en algunos casos, imposible el trabajo de los cuerpos de investigación policial, de los fiscales del ministerio público, y por supuesto, de los jueces penales.

Ahora bien, el planteamiento anterior conlleva a firmar que el actual régimen probatorio venezolano, constituye un factor que viene a limitar tanto la persecución como la penalización de los delitos informáticos.

Convenios y Acuerdos internacionales.

Para el 90% de los encuestados, la celebración de convenios y acuerdos internacionales en materia de delitos informáticos es una pieza clave en la lucha contra la delincuencia informática, debido a los beneficios que estos proporcionarían en la persecución y penalización de los cada vez más numerosos delitos perpetrados en Internet.



Según Cross (2003), el carácter abierto de la Internet permite que los paquetes de datos circulen con facilidad a través de las fronteras geográficas, administrativas y políticas. La cooperación requerida al momento de perseguir un delincuente informático y de establecer responsabilidades señala la celebración de acuerdo o convenios internacionales como la mejor opción en la lucha contra este tipo de actos antijurídicos.

La celebración de este tipo de instrumentos no sólo se limita a la cooperación y asistencia técnica al momento de producirse una persecución en la red, sino también, a la elaboración de una normativa internacional sustantiva que tipifique como delitos aquellos actos antijurídicos, que a juicio de la comunidad internacional, deban ser tipificados como tal.

Los resultados anteriores permiten afirmar que la falta de tratados o convenios internacionales en materia de delitos informáticos, constituye un factor que viene a limitar tanto la persecución como la penalización de aquellos delitos cometidos con la utilización o contra los propios sistemas telemáticos.

CONCLUSIONES

Luego de analizar y discutir los resultados obtenidos de la investigación de campo y considerando la opinión de los expertos, se pudo llegar a las siguientes conclusiones:

- El carácter abierto de la tecnología de redes, los avances de la tecnología telemática, y su extraterritorialidad constituyen factores que inevitablemente afectan o hacen vulnerable los sistemas telemáticos. Estos efectos pueden ser minimizados mediante la implementación de políticas de seguridad que reduzcan al mínimo las vulnerabilidades propias del sistema que se protege.
- La capacitación técnica, las herramientas y las políticas de seguridad, constituyen factores extrínsecos que afectan la vulnerabilidad de los sistemas telemáticos, y en aquellos casos donde más de uno falla, o son débiles las vulnerabilidades propias del sistema, se harán visibles incrementando la posibilidad de recibir un ataque tanto remoto como local.
- En el caso particular de Venezuela donde no existe una cultura de seguridad telemática, la capacitación técnica, las herramientas y las políticas de seguridad constituyen el elemento más débil de la cadena, lo cual



repercute en un incremento de la vulnerabilidad extrínseca de los sistemas telemáticos.

- El carácter técnico de este tipo de delitos complica significativamente la tarea de tipificarlos, ya que no es posible aplicar el criterio de la analogía tan común en el derecho, esto representa una barrera al momento de perseguir y penalizar estos delitos.
- El personal responsable por la investigación, persecución y penalización de los delitos informáticos no cuenta con la capacitación técnica y con las herramientas de seguridad necesarias para realizar su trabajo de modo eficiente.
- La extraterritorialidad de la tecnología, su constate evolución y la falta de acuerdos o convenios internacionales en materia de delitos informáticos constituyen un factor que vienen a limitar de modo directo la persecución y penalización de estos delitos.
- El actual régimen probatorio venezolano no se adapta a este nuevo tipo de delitos, por ello se convierte en una barrera al momento de aplicar la norma sustantiva vigente limitando de este modo su persecución y penalización.

REFERENCIAS BIBLIOGRÁFICAS

Academia De Networking De Cisco Systems (2002). *Guía del primer año. Cisco Systems, Inc. Cisco Networking Academy Program* (2^{da} ed.). España: Pearson Education.

Arias, Fidias G., (1999). *El proyecto de Investigación. Guía para su elaboración*. Caracas: Episteme.

Chávez, N. (1994). *Introducción a la Metodología Educativa*. Maracaibo, Venezuela: Talleres de Ars Gráfica.

Cross, S. E. (2003). *La vulnerabilidad de la Internet*. <http://usinfo.state.gov/journal/ites/0500/ijes/cert-4.htm> (Diciembre 2003).

Garfinkel, S., Spafford, G. (1999). *Seguridad Práctica en Unix e Internet*. México: Editorial McGraw-Hill.



Grisanti Aveledo, H. (1999). *Lecciones de derecho Penal* (11^{va} ed.). Caracas, Venezuela: Editorial Melvin.

Hernández S., R. B., Fernández C., C., Baptista, P. (2003). *Metodología de la Investigación* (3^{ra} ed.). México: McGraw-Hill.

Kargieman, E. (2001). *Seguridad en Internet: el riesgo siempre existe*.
<http://>

cnnespañol.com/especial/2001/mundo.interactivo/stories/entrevi.../emiliano.Kargieman (Octubre 2003).

López, O., Amaya, H., León, R. (2001). *Informática Forense: Generalidades, aspectos técnicos y herramientas*. Universidad de los Andes. Bogotá, Colombia.

Ortiz Oritiz, R. (2001). *Derecho Fundamental y Garantía de Protección de los Derechos de la Personalidad*. Caracas, Venezuela: Fronesis, S.A.

Scambray, J., McClure, S., Kurtz, G. (2001). *HACKERS 2. Secretos y soluciones para la seguridad de redes*. España: McGraw-Hill.