TELEFONÍA MÓVIL Y DELINCUENCIA

Depósito Legal: pp200203AR289

ISBN: 1690-3064

DIAGRAMACION
Dra. Crisálida Villegas G
PORTADA Y FORMATO ELECTRONICO
M. Sc. Nohelia Alfonzo

Fecha de Publicación: Septiembre, 2016

SERIE DERECHO

Volumen 1, Número 1, Año 2016

San Joaquín de Turmero- Universidad Bicentenaria de Aragua

La Serie Derecho es una publicación correspondiente al Fondo Editorial de la Universidad Bicentenaria de Aragua (FEUBA), dirigida a docentes e investigadores de las distintas disciplinas del saber. Tiene como propósito divulgar los avances de estudios, casos o experiencias de interés para el desarrollo de la investigación y la educación en Derecho, desarrollados por estudiantes y docentes de la universidad y la comunidad interuniversitaria. Es una publicación periódica trimestral arbitrada por el sistema doble ciego, el cual asegura la confidencialidad del proceso, al mantener en reserva la identidad de los árbitros.

ÍNDICE

PRESENTACIÓN

La obra que someto a la consideración de la comunidad académica, puede ser de su interés, debido al incremento de los hechos delictivos realizados por intermedio o con el uso de la telefonía celular. Esto con la intención de reflejar la necesidad imperante de dar a conocer los elementos probatorios que se deben presentarse en los procedimientos penales cuando la denuncia o acusación se basa en delitos cometidos que se encuentran tipificados por el Código Penal mediante la utilización de teléfonos celulares.

Así como las distintas evidencias que se encuentran presentes en los actuales dispositivos de telefonía celular, de ahí que la obra puede ser un aporte a los Órganos de Seguridad Ciudadana del Estado, quienes como auxiliares del Ministerio Público en materia de investigación penal, que deben mantenerse actualizados respecto a los últimos hallazgos cognitivos en materia de evidencia electrónica o digital, a fin de evitar y contrarrestar una serie de trabas y obstáculos jurídicos que se originan en el Sistema Penal Venezolano, por la falta de conocimiento acerca de este tipo de evidencias.

En este sentido, puede servir para llamar la atención a la amenaza creciente y constante que constituye el empleo de la telefonía celular para la perpetración de delitos contra personas y sus propiedades, lo cual les permitirá advertir y prevenir tempranamente aquellas conductas delictuales que les podrían convertir en víctimas.

En tal sentido, espero motivar la reflexión, permitiendo a los interesados en la materia de Derecho Penal y Criminología estar a la vanguardia de los conocimientos en el problema mundial y nacional que remite al uso de la tecnología comunicacional con fines contrarios al bienestar social, que permita alcanzar el desarrollo humano al cual todos aspiramos lograr.

INTRODUCCIÓN

A nivel mundial la telefonía móvil, con la incorporación cada vez más de nuevas y mejores tecnologías, constituye un verdadero avance para la sociedad contemporánea por el empleo de distintos y variados modelos de dispositivos digitales, que más que teléfonos, son verdaderos centros comunicacionales donde se puede verificar, en tiempo real, cualquier acontecimiento que ocurra en casi todas las partes de la tierra y hasta en el universo, en los distintos contextos y ámbitos que repercuten de distintas formas sobre la humanidad en un determinado plano temporal.

Los seres humanos, aplicando la inteligencia y el intelecto, se las han ingeniado para fabricar máquinas capaces de simular el comportamiento y acciones de ellos mismos y con cada siglo que pasa se hacen más sofisticadas ya que lo que siempre se ha aspirado es que sea lo más parecida al cerebro humano, al advertirse que este y el sistema nervioso son conductos para la transmisión de impulsos eléctricos.

Sin embargo, este avance tecnológico concebido en pro del desarrollo de la humanidad, además de integrar a sociedad en redes globales, les ha convertido tal como lo señala Whitaker (1999) en un arma de doble filo, por cuanto aumentan las capacidades de las personas, pero también hacen a sus usuarios más vulnerables a la vigilancia y a la manipulación, debido a la presencia del elemento evolutivo del delito, a la par de los avances tecnológicos que afectan las estructuras de las organizaciones delictivas, conjuntamente con los victimarios y las víctimas.

De allí, van a surgir una serie de teorías situacionales sobre el delito, estrechamente vinculadas a las perspectivas de la escogencia racional de la delincuencia, según la cual, la trasgresión se concibe como conducta instrumental encaminada a satisfacer necesidades del agresor, que no

necesariamente están basadas en el dinero. Esta matriz dio lugar a la formalización de las denominadas teorías de las oportunidades recogidas y sintetizadas por Birkbeck (1984-1985), donde es enfatizado el concepto de oportunidad para el delito.

Evidentemente que la incorporación de estas novedosas tecnologías, adicionándoseles Internet, hace que en muchas ocasiones, los conceptos jurídicos tradicionales de carácter criminológicos resulten desfasados o poco adecuados para su incorporación a los procesos penales de acuerdo con la realidad, lo que concierne un futuro prometedor para algunos e incierto para otros.

Si bien es una realidad, que en la legislación penal venezolana se contemplan la gran mayoría de los delitos que se cometen en la actualidad, también es cierto que los transgresores de la norma jurídica han incorporado nuevas formas de llevarlos a cabo, por lo tanto, es ardua la tarea del Ministerio Público para recaudar, clasificar y presentar las pruebas incriminatorias con la finalidad de aplicar el castigo correspondiente a quien haya infringido la ley.

Sin embargo, a pesar de la incertidumbre se cuenta con la Ley Especial contra los Delitos Informáticos (2001) que regula los realizados por medios electrónicos como complemento especial de las disposiciones penales existentes, todo con la finalidad de instrumentar mecanismos legales indispensables cuyo objetivo sea generar confianza en la sociedad venezolana.

De ahí que el libro recoge los elementos de carácter criminógeno y criminalísticos innovadores, dado las nuevas modalidades delictivas que se van generando conforme a los avances tecnológicos, representados por las evidencias digitales que se encuentran presentes en los dispositivos telefónicos móviles.

Puede ser de apoyo de los interesados en la temática por el alcance de los recursos técnicos de carácter probatorios que deben presentarse cuando deba comprobarse un hecho ilícito realizado en un escenario digital, para lo cual debe contarse con técnicos en experticia informática forense suficientemente especializados que coadyuven a la determinación de la verdad procesal. En tal sentido el libro se presenta estructurado en tres capítulos.

El primero, la Telefonía Móvil que contiene los Celulares como herramienta criminal y el Sistema Financiero como Espacio de Riesgo.

El segundo, Los Avances Tecnológicos en la Legislación del Proceso Penal, el cual presenta El Proceso Penal, Legislación y los Órganos Criminológicos; Principios Procesales en la Tutela Judicial, Delito Informático, Informática Jurídica, Teoría General de la Prueba, Prueba y Documentos Electrónicos.

El tercero, Las Redes Sociales como fuente de Delitos Informáticos, que se refiere al Twitter como puente en el Bloqueo de Comunicación y la Seguridad en la Red.

El cuarto, Algunas Ideas Finales incluye Fundamentación de los Delitos Informáticos, Alcance de las Comunicaciones por Telefonía Móvil, Delitos Informáticos y Algunas Acciones a Realizar,

I. TELEFONIA MOVIL

De Bernardo y Priede (2007:1) establecen que, “Motorola Martin Cooper, es considerado como el padre de la telefonía móvil, ya que fue el primero en desarrollar la tecnología inalámbrica inventando el primer teléfono móvil en el año 1973”. Conforme a lo citado, la telefonía móvil constituye una tecnología que ha sido desarrollada partiendo del empleo de la telefonía fija y constituye en la actualidad una de las revoluciones tecnológicas de mayor difusión a nivel mundial, dado que cualquiera puede tener acceso a un dispositivo para comunicarse con otra persona o grupos de personas.

La tecnología representa desarrollo, cambio y mejoras en las condiciones de vida, es por ello que computadoras, televisores, dispositivos de comunicación y otros artefactos electrónicos han llegado a casi todos los lugares del mundo y forman parte de la vida cotidiana de las personas, sean ricas o pobres.

Pero donde parece más obvia la omnipresencia tecnológica es en la proliferación de los teléfonos celulares, muchos de los cuales no son simples teléfonos, ya que hay modelos avanzados que permiten acceder a Internet, enviar y recibir correos electrónicos, mensajes de texto, ver televisión o videos, realizar operaciones matemáticas complejas, asesoramiento científico en tiempo real, disponer de agenda diaria, escuchar música, tomar fotos, orientarse con el sistema de posicionamiento global (GPS) y de paso, hacer y recibir llamadas.

En este sentido, la Revista ¡Despertad! publicada por Watchtower Bible and Tract Society of New York, Inc. (2009), refiere que, “un teléfono inteligente multimedia tiene hoy más capacidad de procesamiento de la que tenía el Comando de Defensa Aérea Norteamericana en 1965” (p. 3). Asimismo agrega que, “actualmente hay u móvil por cada dos personas”,

mostrando sin duda alguna la rápida proliferación y difusión mundial de un producto tecnológico en la historia de la humanidad.

Además, con el desarrollo de Internet, se ampliaron e incrementaron las áreas comunicacionales, es decir, que esta red no es una empresa o una organización determinada, puesto que se trata de un recurso o medio tecnológico que comparten tanto los proveedores de acceso como los proveedores de aplicaciones específicas, tales como e-mail, diseño de páginas web, contenidos, e-commerce, lo que permite que millones de personas de los más variados lugares del mundo se puedan comunicar interactivamente por intermedio de un computador, teléfono celular u otro medio electrónico, con fines laborales, educativos, entretenimiento, de investigación, familiares o criminales.

En este sentido, la globalización de Internet ha cambiado el Derecho Internacional Privado y Público tradicionales, así como los procedimientos procesales, ya que al tratarse de una red telemática pública y abierta, no respeta límites geográficos, no reconoce fronteras o jurisdicción estatal alguna, pues las transmisiones obedecen a respuestas rápidas ante peticiones espontáneas que los usuarios pueden realizar por medio de un computador o teléfono celular.

Esto puede realizarse en cualquier parte del mundo, sin que interese en qué lugar está físicamente instalado el servidor que le provee de información. Esto por cuanto la información está almacenada en millones de otros equipos electrónicos sin presencia de una organización o control alguno. Es por ello que, en fecha 10 de febrero de 2001, el Ejecutivo Nacional promulga la Ley de Mensajes de Datos y Firmas Electrónicas, en cuya exposición de motivos se indica:

> La presentación de un instrumento legal que regule estos mecanismos de intercambio de información, los haga jurídicamente trascendentes a la administración de justicia, y

> les permita apreciar y valorar estas formas de intercambio y soporte de información, con el objeto de garantizar el cumplimiento de las obligaciones asumidas mediante dichos mecanismos y constituirse en un aporte necesario e indispensable que permita construir la base jurídica para el desarrollo de estas tecnologías.

Pudiendo agregarse a este postulado que es una realidad física y virtual que este mundo globalizado y globalizante nos contiene y envuelve sin límites y es que por medio de Internet pueden transmitirse documentos, imágenes, datos o sonidos de diversa naturaleza o contenido, sean lícitos o ilícitos, morales o inmorales, permitidos o prohibidos, debido a que existe una garantía de libre circulación de la información pues no hay censura ni limitación alguna a la libertad de expresión de los usuarios o usuarias.

En efecto, independientemente de que la mayoría de los países han legislado sobre el intercambio de información por medios electrónicos, interponiéndose prácticamente una regulación supraestatal del ciberespacio, también es cierto que no existe suficiente control jurisdiccional sobre estas actividades, por cuanto la red es el espacio de ejecución de las operaciones que se suele llamar cibercriminalidad.

Los Celulares Herramienta Criminal

Es innegable la influencia positiva y negativa que han tenido y tienen los celulares en la sociedad actual, por cuanto así como puede ser un medio efectivo de desarrollo, además de ayudar al crecimiento económico y social de la mayoría, también se pueden transitar zonas delictuales o convertirse en herramienta criminal altamente sofisticada, con la cual no sólo determinadas personas denominadas hacker o piratas informáticos se entrometen en el funcionamiento de otras computadoras accediendo a la información ajena violando no sólo la privacidad de las personas

naturales y de instituciones públicas, sino también para amenazar y señalar secuestros, entre otros delitos.

Sin embargo, existe un grupo especial mucho más peligroso constituido por los hackers internos, es decir, empleados, contratistas o consultores de las mismas empresas, entes y corporaciones, pero sobre todo de entidades bancarias y sistemas financieros, ya que tienen el acceso y conocimiento de los códigos de seguridad lo cual les permite causar el mayor daño con menos esfuerzo que el invasor externo, hecho que la mayoría de las veces se trata de ocultar, sobre todo por los bancos, por temor a las consecuencias de pérdida de credibilidad con sus clientes y usuarios, además de evitar el estímulo de otros hackers para que actúen en contra de esa institución.

El arsenal de armas creadas por los hackers y crackers es tan extensa y variada que es difícil encontrar una clasificación comúnmente aceptada, por cuanto amparados por el anonimato y las complejas técnicas de la programación y un conocimiento especializado, pueden alterar sistemas y procesos de datos frente a los ojos de las víctimas sin que apenas lo puedan notar, tales como robos de las claves o contraseñas de seguridad, alterar los códigos originales de los programas de sus víctimas para manipularlos posteriormente, colocar bombas digitales que se programan para estallar en un determinado momento, alteración de los programas mediante saturación de información con basura electrónica y simulación de identidades, entre otros.

Sobre esta problemática, señala Brizzio (1999), que los expertos del Grupo Diebold, una de las mayores organizaciones mundiales en lo que respecta al asesoramiento en informática, opinan que “el terrorismo en informática constituye el mayor riesgo de este siglo”, sin que puedan emplearse normas jurídicas de Derecho Internacional debido a la ausencia de sanciones aplicadas por un poder centralizado.

Debe señalarse igualmente los accidentes de tránsito ocasionados por el mal uso de los celulares, por ejemplo, los reflejos de conductores y conductoras que conducen hablando por teléfono, aunque usen *manos libres*, quedan mermados como si estuvieran en estado de ebriedad. Igualmente, enviar mensajes de texto o ver videos mientras se conduce, también puede ocasionar accidentes mortales, esto ha dado como consecuencia que las autoridades de tránsito y las compañías de seguros pueden averiguar, mediante experticia, si se estaba utilizando algunos de estos equipos al momento de un accidente.

1.2. El Sistema Financiero como Espacio de Riesgo

Hay que destacar los fraudes electrónicos en el sector bancario a través de internet, ya que Venezuela constituye, a pesar de la legislación al respecto, uno de los paraísos para la comisión de todo tipo de delitos informáticos, por cuanto la debilidad institucional de la División contra la Delincuencia Organizada de la Policía Científica, de la Fiscalía General de la República y del Sistema Judicial con los tribunales penales, además de la falta de un adecuado control de las instituciones bancarias, incluyendo la propia Superintendencia de Bancos y otras instituciones financieras; sumado a esto una escasa cultura teleinformática, es lo que permite que el sistema financiero nacional sufra de ataques delictivos perpetrados mediante el uso y la manipulación de medios electrónicos.

Hay que reconocer que uno de los problemas más importante que tiene en estos momentos la sociedad mundial es indudablemente la confiabilidad que tiene en los medios electrónicos, ya que debido a la finalidad de comunicarse, mantener relaciones laborales, comerciales o realizar transacciones bancarias, entre otras actividades, debe ingresar muchos de los datos particulares, los cuales quedan registrados en diversos archivos, aparentemente *confidenciales*, o por lo menos así es

como se cree como precepto de la inviolabilidad de esos datos personales.

Igualmente en el sistema de los bancos se deben ingresar mucho de los datos personales que servirán de garantía en la seguridad para este tipo de entidades financieras, ya que son éstas donde los cuentahabientes depositan y movilizan su dinero, incluso cuando es adquirido algún bien o servicio el cual se ha cancelado con una tarjeta de crédito o débito, lo cierto es que a todos esos datos personales puede accesar cualquier persona con el software adecuado y sólo hacer clic en un comando de un teléfono celular que esté conectado a Internet, lo que evidencia la vulnerabilidad que entraña que esta base de datos sea mal utilizada o en perjuicio de terceras personas.

En la actualidad, a medida que se van realizando cambios económicos y se incrementa el comercio virtual y el outsourcing, termino en inglés que significa externalización de un proceso o tercerización. Igualmente y con la finalidad de brindarle toda la comodidad posible a los clientes y clientas, en el sector bancario van surgiendo y se van incrementando nuevas tecnologías las cuales han conformado una red especial, que permite a este tipo de instituciones interactuar en tiempo real mediante el intercambio electrónico de información en cualquier parte del mundo. Los certificados de clave pública y las firmas electrónicas cumplen igualmente una función de autorización de usuarios y usuarias para accesar a los servicios bancarios.

También se ha generalizado el uso del manejo de las cuentas bancarias vía telefónica o telebanco, que permite al o la titular de la cuenta, disponer de los fondos existentes en esta con el sólo empleo del correspondiente pin, cuyas siglas en inglés significan (Personal Identification Numbers*)*, además de transferir dinero a otras cuentas, cancelar diversos gastos, pagar las tarjetas de crédito y además se

pueden exigir movimientos y saldos, tanto de las cuentas como de las tarjetas.

Ahora bien, además del beneficio que obtienen los usuarios y usuarias de las instituciones bancarias o financieras, la red sirve de plataforma para una conformación de malhechores tecnológicamente especializados en el manejo del procesamiento de datos que pueden accesar, mediante el equipamiento de software y mecanismos de intercambio electrónicos de información, para realizar y ejecutar operaciones fraudulentas en las cuentas bancarias de personas naturales, jurídicas y/o entes oficiales.

Es decir, que con el avance de la tecnología, también el sector bancario trata de satisfacer los requerimientos del público consumidor mediante los puntos de ventas automatizados, en los cuales el usuario realiza una compra y paga el precio entregando su tarjeta magnética a la persona que vende, quién mediante la máquina, ordena se debite la suma correspondiente a pagar de la cuenta bancaria del comprador, todo a través de la banca en línea (on line o e-banking) por intermedio de un portal de Internet, que permite conectarse con la red de cualquiera de las entidades bancarias y ejecutar, no importa en donde se encuentre, cualquier operación con respecto a sus cuentas.

En esta operación, el usuario introduce su tarjeta de crédito o débito en una máquina que ejecuta el algoritmo secreto contenido en el chip o banda magnética de ésta para determinar cuál es su contraseña, es decir, la clave personal de identificación PIN o password, consiste en una secuencia de letras, números y otros símbolos con finalidad de identificación, si coinciden, se autoriza la operación y la máquina le entrega un recibo para archivar y verificar posteriormente la operación y se le devuelve la tarjeta.

Sin embargo, los infractores informáticos por intermedio de poderosas tecnologías digitales cambian totalmente los mecanismos delictivos tradicionales con nuevos modus operandi pero extremadamente sencillos. Es decir, mediante el uso de lectoras ópticas portátiles que funcionan como escáner de escritorio, donde estos pueden captar imágenes o textos y convertirlas en información digital, las cuales se encuentran instaladas en comercios legales.

Seguidamente, se logra mediante subterfugios capturar la información grabada en la banda magnética de la tarjeta al momento en que el cliente la entrega para realizar el pago, siendo un mecanismo tan simple y rápido que opera incluso delante de las víctimas, quienes ignoran que mientras se solicita la validez de su tarjeta al mismo tiempo es sometida a un proceso de clonación, cuya información será transmitida a una tarjeta virgen que será manipulada por los trasgresores.

Es importante señalar que además a través de la web es muy fácil obtener información personal o económica que puede ser utilizada con muchos y variados propósitos por piratas informáticos, como ocurrió en Bogotá según el Diario El Siglo (2010 : A-7):

> Una banda de piratas informáticos que defraudaba cuentas bancarias en Colombia, Argentina y España fue desmantelada ayer jueves por la Policía Metropolitana de Bogotá, que detuvo a seis de sus integrantes. Los piratas informáticos fueron detenidos en un allanamiento a una residencia de Bogotá donde fueron descubiertos mientras estaban conectados a la base de datos del Banco de Santander de Colombia y a una casa de cambios, informó la policía en un comunicado. Los computadores ejecutaban programas con los cuales se conectaban a varios servidores de España, Argentina y Colombia. Entre los detenidos figura un empleado del Citybank de Colombia, quien se desempeñaba como analista de bolsa y tenía acceso ilimitado a productos de clientes de alta capacidad económica, según la policía. Los hackers afrontarán cargos por el delito de acceso abusivo a sistemas de información. Se

> estima que la banda logró defraudar más de dos millones de dólares en seis meses.

En este sentido estos denominados cyberdelincuentes, la mayor de la veces con complicidad interna dentro de las instituciones bancarias u otros entes oficiales que manejan este tipo de información confidencial o mediante software especial y avanzados conocimientos sobre el sistema bancario, indagan sobre los montos disponibles de los cuentahabientes para defraudar mediante la transferencia de fondos a cuentas fantasmas conformando una victimización múltiple. Rincón, citado por Gabaldón y Becerra (2008) señala:

> … cuatro tipos de riesgos que corren las entidades bancarias que ofrecen servicios electrónicos: operacionales, reputacional, legal y transaccional. El riesgo operacional recae sobre la seguridad y confidencialidad de la información, por deficiencias significativas en la integridad del sistema, quedando expuestos, tanto el banco como su clientela, a accesos no autorizados. Este tipo de riesgo puede presentarse por deficiencias en el sistema de seguridad, falta de políticas de gestión de riesgo, falta o insuficiencia de tecnología, falla en los servicios del proveedor o falta de precaución por parte del cliente, asociándose a la introducción de virus, robo de datos, fraudes y otros ataques.

Asimismo, Fernández y otros también citados por Gabaldón y Becerra (2008), indican que:

> El riesgo operacional es uno de los más difíciles de manejar, debido a que los mismos avances tecnológicos crean diversas posibilidades de ataque a los sistemas informáticos de las entidades bancarias y, por lo tanto, a las cuentas de sus clientes. Rápidamente se hacen obsoletos los sistemas de seguridad más sofisticados que puedan haberse implementados y los ataques más frecuentes son realizados por piratas informáticos o por los mismos empleados del banco. Las personas, singulares o en organizaciones delictivas, efectúan la denominada pesca electrónica (phishing*)*, emplean troyanos o simulan portales (pharming*)*, que son las principales formas de obtención de información sensible a través de la red.

> El común denominador es la captura del nombre de usuario y la contraseña, lo cual permite el acceso a los sitios web de la entidad financiera o a puntos de comercio electrónico.

Es decir, que este tipo de personas que se dedican a los fraudes electrónicos evolucionan con tal celeridad que a los departamentos de seguridad de las entidades bancarias les es casi imposible descubrirlos y mucho menos castigarlos mediante la aplicación de una ley penal, por cuanto no pueden ser localizados y cometen estos delitos de manera invisibles.

De igual manera, en correlación al hurto y robo de dispositivos móviles de comunicación, dentro del acontecer diario, los venezolanos se informan y hacen eco de los distintos hechos delictivos sucedidos en distintas partes del país, que precisamente a través del uso de las redes sociales dispuestas en los dispositivos precitados o los distintos medios de comunicación social que registran e informan los actos perpetrados desde distintas modalidades donde ocurre:

El robo de teléfonos móviles bajo amenaza con el empleo de armas de fuego o armas blancas.

El hurto de teléfonos móviles.

Los homicidios perpetrados con el uso de armas de fuego para ejecutar el robo de teléfonos móviles acompañados de una elevada violencia.

Las extorsiones mediante la comunicación por teléfonos móviles bajo amenazas de muerte a las personas que son víctimas de tales acciones.

Los secuestros ficticios o virtuales.

Asimismo las pruebas en memorias de equipos electrónicos comunicacionales en el campo del Derecho, el concepto de acto jurídico se viene identificando con la manifestación de voluntad de la persona

destinada a producir un determinado efecto sobre el mismo. Caso contrario ocurre con los hechos jurídicos, que si bien producen efectos en este mismo ámbito, son independientes de la voluntad de los sujetos obligados por el hecho en cuestión y es que los actos jurídicos por lo general se expresan a través de un soporte o medio documental que refleja esa manifestación de voluntad y que debe ser firmado por los declarante, tradicionalmente con su firma autógrafa, en señal de conformidad de lo allí expresado.

Ahora bien, los actos jurídicos formulados por un medio electrónico o digital, sigue siendo una manifestación de voluntad de quien emana, pero con la salvedad que viene instrumentada a través de un material distinto al papel u otro soporte físico, la mayor de las veces intangible, donde sin embargo, el signatario expresa su conformidad de manera diferente a la forma tradicional o sea mediante la sustitución de su firma manuscrita por una firma electrónica o cualquier otro medio alternativo de autenticación.

II. LOS AVANCES TECNOLÓGICOS EN LA LEGISLACIÓN DEL PROCESO PENAL

Esta nueva forma de aplicación del Derecho no se puede considerar inmersa de manera exclusiva dentro del sistema de un determinado país, como lo especifica Chacín Fuenmayor (2000):

> Los avances tecnológicos se han extendido en todas las esferas de la sociedad, siendo las relaciones jurídicas unos de los ámbitos de mayor desarrollo, el cual se ha puesto de manifiesto a través de las transformaciones jurídicas consecuencias de las prácticas informático-jurídicas que han dado lugar a la formación del Derecho Informático y a la gran diversidad de actividades del jurista para el conocimiento, creación y aplicación del Derecho, impactadas fuertemente por la transversalidad de los usos computacionales en el desenvolvimiento del Derecho.

Es que sin duda, para conocer de estas nuevas situaciones, la Ciencia del Derecho debió adaptarse a esta revolución tecnológica producida en todo el planeta, por cuanto en las normas jurídicas establecidas, sobre todo en el contexto del derecho escrito o codificado, no se encontraban instituidas en ninguna ley y ante esta ausencia, la nueva delincuencia hacía estragos, ya que los trasgresores siempre van a la vanguardia de las legislaciones, como muy bien lo comenta Durkheim citado por Luciani (2001) cuando establece que, “La Criminalidad evoluciona y se transforma en la misma medida que la sociedad” (p. 506).

No obstante, desde un enfoque penal y criminológico se ha generado un fenómeno ante el cual Mercado (2011), plantea que las, nuevas formas de delinquir; también están adaptadas a los nuevos avances de las comunicaciones, trasgrediendo todo ordenamiento jurídico vigente en el país. Lo cual es consistente en la apropiación y empleo anómalo de la telefonía móvil, por parte del flagelo permanente que representa *la* delincuencia organizada. La Ley Orgánica contra la

Delincuencia Organizada y Financiamiento al Terrorismo(2012) en su artículo 4, numeral 9 la definida como, “la acción u omisión de tres o más personas asociadas por cierto tiempo con la intención de cometer delitos… y obtener directa o indirectamente, un beneficio económico o de cualquier índole para sí o para terceros” .

Consecuentemente, la delincuencia organizada ha realizado diversos actos delictivos que tergiversan el espíritu de avance y desarrollo que traen consigo las comunicaciones. Ante este fenómeno, Mercado (), establece que la delincuencia organizada opera con capital financiero y medios tecnológicos, electrónicos, digital, informático o de cualquier otro medio científico utilizado para aumentar o potenciar la capacidad o acción delictiva y actuar como una organización criminal para lograr mayor acción y mayor ingresos financieros.

Es así, como mediante las modalidades citadas que las personas han sido víctimas de diversos actos delictivos perpetrados por la delincuencia organizada, vislumbrada como una seria amenaza a la Seguridad Ciudadana definida por la Ley de Coordinación de Seguridad Ciudadana (2001) en su artículo 1 como “el estado de sosiego, certidumbre y confianza que debe proporcionarse a la población, residente o de tránsito, mediante acciones dirigidas a proteger su integridad física y propiedades”.

Por consiguiente, es una realidad social venezolana que los delitos de robo, hurto, homicidio, extorsión y secuestro, gravitan en el empleo de la telefonía móvil, igualmente conocida como telefonía celular, la cual en la actualidad es digitalizada, de esta manera se hace aplicable la validez de la evidencia digital que se encuentran en los dispositivos telefónicos móviles.

Proceso Penal. Legislación y Órganos Criminológicos

El Proceso Penal es un conjunto de actos tendientes a la investigación y esclarecimiento de hechos punibles, con el fin de determinar la responsabilidad penal de las personas involucradas en tales delitos y establecer su culpabilidad o inocencia. En Venezuela, el proceso penal se rige por un sistema acusatorio en donde el Estado, por el carácter social que reviste la realización de un hecho punible, es quien mediante sus órganos, tiene la facultad de perseguir y procurar la consecución de este proceso.

Asimismo el Proceso Penal Venezolano está constituido por varias fases, las cuales, tienen su fundamento en el Procedimiento Ordinario previsto en el Código Orgánico Procesal Penal, teniendo como finalidad, el establecer la verdad de los hechos por las vías jurídicas y la justicia en la aplicación del derecho con la debida observancia de sus principios.

Una vez interpuesta la denuncia, recibida la querella por la realización de un hecho punible o de oficio, procederá el representante del Ministerio Público, siendo titular de la acción penal, a ordenar el inicio de la investigación, disponiendo de la práctica de todas las diligencias necesarias y tendientes a determinar las circunstancias que puedan influir: (a)En la calificación del hecho, (b) En la responsabilidad de sus autores y (c) En el aseguramiento de las evidencias relacionadas con su perpetración.

Entonces, previa denuncia, querella, o apertura de oficio por parte de la Fiscalía del Ministerio Público, es como procede la investigación realizada y coordinada con los órganos de policía de investigación penal (CICPC), constituyendo ello la primera fase del proceso penal o fase de investigación o Fase Preparatoria prevista en el Código Orgánico Procesal Penal.

Recabados los elementos de convicción que sirven de base para un juicio de carácter penal, el Fiscal del Ministerio Público presenta acusación penal contra el investigado por ante el Tribunal de Control, adquiriendo el investigado la calidad de imputado, teniendo su desarrollo por Audiencia Preliminar, discutiéndose en esta: (a)Los elementos probatorios a ser recibidos y (b) La calidad del hecho delictivo determinándose si procede o no el enjuiciamiento o Fase Intermedia.

En este estado, el principio de publicidad no toma de manera plena su espacio, puesto que en esta audiencia, sólo su conocimiento es reservada a las partes involucradas en el proceso. En caso de que el Juez constate la existencia de un hecho punible y por lo tanto su enjuiciamiento, procederá a dictar Auto de Apertura a Juicio, adquiriendo el imputado la calidad de acusado (Art. 124, COPP).

Se inicia así, la etapa del juicio oral y público que, como lo indica su nombre, prevalece en esta la oralidad, la publicidad, juntos con los principios de inmediación, contradicción y concentración como principios rectores, y desarrollado por medio de los Tribunales de Juicio bien sean éstos unipersonales o mixtos de acuerdo a la gravedad del delito, constituyendo ésta la fase de juicio, que es de carácter oral y público, y que en vista de su accesibilidad es posible conocer de esta fase en forma directa, presencial, física y material.

Más sin embargo, el proceso no se finaliza allí, puesto que luego de dictada la sentencia, se procede a la ejecución de la misma: fase de ejecución que como su nombre lo indica corresponde al Tribunal de Ejecución.

En cuanto a Leyes que regulan este proceso en el país evidentemente la principal es la Constitución de la República Bolivariana de Venezuela (1999) denominada igualmente Carta Magna, representa la

norma suprema en el Estado de Derecho, dada su organización y aceptación para su seguimiento y cumplimiento por contener los deberes y derechos de todas las personas que se encuentran en el país.

En su artículo 49, establece que toda persona posee el derecho a su notificación sobre los cargos por los cuales se le investiga, de acceder a las distintas pruebas y disponer del tiempo y medios adecuados para realizar su defensa. En este sentido, el Estado Venezolano debe intervenir para brindarles protección a todas las personas ante situaciones que revistan riesgo o amenaza (CRBV, art. 55).

El segundo instrumento legal es el Código Orgánico Procesal Penal (2001), el cual permite fundamentar el Derecho Procesal Penal en Venezuela, para ello establece principios y garantías procesales, para que ninguna persona sea condenada sin un juicio previo, oral y público, realizado, sin dilaciones indebidas, ante un juez o tribunal imparcial, conforme a las disposiciones de este Código y con salvaguarda de todos los derechos y garantías del debido proceso.

Los medios probatorios deberán ser apreciados por el tribunal según su libre convicción, observando las reglas de la lógica, los conocimientos científicos y la máxima experiencia, descantándose la apreciación arbitraria, pues, el tribunal deberá hacer un juicio libre, pero razonado, estimando lógicamente cada una de las pruebas practicadas.

El artículo 197, prohíbe el empleo de la información obtenida mediante tortura, maltrato, coacción, amenaza, engaño, indebida intromisión en la intimidad del domicilio, en la correspondencia, las comunicaciones, los papeles y los archivos privados, ni la obtenida por otro medio que menoscabe la voluntad o viole los derechos fundamentales de las personas.

Mientras que el artículo 198, 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. Los tribunales podrán limitar los medios de prueba ofrecidos para demostrar un hecho o una circunstancia, cuando haya quedado suficientemente comprobado con las pruebas ya practicadas. El tribunal puede prescindir de la prueba cuando ésta sea ofrecida para acreditar un hecho notorio.

Otro instrumento legal es la Ley Especial Contra Delitos Informáticos (2001) que tiene como objeto la protección de los sistemas y tecnologías de información (Art. 1). Además de prescribir la prevención y sanción de los delitos cometidos contra: los sistemas que utilizan tecnologías de la información, la propiedad, la privacidad de las personas y las comunicaciones; niños, niñas y adolescentes y el orden interno.

Igualmente, la Providencia Administrativa. Normas Relativas al Requerimiento de Información en el Servicio de Telefonía Móvil (2005) permite normar los aspectos inherentes a la prestación del servicio de telefonía móvil en el país, especialmente en lo referente, “al suministro de información por parte de los operadores del servicio de telefonía móvil a los órganos de seguridad del Estado, con ocasión de una investigación penal” (Art. 1).

En este sentido, el artículo 9 establece el deber que tienen las operadoras de servicio de telefonía móvil que operan en el país de suministrar la información que les sea solicitada por los órganos de seguridad del Estado Venezolano facultados para llevar a cabo la, “instrucción, la información que éstos soliciten, de forma expedita y sin dilaciones, a los fines de contribuir con las investigaciones que se lleven a cabo en el ámbito de sus funciones de conformidad con la ley”.

Por su parte, entre los órganos del ámbito criminalístico se tiene al Cuerpo de Investigaciones Científicas Penales y Criminalística (CICPC) y el Servicio Bolivariano de Inteligencia (SEBIN), por contar con los recursos humanos y tecnológicos que permiten la aplicación de experticias a los dispositivos de telefonía móvil que son empleados por la delincuencia organizada para la perpetración de hechos delictivos mediante el empleo de tal avance tecnológico. Igualmente el Ministerio Público, cuenta con un Departamento de Informática Forense, encargado de analizar específicamente los dispositivos de telefonía móvil en los cuales pueden ser encontradas ciertas evidencias digitales de interés criminalístico.

Principios Procesales en la Tutela Judicial

Sobre este particular, el proceso penal venezolano establece los principios procesales fundamentales para hacer efectiva la aplicación de la tutela judicial efectiva en la práctica de la obtención de las pruebas, bien sea mediante la relación de llamadas telefónicas emitidas por unas de las empresas que funcionan en el país, o la información colectada por alguna experticia técnica al equipo telefónico.

Al respecto deben respetarse los convenios, tratados y acuerdos internacionales suscritos por el país que son plasmados en la Constitución de la República Bolivariana de Venezuela, principalmente y de forma específica en el Código Orgánico Procesal Penal (2012), que establece el Régimen Probatorio los artículos aplicables a las particularidades de la telefonía móvil.

En otras palabras, es necesario señalar que la difusión de la tecnología informática por intermedio de teléfonos celulares o cualquier otro medio electrónico, ya no se da sólo en los países industrializados, también llamados desarrollados, sino que esta novedad se realiza

también en los que están en vía de desarrollo y en los cuales juega un papel preponderante como uno de los elementos más importantes en sus luchas para lograr el tan ansiado control del flagelo criminal. En este sentido, la Ley Especial Contra los Delitos Informáticos (2001) en su Título I. Artículo 1º señala que "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.

En este sentido, la aplicación de esta tecnología contribuye a generar cambios radicales en las relaciones sociales, comerciales y jurídicas en todo el mundo, por cuanto su impacto transforma los paradigmas conductuales que regían a la humanidad, ya que modifica la creación y aplicabilidad, no sólo de la Ciencia del Derecho al concebirse un nuevo ordenamiento con características propias, cuyas implicaciones deben ser resueltas mediante métodos nada ortodoxos, ni tradicionales y donde el valor jurídico de los medios probatorios se pueden encontrar dispersos en una red mundial sino de la manera conductual de casi toda la humanidad.

Derecho Informático

El Derecho Informático son la universalidad de problemas que surgen de las transformaciones que el derecho ha realizado como imposición de ciertas actividades novedosas que se desarrollan en el ámbito social y que requieren nuevas regulaciones o una reinterpretación de las existentes. La Informática y el Derecho son dos ciencias que en la actualidad se complementan, como lo establece Peñaranda (2001) cuando afirma:

> De esta manera, tenemos a la ciencia informática y por otro lado a la ciencia del Derecho; ambas disciplinas interrelacionadas funcionan más eficiente y eficazmente, por cuanto el Derecho en su aplicación, es ayudado por la Informática Jurídica. Pero resulta que la Informática debe estar estructurada en base a ciertas reglas y criterios que aseguren el cumplimiento y respeto de las pautas tecnológicas; así pues, nace el Derecho Informático como una ciencia que surge a raíz de la cibernética, que trata la relación Derecho e Informática desde el punto de vista del conjunto de normas, doctrina y jurisprudencia, que van a establecer y regular en su complejidad las acciones, procesos, aplicaciones y relaciones jurídicas de la Informática.

De allí, que las controversias suscitadas en virtud de hechos derivados de las Tecnologías de la Información, que implican la consideración de reglamentaciones internacionales, por supuesto, sobre la base de un Derecho Comparado coherente y el análisis de la marcada relación que existe entre la Informática y los aspectos que estudia el Derecho Internacional Privado en sus diversas ramas. Esta nueva ciencia trata las situaciones y controversias que pudieren surgir en el ámbito de, no sólo en las transferencia de datos, sino también las que pudieran derivarse de la copia, reproducción o re-programación, distribución y/o venta no autorizada de hardware y de software.

En este sentido, el estudio del Derecho en la Informática o en las Tecnologías de la Información constituye toda una realidad en el mundo jurídico del siglo XXI, así como su estudio y desarrollo, en la actualidad, en países del mundo entero, ya que con una simple búsqueda por Internet, puede evidenciarse como en muchos países existen leyes, doctrinas y jurisprudencias sobre el tema.

Es por ello, que debido al afán de buscar la verdad próxima a la realidad y aunque los jueces todavía no las han aceptado en su totalidad, se han incorporado como modos auxiliares de justicia, medios probatorios donde puede establecerse la credibilidad de un documento electrónico,

previo el estudio para demostrar la veracidad de las firmas electrónicas y garantizar las operaciones lícitas o ilícitas realizadas por medios digitales, aplicando el principio de la autorización previa, y el principio de reconocimiento de autoría a los fines de prevenir futuras controversias. Asimismo también podrían considerarse como ciertas las sentencias definitivamente firmes y con autoridad de cosa juzgada emanadas del Tribunal Supremo de Justicia (TSJ) así como de los diferentes tribunales del país.

Igualmente puede afirmarse el estudio de aspectos como lo son los Domain Name System (DNS), nombres de dominio por sus siglas en inglés, propiedad intelectual, firma digital y certificado digital, contratos electrónicos y telemáticos tanto en la órbita del sector público como privado, aduanas, tributación y facturación, protección del consumidor y publicidad, privacidad, resolución de conflictos, medios de pago, delitos informáticos, prácticas restrictivas de la competencia, seguridad tecnológica y seguridad legal.

Informática Jurídica

El uso masivo de medios y dispositivos técnicos de comunicación que facilitan la trasmisión y recepción de información los que se circunscriben al marco de una revolución electrónica, ha conllevado a la sociedad a la adopción de una actitud reflexiva, crítica y responsable ante nuevos problemas que derivan de su utilización.

De ahí que hay que tomar una perspectiva jurídica diferente, pues se trata de la ciencia aplicada a la tecnología, facilitando la familiarización con aspectos científicos e informáticos, mediante la incorporación de nueva doctrina desentrañando otro léxico con la finalidad de la aplicación de las normas especiales. De allí, en el año 2000, emerge la Informática

Jurídica, definida como la aplicación de los instrumentos tecnológicos a las operaciones que realizan quienes actúan en el ámbito del derecho.

Al respecto se debe diferenciar la técnica de la tecnología, aludiendo que la primera, se refiere al uso instrumental, práctico, mientras que la Tecnología de teckné y logos se refiere a la ciencia de la técnica, a la reflexión racional que sobre lo instrumental debería realizarse para producirse un conocimiento y aplicación trascendentes, más allá del uso de la técnica por la técnica misma. Tal diferenciación, circunscribe la definición de la Informática Jurídica como, la ciencia del tratamiento racional y automático de la información de contenido jurídico. De ahí se derivan tres principios: tratamiento racional, tratamiento operativo y tratamiento semántico.

El tratamiento racional se refiere al análisis, organización y clasificación, como condiciones necesarias para la adecuada transformación y traslado de la información jurídica desde sus fuentes o soportes tradicionales (códigos, sentencias, expedientes judiciales, actas, citaciones), hasta los formatos adecuados y previos al tratamiento informático.

El tratamiento automático es el uso de las máquinas computadoras. Una vez que ya se ha analizado el contenido de la información a tratarse y se la ha racionalizado vienen a establecerse los algoritmos o programas, los mismos que desarrollarán -en forma automática- las diversas tareas de procesamiento o tratamiento (automático) de la información.

El tratamiento semántico se refiere al tratamiento procesamiento de referencias documentarias o bibliográficas de carácter jurídico, tales como leyes, sentencias o doctrina.

La adecuación de normas a los sistemas informáticos demanda la existencia de una interdisciplina, además de la creación de teorías que se ajusten a la esencia de las ciencias jurídicas, cuya génesis versa en la presencia automatización o sistematización. Al respecto Losano (2010), define la teoría de las comunicaciones jurídicas como un conjunto de estructura cuya sujeción directa se vincula con la cibernética, generando un especial énfasis en el estudio de las comunicaciones, mensajes y la forma como se encuentran regulados internamente todos los sistemas, considerado desde la perspectiva jurídica. De ahí que Chirinos (2011), asevera que:

> Las comunicaciones jurídicas gira en torno a la cibernética, que estudia la comunicación basada en una plataforma tecnológica, las telecomunicaciones y la informática, las cuales se han unido para la prestación de servicios y apoyo al tratamiento de la información a distancia; esto significa que la iuscibernética es aplicada a las telecomunicaciones, o sea que el desarrollo de la tecnología avanzada o de punta afecta a la sociedad mundialmente, esa interrelación inmediata que tienen ahora las personas, donde se aprovecha para intercambiar información o descubrir nuevos contactos comerciales, han generado nuevas figuras jurídicas que debe estudiar el Derecho.

La ordenación electrónica viene a ofrecer al Derecho nuevas posibilidades tanto de agregación como de selección de datos jurídicamente relevantes, no sólo lo concerniente a normas sino también a datos estadísticos, socioeconómicos y documentales sobre los que se basa la emisión y la aplicación de normas jurídicas, que inobjetablemente requiere adecuación, a la luz de los cambios tecnológicos que trae consigo la Informática, donde el empleo de los nuevos dispositivos y aplicaciones se hace global en la actualidad.

Teoría General de las Pruebas

La teoría general de la prueba, expone el pensamiento de Vicenzo Manzini (1982), en los aspectos referentes a las pruebas en el proceso penal. Esta señala que la prueba sirve para sustentar los hechos que afirma cada una de las partes en el proceso, aludiendo a los actos que dieron origen al litigio que se sigue. Manzini, al igual que otros autores, establece que la función primordial de la prueba es crear convicción o certeza en el juez o magistrado acerca de lo que se está afirmando.

Por lo tanto, la prueba está encaminada a ser exhibida ante el órgano jurisdiccional, a crear un ánimo en él, con el objeto de que éste conceda la razón en lo que se está planteando, ya sea como acusador o defensor del inculpado. La prueba constituye, en cualquier proceso un papel fundamental, por cuanto se desprenden de esta las pretensiones a ser aceptadas o no como ciertas por el órgano jurisdiccional y por ende se obtiene o no un fallo favorable en el litigio.

En materia penal, la prueba es la actividad procesal dirigida a obtener la certeza judicial, conforme al criterio de verdad real, relativa a la imputación o de otra afirmación o negación que interese a una providencia del juez. Conforme a lo mencionado, el fin último de la prueba, se orienta hacia el convencimiento por parte del juez respecto a aquello, que la parte que alcance a exhibir la prueba afirme o niegue. En este sentido, Manzini divide la prueba en tres fases o etapas:

Producción*:* La prueba consiste en una manifestación o declaración de voluntad hecha por un sujeto de la relación procesal dirigida a introducir en el proceso un determinado medio de certeza.

Recepción: Es el hecho de que el órgano jurisdiccional toma conocimiento de la prueba, siempre que sea en el modo prescrito por la ley.

Valoración: Consiste en el análisis crítico, hecho por el magistrado, del resultado del examen probatorio y en la consiguiente libre convicción de él acerca de lo concluyente de esa misma prueba a los fines procesales.

Es objeto de especial atención, a la fase del desahogo. Dado, que esta constituye un pilar esencial en determinados medios probatorios, tales como la confesional, la testimonial y la pericial, lo cual alude a un entramado de situaciones que puedan desprenderse en el proceso.

Manzini, establece que es natural que la llamada carga de la prueba, o sea la necesidad de suministrarla, corresponda a quien acusa. Lo cual se traduce en el hecho que un individuo que afirma ante el órgano jurisdiccional que alguno de sus bienes jurídicos tutelados ha sido vulnerado, deberá probar que realmente se ha atacado el bien en comento, la manera en que se ha violado dicho bien, así como, los medios de comisión. El principio de que la carga de la prueba incumbe al que acusa es un simple principio lógico, por constituir la parte agraviada, resultado así una sencilla afirmación de sentido común, más que una regla de derecho.

Ahora bien, el objeto de la prueba según el autor, “son todos los hechos, principales o secundarios, que interesan a una providencia del juez y exigen una comprobación”. Conforme a lo mencionado, se diferencia la prueba en genérica y específica.

Designándose, la prueba genérica como aquella, que se encuentra dirigida a comprobar la materialidad del hecho desde su existencia el

hecho, la fuente humana que dio origen al hecho, los efectos que haya producido y la especificación de los mismos.

Mientras, que la prueba específica es aquella que integra la prueba genérica a los fines de imputabilidad del hecho delictivo, implicando la identificación del autor del hecho y la constatación de las condiciones relativas a la imputabilidad de ese mismo hecho al mencionado autor. Lo cual implica, que ha de probarse en el proceso penal, según Manzini, es en todo caso un hecho. Aun cuando se trata de probar un derecho subjetivo, como sucede en el delito de abandono de personas por falta de pago de alimentos o del despojo, lo que en realidad se prueba es el hecho de la existencia de ese derecho (extrapenal).

A este respecto, Manzini considera que la fuente de la prueba es todo lo que, aun sin constituirse por sí mismo medio o elemento de prueba puede, sin embargo, suministrar indicaciones útiles para determinadas comprobaciones. En relación a los medios de prueba, considera que es todo lo que puede servir directamente a la comprobación de la verdad. Mientras, que por otro lado, considera, que los elementos de prueba son los hechos y circunstancias en que se funda la convicción del juez.

Igualmente las llamadas reglas de la experiencia común no son medios de prueba, sino preceptos lógicos que asumen a veces el carácter de la presunción, o conocimientos comunes utilizables para el juicio, en cuanto sirven para la valoración de hechos o de circunstancias. En el derecho, pero especialmente en el penal, se deben probar los hechos con cualquier medio que no se encuentre excluido por las normas jurídicas.

Ahora bien, cuando se hace referencia a la duda, se tiene que decir que es subjetiva, o sea no confirmada por ninguna prueba externa, cuando, aun habiendo fallado toda prueba, queda en la mente del juez

una sospecha más o menos razonable. Por el contrario, con la certeza se tiene la plena seguridad de lo que sucedió, y con ello se logra determinar la culpabilidad o la inocencia de los procesados.

La duda, la sospecha resultan gratuita, no sólo no puede autorizar el reenvío a juicio ni la condena, sino que, precisamente porque falta todo medio probatorio, se debe absolver al imputado como si se tuviera prueba sobre su inculpabilidad. Es en éste caso donde se aplica la máxima in dubio pro reo, ya que en la duda es preferible la no punibilidad de un culpable al castigo de un inocente. De lo anterior, se desprende que de la exhibición de las pruebas se obtiene la convicción del juez para que incline la balanza de la justicia hacia uno u otro lado.

Una sólida investigación científica de los delitos, no sólo es imprescindible, sino fundamental para acreditar ya sea la culpabilidad o inocencia de los imputados; es por eso que solo una prueba eficiente puede garantizar a la sociedad que sea ésta, organizada jurídicamente, la que imponga las sanciones o medidas adecuadas a los victimarios.

La Prueba Electrónica

Este aparte responde a esta interrogante: ¿Que es la prueba electrónica? Di Totto (2005) la define como un elemento de convicción que está contenido dentro de sistemas o dispositivos que funcionan mediante la tecnología de información y al cual sólo puede accederse a través del uso de esta tecnología. Es decir, que para desarrollarla se debe contar con la colaboración de personal en calidad de expertos para determinar la autenticidad de la información que se requiere probar, incluso hasta su autoría.

Esto por cuanto los proveedores de servicios de Internet, así como los verificadores de registros de dominios suelen guardar y poner a

disposición de quien los solicite, los registros acerca de los contenidos puestos en línea y también los datos de identificación de los administradores, contactos técnicos y pagadores de los dominios desde donde se hubieren generado los contenidos.

Asimismo, resulta importante establecer aquellos elementos de interés criminalístico que son colectados por los órganos de seguridad ciudadana e inteligencia de Estado, relativos a los dispositivos de telefonía celular que poseen valor probatorio y van a relacionar al presunto imputado con la perpetración de un hecho delictivo. Estos aspectos van a resultar más interesantes aún, cuando se plantea la relación entre ambos, desde la perspectiva del fenómeno relativo al empleo desviado de la telefonía celular junto a los elementos criminalísticos inherentes como medios probatorios en el proceso penal.

En este sentido, la utilización de este tipo de documentos ha originado a un cambio radical en las facultades oficiosas de los jueces, sobre todo en materia probatoria, ya que al no estar nombradas en forma expresa en las leyes procesales y por desconocimiento manifiesto sobre la materia, los y las administradoras de justicia se pudieran encontrar en la disyuntiva de decidir si las aceptan como pruebas o no. Y en caso de aceptarlos, cual es el valor que se les debe otorgar, siempre con el objeto de no dejar en estado de indefensión o inseguridad jurídica a ninguna de las partes actuantes en ese proceso.

Por los tanto, cuando se plantea la disyuntiva de presentar uno o más documentos electrónicos como medio de prueba dentro de un proceso penal, se debe tener la seguridad que el juez que conozca del caso, si no tiene los conocimientos necesarios para realizar el análisis correspondiente, deberá tener a su alcance los elementos suficientes para cubrir esa carencia, por cuanto no se puede calificar ni dársele el mismo

tratamiento a este tipo de pruebas como a las que se presentaban hasta hace pocos años.

Documentos Electrónico

Si bien es cierto que la prueba no es más que un instrumento o medio con que se pretende mostrar y hacer valer la verdad o falsedad de algo; y que el documento es aquel escrito en el que constan datos fidedignos o susceptibles de ser empleados para probar algo y crear un efecto jurídico, en este caso, la complejidad se manifiesta por el soporte en el que se asienta tal manifestación de voluntad.

En este sentido, cuando se trate de un documento inscrito en una oficina de Registro, el soporte será el papel, si se trata de una grabación, será la cinta magnética, en el caso del negativo de una fotografía, el soporte será la película, y en el documento electrónico sin embargo, no existe un soporte único, ya que el mismo queda registrado en un soporte magnético y deberá ser decodificado, por personas facultadas para ello.

Dado que esa codificación se hace mediante el hardware, que equivale a las piezas físicas de la computadora o teléfono celular y el software, es el conjunto de programas destinados a que estos equipos realicen sus funciones, siempre que estén expresados en un lenguaje inteligible que pueda representar un pensamiento lógico. De acuerdo con Parilli (1996), los documentos electrónicos son:

> Todos aquellos que se realizan utilizando los medios del sistema mecanizado, sea por la creación en el mismo, por transmisión o por reproducción de otro documento. El sistema mecanizado actúa electrónicamente en la producción del documento bien sea utilizando la impresora de una computadora o bien con tarjetas de plástico con agregado magnético.

Desde esta perspectiva, igual importancia se debe considerar en la definición de documento electrónico, que efectúa Servidio citada por Cornejo (2006) cuando lo señala como “aquel documento elaborado por medio de una computadora siendo su autor identificable por medio de un código, clave u otros procedimientos técnicos y conservado en la memoria de ésta o en memorias electrónicas de masa.” De ahí que puede ser reproducido en formato papel o en otro medio periférico constituyendo un documento asimilable al escrito por cuanto después de impreso admite la firma de su emisor o emisora.

Además de la importancia de la conservación del mensaje y la posibilidad de recuperación como requisito esencial en el momento de producir el documento como medio de prueba. A tal efecto, el Artículo 8 de la Ley de Mensaje de Datos y Firmas Electrónicas ( ) establece que “Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un mensaje de datos, si la información que éste contiene es accesible para su ulterior consulta. (....), destacándose la necesidad de conservar el mensaje en su formato original o en algún otro que permita demostrar la reproducción de la información generada, enviada o recibida con exactitud.

En lo que respecta a su legibilidad para ser objeto de prueba, los documentos electrónicos se caracterizan porque sólo pueden ser leídos gracias a la intervención de sistemas traductores que hacen comprensibles las señales digitales, esta legibilidad implica su posibilidad de lectura y comprensión en el entendido de que el lenguaje en que se redacta es diferente al alfanumérico o lenguaje binario, pero que sin embargo, el mismo sistema se encarga de traducir el código utilizado a un lenguaje comprensible por la mente humana.

Asimismo, debe atribuírsele a una persona determinada en calidad de autora del documento electrónico, es decir, que el mismo sea

auténtico, lo cual se acredita mediante la firma electrónica, lo que crea la posibilidad de identificación de los sujetos participantes y las operaciones realizadas por cada uno de ellos en el proceso de elaboración del documento.

Por consiguiente, este conjunto de datos magnético grabados en un soporte susceptible de ser reproducidos, funge como objeto de prueba, es decir, el documento electrónico es un escrito remitido de un sujeto a otro a través de un medio digital que contiene un hecho cualquiera, jurídico o no, que puede demostrar la existencia, extinción, modificación o validez de una obligación y está representado por las variaciones de los campos magnéticos y ópticos registrados en el soporte, en consecuencia, éste no forma parte del documento ni el medio de entrada como el vehículo de la grafía que representa la manifestación del pensamiento ni la salida del mismo en cualquiera de sus manifestaciones, por lo tanto, es el documento electrónico el objeto de la prueba y no el medio o vehículo para presentarlo.

Por lo tanto, es de interés como evidencia física por una parte la Memoria RAM (Random Access Memory), como una memoria temporal, que sirve para guardar los programas que abre el usuario al momento de emplear el teléfono móvil; mientras que la memoria interna almacena archivos (videos, fotografías, música) y finalmente la memoria externa sirve para complementar la memoria interna, al poseer una capacidad mayor de almacenamiento de los archivos arriba citados.

Mientras que las tres memorias pueden servir como medio probatorio, por cuanto Escobar (2012), resalta que, “gracias a fenómenos electromagnéticos… la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada”. En este sentido, se destaca la evidencia digital, la cual según Rujano (2012), permite, “establecer la responsabilidad del posible autor y se pueden probar los hechos”.

Lo citado anteriormente, significa que la evidencia digital se encuentra almacenada en las memorias mencionadas y puede demostrar una relación del investigado con el caso, bien sea con el resto de los involucrados en el hecho, su relación con la víctima e incluso su presunta actuación en el hecho, por encontrarse en uno de los lugares de interés criminalístico en el delito investigado; dados los elementos de convicción que se encuentran almacenados y registrados, junto a las relaciones de llamadas aportadas por las empresas de telecomunicación. Resultando así de interés para dotar a la prueba de una relevancia especial con el propósito de generar en el juzgador, convicción con sustento material sobre determinado hecho punible.

En materia de eficacia probatoria, aparte de las disposiciones que rigen el uso de la informática en la vigente Constitución establecidas en sus artículos 60 y 180, se debe hacer referencia al Decreto-Ley sobre Mensaje de Datos y Firma Electrónica (2001) el cual señala en su artículo 4º lo siguiente:

> Los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.La información contenida en un mensaje de datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Ahora bien, para valorar la fuerza probatoria de la información emitida desde un teléfono celular, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida, archivada de manera que pueda ser reproducida nuevamente para su posterior consulta y si es posible relacionarla con una determinada persona con la finalidad de atribuirle la responsabilidad de dicha

información. Conforme a lo expuesto y de manera particular, valoración de la prueba, según González Rivas (2001) es:

> La operación mediante la cual el Juez contrasta la realidad de las probanzas practicadas en el proceso para obtener unos resultados que le permitirán decir y afirmar, si los hechos constitutivos de la pretensión o, en su caso, los impeditivos, optativos y exentivos aparecen acreditados. Según que esta operación de comprobación entre el resultado de la prueba y el tema de la misma aparezca reglado normativamente o no, puede hablarse de prueba legal o prueba libre.

Desde esta perspectiva, existen tres criterios fundamentales para la valoración de las pruebas: la prueba tasada, la libre y la mixta. El primero, supone una imposición a los jueces por parte de la ley de manera abstracta y preestablecida, del valor que debe atribuir a cada medio probatorios que conste en el proceso penal bajo su conocimiento. El segundo, como criterio de prueba libre, consiste en la libertad que tiene el juzgador de estimar el valor, según su convicción, a cada prueba presentada.

El sistema mixto, donde los administradores de justicia, adoptan el criterio de prueba legal para determinados medios probatorios como los instrumentos públicos y el de libre apreciación conforme a la regla de la sana crítica para los restantes medios de prueba no excluidos expresamente por la ley. Con la salvedad que todos los criterios deben cumplir con los requisitos de legalidad, licitud, idoneidad y utilidad.

Es así, como para todos los efectos de la validez de los documentos electrónicos, como prueba fundamental, la Ley de Mensajes de Datos y Firmas Electrónicas (2001) establece en su Artículo 1º, que:

> El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico,

> independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos… será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas.

Por consiguiente, como lo señala la norma antes descrita, se le da el reconocimiento de prueba documental a toda información inteligible en formato electrónico, independientemente de su soporte material, “que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.” Según el Art. 26 del Código Penal Español, a lo que se podría agregar que este transcrito en un determinado idioma.

Ante esta realidad y sobre la base de lo anteriormente expuesto, se plantea la forma de presentar las pruebas incriminatorias realizadas o relacionadas con hechos delincuenciales cometidos por intermedio de teléfonos celulares para ilustrar criterios de juzgadores dado que son instrumentos de convicción con los cuales se demuestra, de manera procesal, la responsabilidad o no de si una persona cometió un hecho punible.

III. REDES SOCIALES Y LOS DELITOS INFORMATICOS

La telefonía móvil parte del concepto de red celular propuesto por Douglas Ring en (1947:2) tras la aparición del transistor, por lo cual:

> Este concepto de red celular proponía dividir el espectro disponible de varios canales, limitar la potencia de los transistores y extender la cobertura instalando un número mayor de éstos. A la zona cubierta por un transistor se le denominó célula y, por eso, la telefonía móvil también se conoce como telefonía celular.

Una de las redes que más populares es facebook que se centra en la búsqueda e inclusión de amigos, amigas, compañeros de estudios, colegas, integrantes de equipos deportivos y agrupaciones de cualquier índole o como forma de hacer contactos con otras personas, por cuanto se trata de una nueva dimensión expansiva de las relaciones personales que antes no podía ser alcanzada y es que con la incorporación de imágenes, videos y sonidos se pueden elaborar fichas personales de cada usuario que son verdaderos resúmenes de información confidencial.

Estas páginas web almacenan datos personales que sirven para obtener desde fechas de nacimientos hasta perfiles psicológicos de los usuarios, que pueden ser utilizados por cyberdelincuentes como medio de suplantación de identidad para obtener acceso a cuentas bancarias en línea o como información a organizaciones criminales del mundo real y físico, ya que al inscribirse en páginas como facebook o my space, se debe colocar la verdadera información a efectos de ser ubicados por las personas con intereses comunes.

Como la gran mayoría de los usuarios actúa de buena fe, al incorporarse a la red suministra una serie de datos personales que están al alcance de cualquiera y así pueden facilitar el fraude, ya que la fecha

de nacimiento es utilizada por el 10% de los usuarios de Internet como contraseña de acceso o como parte de estas para acceder a sistemas protegidos. Igualmente el 15% de los usuarios de sistemas de información como *password* o palabras claves utiliza su nombre y apellidos para acceder al sistema, quedando en un estado de indefensión frente a estas personas inescrupulosas que manejan muy bien el área de informática.

Al incorporar una foto personal, que en la mayor de las veces son close-ups, conjuntamente con el informe personal se puede establecer no sólo el nivel de educación, empresas donde trabaja o trabajó, cargos desempeñados, dirección de habitación, teléfonos privados, pasatiempos, sino la identificación de cualquier ciudadano, estando a merced de quien quiera darle cualquier uso a esa información, incluso hasta poder hurtar su identidad con fines inimaginables.

El perfil económico en facebook como principal red puede hacerse visible en esta, por cuanto existen aplicaciones que innecesariamente se agregan a la página, tales como las ciudades que conoce cuando ha visitado otros países, por fotos tomadas en los sitios, la descripción de los vehículos de lujo que posee, el inmueble donde habita, lo cual puede determinar el poder adquisitivo de la persona. Asimismo el aspecto laboral con el cual pueden identificar a gerentes y empleados de seguridad y auditoria informática en el área financiera o industrial para obligarlos a cometer delitos contra la propiedad o contra las personas mediante la extorsión.

Una de las opciones de la inscripción en estos sitios web es el que se indique si el usuario está buscando pareja, relaciones, amigos o amigas y aunque el anonimato de Internet hace muy peligroso este tipo de aventura, la cual se inicia como virtual, las estadísticas indican que uno de cada cinco encuentros de este tipo culmina con agresiones físicas o

psicológicas a mujeres, incluyendo delitos sexuales, no recomendándose este tipo de relación.

La principal conclusión de un estudio realizado por la firma de seguridad Sophos sobre los riesgos de hurtos de identidad en las redes sociales de Internet fue “que los usuarios de facebook facilitan el robo de su información personal” ya que el 41% de los usuarios no tiene inconveniente en suministrar datos personales, como nombres y apellidos, dirección de correo electrónico, fecha de nacimiento o teléfono celular a cualquier desconocido, pudiendo, con los datos obtenidos, crear correos *phishing* que se usan para robar información financiera, adivinar contraseñas de usuarios e incluso hacerse pasar por ellos para conseguir información adicional de su grupo social.

Son muchos y variados los tips de seguridad que deben seguir los usuarios de redes sociales y que se deben implementar a fin de evitar el suministro de información confidencial, tales como cambiar la configuración de la seguridad del facebook para que sólo las personas que desea y no los amigos de los amigos puedan ver la foto principal del perfil.

Así como cambiar la fecha de nacimiento sumando cifras iguales al día, mes y año; no escoger las opciones de privacidad mis redes o amigos de mis amigos; no colocar la ubicación o actividad actual; no agregar aplicaciones familiares para no puedan ubicar su entorno inmediato; supervisar a los contactos de sus hijos e hijas para tener conocimiento de los mismos; denunciar actividades irregulares y acoso de personas en la web.

Twitter como Puente de Bloqueo Informativo

El twitter surgió como red social de comunicación en el mes de marzo de 2006 como un pequeño proyecto de investigación y desarrollo de Obvious, LLC, Start-up en San Francisco, California, EEUU, bajo la dirección de Jack Dorsey, con el fin de mantener comunicados a los empleados de la misma empresa, fungiendo como una especie de intranet, haciendo las veces del mismo servicio entre quienes laboran en el mismo lugar. No obstante, en el mes de octubre del mismo año, fue hecho público el conocimiento de la red, ganando tantos adeptos en muy corto tiempo que logró ganar en marzo del año siguiente el premio Sound by Southwest Web Award en la categoría de blog.

En Venezuela, esta red social de comentarios y participación ha crecido en el último año 2.500% según estudios de Comscore lo cual demuestra un crecimiento insólito, a pesar de la cantidad de información de que puede disponer el usuario de twitter son cada vez más quienes se integran debido a sencilla tecnología que se necesita para interactuar en esta y a los dispositivos móviles con acceso a banda ancha de Internet que conceden un máximo grado de comunicación y aprovechamiento según el Diario El Nacional(2009: 4).

Para ingresar a esta red social se requiere responder una pregunta clave del perfil del usuario que quiere accesar a ella ¿Qué estás haciendo ahora?, lo que le permite al resto de sus contactos estar al tanto de lo que realiza y demás actualidades que les puedan interesar. Además la red posee enlaces con otros sitios web, como medios de comunicación social, organismos oficiales, empresas, comercios, ya que es una forma simple y sencilla de estar actualizado, de interactuar con el resto del mundo e incluso conocer sobre la vida de personas famosas, ya que muchas se encuentran en Twitter de acuerdo al Diario El Universal (2009).

Incluso, muchos periódicos y medios audiovisuales se han incorporado a la red, con la finalidad de mantener informados a sus lectores y seguidores en tiempo real, de todo lo que sucede en el país y en el mundo. Es muy fácil incorporarse a esta red. Evidentemente que twitter es diferente a facebook en la forma de integrar la red de amigos. En la primera, el usuario puede escoger libremente a quien seguir, mientras que en la segunda, debe haber una solicitud de amistad que puede ser aceptada o no.

Asimismo, hay catálogos extensos que facilitan la escogencia de usuarios a los que seguir con fines relacionados con un determinado tema. Uno de ellos es twellow que es denominada las páginas amarillas de twitter. Igualmente, quienes buscan en twitter ideas e insumos valiosos sobre temas específicos cuentan con herramientas para ubicar a los más prominentes en cada campo como twellow.com, equivalente a las páginas amarillas.

Para los meses de mayo y junio de 2009, twitter, como red social de microblogs, se convirtió en el elemento fundamental de la crisis política post-electoral en Irán según el Diario El Universal (2009), ya que las autoridades iraníes han mantenido un extremado control sobre las comunicaciones en ese país, incluso llegando a decomisar los teléfonos celulares y cámaras de los manifestantes con los cuales grababan las acciones represivas de las fuerzas especiales de la policía.

En Teherán, miles de manifestantes movilizados a favor de la oposición del actual gobernante, se radicalizaron después que se confirmara su sorprendente victoria de las elecciones de ese año, de las cuales muchos de tomaron videos aficionados que mostraban las agresiones de la policía, el lanzamiento de gases lacrimógenos y los chorros de agua a pesar de las restricciones gubernamentales al flujo libre de la información y al trabajo de los periodistas.

Así la red social twitter se convirtió en la alternativa comunicacional con el resto del mundo para divulgar lo que estaba pasando en Irán, que incluso medios tradicionales y cadenas de televisión se han servido de estos mensajes, eludiendo así la censura del gobierno, permitiendo burlar los filtros regionales y locales. A raíz de esto, los internautas comenzaron a solicitar, a través de este medio, que los habitantes de cada país se comunicaran con sus embajadas para que abrieran sus puertas a los afectados por el conflicto, por cuanto la comunidad internacional no podía ni debía tolerar esta situación de acallar a la prensa.

La Seguridad en la Red

Al hablar de seguridad en el entorno digital, no se trata sólo de mantener bajo control la información financiera, sí también las transacciones bancarias. Aunque cada día un mayor número de personas, empresas, organizaciones y entes públicos y privados dependen cada vez más de las redes de datos y de la información computarizada para su funcionamiento, administración, gestión y operaciones de los sistemas informáticos.

Así como la interconexión de complejas bases de datos que intercambian y procesan información, tales como los sistemas de control aéreos, registros de contribuyentes o de información de los ciudadanos y hasta los sistemas de seguridad y defensa entre otros. Todos estos sistemas pueden ser invadidos en cualquier momento sin previa autorización.

En este sentido, la explosiva expansión de Internet, ha permitido que cada vez un mayor número de personas acceda a datos de otras y exponga su intimidad a la vista de los demás, es decir, que se puede hacer pública informaciones personales tales como gustos de consumos, niveles de ingresos, registros médicos y buena parte de su vida íntima, al

circular por las redes sin controles y sin reglas, por lo tanto, la vida de cualquiera puede ser alterada en forma remota sin previo aviso, pues cada conexión aunque potencia la capacidad y posibilidad de conocimiento, de una u otra forma hace más vulnerables a la sociedad.

Ahora bien, es importante señalar que en el espacio de la red o ciberespacio, las necesidades se relegaron a segundo plano, lo único que parece regir la conducta de navegantes, usuarios, es simplemente la razón o el pensamiento de cada cual, su moral interna, sus principios e ideología, ya que en Internet no existe censura y no debe existir, en atención a los derechos subjetivos de los ciudadanos, como el de libertad de expresión.

Esto por cuanto el sistema se concibió y desarrolló con la idea de proporcionar un acceso fácil a la información y servir como un medio de comunicación rápido y efectivo. No obstante, la red no puede configurarse como una especie de pandemónium, en donde cada cual hace lo que le venga en ganas, afectando el interés y el derecho ajeno.

En este sentido y teniendo en mente este objetivo fundamental, toda actuación debe ser canalizada de tal forma que en su libre andar por los caminos de las ideas, nunca vulnere el pensar del resto de la población, de igual forma se debe canalizar la forma de actuar y lograr así establecer un ciclo perfecto. Es decir, que se establezcan conductas que de una manera armónica acerquen a las personas a fin de lograr el ideal de una sociedad sin violaciones, ni abusos entre los individuos que la integran.

Sin embargo, Internet y todo lo que ella implica no escapa de este fallo, por cuanto es de todos conocido que, lo que para alguien puede ser un hecho perfectamente valedero y legal, para otro pudiere configurarse una acción total y perfectamente punible, de la cual exista una

responsabilidad y que pueda efectivamente ser sancionado o sancionada por el hecho cometido, bien en su dolo o en su culpa.

Es decir, que aunque todos los días se incorpore a la red información valiosa para la investigación científica y social que presta una gran ayuda a la sociedad, también el espacio virtual es un terreno fértil para el delito, donde la maldad puede ir al lado de la bondad, la cooperación con el afán de lucro, la solidaridad con el fraude, todo con la finalidad de violar y sabotear secretos corporativos y privacidades personales, apropiarse de derechos de autores, ya que la humanidad se enfrenta a nuevas amenazas y riesgos más complejos y variados.

En este sentido, el aumento de los delitos cometidos en el ámbito informático es un hecho reconocido de forma unánime como una amenaza grave para la sociedad, por cuanto la manipulación remota de los sistemas informáticos, la asincronicidad de los procesos y la propia flexibilidad de las tecnologías de la información, constituyen rasgos que dificultan el control de los comportamientos no éticos y antijurídicos por parte de las autoridades. De ahí que, los planteamientos no se presentan tan fáciles de dilucidar como en las demás ramas del Derecho, ya que no existe un único delito informático, sino un complejo conjunto de conductas de muy diversos signos que pueden ser calificados como tales.

Cabe destacar, que por su naturaleza, influencia y poder, las redes telemáticas configuran al mismo tiempo, tanto un medio susceptible de ser usado para delinquir como un campo propicio para el surgimiento o refinamiento de conductas delictivas tradicionales, por cuanto lograr la tipificación y diferenciación de estos actos ilegales, tiene una trascendental importancia para determinar la ley que se debe aplicar a cada caso en particular sin que haya un conflicto de competencia.

Por lo tanto, el sistema según el cual se rige Internet, plantea un mundo sin fronteras ni límites, ya que en la red se experimenta la tan ansiada aldea global, en la que jurisdicciones, leyes, reglament sanciones, ideologías, parecieran ser total y completamente inútiles

IV. ALGUNAS IDEAS FINALES

El Derecho Penal constituye la rama encargada de prescribir aquellas conductas lesivas que constituyen delitos y faltas cometidas contra bienes y valores imprescindibles para la existencia y desarrollo de la sociedad. Lo cual, requiere la constante promoción de los conocimientos teóricos, prácticos y técnicos, relativos a las acciones concernientes al empleo de los dispositivos telefónicos móviles con fines contrarios al beneficio de las personas. Esto debido el aumento de los delitos que son cometidos a través del uso indebido de la informática y de la telefonía móvil, evolucionando una nueva forma de criminalidad, que se distingue por una gran variedad de delitos.

Por lo tanto, se van a suceder una serie de cambios y transformaciones jurídicas inherentes, en virtud de la emergencia que representa para el Estado Venezolano intervenir para contrarrestar este tipo de acciones, mediante la promulgación de instrumentos jurídicos adecuados como la Ley Especial Contra Delitos Informáticos (2001) y la Providencia Administrativa 572 (2005), emitida por la Comisión Nacional de Telecomunicaciones.

En virtud de los cuales junto a otros instrumentos, van a orientar el procedimiento acusatorio, al igual que en el juicio oral y público, el cual consiste en un debate contradictorio entre las partes, mediante la igualdad de oportunidades que van a requerir un amplio y cabal reconocimiento del derecho de defensa, fundamentado en las evidencias electrónicas que sean colectadas mediante los dispositivos de telefonía móvil, servida del

racionalismo y legitimidad de la persecución penal y la pena, que alcance a ser impuesta en el juicio.

De esta manera, se comprende que en el Proceso Penal al denunciarse la comisión de delitos concerniente al uso indebido de la telefonía móvil comprendida como el sistema informático o hardware, se requiere una clara certeza y conocimiento de la naturaleza que encierra la evidencia electrónica, comprendida por la información contenida (mensajes de texto, mensajes de voz, fotografías, videos, correos electrónicos, redes sociales), que van a definir la situación jurídica del procesado, bien sea a través del archivo del proceso, la condonación absolución del proceso o su condonación.

Esto, permite desde la criminología, observar y distinguir a las personas incursas en la comisión de distintos delitos mediante la telefonía móvil en la sociedad venezolana, en las cuales resulta de interés los factores que intervienen en el comportamiento criminal, devenidos del empleo de medio tecnológico, mediante la generación de medidas que modifiquen el accionar delictivo.

Fundamentación de los Delitos Informáticos

Las comunicaciones jurídicas, se orienta hacia la familiarización mediante la incorporación de nuevos vocablos tecnológicos, inherentes a la configuración de la Informática Jurídica para enfrentar los desafíos devenidos de las nuevas técnicas que puedan desarrollarse en el ámbito de la informática y sean desvirtuadas para la perpetración de hechos delictivos, dados los elementos que estos presenten, para determinar la certeza de tales hechos, conforme al carácter digital de la evidencia, como elemento probatorio en el proceso judicial.

Por tal razón, se comprende como raíz fundamental para la generación del conocimiento lesivo de la telefonía celular; la diferencia entre la técnica y la tecnología por constituir un ingenio de la mente humana, cuya evolución es directamente proporcional a la aparición de innovaciones que han sido incorporadas tales como cámara fotográfica, cámara de video, internet del cual se deriva la implementación de las redes sociales.

La técnica, viene a relacionarse directamente con el uso pernicioso como instrumento que permite una práctica generativa y creciente del aprovechamiento y desvió de la telefonía móvil hacia el accionar delictivo. Lo cual, se corresponde con el surgimiento progresivo de una terminología univoca para relacionar todos los elementos criminalísticos, concernientes a la telefonía móvil. Mientras, que la tecnología, se dirige hacia la búsqueda de respuestas relativas a los comportamientos criminales como fuentes generadoras de nuevas formas de acción delictiva; de allí su orientación criminológica.

Esto, conlleva además a la inclusión de una serie de disciplinas dentro de un sistema abierto, inherentes al contexto que envuelve el delito y toda una serie de términos novedosos. De allí su complejidad como elemento dinámico de la teoría, que se encuentra inmersa en los avances tecnológicos desde los que emergen nuevos elementos que llevan a entrelazar la técnica y la tecnología, mediante un nuevo tejido de figuras jurídicas, que necesariamente debe ser conocido por todos los actores sociales y jurídicos inmersos dentro del ámbito del proceso penal.

Al respecto, la Ley Especial Contra Delitos Informáticos (2001), prescribe en su artículo 2, quince definiciones elementales respecto a las tecnologías de información, que implica la adopción paulatina de una serie de términos a ser aplicados dentro del proceso de recopilación de aquellos documentos contenidos en teléfonos móviles enfocados al

principio de la inmediatez de la evidencia, relativo a la relación del hecho delictivo con la prueba digital, también denominada prueba electrónica presentada, que requiere un tratamiento particular dado su carácter intangible.

Por su parte, la teoría General de la Prueba, orientada hacia las evidencias digitales, como elemento sustentador de uno o varios hechos delictivos. De allí el conocimiento que deben poseer los jueces respecto a la definición de los elementos que componen la prueba como un todo, a fin de permitir una reflexión profunda sobre la misma, no solo como un ingenio que almacene datos electrónicos, configurados en un documento relativo a imágenes fotográficas, videos, mensajes de voz o texto, que al ser observados permiten establecer la inocencia o culpabilidad del imputado.

En este contexto, desde la criminalística emerge una nueva rama denominada Informática Jurídica, que hace uso de las técnicas y procedimientos criminalísticos, precisamente en atención al carácter volátil que presentan las evidencias digitales. Por lo tanto, este tipo de evidencias deben encontrarse debidamente autorizadas las diligencias a practicarse sobre el dispositivo de telefonía móvil a fin de evitar la violación de la Constitución que en su artículo 48, que textualmente dice:

> Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.

Por su parte, el artículo 49 establece claramente que: “El debido proceso se aplicará a todas las actuaciones judiciales y administrativas”, contemplando específicamente en el numeral 1 que: “Serán nulas las pruebas obtenidas mediante violación del debido proceso”.

Por lo tanto, los mismos no deben sufrir modificación alguna, para ello los operadores deberán encontrarse capacitados en su manejo para alcanzar su traducción a lenguaje visual. Por lo que debe documentarse el proceso de adquisición, acceso, almacenamiento y/o transferencia de toda evidencia digital o prueba electrónica que permitirá acreditar algún hecho que dicha evidencia registre; dado que el legislador consagra el principio de la legalidad y licitud de las pruebas.

Dicho principio, consiste que solo puede practicarse y ser incorporadas al proceso aquellos medios cuya obtención se haya realizado con sujeción a las reglas que la establece, lo que implica el cumplimiento de las formalidades esenciales establecidas para la obtención de las evidencias y para hacerlas valer ante el juzgador, todo con la finalidad de formar su convicción, o sea que sería ilícita una prueba ilegalmente lograda, como ilegalmente incorporada.

Alcance de las Comunicaciones por Telefonía Móvil

Las comunicaciones realizadas por intermedio de la telefonía móvil pueden considerarse medio probatorio en el proceso penal, ya que la transmisión de una o varias informaciones a una o diversas personas, mediante el sonido de la voz, escrita o gráficamente, almacenados en el dispositivo, computadora o internet, registran la fecha y hora de emisión y recepción, así como el número designado al dispositivo emisor.

. De esta manera, se presentan las siguientes funciones que poseen la mayoría de los dispositivos de telefonía móvil, sensibles de ser empleadas con fines delictivos partiendo de los datos que integran la información vertida en un documento, objeto de ser manejada por el trasgresor de la ley con fines delictivos, tras ser recibida por la victima mediante otro dispositivo de telefonía móvil, en el cual es recibido uno o varios mensajes lesivos a su seguridad personal:

Mensajes de Texto (SMS Short Message Service/Servicio de Mensajes Cortos). Es el mensaje realizado o recibido por el usuario a través de la escritura electrónica efectuada mediante la manipulación del teclado del dispositivo móvil según su diseño (teclado físico o digital). El mensaje puede visualizarse en la pantalla del dispositivo y puede ser almacenado en el mismo. Constituye una forma rápida, sencilla de comunicarse en forma escrita muy difundida entre los usuarios de la telefonía móvil.

Mensajes de Voz. Es una información realizada en forma oral por parte del usuario del dispositivo, cuando la línea del dispositivo no se encuentra disponible. Asimismo posee la figura de nota de voz, que es enviado cuando la línea del receptor está disponible o no.

Fotografías Digitales. En la actualidad la mayoría de los dispositivos de telefonía móvil poseen cámaras fotográficas digitales, que permiten al usuario tomar imágenes de elevada calidad en distintos formatos, principalmente JPEG (Joint Photographic Experts Group/ Grupo Conjunto de Expertos en Fotografía). Estas imágenes pueden almacenarse en el dispositivo y pueden ser transmitidas a otro dispositivo mediante distintas formas de conexión inalámbrica (Bluetooh, Infrarrojo, WI-FI).

Videos. Al igual que las fotografías digitales, los dispositivos de telefonía móvil poseen cámaras de video, las cuales al ser operadas por el usuario captan la imagen y el sonido de una escena de interés para el usuario en formatos MP4 (Moving Picture/Imagen en Movimiento). También pueden ser transmitidas mediante conexión inalámbrica.

Correos Electrónicos. Es un servicio de internet que permite enviar y recibir mediante una cuenta personal del usuario mensajes, además de todo tipo de documentos electrónicos desde textos, fotografías y videos.

Redes Sociales**.** Son servicios de internet que permiten agrupar personas conforme a la variedad de grupos culturales existentes a nivel global, más allá de las computadoras fijas y portátiles, los dispositivos telefónicos móviles poseen acceso a internet y por ende a las redes sociales existentes y de mayor difusión como facebook y twitter, transmitiendo un sinnúmero de mensajes, documentos, fotografías y videos diariamente con un alcance global.

Llamadas entrantes y salientes. Es la comunicación entablada entre una o varias personas a través de uno o varios dispositivos telefónicos móviles. Los contenidos de los mensajes son producto de las necesidades de transmitir ideas y pensamientos para dinamizar las relaciones humanas.

Las entidades teóricas descritas, se orientan en su conjunto hacia el carácter lesivo en las cuales estas se ven envueltas para atentar contra un bien jurídico protegido, dada la transformación de la naturaleza beneficiosa y progresista de su empleo en pro del desarrollo humano mediante la simplificación y difusión masiva de las comunicaciones que a diario realizan las personas que integran los ámbitos económico, social, político, cultural, geográfico, ambiental y militar a través de los distintos tipos de documentos electrónicos que son generados dentro de un proceso dinámico de transferencia e intercambio entre las mismas de distintos documentos electrónicos.

De allí, han surgido conductas orientadas a la perpetración de delitos previstos en el ordenamiento jurídico vigente. Esto conlleva a la descripción de una serie de terminologías inherentes a la tecnología informática, donde son aprovechadas las funciones antes mencionadas. En virtud de que las mismas permiten la imputabilidad a dolo por su intencionalidad de empleo lesivo, prescrita dentro del ordenamiento jurídico vigente. Seguidamente se muestra en la siguiente el alcance de

las comunicaciones de las comunicaciones realizadas por intermedio de la telefonía móvil:

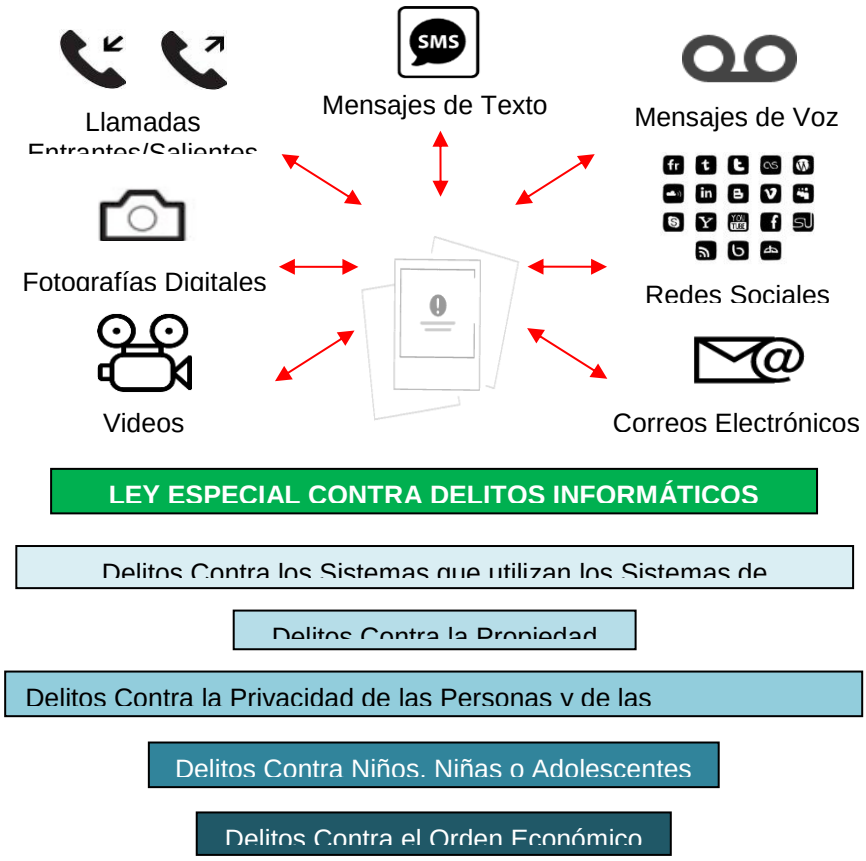

Figura *1*. Alcance de las comunicaciones por intermedio de la telefonía móvil

En la figura 1 se destacan los contenidos reflejados en la pantalla del dispositivo de telefonía móvil del usuario, comprendido por la persona emisora que observa y se escucha asimismo, respecto al documento electrónico que es enviado al receptor, que observa el mensaje enviado o escucha para intimidar a la víctima quien visualiza o escucha el mensaje emitido.

En este sentido, se destaca que el documento electrónico constituye per se, un documento dado que está contenido en una memoria del dispositivo del telefonía móvil que es tangible, puede ser extraído y

sometido a experticia mediante la Informática Forense. Asimismo posee un contenido que puede ser visualizado o escuchado a fin de transmitir una idea o pensamiento que genera o no un efecto en el receptor.

A este respecto, se destaca en relación al documento electrónico los nombres de los servidores involucrados en la transferencia del correo, las direcciones IP de los dispositivos de telefonía móvil empleados, en los cuales se refleja la fecha y la hora de emisión y recepción, al igual que los números de identificación de mensajes.

De esta manera se comprende, que tras practicarse el análisis de estos elementos, complementado el análisis de los registros de transacciones de los servidores, así como las condiciones de presentes en la red de Internet para el momento del hecho, van a permitir encaminar si un documento fue enviado o no por la persona a la cual se le imputan determinados hechos.

Delitos Informáticos

El Estado Venezolano brinda protección a la tecnología de la información, mediante la prescripción de los comportamientos perniciosos relativos a este ámbito desde el cual se destacan los dispositivos de telefonía móvil. Para ello se establece un sistema binario de penas privativas de libertad y pecuniarias, aunadas las penas accesorias que en estas se establecen.

De esta manera en el Título II relativo a los delitos, en su capítulo I denominado De los Delitos Contra los Sistemas que utilizan los Sistemas de Información, menciona los siguientes:

Artículo 6. Acceso indebido.

Artículo 7. Sabotaje o daño a sistemas.

Artículo 8. Favorecimiento culposo del sabotaje o daño.

Artículo 9. Acceso indebido o sabotaje a sistemas protegidos.

Artículo 10. Posesión de equipos o prestación de servicios de sabotaje.

Artículo 11. Espionaje informático.

Artículo 12. Falsificación de documentos

En relación al Capítulo II, llamado De los Delitos Contra la Propiedad,

se contemplan los siguientes:

Artículo 13. Hurto.

Artículo 14. Fraude.

Artículo 15. Obtención indebida de bienes o servicios.

Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.

Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos.

Artículo 18. Provisión indebida de bienes o servicios.

Artículo 19. Posesión de equipo para falsificaciones.

Mientras, que el Capítulo III, designado como De los Delitos Contra la

Privacidad de las Personas y de las Comunicaciones, prescribe los siguientes:

Artículo 20. Violación de la privacidad de la data o información de carácter personal.

Artículo 21. Violación de la privacidad de las comunicaciones.

Artículo 22. Revelación indebida de data o información de carácter personal.

El Capítulo IV, llamado De los Delitos Contra Niños, Niñas o

Adolescentes, establece los siguientes:

Artículo 23. Difusión o exhibición de material pornográfico.

Artículo 24. Exhibición pornográfica de niños o adolescentes.

El Capítulo V, De los Delitos Contra el Orden Económico, establece los

Siguientes:

Artículo 25. Apropiación de propiedad intelectual.

Artículo 26. Oferta engañosa.

Esto, permite extender el abanico de posibles formas de acción delictiva que han venido manifestándose dentro de la sociedad venezolana produciendo un incremento en el problema de seguridad ciudadana que atraviesa el país.

Por ello, se ha logrado como respuestas del Estado Venezolano en lo relativo a la obligación de brindar protección a las personas, la promulgación de instrumentos jurídicos como la Ley Especial Contra Delitos Informáticos (2001) y la Providencia Administrativa 572 (2005), emitida por la Comisión Nacional de Telecomunicaciones ..

Por lo tanto, se contempla que en el Proceso Penal al ser denunciada la comisión de delitos concerniente al uso indebido de la telefonía móvil, se requiere una clara certeza y conocimiento de la naturaleza de la evidencia electrónica, que de este deriva. De ahí que, la criminología, se remite hacia la observación y distinción de las personas incursas en la comisión de delitos mediante la telefonía móvil, resultando

de interés los diversos factores intervinientes en el comportamiento criminal.

Algunas Acciones a Realizar

El Estado Venezolano, a la luz de la Constitución Nacional, establece su responsabilidad para brindar protección a las personas y los bienes tanto públicos como privados a través de los órganos de seguridad ciudadana, debe revisar las desarrolladas hasta el presente políticas públicas en la materia.

Particularmente aquellas que son relativas a la prevención y reducción de los delitos informáticos, que día a día abruman y comprometen la seguridad, la vida y la libertad de todos los ciudadanos en todos los ámbitos. Para ello deberá fomentar campañas orientadas dentro del marco de la prevención para que las personas no proporcionen información de tipo personal, familiar o empresarial, cuando estén en espacios públicos o privados, desde los cuales se puedan ejecutar delitos informáticos, mediante el empleo de los dispositivos de telefonía móvil por parte de grupos de la delincuencia organizada que operan dentro y fuera del país.

En virtud, que al Poder Judicial le corresponde a través de sus órganos conocer de las causas y asuntos de su competencia mediante los procedimientos que determinen las leyes, y ejecutar o hacer ejecutar sus sentencias, este debe considerar los avances concernientes a la Informática en virtud del desarrollo de tecnología en todas sus formas.

De ahí que se debe mantener al día los conocimientos relativos a la telefonía móvil y otros medios tecnológicos conexos como lo constituyen los satélites, las redes, las computadoras, la fibra óptica, la televisión y

demás tecnologías que integran la infraestructura del ciberespacio. Los cuales son aprovechados en forma antagónica por parte de los grupos delictivos de la delincuencia organizada para cometer delitos que deben ser puestos al descubierto, perseguidos y castigados sus autores a fin de alcanzar el Estado Social, de Derecho y Justicia que prescribe la Constitución Nacional.

En tal sentido realizar acciones para mejorar los contenidos relacionados con la evidencia digital que contempla el Manual Único de Procedimientos en Materia de Cadena de Custodia de Evidencias Físicas emitido por dicho ente. De ahí que se requiere de la capacitación constante de los diversos actores que integran el Ministerio Público en materia de evidencia digital devenida de la telefonía móvil. Igualmente, la dotación adecuada del personal que desarrolla labores investigativas mediante el aseguramiento, fijación, colección, embalaje, traslado y almacenamiento de evidencias digitales.

Esto en virtud de la incorporación de nuevos métodos investigativos y medios probatorios del proceso, dado el elemento evolutivo que lleva a la creación de nuevos dispositivos de telefonía celular, que inquiere de igual manera la revisión de los métodos y medios previos, apoyados en los avances técnicos surgidos, a fin de mantener la eficacia de los mismos, dada la adopción y avance constante de los modus operandi de la delincuencia organizada a nivel global, regional y local.

REFERENCIAS

Arteaga Sánchez, Al. (2009). **Derecho Penal Venezolano**. Caracas. Mc Graw Hill.

Brizzio, C. (1999). **La Informática en el Nuevo Derecho.** Argentina: Abeledo-Perrot.

Código Orgánico Procesal Penal. (2012). **Gaceta Oficial No. 9.042.** 12 de junio de 2012.

Código Penal. (2005). **Gaceta Oficial No.5786E.** 13 de Abril de 2005.

Constitución de la República Bolivariana de Venezuela. (1999). **Gaceta Oficial No. 36.680.** 30 de Diciembre de 1999.

Cornejo, V. (2006). **Los Medios Electrónicos Regulados**: Sista

Chacín Fuenmayor, R. (2000). Sobre las Implicaciones Jusfilosóficas de la Informática en el Derecho. Separata de la **Revista de Derecho** Nº 2. Tribunal Supremo de Justicia. Caracas. Venezuela.

Chirinos, A. (2011). **Las Teorías y sus aportes**. Valencia: ABC.

Decreto con Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas (2001) **Gaceta Oficial Nº 37.076**.

Di Totto Blanco, B. (2005).La "Prueba Electrónica" en el Proceso Penal Venezolano **en Pruebas, procedimientos especiales y ejecución penal. VII y VIII Jornadas de Derecho Procesal Penal. Caracas: Universidad Católica Andrés Bello**

De Bernardo, González, C. M. y Priede Bergamini, T. (2007). **Marketing Móvil: Una Nueva Herramienta de comunicación.** España: Gesbiblo S.L.

Delgado, E. (2009). **La Evidencia Digital como Medio de Prueba en el Proceso Penal Venezolano**. Trabajo Final de Investigación. Turmero: Universidad Bicentenaria de Aragua

Escobar, O. (2012). **La Informática Forense en el Ámbito de la Investigación Criminal**. Trabajo Final de Investigación. Turmero: Universidad Bicentenaria de Aragua

Gabaldón, L y Becerra, N. (2008). **Variables asociadas a la consumación y al agotamiento del fraude mediante transferencias bancarias por vía electrónica.** En Capítulo Criminológico. Volumen 36, Nº 2. Venezuela: Universidad del Zulia. Maracaibo. Venezuela.

González Rivas, J. (2001). **El Procedimiento Probatorio**. En Actos del Juez y Prueba Civil. Venezuela: Editorial Jurídica Bolivariana

Ley de Coordinación de Seguridad Ciudadana. (2001). **Gaceta Oficial No. 37.318.** 6 de Noviembre de 2001.

Ley Especial contra los Delitos Informáticos (2001). **Gaceta Oficial No. 37.313,** del 30 de octubre de 2001.

Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo. (2012). **Gaceta Oficial No. 39.912.** 30 de Abril de 2012.

Losano, K. (2010). **Las Teorías y su importancia**. Caracas. Panapo.

Luciani Gutiérrez, J, (2001) La criminalidad informática y la estafa a través de Internet. **Revista de la Facultad de Derecho 57, 506.** Caracas: UCAB

Manzini, V. (1982) **Tratado de Derecho Procesal Penal,** Buenos Aires Argentina Tomo III. Argentina: Ediciones jurídica Europa–América.

Mercado, A. (2011). **El Secuestro Virtual bajo el Enfoque de la Teoría del Delito de Zaffaroni**. Trabajo Final de Investigación. Turmero: Universidad Bicentenaria de Aragua.

Navas, C. (2012). **La Inspección Técnica como Medio de Prueba en el Código Orgánico Procesal Penal en el Estado Apure**. Trabajo Final. Turmero: Universidad Bicentenaria de Aragua

Palencia-Lefler, O. (2011). **90 Técnicas de Comunicación y Relaciones Públicas: Manual de Comunicación Corporativa.** España**:** Profit

Parilli Araujo, O. (1996). **La Prueba y sus Medios Escritos**. Caracas: Mobil-Libros. Caracas.

Peñaranda, H. (2001). **Iuscibernética: Interrelación entre el Derecho y la Informática.** Caracas, Venezuela**:** Fondo Editorial para el Desarrollo de la Educación Superior (FEDES)

Providencia Administrativa. Normas Relativas al Requerimiento de Información en el Servicio de Telefonía Móvil (2005). **No. 152**. Caracas

Rujano, J. (2012). La Validez de la Prueba Electrónica en el Proceso Penal Venezolano. Trabajo Final de Investigación. Turmero: Universidad Bicentenaria de Aragua.

Watchtower Bible and Tract Society (2009). Una Explosión Tecnológica. **Revista ¡Despertad!** (11), 3.

Whitaker, R. (1999). **El Fin de la Privacidad: Cómo la Vigilancia Total se está convirtiendo en Realidad**. Barcelona. España. Paidós.