INTRODUCCIÓN

Las nuevas tecnologías han traído al Universo, grandes cambios, conllevando en su interior la inevitable modernización en todos los aspectos de la vida Ciudadana. Es asombroso, como se observa que en cada momento de la cotidianidad del ser humano, se está sujeto a la Informática, es de esta manera como se ofrece toda la información, convirtiéndola prácticamente en Historial de cada Ciudadano, desde la mínima compra hasta el pago de cualquier servicio, en cualquier establecimiento comercial o cualquier trámite en Oficinas Públicas o Privadas. Desde allí, sin percatarse, se está entregando todos los datos necesarios para controlarlo y en el peor de los casos, ante la tentación, puede utilizarlo en provecho propio o de terceros. Siendo muy común en Venezuela, bajo la excusa Tributaria, la entrega de todos los datos personales en cualquier establecimiento comercial, el uso de tarjetas de crédito o debito, entre otras, es por ello, que el autor ha plasmado, en el presente Trabajo, la necesidad de regular dicha situación, para llegar al respeto y a la buena utilización de tan delicada información.

El mundo está experimentando la ola de cambios más grande luego de la Revolución Industrial, impulsada por tecnologías muy poderosas, ejerciendo cambios desde todo punto de vista, vale decir, en los valores, la cultura, la economía, las legislaciones, en las formas de ejercer el comercio y otros aspectos de la vida y existencia social, todo esto, viene dando un cambio en la civilización misma, como un proceso de globalización, que tiene una fuerza tan poderosa que difícilmente podrá frenarse, a pesar de las dudas sobre su efectividad o confiabilidad, ni mucho menos encerrarse a los cambios, Parafraseando a Down habla que cuando habla que ningún hombre es una isla, viendo que hoy para bien o para mal, ninguna isla es una

isla, llegando a tener formas de comunicarse y hacer cualquier trámite mercantil de manera novedosa e inmediata.

Uno de los principales motivos, tiene su origen en la nueva Revolución denominada Informática, lo cual trae consigo profundas transformaciones en la historia, luego de la Revolución Agrícola y la Industrial, como indica Alvin Toffer [1]

" …más profunda que los cambios anteriores, por dos razones, primero, porque es global y segundo porque es acelerado",

Es decir, la influencia en una transición del modelo económico industrial que rige la humanidad y que crea una nueva Economía Digital y al mismo tiempo, invadiendo el terreno de la Intimidad personal y familiar, a través de la ubicación fácilmente de sus datos personales, en diferentes instancias, como son en las entidades Bancarias, oficinas públicas o privadas, universidades, enumerando las anteriores como ejemplos, convirtiéndose más adelante en algunos casos de uso perjudicial al Derecho del Honor, la Reputación, la intimidad personal, configurándose los Delitos Informáticos, establecidos en su Ley quien junto a la Ley de Mensajes y Firmas Electrónicas, conforman las normas en esta materia , ofreciendo un panorama diferente acerca del fundamento de la necesidad de aplicación de nuevas concepciones jurídicas a la defensa de esos Derechos, creando en sus comienzos una diferencia radical entre Delitos Informáticos y los tradicionales, permitiendo la desaparición del espacio y tiempo, creando una incertidumbre para el Derecho.

_____

1. *ALVIN Toffler. La transformación Mundial y sus Implicaciones para Venezuela*. Caracas. Ponencia ante conindustria.1999, pag.4

Indudablemente, el mundo informático elimina costos, reduce el precio de los productos y los servicios, pero también se deduce que puede cometerse hechos punibles. La diferencia es tan grande que lógicamente cada día tiende a ser más popular y su crecimiento desmedido en los años por venir, siendo esta una de las razones por las cuales las acciones de Internet han subido vertiginosamente, aunado al uso de computadoras, teniendo acceso las veinticuatro (24) horas del día para realizar cualquier tipo de negocio y entregar sus datos a través de registros para su uso.

En tal sentido, los contratos electrónicos o Informáticos, vienen a satisfacer las necesidades actuales, basándose en la economía del futuro, reflejándose el criterio en la actualidad, donde en cualquier entidad bancaria venezolana o extranjera, se observa cómo cada día invierten más recursos para llegar a la consolidación de las bancas on line, realizado contratos, teniendo igualdad de condiciones ante las bondades de la informática en todos los estamentos de la sociedad. De esta manera, otras personas, bajo el manto de la tecnología de punta, va creando nuevas formas de delinquir.

De manera que a medida que se supera la barrera de la inseguridad de las comunicaciones en Internet, van apareciendo las formas de ir configurando el delito en todos su niveles, atacando la dignidad humana, la cual se encuentra protegida constitucionalmente por el Estado, pero a medida que crezca la población, va perdiendo el control sobre ella, optando por la masificación del Internet, de registros con datos personales, organismos como La Superintendencia Nacional Integrada Aduanera y Tributaria (SENIAT), o sencillamente en un supermercado cuando se haga una compra, unido al crecimiento de redes de amigos en Internet, como el Facebook,[2] que estaba llegando en 2011 a los 700 millones de usuarios en

_____
http://www.vuelodigital.com/2011/06/15/facebook-llega-a-los-700-millones-de-usuarios/
consulta: 2012. Enero 20.

todo el mundo. A este paso podríamos decir que para el próximo año Facebook estaría llegando a los mil millones de usuarios.

En este mismo orden de ideas, la dignidad humana constituye no solo la garantía de que la persona no va a ser objeto de ofensas o humillaciones, sino que entraña también la afirmación positiva del pleno desarrollo de la personalidad de cada individuo.

El pleno desarrollo de la personalidad supone, a su vez, de un lado, el reconocimiento de la total autodisponibilidad, sin interferencias o impedimentos externos, de las posibilidades de actuación propias de cada hombre; de otro, la autodeterminación que surge de la libre proyección histórica de la razón humana, antes que de una predeterminación dada por la naturaleza .

De esta manera se implica en la práctica, la indefensión de los atributos o manifestaciones más íntimamente vinculados con la subjetividad. Esto conlleva a la necesidad de reconocer los derechos a la personalidad, como derechos fundamentales, entre otros al honor, a la intimidad y a la propia imagen.

De forma que se encuentra en una encrucijada decisiva para el avance de una herramienta como Internet, pero unido a la desregulación legal, a pesar de los esfuerzos de los Organismos Internacionales, pudiéndose volver la peor amenaza debido al desarrollo de este medio. Al paso de esta fulgurante Revolución han aparecido escándalos públicos relacionados con la violación de seguridad de la confidencialidad de sus datos personales, a través de los “hackers” (piratas informáticos), conllevando esto a establecer sistemas de garantía y seguridad de los datos en los intercambios económicos electrónicos, buscando que se haga difícil el

fraude, teniendo como ejemplo[2]: Visa y Máster Card han suscrito un acuerdo para estudiar un protocolo de seguridad. debido a que MasterCard alertó hoy de una posible violación a la seguridad de uno de sus procesadores de tarjetas de crédito en Estados Unidos, que según un blog especializado afecta también a su competidora Visa y puso en peligro los datos de un total de diez millones de cuentas en este país.

Como se puede notar, la noción del Ciberespacio[3] surge en la practica en referencia a un mundo utópico e irreal, el cual probablemente nadie imaginó que existiría. Por ello se tiene un mundo lleno de redes de computadoras, por las cuales fluye constantemente información, textos, sonidos, datos que se transmiten en segundos y que eliminan las barreras geográficas y jurídicas existentes en el mundo atómico, pero ante esta importancia, nadie tiene la capacidad para negar los cambios vertiginosos en la sociedad como resultado de avance tecnológico y de la Informática, por ello el Derecho de la Personalidad es una de las áreas que más se ve afectada con la llegada del Internet, pues muchas de sus concepciones tradicionales deberán cambiar para adaptarse al nuevo entorno digital, surgiendo grandes interrogantes que tiene que ver con su efectividad, seguridad, fiabilidad, entre otras tantas formas para obtener un marco legal que lo proteja.

El Derecho a la Privacidad implica la imposición de condiciones de respeto y limitaciones en el manejo de Información de Carácter Personal de los ciudadanos. Así mismo implica el Derecho a la Autodeterminación Informática, por medio de la cual los ciudadanos pueden controlar la información que sobre cada uno de ellos, manejan

2.-http://imaginamos-larepublica.com/node/6128 (Consulta: 2012. Abril 25)
3.- http://www.alfa-redi.org/node/9583 (consulta : 2012, Enero , 16)

tanto el Estado, como los particulares, quienes se ven obligados a permitir el acceso a dicha información, así como a corregir, eliminar ó clasificar en sus archivos, todos aquellos datos que se refieran a las personas, acceder a la tutela efectiva de la Administración de Justicia de acuerdo al conocimiento del valor jurídico del derecho a la intimidad y su marco legal.

Por ello se formulan las siguientes interrogantes:

¿Cuál es el marco legal del Derecho de la Intimidad en la sociedad informatizada desde el punto de vista Penal?.

De acuerdo al planteamiento precedente, surgen las siguientes interrogantes:

¿Cuál es el Valor Jurídico del Derecho de la Intimidad?

¿Cuál es el marco legal del Derecho a la Intimidad en la Sociedad Informatizada desde el punto de vista Penal en Venezuela?

Análisis del Valor Jurídico del Derecho de la Intimidad

Marco legal del Derecho a la Intimidad en la Sociedad Informatizada desde el punto de vista Penal en Venezuela.

Esta investigación se puede determinar que por lo novedoso de la Legislación y del tema, el presente trabajo se clasifica como Explorativa - Explicativa, siendo señalado el estudio sobre el tema, con enfoque sobre posiciones teóricas como una modalidad jurídica de lo que se ha investigado,

lo cual las remisiones teóricas y bibliográficas se circunscriben a su aplicación.

Al mismo tiempo, en el Diseño de la Investigación, se puede deducir que se refleja la Investigación en el orden Documental, el cual, ha consistido en el análisis de la información obtenida, fundamentándose en la acumulación jurídica teórica contenida en documentos con énfasis especial en las leyes que rigen la materia como son el Decreto- Ley sobre Manejo de Datos y Firmas Electrónicas, La Constitución de la Republica Bolivariana de Venezuela, concatenado con Textos de importantes autores que han tratado la materia.

En cuanto, a las Técnicas de Recolección de Datos esta investigación se encuentra en la observación documental, el cual, exige la revisión de los principios, Fuentes, citas bibliográficas y parafraseadas, monografías y documentos como las leyes ya señaladas anteriormente, ubicadas a través de Internet y textos, entre los más importantes, que tienen que ver con la aplicación de la Ley y de su jurisdicción. Introduciendo en primer término las técnicas relacionadas con el análisis documental, en segundo lugar con las técnicas operacionales que van a garantizar el procesamiento de datos.

En las Técnicas de Procesamiento de Datos, con base a la técnica de observación documental, se realiza el análisis del problema y se procesan las técnicas de observación documental con miras a extraer todos los datos para analizar y profundizar la temática, extraer de las fuentes por medio de lecturas , llegando al resumen , desarrollando el aporte que ofrece desde su punto de vista el autor, logrando así la ilustración en la Investigación, donde el cual, lleva la idea principal de lo general a lo particular, tomando al igual la Inducción.

CAPÍTULO I

ANÁLISIS DEL VALOR JURÍDICO DEL DERECHO A LA INTIMIDAD

El valor jurídico de las normas radica en el espíritu del Legislador y lógicamente, su puesta en practica amerita que se configure una serie de comportamientos, debido a la novedad de la normativa , aunque el tema se haya tratado desde hace varios años atrás y las leyes que rigen la materia en Venezuela tengan su aprobación dentro de los últimos diez o doce (10 - 12) años, es posible, que por tener una población, hasta cierto punto conservadora en su comportamiento y en común a toda sociedad resistente a los cambios, se ha ido aplazando su puesta en practica.

En tal sentido, se tendría que desglosar el termino Derecho a la Intimidad, recordando al derecho como una ciencia social que busca regular una vida sana en sociedad y por otra parte, una Intimidad , que es propia de los seres humanos , seria hablar de su yo interno, de lo mas preciado como son sus valores , los principios que guían su vida, su sentir; existe intimidad cuando se habla de una relación sexual o cuando se habla de un comportamiento de si mismo , de la intimidad de su ser , por ello puede deducirse de manera practica y coloquial que el Derecho a la Intimidad , se acerca a pensar en el derecho que tienen los ciudadanos a mantener bajo su reserva su comportamiento interno, sus actividades o sus practicas de acuerdo a sus principios y valores , es decir , mantener protegida y bajo su mas absoluta reserva su vida personal, su propia identidad, Por ello, M. Iraburu[4], al escribir sobre el Derecho a la Intimidad lo señala de la siguiente manera :

"Es como si cada persona dispusiera de un velo con el que poder

---

4.-M.Iraburu. http://www.cfnavarra.es/salud/anales/textos/vol29/sup3/suple6a.html
Consulta : 2012, Enero 20

ocultar -de su ser y de su hacer- lo que no quiere mostrar a los demás. Todo aquello que decida velar formará parte de su intimidad y sólo él podrá desvelar lo que quiera y a quien quiera. Por tanto, cada adulto tiene derecho a definir el contenido y los límites de su intimidad. Así, hay datos personales -ideas políticas, creencias, hábitos sexuales- que todos entenderíamos que forman parte de esta esfera, pero hay otras informaciones que unas personas pueden considerarlas reservadas y otras personas, no."

Ahora bien, a lo largo del avance de la tecnología concatenado con el derecho, han plasmado la idea de tener que diferenciar entre Intimidad y Privacidad, planteándose una posible confusión en los términos, que debe aclararse para lograr la protección de los derechos tal como lo refleja Flor Ávila, Katia Castaldo, Anthony Urdaneta [5]:

"El derecho a la intimidad protege la parte más íntima de una persona, esto es, esa esfera personal que define qué es y qué no es privado, dicho de otra forma, hablar de intimidad es hablar de sentimientos, de creencias (políticas, religiosas), pensamientos o de una información, o la relativa a la vida sexual, cuya difusión puede producir ciertas reservas al individuo. Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente.

La privacidad, sin embargo, es un término más amplio: se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por sí misma puede no ser relevante, pero que

_____

5.-Flor Ávila, Katia Castaldo, Anthony Urdaneta *Los derechos humanos a la intimidad y a la privacidad en Venezuela y en el Derecho comparado.* Revista Telemática de Filosofía del Derecho, nº 11, 2007/2008, pp. 314.

analizada en un momento o contexto concretos puede llevarnos a la construcción de un perfil muy fiable del individuo que permita su caracterización e identificación".

Desde este punto de vista, se puede deducir que la relación entre Intimidad y Privacidad , aunque pueden ir estrechas , no pueden mezclarse, "la Intimidad" debe concebirse como lo que corresponde a los sentimientos , a sus creencias y "la Privacidad" puede permitir su identificación y su caracterización , basándose en la información que se obtenga de la persona , formándose su propio perfil y llegando a su pleno conocimiento.

Guillermo Cabanellas[6], por su parte, en su diccionario enciclopédico de derecho usual, reseña al Derecho a la Dignidad Humana como:

"El que tiene un hombre para que se le recononozca como ser dotado de un fin propio, y no cual simple medio para fines de otros"

En este aspecto, el Derecho a la Intimidad, tiene que tratarse como base fundamental el Derecho a la Dignidad de cada Ciudadano , tal como lo trata Cabanellas, donde el hombre debe tener su propia identidad, debe contar con sus propios fines , su propia personalidad que le permita mantenerse con un fin propio , objeto de derechos fundamentales en su accionar. El derecho a la dignidad humana conlleva a la exigibilidad de ser respetado y al mismo tiempo protegido, y es a traves del Estado , de sus instituciones que debe velar por garantizar la protección a estos derechos .

Al mismo tiempo, Flor Ávila, Katia Castaldo, y Anthony Urdaneta [7], soportan sus afirmaciones, en lo señalado por Eusebio Fernández:

"El concepto de dignidad humana gira en torno a que cada uno de los seres humanos tiene un valor moral especial, que ha de ser reconocido y garantizado por las leyes y que significa, al mismo tiempo, el derecho a tener unos derechos básicos e inviolables."

Dentro del reconocimiento y respeto a la dignidad humana, debe sujetarse a "…un valor moral especial…" donde las leyes debe jugar un papel muy importante, a fin de protegerlas, basándose en su propia normativa con derechos mínimos y con la figura protectiva del mismo. Es así, como los ciudadanos dentro de su propia personalidad cultivan su yo interno, a través de la moral, de lo que ellos pueden llamar como su dignidad, lo cual transita por diversas concepciones hasta llegar al plano de la Intimidad.

En el campo de la moral, ha sido mucho lo que se ha hablado sobre cual es la moral que debe ser respetada y protegida, siendo un concepto que difícilmente pueda enumerarse por su propia dimensión personal, incluso Guillermo Cabanellas[8], habla del Derecho a la Integridad Moral, pero con lo difícil de su origen, lo señala:

"… menos concreto que el anterior y parónimo, se revela este derecho, por resultar siempre lo abstracto de encuadramiento legal o jurídico mas difícil, por su propia naturaleza"

Por ello, la legislación establece el cumplimiento de derechos básicos que engloban toda la materia, como son el derecho a la dignidad, el derecho a la intimidad, entre otras, pero que en todo caso vienen a

_____

7.-Flor Ávila, Katia Castaldo, Anthony Urdaneta *Los derechos humanos a la intimidad y a la privacidad en Venezuela y en el Derecho comparado.* ob. cit. pp. 314.

8.- Guillermo Cabanellas, Diccionario Enciclopédica de Derecho Usual, Tomo II, ob. cit. p.569

dejar establecido el cumplimiento y protección de los derechos de acuerdo a las condiciones mínimas de convivencia en una sociedad.

En el mismo orden e ideas, se resalta que los derechos a la Intimidad , han sido tratados desde los inicios del Derecho , pero en la sociedad actual , con la llegada de la Revolución Informática y las exigencias de exponer los datos personales por razones de contratos o servicios , unido al crecimiento de la Población, aparición de nuevas tecnologías de información, viene a tomar mayor auge su aplicación y porque cada día se presentan mayores situaciones que ameritan la protección de la intimidad personal y mayor facilidad para obtener datos personales que luego pueden ser tentativamente usados como figuras delictivas.

Cuando se habla de la Intimidad personal, de manera coloquial, siempre se inclina hacia comportamientos de pareja, de amigos o amigas , con la familia pero la realidad es que la Intimidad personal abarca otros campos de la dignidad humana , como es usar la información de cada quien para convertirlo en instrumento de presión o lucrativo y de acuerdo a la actividad que ejerza , captando información bajo figuras legales que de manera disimulada violan la intimidad de los ciudadanos, entregando sus datos personales y comportamientos , solo confiando en la lealtad de quien recibe la información y casos mas graves como la información que se entrega bajo una condición de confidencialidad, como las historias medicas, datos al servicio bancario, tarjetas de uso bancario , universidades y/o cualquier tipo de servicio.

Por tal motivo, se coincide con Guillermo Cabanellas[9] cuando afirma:

_____

9.- Guillermo Cabanellas, Diccionario Enciclopédica de Derecho Usual, Tomo II, ob. cit. p.569

".. el derecho a la intimidad se pretende que la vida de cada cual, a menos de espontaneas revelaciones propias, resulte tan impenetrable como el fuero de la conciencia."

Este concepto viene a ser mas amplio, Es decir, el derecho a la intimidad es todo lo que conserve como su vida , lo tenga para si, lo tenga como su propia personalidad y bajo ningún concepto , la persona se encargue de divulgarlo a sus amigos o públicamente , partiendo de allí, la configuración del delito o no .

Por otra parte, en cuanto a la valoración, es necesario saber que el derecho a la intimidad, se inicia cuando el ciudadano resguarda sus datos personales, cuando conserva para si mismo su actividad personal, pero, en la actualidad, se presenta las nuevas tecnologías, la informática abre las puertas de la intimidad y se refleja el mayor auge de la violación al derecho a la intimidad personal, derechos estos, que habían sido especial y cuidadosamente protegidos por los ciudadanos.

Con las puertas abiertas a la informática, también se abre las de la intimidad y de manera legal , se comienza por registrarse[10] en redes sociales y con ese fin, entregan datos personales, signos, trabajo, vehículos, viajes, hoteles, redes sociales, contactos con personas extrañas a la vida cotidiana, porque no solo se busca al amigo ya conocido, se aportan datos personales que capte amigos o amigas extrañas a sus alrededores, con la finalidad que se quiera, incluso los links , dan la opción , si es para fines de diferente naturaleza, de parejas, de trabajo, sexuales, de negocio, amigos o amigas.

De esta forma, se puede observar que la situación sobre el derecho a

_____

10.- http://www.myspace.com. (consulta 2012. Abril 24)

la Intimidad , en la practica se presenta el termino de la naturalidad en el suministro de información, pierde el derecho a la intimidad, pero también es cierto que en las redes en su mayoría los usuarios suministran datos personales, por ejemplo: los servicios bancarios, en algunos casos, que empleados usando los datos personales para terceras personas, presuntamente con fines lucrativos por empresas llamadas fantasmas, al recibir las llamadas, si entregas los números de tarjetas , bajo la ingenuidad y del engaño para supuestas empresas dependientes del banco, al ejercer el reclamo , se toma que allí, predominó la espontaneidad de suministro y por lo tanto , el reclamo es declarado sin lugar , quedando el usuario con la deuda por el monto de la operación.

Por ello, es tan importante, la valoración Jurídica del derecho a la intimidad, donde la información juega un papel preponderante , debido a lo celoso que debe ser el ciudadano y en muchos casos tener conocimientos de dicha materia para que actúe en defensa de sus derechos y proteja su intimidad personal y de su familia.

Esto es, valorando su propia intimidad, resguardando su propia familia de terceras personas, inicia la valoración jurídica del derecho a la intimidad de los hechos tentativos de punibilidad, a que se esta expuesto por las “bondades” informáticas y por las “gentiles” entregas de datos en cada servicio que requiere un usuario en todos los niveles y en todas las circunstancias. Naciendo la legislación para dirimir estas situaciones y ejercer la prevención de esas conductas y castigar otras, que de acuerdo al estado se configuran como hechos punibles.

En la materia, se presenta un criterio sobre los bienes jurídicos a ser tutelados penalmente como derechos de cada persona, tal como lo expone Fernando Fernandez[11] :

- “Libertad, seguridad, confidencialidad e intimidad de las telecomunicaciones y de la información que circula en la red.

- La confianza mutua y la seguridad del cumplimiento de las transacciones y comercio electrónico.

- El espacio cibernético, considerado como un bien cultural, educativo y comercial.

- El acceso al conocimiento, como una forma de desarrollo de la personalidad.

- El libre acceso y uso de la Internet, como parte de la política prioritaria del Estado venezolano para el desarrollo cultural, social y político de Venezuela (Decreto 825 del Ejecutivo Nacional).

- Seguridad y defensa del Estado. “

De lo antes expuesto, se puede deducir que los bienes jurídicos tutelados penalmente , no puede estar ajenos a la protección de derechos como la libertad , la seguridad, la intimidad y la confidencialidad, aunado a la confianza que debe gozar el usuario de un negocio jurídico por internet o el interés que simplemente lleva para incorporarse en alguna red social,

aspirando a tener la seguridad debida, de acuerdo a la confianza mutua entre las partes y resguardando el espacio cibernético, tambien es protegido el libre acceso.

Lo que sucede es que el Derecho a la intimidad, es muy amplio y se transcurre por toda una actividad diversa, desde la libertad con que debe disfrutar el ser humano, pasando por las labores informáticas.

El auge de la actividad Informática , dentro del marco de respeto a derechos, se perfila como una figura que es amplia y fervorosa , unida a la libertad de uso de las tecnologías de la información, porque su evolución tan violenta ,nadie esperó que con el tiempo fuese a convertirse en la necesidad de la sociedad, viéndose como un fenómeno, donde la información hace referencia por su propio dinamismo a diversas innovaciones.

Se percibe a diario, la influencia del avance de las tecnologías de la información es de tanta importancia que se estima que en los años venideros, la mayor parte de los ciudadanos tendrán una actividad relacionada o dependiente de la Informática y su modernización, con sistemas cada día más exactos, más cómodos, pero con mayores incidencias.

Esto trajo como consecuencia , un crecimiento vertiginoso , no solo en producción de equipos , sino también en tecnología , donde mientras salía al mercado un modelo , ya estaba otro modelo esperando turno para ser presentado, comienza las bases de datos , procesando en tiempo record y almacenando y distribuyendo en una sola red toda la información y traspasando la misma , incluso a nivel internacional, afectándose los

_____

11. http:www.veneconomy.com/site/files/artículos/artEsp174_7 PDF (consulta 2012. Abril 16)

Derechos Humanos de manera visible, por la forma desmedida de su operatividad.

De allí, se pasa a presentarse nuevos peligros a toda la administración, tanto publica como privada, porque en años anteriores se mantenían o se conservaba la información de manera manual , bajo la custodia de una sola persona , en muchos casos, los libros de administración o de contabilidad , era a través de un libro, es decir la información sobre el movimiento de la empresa era de uso personal , los datos de las personas o nominas eran también manuales , creándose así amenazas directas sobre los derechos de cada uno y de manera individual , por el hecho de recibir un servicio, un estacionamiento , no era necesario entregar toda la información de sus datos personales a un desconocido , donde se entrega hasta el números telefónico, dirección, correo electrónico y por otra parte, se presenta la amenaza latente de la perdida de la información por un virus o un pirata informático que acabe con el soporte o se apropie de la base de datos con otros fines , los modifique y los manipule. De hecho se viene observando casos donde los bancos de datos personales son vendidos en su totalidad para preparar hechos punibles y estimular al delito, incluso desde los propios centros penitenciarios.

Al tratar la Intimidad, es lógico pensar en las amenazas a la privacidad y en el sin numero de actividades o comportamientos que conjugan la intimidad y que viéndola desde un punto de vista cotidiano no representan ningún peligro. Ahora bien, la amenaza se consolida cuando sin tener la previsión y en un mundo invadido por la inseguridad personal, donde todo es posible para obtener provecho económico y mezclando la necesidad de un servicio, se lesiona directamente a los individuos, porque allí, se pueden obtener informaciones sobre enfermedades, sobre

comportamientos confidenciales, su vida en pareja, uso de las tarjetas de crédito o debito, cuentas bancarias, etc.

Los nuevos tiempos tecnológicos conllevan al peligro incluso , solo para optar un empleo,, entregando un resumen curricular , haciéndose un perfil del candidato , con dos vertientes : 1.- que se usan en contra del aspirante y 2.- el aspirante no sea sincero en su resumen y sea preparado para entrar al puesto de trabajo con otros fines , exponiendo la dignidad humana por datos contenidos y entregados de buena fe en el primer caso, causándoles ofensas, violando toda normativa constitucional de la intimidad personal , de honor y de su propia imagen.

El avance tecnológico tiene en su espíritu, que llega a ser el conductor de ventajas o desventajas, tomando en cuenta que es producto del ingenio humano y cada día, surgen nuevas circunstancias que obligan a buscar otras vías de garantías a la practica informática y al uso de los datos personales con seguridad y respeto de los Derechos Humanos como parte de la globalización , en la búsqueda de soluciones y protección a los problemas que emergen de la actividad informática.

En los últimos años se observa el auge de la implantación y protección al Derecho a la Intimidad, por ser una garantía que debe protegerse de manera especial por el continuo avance tecnológico y sus incidencias. En este campo, es oportuno que se desarrolle esta protección, se analice las razones , sus amenazas y las vías que tiene para que sea realmente garantizada el respeto a la dignidad humana , a sus principios y valores como sinónimo de libertad , como lo mas preciado de la vida democrática.

No es fácil, en el caso de la actividad informática, hacer comprender a quienes tienen el ingenio humano, de preparar los sistemas, las bases de

datos, de ir estudiando cual será el próximo paso en el avance tecnológico, de que al mismo tiempo, que se crea una nueva modalidad, también debe instalarse una modalidad de seguridad a la privacidad, a la intimidad , corriendo el riesgo que con el pasar de los años , la tecnología se obtenga el rechazo de los usuarios por las violaciones permanentes a las personas y a las empresas.

En el ciberespacio no basta con colocar un aviso que recomiende a los usuarios y operadores, de adecuarse a sus normas, evitando la divulgación de textos e imágenes, incluso de textos que confunden criterios de doctrina en todas las materias y áreas, por la plena y excesiva libertad de publicación, incluso, recientemente, en clara violación al derecho a la intimidad se publicó , el libro que hablaba de la historia médica y política Ex-Presidente de la República Francesa, François Mitterrand, libro titulado “Le Grand secret”, estuvo disponible en Internet sólo unos días, siendo prohibida su venta en librerías, debido a la violación de los derechos de autor y de propiedad intelectual[12].

Ahora bien, pero estos casos previos, conlleva a nueva discusión, como es la separación que debe existir entre el derecho a la intimidad y la libertad de expresión como valor democrático. En una sociedad como la actual es difícil mantener o comenzar a restringir las libertades y derechos ya obtenidos sin que pueda acusarse de que el Derecho a la dignidad humana , el derecho a la intimidad, al honor y a la reputación van a limitar a las libertades adquiridas como es la libertad de expresión.

Estos derechos son enunciación fiel de las tecnologías de información en un mundo globalizado, donde esta interconectado y en cuestión de segundos una noticia puede dar la vuelta al mundo , aún con controles de paginas , como es el caso de Túnez y Egipto[13], donde

recientemente, fue la vía de comunicación para convocar al pueblo, para hacer marchas y protestas contra el Gobierno y a pesar del bloqueo de internet, la empresa proveedora pudo difundir las informaciones interna e internacionalmente.

Siendo en este caso, de beneficio pero también se presentan casos contrarios, donde son usados para perjudicar a una persona o alguna institución, partiendo de allí, el estudio a cada caso en particular, pero imponiéndose la libertad de expresión.

La empresas de internet, aparentemente y por logica, se dedican a producir, nuevas y mejores técnicas de información, pero se observa poco interés por los problemas que puedan presentarse, en un mundo sin fronteras y sin la menor orientación de protección y respeto por los derechos a la intimidad o a la dignidad humana, a la privacidad en cualquier parte del mundo donde llega la señal de internet, sin importar los derechos fundamentales y universales.

En este caso, lo único es suministrar la tecnología y que cada persona se preocupe por su seguridad, incluso hay empresas especializadas en el espionaje tecnológico y extraen información, interceptan correos electrónicos como intervenir cualquier teléfono y posteriormente publican toda la información, en casos por vías de intereses empresariales, gobiernos, bolsa bursátil y en fin, toda clase de provecho económico.

Por otra parte, se deja que se viole constantemente los derechos fundamentales por parte de las empresas proveedoras de internet pero

---

12- Cinta Castillo Jimenez. Prooteccion del derecho a la intimidad y uso de las nuevas tecnologías de la información. Sevilla. España. Pag.5

13.- http://www.ticbeat.com/socialmedia/redes-sociales-vehiculo-revoluciones-reportaje/ *(consuilta 2012, abril 20)*

cuando se trata de comunicaciones entre particulares, se llega al extremo, porque están sujetos a sanciones penales que castigan severamente dichas violaciones

En ese proceso de progreso constante y de estudio sobre la materia, a lo largo del paso de los años y de las diversas situaciones , la influencia practica han venido ampliándose, como producto de la constante lucha de defensores de derechos humanos , de estudiosos de la materia , en su afán por adaptar a las nuevas exigencias y a los nuevos tiempos el proceso informático, aunado a las nuevas exigencias de leyes tributarias, haciéndose mas prudente por parte del legislador , llevándolo al rango constitucional, ofreciendo un soporte real a la norma Penal.

La aplicación efectiva de las normas de carácter administrativas en materia de Certificación, lógicamente que conlleva a una garantía y cumplimiento fiel a los derechos de la personalidad, a esa intimidad personal, dentro de un mundo informatizado y que en cada momento de la vida, el ciudadano se ve obligado a aportar sus datos personales, como un requerimiento en materia tributaria para quien ofrezca bienes y servicios. Por ello, el usuario no tiene la discrecionalidad de aportar sus datos o no, de escoger en quien confía sus datos personales, en caso contrario, no puede tener el servicio, como es el caso de la vida cotidiana en un estacionamiento, en cualquier venta de alimentos, bancos, supermercados y en fin en toda actividad con la finalidad de obtener un servicio.

En el mismo orden de ideas, sucede con las famosas redes sociales de hoy, pero con la diferencia que en la practica, el usuario tiene la discreción de ingresar a estas redes como Myspace, Faceboock, twitter entre otras y es el usuario quien determina con quien trata, que datos personales aporta, que

información ofrece y que grado de privacidad o seguridad escoge. Pero también se presenta la publicación por otro usuario de datos personales ajenos, fotografías, comentarios o diferentes publicaciones. En este campo la empresa proveedora del servicio no publica, nada que oriente, solo, es discrecional y personal como quiera el usuario tratar su permanencia y su seguridad.

Si existiera una verdadera difusión se observaría una reducción drástica en los delitos informáticos, dándose apertura a un clima de seguridad legal a la hora de realizar cualquier contrato, tomando en consideración que en la actualidad, en algunos casos, hay necesidad de realizarlos por la vía de la Informática, es decir no hay otra manera para hacerlos, unido al crecimiento de la población, buscando menores costos operativos y al mismo tiempo, poder ofrecer un mejor servicio, pero, para lograrlo, se necesita claridad, confianza en las transacciones, privacidad, seguridad, y hoy no se cuenta con ese especial requisito, aún cuando se sigue profundizando en los mismos, se hace en forma masiva diversas negociaciones con la incertidumbre de las consecuencias que puedan acarrear para el consumidor, en este caso.

De esta manera se puede señalar, que existen dos variantes por parte del Estado, o no tiene la voluntad de adaptar a los nuevos tiempos, por medio del marco legal, el cual permita una navegación internauta segura, para hacer negocios y puedan respetarse los derechos fundamentales y no ser utilizados sus datos aportados por esta vía para manejos delictuales, o simplemente no tiene los medios idóneos para hacer que se respete la intimidad de sus ciudadanos.

Nadie ignora que el estado social y democrático de este tiempo precisa para su normal funcionamiento de un cúmulo de informaciones como

la planificación económica, la política tributaria, la atención médica la seguridad social y la persecución de las actividades delictivas son hoy tareas irrealizables sin la ayuda de un amplio aparato informativo. Es preocupación de los usuarios que existen los medios para que su formación escolar y universitaria, sus operaciones financieras, su trayectoria profesional, sus hábitos de vida, sus viajes, su recreación, su historia clínica, o hasta sus creencias religiosas o políticas, se hallen registrados en archivos susceptibles de incorporarse a una red general. Pero es el estado quien recoge mayor información a través de las declaraciones de impuestos y lógicamente nace la preocupación sobre su la intimidad de su vida.

Ante esta realidad el Código Penal, tipifica los tipos delictuales, pero no los enumera sobre una base en materia informática, adicionándole solo las características de los mismos, siempre y cuando sean cometidos y se configure cualquier delito bajo el uso o artificio, dejando allí la posibilidad del uso de la informática para ser reputado como delito. Haciéndose necesaria la posibilidad de legislar sobre la materia para obtener mayor seguridad sobre las actividades y no se penetre en intimidad y en la vida cotidiana del individuo.

La Sociedad informatizada se ha reflejado como la invasión de la Intimidad personal en los nuevos tiempos, con la exclusiva diferencia del medio con el cual se puede realizar, como es a través de la Informática, pero en todo caso se estaría configurando la figura de la violación de la intimidad, a través de prácticas informáticas sin el consentimiento de sus titulares, es decir que el solo hecho de usar la Informática, puede tener esa configuración de delito.

Pérez Luño[14] analiza la intimidad personal de la siguiente manera:

Lo relaciona con la relevancia hermenéutica del Principio *"IN DUBIO PRO LIBÉRTAE"*, porque se alude directamente en términos generales a favor de las Libertades del Ciudadano, traduciéndose en posiciones hermenéuticas de orientación conservadora o progresista de la normativa constitucional. Esto implica la adecuación y el reemplazo de la interpretación estática y defensiva de dicho Principio, por su caracterización positiva y dinámica, otorgándole un plano unitario a los Derechos y Libertades fundamentales del Ciudadano **.**

Estrictamente interpretar el sentir y el sentido de los derechos fundamentales, llevándolos a un plano mas personal, mas directo al ciudadano a fin de que pueda ejercer su protección con mayor efectividad y ajustándose a los nuevos tiempos. Es decir, utilizar las nuevas tecnologías y la dinámica de su orientación para llevarla a un sentido mas directo, dejando de ser simplemente un derecho.

De lo antes descrito, se deduce que debe insistirse en las cuestiones sobre las que se cimienta la disciplina jurídica de la intimidad, porque han perdido su exclusividad de ser individual y personal, para asumir progresivamente, de acuerdo a la vida diaria, una significación pública y colectiva. El problema del suministro de datos personales a la administración es lógico que atañe a los individuos, pero también a toda la sociedad.

En Venezuela, se tiene rango Constitucional, tal como aparece en la Constitución de la República Bolivariana de Venezuela:

> Artículo 60. Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen,

_____

9. Pérez Luño. *Derechos Humanos, Estado de Derecho y Constitución*. Editorial Tecno. Madrid. España 2003

> confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

Se observa que en Venezuela, el tema en especifico no se ha desarrollado lo suficientemente, incluso solo ha limitado a hacer enunciados de derechos que tiene el ciudadano como humanos y fundamentales, tal como lo establece el artículo 28 ejusdem:

> Artículo 28. Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.

Ante la situación planteada, es bueno señalar como complemento que la Legislación Venezolana está en mora con el desarrollo de la normativa sobre la materia, la única Ley consagrada a tal efecto es la Ley sobre

Mensaje de datos y Firmas electrónicas, el cual regirá de la siguiente manera:

> Artículo 1. 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.
>
> El presente Decreto-Ley 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.
>
> La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

La doctrina en su análisis ha determinado que el manejo electrónico debe cumplir con una serie de requisitos sirviendo de base para la consolidación del Comercio Electrónico y la vida informatizada que pueda disponer de una serie de principios propios que le han sido formulados, para

la armonización y el desarrollo legal de la actividad, dada su trascendencia, expresa Mariliana Rico[15]:

1) La Equivalencia Funcional, el cual permite ampliar a los mensajes de datos un principio de no discriminación respecto de las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas, de este modo, los efectos jurídicos deseados por el emisor se producirán con independencia del soporte donde conste la declaración. En Venezuela es reconocido este principio, otorgándole el valor jurídico de los mensajes de datos como toda información inteligible en formato electrónico que pueda ser almacenada o intercambiada por cualquier medio.

2) El Principio de la Neutralidad Tecnológica, se basa en el respeto al uso de cualquier tecnología que se utilice o pueda usarse en el futuro a efectos de transmitir un mensaje de datos o insertar una firma electrónica, por lo tanto implica no favorecer unas tecnologías sobre otras con la finalidad de evitar posibles obsolescencias legales. En este caso hay que resaltar el hecho que en Venezuela por respeto a este principio está contemplado en la Ley, en contraposición con otros países como en Colombia, Argentina, Puerto Rico, Chile y Costa Rica.

3) El Principio de la Inalteración del Derecho Preexistente de Obligaciones y Contratos. Según este principio, los elementos esenciales del negocio jurídico no deben modificarse cuando el contrato se perfecciona por vía electrónica, ya que se trata de un medio de representación de la voluntad negocial.

_____
15. Mariliana Rico Comercio Electrónico Internet y Derecho. Editorial Legis Colombia, 2005. Pág. 66

4) El Principio de la Buena Fe. Éste se toma como una consecuencia del Principio de la Inalteración del Derecho Preexistente de obligaciones y Contratos, donde priva la buena fe en la interpretación de los acuerdos contractuales. Es en este Principio donde reside toda la actividad, de importancia superior para poder llegar a negocios y contratos claros y transparentes, así como el cumplimiento de los mismos.

5) El Principio de la Libertad Contractual, ya analizado anteriormente cuando se refería a la Autonomía de la Voluntad de las Partes, lo cual traduce en la escogencia del medio empleado para ejercer su fin y por la otra, la libertad para incorporar las cláusulas que crea conveniente .

En esta materia, se trata de adaptar a las nuevas exigencias de continuar con la actividad económica a través del mundo informático, resguardando sus datos y al mismo tiempo, tratando de tener seguridad en el desarrollo de esas relaciones comerciales y personales; de allí parte la idea anterior sobre los principios que deben considerarse en el momento de establecer una relación por vía informática.

Teniendo la necesidad de que el sistema de almacenamiento de datos o intercambio de los mismos , sean con plena libertad y consentimiento, para que tenga su justa valoración, bajo la discrecionalidad de utilizar los equipos tecnológicos que crea conveniente, no existe limitación en cuanto el medio que use , otorgándole plena validez a la suscripción de contratos por esta vía , porque el hecho de manifestar su consentimiento, eso es lo importante, con un principio de buena fe , tal como lo establece cualquier contrato , que exista la buena intención de realizar un contrato o un intercambio de datos, con la premisa de la plena libertad con que se actúa; en todos los contratos , lo mas importante es la libertad del ciudadano para ejercer y escoger la vía mas adecuada para lograr dentro del marco legal una relación contractual o

en todo caso, personal con intercambio de datos . De esta manera, se coincide con la espontaneidad del comportamiento bajo un clima de buena fe.

Mariliana Rico[16] refleja que También debe señalarse, para que pueda ser reconocido o aceptado el documento electrónico como medio de prueba, es necesario que cumpla con una serie de requisitos:

1) La calidad de los sistemas utilizados, incluyendo el Hardware y el Software.

2) Veracidad de la información.

3) La conservación del mensaje y la posibilidad de recuperación.

4) Su legibilidad.

5) La posibilidad de identificación de los sujetos participantes y las operaciones realizadas por cada uno de ellos en el proceso de elaboración del documento.

6) La atribución a una persona determinada en calidad de autor.

7) La fiabilidad de los sistemas utilizados para la autenticación del documento.

Mucho se ha tratado de lograr la garantía y la seguridad que pueda ser

16. Mariliana Rico Comercio Electrónico Internet y Derecho. Op.cit.pp 103

traducida en valoración jurídica del derecho a la intimidad y a todo lo que significa dignidad humana, siendo las relaciones comerciales las mas delicadas por los riesgos que debe asumir quienes se inclinan o por razones de territorio acuden a esta vía para hacer contratos , con la previsión de que pueda en el futuro inmediato , ante una circunstancia de incumplimiento o de fraude , pueda reclamar sus derechos , por eso , debe contar con la calidad de los sistemas utilizados.

En este momento existe en Venezuela la Superintendencia de certificación electrónica y esta en capacidad de ofrecer ese servicio para ofrecer seguridad en la comunicación; debe tener la seguridad que la información es real , que su procedencia sea verdadera , con la previsión de que los mensajes intercambiados tenga la seguridad de ser conservados y en aquellos casos que por razones técnicas puedan verse afectados, tenga la oportunidad de recuperarlos en su totalidad para ser interpuesto como prueba en un momento determinado .

En ese mismo orden de ideas, los mensajes o contratos deben tener la claridad de fácil interpretación, deben ser legibles, a fin de que nadie pueda verse perjudicado por las deficiencias en su contenido por no lograr determinar las condiciones contractuales , que su letra y su contenido sea claro, donde se pueda identificar a los participantes con normalidad, saber con quien se hace un negocio o con quien trato.

Quedando la constancia de los intercambios de información y quedando, en forma transparente con quien trata y con quien asume su rol como autor, como responsable de dichas informaciones o compromisos que puedan adquirirse por esta vía y finalmente luego de cumplir con lo indicado , tener la confianza real de los medios que utilizará para autenticar dicho documento, como resultado de toda un intercambio o negociación .

En todos los negocios o intercambios radica la libertad plena y la seguridad con que se actúa, a fin de que no tenga una perdida o fraude en su actividad, sin obtener los medios probatorios que respalde su posible acusación para que sea reparado el daño causado.

Mariliana Rico[17] agrega:

"Una vez establecida la posibilidad de admisión del documento electrónico en el proceso, el segundo problema a resolver viene determinado por la forma cómo se va a incorporar este nuevo medio probatorio a las actuaciones judiciales. En este caso la propia Ley de Mensajes de Datos y Firmas Electrónicas (LMDFE) nos remite al sistema de promoción de pruebas libres de acuerdo al Código de Procedimiento Civil, el cual los mensajes de datos deben promoverse como prueba documental, sin perjuicio, si lo creen conveniente se solicite la asistencia de una experticia para tal fin, a fin de ofrecer la seguridad requerida."

La legislación Venezolana remite de acuerdo con la Ley de Mensajes de Datos y Firmas Electrónicas (LMDFE) al código de procedimiento civil para incorporar las pruebas como documentales al juicio, siendo en este campo mas realista , porque la via procesal civil se condensa en este código, siendo mas expedita su aplicación sin buscar interpretaciones a posibles lagunas jurídicas.

En la producción de medios electrónicos como aportación de pruebas, Rodrigo Rivera Morales,[18] señala:

---

17. Mariliana Rico Comercio Electrónico Internet y Derecho. Op.cit.pp 104

18. Rodrigo Rivera Morales .Actividad probatoria y valoración racional de la prueba, 2010. Pág. 384

“Entonces desde el punto de vista procesal, pensamos que los medios informáticos pueden ser considerados como: a) fuente de prueba dado que contienen dentro de ellos información o datos; b) como medio de prueba en cuyo caso es un mecanismo o instrumento que sirve para introducción en el proceso de las fuentes de prueba y c) como objeto de prueba .“

Desde este punto de vista probatorio, se aclara sobre el sentido real y de su valoración jurídica y especialmente Procesal, por lo novedoso de los temas informáticos dentro del mundo jurídico, debido a que mientras sean instrumentos que contengan información que puedan aportar al proceso y a la pretensión, deben ser tomados en consideración en el momento de aportación de pruebas, obteniendo todo el valor jurídico y eficacia probatoria.

En materia de Derechos Humanos, la Declaración Universal de Derechos del Hombre’ de 10 de Diciembre de 1948, la Asamblea de la ONU, en su discusión, estatuye en su artículo 12, el Derecho a la intimidad personal y familiar como un Derecho Fundamental del Hombre**.**

El Convenio para la protección de los Derechos Humanos y las Libertades fundamentales de Roma, llamado Convenio de Roma de 1950

Es bien sabido que la protección de los derechos humanos es la resultante de la unión de los países aglutinados en diferentes organizaciones mundiales como la Organización de las Naciones Unidas , observándose, tanto en Latinoamérica como en Europa o Asia. Incorporando una referencia importante sobre el presente convenio expresado por Libardo Riascos G.[19]:

"Los Estados miembros del Consejo de Europa, de aquélla época, tras la Declaratoria Universal de los Derechos Humanos, creyeron conveniente asegurar el reconocimiento y aplicación efectivos de los derechos proclamas por la Asamblea General de las Naciones Unidas el 10 de Diciembre de 1948, a fin de afianzar las bases mismas de la justicia y de la paz en el mundo. Para fortalecer hacia el futuro estos ideales, el Consejo de Europa, acordó la emisión del Convenio de protección de Derechos Humanos y libertades fundamentales, actualmente conocido como *Convenio de Roma de 1950,* y el cual tardíamente fue ratificado por España, mediante instrumento de 26 de Octubre de 1979."

El Convenio en su Artículo 8, establece lo siguiente:

Artículo 8:

> Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

19.-Libardo Riascos G. *Derecho a la intimidad, la visión iusinformatica y el delito de los datos personales.Lleida. España*. 1999. p.48-63.

En este orden de ideas, los derechos humanos , como nivel de afecto a la dignidad humana , han ido creciendo y se observa que al transcurrir de los años , se ha ido perfeccionando, se ha ido desglosando los derechos de manera individual y colectiva , obligando a países como España, luego de varios años , ratificar este convenio. Que no es otra cosa, sino ratificar la protección de los derechos inherentes a la dignidad humana, a la intimidad, al honor, a la privacidad, a la imagen .

Por ello, existen una serie de instrumentos aprobados por las Organización de la Naciones Unidas , que a todas luces se observa que el proceso de ratificación con el paso de los años de la protección de estos derechos , en su afán por el cumplimiento , por una sociedad mas justa, mas respetada , una privacidad mas cónsona con el mundo actual , por una vida donde sea rebasada su intimidad por el fuero tecnológico , donde la libertad de expresión no se convierta en el verdugo de estos derechos , que puedan convivir para que no se vea lesionada las libertades publicas y las grandes conquistas que ha tenido los pueblos en su historia . Brevemente dichos instrumentos fueron reseñados por Libardo Riascos G.[20] :

- **El Pacto Internacional de Derechos Económicos, Sociales y Culturales**

  Fue adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas en la Resolución 2200a (XI) de 16 de diciembre de 1966.

20.-Libardo Riascos G. *Derecho a la intimidad, la visión iusinformatica y el delito de los datos personales .Lleida. España*. 1999. p.48-63.

- **El Pacto Internacional de Derechos Civiles y políticos, o también, Pacto de New York**

  El articulado fue adoptado y abierto a firma, ratificación y adhesión por la Asamblea General por medio de la Resolución 2200A (XXI) de fecha 16 de diciembre de 1966.

- **La Convención Americana Sobre Derechos Humanos o Pacto de San José de Costa Rica**.

  La Convención se suscribió el 22 de noviembre de 1969, en la conferencia especializada interamericana de Derechos Humanos, de la esencia del derecho a la intimidad es el derecho que el Pacto denomina: Derecho a la integridad física.

- **Declaración de los Derechos de los Niños**

  Aprobado en fecha de 20 de Noviembre de 1959 (Resol. 1386), por la Asamblea General de las Naciones Unidas

- **El Convenio de la Haya**

  Aprobado en fecha 5 de Octubre de 1961

Caso Faceboock en Venezuela

Raymond Orta Martínez[21] expresa:

“El contrato de uso de Facebook, se trata de un contrato de adhesión en el que los usuarios aceptan para poder crear una cuenta de usuario. Se trata de un contrato de aceptación vía clic o “click through” “.

Los contratos de adhesión tiene en su característica mas importante que no son discutidos con la otra parte, solo si acepta las condiciones que impone en este caso Faceboock y se somete el usuario pero es común que nadie se detiene a revisar ese contrato , solo se ve como una opción para entrar a la pagina o al servicio, automáticamente con un clic , comienzan sus problemas .

Continúa expresando que Raymond Orta Martínez:

“El que cediera ilimitadamente los textos, artículos, videos, imágenes producto de la creación de los usuario, ponía en peligro derechos humanos y personales como el derecho a la privacidad y así como la renuncia a derechos económicos derivados de la propiedad intelectual, como lo son los derechos de autor, por cuanto, serían automáticamente cedidos sin pago o contraprestación alguna con una licencia mundial e ilimitada”.

De allí radica los problemas de las redes sociales , donde no se determinan clausulas que se acuerden y sin leer , se aprueba , pero posteriormente se esta cediendo toda la información personal en una red mundial

Raymond Orta Martínez, indica cuales son las Clausulas actuales y sus efectos jurídicos en Venezuela, de la siguiente manera:

1) Suministro de la identidad verdadera: En algunos países existe el

_____

17. *Dr. Raymond Orta. Efectos Jurídicos del Cambio de Clausulas legales en Facebook*. (2009) www.raymondorta.com (consulta 2012. Abril 17)

derecho del usuario a no registrarse con su identificación real siempre y cuando no se haga pasar por otra persona suplantando su identidad lo cual sería un delito de falsificación electrónica.

2) Ser mayor de 13, en el caso de Venezuela y la mayoría de los países los menores no tienen capacidad para celebrar contratos y menos

tendría efectos la cesión de los derechos pretendidos por el cambio. Existen sitios que obligan a los representantes de los menores a aceptar en su nombre las clausulas de los sitios web como por ejemplo el “Club Penguin”.

3) Derechos exclusivos sobre el Contenido del sitio (licencia limitada). Todo el contenido disponible a través del Servicio, incluyendo diseños, texto, gráficos, imágenes, vídeo, información, aplicaciones, software, música, sonido y otros archivos, así como su selección y disposición (el “Contenido del sitio”), son propiedad exclusiva de la Compañía (Facebook), de sus usuarios o de sus licenciantes, con todos los derechos reservados.

CAPÍTULO II

MARCO LEGAL DEL DERECHO A LA INTIMIDAD EN LA SOCIEDAD INFORMATIZADA DESDE EL PUNTO DE VISTA PENAL EN VENEZUELA

El Ordenamiento Jurídico Venezolano, específicamente a la Constitución de la República Bolivariana de Venezuela, Código Penal, Decreto con Rango y Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, (Decreto Nº 1024 de fecha 10 de Febrero de 2001) y Ley especial contra los Delitos Informáticos publicada en gaceta oficial nº 37313 de fecha 30/10/2001.

Es obligante señalar la base fundamental del Derecho que tienen los Ciudadanos en Venezuela, donde el constituyente quiso dar un paso adelante de la tecnología y prever que sea el Estado quien controle y proteja a la sociedad, para así evitar que se violen o lesionen derechos de las personas, a través de la Carta Magna, como es la Constitución de la República Bolivariana de Venezuela[17], lo cual consagra lo siguiente:

Artículo 28:

> Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de

cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.

Artículo 48.

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.

Artículo 60:

Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos".

.

Con estas normas de carácter estricto, estatuida, sin opción a cambio, con toda la firmeza de su espíritu, se establece en la República Bolivariana de Venezuela a través de su Constitución, las líneas maestras que sirven de base al desarrollo de normas legales más especificas, tomando en consideración lo amplio del tema y lo nuevo relativamente para Venezuela.

17.-Constitución de la República Bolivariana de Venezuela (1999)

deben ser regulados y protegidos, tanto desde el punto de vista personal, como por la vía Informática.

En estos artículos se desprende todo una serie de comportamientos que De esta forma se le otorga rango Constitucional y se estatuyen como Derechos Fundamentales, la intimidad, al honor, la vida privada, su propia imagen, confidencialidad y reputación, interpretando el respeto por los derechos humanos y en forma general a la dignidad humana.

En este orden de ideas, se plasmó la protección de los datos personales y estableció la vía legal, en caso de ser necesario obtenerlos, también hace la salvedad del secreto periodístico y de otras profesiones. En puntos anteriores se habló de la situación de la discusión entre derecho a la intimidad y la libertad de expresión , en este caso Venezuela, otorga pleno protección al secreto periodístico pero también protege al derecho a la intimidad, perfilándose como una contradicción porque al ejercer la libertad de expresión puedo violar el derecho a la intimidad, al honor pero puede escudarse el ejercicio periodístico bajo la figura del secreto profesional , sometiendo al escarnio publico a cualquier ciudadano .

En todo caso, habría que analizar los casos que puedan presentarse y tratar de darle buen uso al secreto profesional y concatenarlo con el articulo 60 ejusdem, donde se establece el derecho a la protección de su intimidad, honor, vida privada, propia imagen, confidencialidad y reputación y al mismo tiempo, le ofrece normas contempladas en el Código Penal Venezolano, donde se desarrolla la difamación.

Ha sido luchas permanentes desde antes de 1948 cuando se aprueba la Declaración Universal de los derechos humanos, la consecución de normas que protejan a la intimidad de las personas, antes por los abusos de

las situaciones bélicas , enfrentamientos entre pueblos que llevaron a determinar normas que debían regirse en momentos de guerras , en protección a ciertas áreas, determinadas personas entre niños y mujeres, pero es en el año de 1948, cuando se aprueba la Declaración Universal de los Derechos Humanos y comienzan a desarrollarse el ordenamiento jurídico con dichas previsiones en defensa y protección a las libertades publicas, a la dignidad humana, a la intimidad, llamando a la intimidad desde su persona hasta su morada y sus datos personales, por ello también se plantea en la Constitución de la República Bolivariana de Venezuela que el legislador debe instrumentar leyes que desarrolle la limitación al uso de las vías informáticas en perjuicio de los ciudadanos y de las ciudadanas .

En materia constitucional, estos derechos, de acuerdo a sus principios fundamentales , están garantizados, pero si no se desarrollan leyes que vengan a regir las posibles lagunas jurídicas o nuevas situaciones , porque cuando se administra Justicia , deben comenzar tanto Fiscales del Ministerio Publico como Jueces , a tratar de encuadrar ciertas conductas en estas normas , con el fin de combatir la impunidad pero también se dan los casos que personas inocentes , se les cause daño , se les cause perjuicio por malas interpretaciones a las normas existentes , ante la falta de leyes mas directas y concretas.

En todo caso, en Venezuela, se ha venido aprobando leyes en todas las materias, sin ningún parámetro legal, ni técnica jurídica, causando ciertas incomodidades a la hora de ejercer el derecho y administrar Justicia, es decir , se aprueban unas y sigue en mora con otras de mayor relevancia y necesidad, teniendo que recurrir a una figura jurídica importante para lograr protección ante el uso abusivo de sus datos personales , como es el Derecho de Habeas Data.

El Derecho de Hábeas Data:

,La figura jurídica del Habeas Data, viene a ejercer un papel preponderante en los términos de protección de la intimidad personal a través de los datos y de los suministros de información, que posteriormente, presentan el uso abusivo de los mismos y obliga, en caso de declararse con lugar, de enmendar y corregir el abuso cometido.

En este camino por tratar de lograr un concepto adecuado a la realidad, Flor Ávila, Katia Castaldo y Anthony Urdaneta[21] han estudiado la figura del *habeas data*, de la siguiente, manera:

"El vocablo "habeas" proviene del latín *habere*, que significa téngase en su posesión y "*data*", proviene del inglés que significa datos, definido por los diccionarios como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación y procesamiento por medios automáticos.

Afirma mas adelante Flor Ávila, Katia Castaldo y Anthony Urdaneta[22]:

"…podemos colegir que el *habeas data* es considerado como una posible acción judicial tendiente a permitir el acceso a los datos que se encuentran almacenados en registros, tanto públicos como privados, a los fines de controlar dicha información y, en caso de que dicha información sea falsa o discriminatoria, se podrá solicitar la supresión, rectificación, confidencialidad o actualización de ésta. Los motivos del *habeas data*, según

_____

21.--Flor Ávila, Katia Castaldo, Anthony Urdaneta *Los derechos humanos a la intimidad y a la privacidad en Venezuela y en el Derecho comparado.* Op.cit, pp.315

22.--Flor Ávila, Katia Castaldo, Anthony Urdaneta *Los derechos humanos a la intimidad y a la privacidad en Venezuela y en el Derecho comparado.* Op.cit, pp.315

la legislación citada, permite que sea dividido en dos etapas, el derecho al acceso y, posteriormente, el derecho a la supresión, rectificación o confidencialidad, en el supuesto de que sea falsa o errónea."

En la figura jurídica del habeas data, contempla en su espíritu la garantía para que el ciudadano pueda acceder en conformidad con el articulo 28 Constitucional, a la base de datos que presuntamente es mal utilizado en su contra pero también tiene la opción de exigir que sea corregido sus datos o en todo caso que sea eliminado de ese banco de datos, bajo la figura que le causa daño a su intimidad, a su honor, encuadrando en el texto constitucional

El presente articulo viene a tener una aplicación muy especial , debido a que siendo un articulo tan extenso , contentivo de derechos fundamentales , pero sin una regulación, que permita su mejor aplicación y mayor defensa al ciudadano , cuestión que ha obligado a la Jurisprudencia del Tribunal Supremo de Justicia, ha establecer su naturaleza y su correcta aplicación.

El Tribunal Supremo de Justicia, en Sala Constitucional[21], por medio de la Sentencia N° 1050, dictada el 23 de Agosto del 2000 (caso: Ruth Capriles y otros), Magistrado-Ponente: Jesús Eduardo Cabrera Romero donde se desarrolla el Articulo 28 y lo encuadra dentro de la figura jurídica del Habeas Data, estableciendo los supuestos y ordenando su procedencia y analizando brevemente el articulo 28 de la siguiente manera:

21.-Tribunal Supremo de Justicia de Venezuela, Sala Constitucional. Sentencia N° 1050, dictada el 23 de Agosto del 2000 (caso: Ruth Capriles y otros),

"El artículo 28 de la vigente Constitución establece el derecho de las personas a conocer la información que sobre ellas, hayan sido compiladas por otras. Dicha norma reproduce un derecho reconocido en varios países como Suecia, Noruega, Francia y Austria, entre otros. Tanto el Estado, como los particulares, mediante diversas formas de compilación de datos: manuales, computarizados, etc., registran y almacenan datos e informaciones sobre las personas o sobre sus bienes, y en vista que tal recopilación puede afectar la vida privada, la intimidad, el honor, la reputación, la vida económica y otros valores constitucionales de las personas naturales o jurídicas, la Constitución, para controlar tales registros, otorga varios derechos a la ciudadanía que aparecen recogidos en el artículo 28 citado. Estos derechos son:

1) El derecho de conocer sobre la existencia de tales registros.

2) El derecho de acceso individual a la información, la cual puede ser nominativa, o donde la persona queda vinculada a comunidades o a grupos de personas.

3) El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él.

4) El derecho de conocer el uso y finalidad que hace de la información quien la registra.

5) El derecho de actualización, a fin que se corrija lo que resulta inexacto o se transformó por el transcurso del tiempo.

6) El derecho a la rectificación del dato falso o incompleto.

7) El derecho de destrucción de los datos erróneos o que afectan ilegítimamente los derechos de las personas.

Se trata de derechos que giran alrededor de los datos recopilados sobre las personas o sobre sus bienes, por lo que se requiere un interés, personal, legítimo y directo en quien ejerza estos derechos, ya que es la información sobre su persona y bienes el que lo origina. Basta leer el artículo 28 de la vigente Constitución, para que todos estos derechos puedan identificarse. Dicha norma reza:

" Articulo 28.-Toda persona tiene derecho de acceder [derecho de acceso] a la información y a los datos que sobre sí misma o sobre sus bienes [necesidad de interés personal y directo] consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso [derecho de conocimiento] que se haga de los mismos y su finalidad [derecho de conocer uso y finalidad], y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos [derecho de respuesta, actualización, rectificación y destrucción]. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley". (Corchetes de la Sala)."

La Sala Constitucional , desglosa los derechos que responden a la necesidad de establecer para que recoja el sentir de su procedencia como acción judicial en protección a su intimidad, por ello, refiere el Derecho de acceder a la información, no puede ser negada , la persona o el funcionario esta en la obligación de permitir el conocimiento a su titular de sus datos, también refleja la Sala Constitucional el derecho al conocimiento del uso que

le han dado y que le van a dar a sus datos personales o la información suministrada , así como el Derecho de conocer y de uso de su información y finalmente , en caso de ser declarado su acción con lugar ante un tribunal competente, tendría una figura administrativa como es el derecho a la respuesta, la actualización de sus datos , la rectificación de los mismos o la destrucción, siendo de esta manera, la acción inmediata al momento de defender y proteger del mal uso de sus datos personales.

En materia probatoria, la Sala Constitucional[22] aclara sobre la necesidad de no usar , bajo ningún concepto el habeas data como un instrumento que pueda ser interpuesto para obtener datos , anticipando u obteniendo pruebas, ni retardo perjudicial por temor fundado , la sala constitucional , señala que en ese caso, el demandante tiene otras vías para ejercer sus derechos, dejando claro su criterio de que la aplicación del Articulo 28 tiene una finalidad especifica , tal como se desprende de la forma siguiente :

"En consecuencia, el habeas data no es un procedimiento para anticipar u obtener pruebas, y quien pretende por esta vía sustituir un retardo perjudicial por temor fundado, no estaría usando la acción con los fines que la creó la Constitución. Es más, el derecho previsto en el artículo 28 de la vigente Constitución, ni siquiera equivale al que pudiesen tener las partes de un proceso para informarse antes o durante un juicio, sobre los hechos básicos útiles para la demanda o la contestación, conocimiento que no corresponde a una actividad probatoria, sino de los hechos, para poder ejercer a plenitud el derecho de defensa. Una acción en este sentido, fundada no sólo en el carácter de orden público del derecho de defensa,

_____

24.-Tribunal Supremo de Justicia de Venezuela, Sala Constitucional. Sentencia N° 1050, dictada el 23 de Agosto del 2000 (caso: Ruth Capriles y otros),

sino en el artículo 19 de la Ley Aprobatoria del Pacto Internacional sobre Derechos Civiles y Políticos y en el 13 de la Ley Aprobatoria de la Convención Americana de Derechos Humanos, Pacto de San José de Costa Rica, es totalmente distinta a la prevenida en el artículo 28 aludido, que persigue otra finalidad, y procede sólo si se va a iniciar una causa o se va a contestar una demanda, lo que sería necesario alegarlo (Ver Cabrera Romero, Jesús Eduardo: *"El derecho del demandado de preparar su contestación y su prueba. Derecho a conocer"*, en Revista de Derecho Probatorio N° 6, Caracas, 1995)."

En el caso Venezolano, mediante la presente Sentencia del Máximo Tribunal de Justicia, siendo vinculante su decisión por ser emanada de la Sala Constitucional, determina que el habeas data es una acción autónoma y no forma parte de los recursos de amparo a los derechos y garantías constitucionales, en ese caso tendría otro tratamiento y otras vías. Tomando en consideración que el artículo 28 ejusdem se circunscribe a los datos personales.

En consecuencia , debido a la sentencia anterior, la protección de los datos personales , estaría sujeta a las acciones de habeas data , en concordancia del articulo 28 Constitucional , en el entendido que ha sido una interpretación por vía Jurisprudencial como solución a la situación que se ha planteado, fue preferible , dictar la Sentencia con el fin de regular el Habeas Data , que esperar la aprobación de una Ley que tratara el tema , basándose en el mismo articulo 28 y habría que tomar en cuenta que la sentencia referida es del año 2000 y aún no existe la Ley que regule estrictamente todas las situaciones de datos personales archivados en los bancos de datos. En todo caso, tampoco es ilegal que suceda la presente interpretación, porque es una facultad prevista en la Constitución y en la Ley del Tribunal Supremo de Justicia, con efecto vinculante a toda la administración de

Justicia. Dejando a salvo las acciones legales posteriores por el uso abusivo de estos datos.

Por otra parte, en Doctrina Penal, para la existencia del delito, es necesaria la conjunción de varios elementos básicos, según la Teoría General del Delito y a decir de autores clásicos en la materia como Jiménez[25] , estos elementos pueden resumirse en siete:

"Acción, tipicidad, antijuricidad, imputabilidad, culpabilidad, condicionalidad objetiva y punibilidad. De estos, es la tipicidad entendida como la descripción de una conducta por medio de la norma penal para que sea considerada como delito, es el más perfectible y delicado de estos, por ser precisamente, el freno a la pretensión punitiva del Estado, y constituir la primera defensa al respeto de los derechos humanos".

Se ha hablado de las normas que son bases indispensable, en el caso de la protección del derecho a la intimidad y a la privacidad , aplicable como derecho fundamental , a fin de encuadrar el hecho como punible, por ello, la tipificación es de suma importancia para hacer la debida configuración con la finalidad de que no quede impune cualquier hecho catalogado como punible o tampoco se abuse de un inocente o se viole su derecho a la intimidad en el afán por considerar cualquier hecho presuntamente delictivo. Por tal motivo, la configuración de un hecho delictivo, para que sea reputado como tal, debe estar tipificado en el ordenamiento jurídico, en caso contrario, no puede ser perseguida por hechos que no constituyen delito. De allí nace, el Artículo 1 del Código Penal, de la siguiente manera:

22.- Jiménez, L. *La Ley y el Delito*. Buenos Aires: Sudamericana. (1980).

Artículo 1

> "Nadie podrá ser castigado por un hecho que no estuviese expresamente previsto como punible por la ley"

En la Constitución de la República Bolivariana de Venezuela, en su Artículo 49 numeral 7, el cual expresa:

Artículo 49 numeral 7:

> "Ninguna persona podrá ser sancionada por actos u omisiones que no fueren previstos como delitos, faltas o infracciones en leyes preexistentes".

No hay que dejar de lado, que en la legislación nacional desde hace años, están en vigencia normas que pueden ser adaptables al nuevo tiempo y a las nuevas tecnologías como la Ley sobre Derecho de Autor (1993), o las relativas a la difamación e injuria contempladas en el Código Penal (1964).

Es justificado que se hable de los delitos tipificados en el Código Penal venezolano , pero de difícil aplicación por la administración de justicia , por cuanto al hacer la configuración de los delitos tipificados en el mismo, con las nuevas modalidades de delito, en esta revolución informática de los nuevos tiempos , con sistemas informáticos, incluso , la realidad de que a la hora de entregar los datos personales en cualquier parte , los jueces no están exentos , siendo tratados hasta este momento, con cierta reserva por razones de seguridad en algunos casos . Es decir que es tratar de hacer una especie de rompecabezas jurídico y criminalística para llegar a una configuración delictiva o sencillamente se determine que no hay delito, no hay hecho punible, aun cuando en la practica se haya cometido un perjuicio o

daño irreparable, en ese caso, el comportamiento no sería antijurídico y por lo tanto , no puede ser reputado como delito.

Cuando se habla de la culpabilidad como elemento del delito, es referente al sujeto activo, es decir que tuvo la intención de cometer un delito, que tuvo conocimiento previo de la situación, que actuó con plena conciencia y en pleno convencimiento de su responsabilidad y de su castigo, pero si es demostrado lo contrario, no podría ser enjuiciado por falta de elementos de juicio y por falta de merito para una acusación fiscal, tal como lo reza el artículo 61 del Código Penal Venezolano:

"Nadie podrá ser castigado como reo de delito no habiendo tenido la intención de realizar el hecho que lo constituye, excepto cuando la ley se lo atribuye como consecuencia de su acción u omisión".

Referente a la Ley Sobre Mensajes de Datos y Firmas Electrónicas a pesar de haber entrado en vigencia en el año 2001, sigue siendo una Ley novedosa por su lenta aplicación, señalando el deseo y necesidad de implantación definitiva, calificando, como de suma importancia el hecho de los efectos de la misma cuando en conformidad con el Artículo 16; se reconoce la fuerza probatoria y validez jurídica de los mensajes de datos, cualquiera que sea su forma, teniendo la misma valoración probatoria y los mismos efectos jurídicos que los impresos reconocidos por la Legislación Nacional, pero se restringe cuando por determinados actos se exige la formalidad del contrato, estableciendo en su Artículo 6 ejusdem de la siguiente manera:

Artículo 6.

Cuando por determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley.

Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un Mensaje de Datos al tener asociado una Firma Electrónica.

Haciendo mención a los requisitos, se señala la disposición de realizarse por la misma vía electrónica todo el proceso, es decir que tendría que realizarse a través del soporte electrónico teniendo como ejemplo de esta norma que se exige el reconocimiento de un documento ante la Notaría Pública, el documento se envía por Internet, es otorgado por el "cybernotario" y devuelto a su emisor por la misma vía. Es decir que se creó una Ley para otorgar seguridad, la eficacia y valor jurídico en forma de mensajes de datos y firmas electrónicas, abarcando las actividades comerciales, civiles o administrativas, pero no tiene el basamento para poder ejecutarse en la actualidad, producto que no cuenta con la infraestructura, equipos, seguridad, incluso, disposición personal, necesaria para cumplir con los fines de la Ley.

Al mismo tiempo, la Ley contempla entre los requisitos para lograr la validez y la eficacia de la Firma Electrónica, de acuerdo a la siguiente norma de la LMDFE:

Artículo 16

La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la

misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:

1º.- Garantizar que los datos utilizados para su generación puedan producirse solo una vez, y asegurar, razonablemente, su confidencialidad.

2º.- Ofrece seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.

3º.- No alterar la integridad del Mensaje de Datos.

Es decir, señala en primer término, el aseguramiento de la confidencialidad de la Firma Electrónica, en segundo término, que no pueda ser falsificada con la tecnología del momento y en tercer lugar que no altere la integridad del Mensaje de Datos. Observando desde un punto de vista positivo, sería revestida de garantía ese proceso, pero en todo caso se reserva en un tercero la Certificación de la misma para su veracidad.

Ahora bien, para cumplir con tal requisito se crea la Institución de la Superintendencia de Servicios de Certificación Electrónica, en conformidad con la norma siguiente:

Artículo 20

Se crea la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Artículo 21

La Superintendencia de Servicios de Certificación Electrónica tiene por objeto acreditar, supervisar y controlar en los términos previstos en este Decreto-Ley y sus reglamentos, a los proveedores de Servicios de Certificación públicos o privados.

Se crea esta figura para que adelante todo lo concerniente a la acreditación, supervisión y control a todos los proveedores de Servicios de Certificación públicos o privados, certificación que debe ser otorgada por el Estado a empresas especialistas en el ramo, de forma tal que puedan ser calificadas como comunicaciones seguras, que es al fin y al cabo, lo que busca el usuario para configurar el contrato electrónico, relaciones personales y convertirlo masivamente en un medio idóneo para sus intereses comerciales pues bien, en Venezuela, el Proceso fue muy lento , pero finalmente fue implementada dicha certificación.

La actividad definitiva del Proceso de Certificación, ha sido en todo caso lento, vale decir que la Ley data del año 2001, unida a la falta de conocimiento de los Ciudadanos, y es recientemente cuando se ha iniciado con una base de certificación que comienza a dar la sensación y al mismo tiempo ofrecer la seguridad requerida, adscritas al Ministerio del Poder Popular para la Ciencia y Tecnología e Industrias Intermedias, denominada Superintendencia de Servicios de Certificación Electrónica[23] (SUSCERTE) como Rector en materia de Certificación Electrónica del Estado y tiene como apoyo en determinadas áreas, como es el Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT) y El Centro Nacional de Informática Forense (CENIF).

Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) en su afán por establecer la normativa ya referida, aunado que estaba en mora con ella, inició la adaptación y cumplimiento de las Leyes sobre la materia, teniendo su pagina Web e ilustrando a los usuarios sobre la necesidad de obtener servicios de calidad y seguras , con el fin de evitar la fuga o extracción de datos personales y de personas jurídicas, con la intención de cometer hechos punibles con la información obtenida, por ello SUSCERTE, resalta la figura de la certificación electrónica como una garantía a la seguridad de las operaciones y Suministros de datos personales de los usuarios,

Las labores de certificación electrónica, se puede decir que es el punto de partida hacia una practica informática segura, en este caso, contra aquellas personas que tratan con su ingenio de obtener información que contiene las bases de datos, es decir, puede obtener la información por otra vía, pero no por el acceso directo a los servidores, evitando que sus datos personales y sus operaciones sean develadas y violadas. Esta es una forma de protección para todos los usuarios que así lo soliciten ante esta oficina pública del Estado Venezolano.

En consecuencia, SUSCERTE[26] , publica una serie de conceptos que ilustran al usuario sobre la necesidad de obtener una Certificación Electrónica, de la siguiente manera:

¿Qué es la Certificación Electrónica?

La Certificación Electrónica es un área que involucra políticas,

26.-http//www.Suscerte.gov.ve (consulta 2012. Abril 20) Venezuela .

procedimientos, infraestructura, estándares y equipamiento, que hacen posible el ciclo de vida de un certificado y su uso, con las garantías que dictan los estándares de seguridad electrónica. Esto permite al usuario confiar en operaciones como la firma electrónica, correo electrónico seguro, fecha y hora certificada, entre otras.

Es importante cuando se realizan negocios o se suministra información que para el usuario y para el receptor es considerada como confidencial por ejercer el respeto al derecho a la intimidad, es allí, donde entra a jugar su papel preponderante , que sea una pagina segura , que no sea de fácil y cómodo acceso, que no sea abierta al publico en cuanto a la información suministrada o captada por el receptor; siendo la superintendencia de certificación electrónica quien otorga la Certificación Electrónica , bajo procedimientos especiales para que una pagina tenga esa condición de seguridad .

¿Qué es un Certificado Electrónico?

Un Certificado Electrónico es un documento electrónico emitido por un Proveedor de Servicios de Certificación, que vincula a un usuario (signatario) con su firma electrónica, el mismo está compuesto por dos elementos (clave pública y clave privada), con el cual se identifica al propietario del mismo y permite la generación de firmas electrónicas.

Un certificado electrónico, es un documento que deja constancia, que efectivamente su pagina es segura, donde su firma electrónica es registrada y le entregan dos claves, que sirven de identificación cada vez que va a acceder al servicio.

¿Qué es la Clave Pública?

Es un conjunto de datos de carácter público que vinculan al remitente con el mensaje y que permiten cifrarlo.

En este caso, el remitente mantiene su cuenta y es solo de su uso pero pueden tener acceso otras personas determinadas con su clave.

¿Qué es la clave privada?

Es aquella combinación secreta que se utiliza para descifrar el mensaje y sólo la posee el receptor.

La clave privada es otorgada a un usuario y solo el, puede tener acceso.

Es menester del Estado Venezolano la búsqueda de acercarse a la protección real, por ello la Superintendencia de certificación electrónica, dependiente del ministerio del poder popular para la Ciencia y Tecnología es la encargada de proveer Servicios de Certificación Electrónica y emitir los Certificados Electrónicos a los usuarios que ha sido previamente acreditado por Suscerte para tal fin.

Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT)

Al mismo tiempo, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) cuenta con unidades de apoyo como el Sistema Nacional de Gestión de Incidentes Telemáticos de la

República Bolivariana de Venezuela (VenCERT). Su principal objetivo, como ente gubernamental es la prevención, detección y gestión de los incidentes generados en los sistemas de información de la Administración

Pública Nacional y los Entes Públicos a cargo de la gestión de Infraestructuras Críticas de la Nación.

Su creación responde a la necesidad estratégica de dotar al Estado de los mecanismos más adecuados para prevenir y actuar con efectividad ante los nuevos riesgos generados por el desarrollo de las nuevas tecnologías. De hecho, la seguridad de los sistemas y redes de información del sector público es un componente fundamental de la seguridad de un país.

La Superintendencia de certificación electrónica, a fin de cumplir con su labor eficientemente, requiere de unidades que apoyan y soportan su trabajo, porque no solo es otorgar Certificaciones Electrónicas, es también proteger, prevenir o detectar cualquier anomalía, ante la cantidad de riesgos que conlleva la practica informática.

La misión asignada al VenCERT para contribuir al objetivo general de Sistema Nacional de Seguridad de la Información se puede descomponer en los siguientes puntos:

- **Prevención, detección y gestión de los incidentes** generados en los Sistemas de Información del Estado y entidades gestoras de Infraestructuras Críticas de la Nación (IC nacionales).

- **Punto principal de coordinación nacional** de otros centros de gestión de incidentes en el país y en el extranjero.

- **Asesoramiento, apoyo y formación** en materia de seguridad a los diferentes responsables de TIC en organismos del Estado o de

entidades gestoras de la gestión de Infraestructuras Críticas Nacional.

- **Coordinación de iniciativas públicas o privadas relativas a seguridad de las TIC** en el Estado, materializadas a través de proyectos I+D, acciones de formación y sensibilización, elaboración de políticas normas o guías, tanto para beneficio de la comunidad (Estado y gestores de IC nacionales) como para la mejora de los servicios prestados en el VenCERT.

Esta unidad de acuerdo con las áreas que cobija, se convierte en pilar fundamental de las Certificaciones Electrónicas, por cuanto en ella reposa todo el aparato previo a la Certificación y al mismo tiempo, tiene las funciones de prevención y detección de incidentes telemáticos, así como el asesoramiento técnico, colocar oficinas o puntos en cualquier parte del país y coordinar las labores de formación y sensibilización sobre el tema.

Estas unidades tratan de venir a establecer el respeto y la seguridad en esta materia, por ello VenCERT se erige, como el CERT gubernamental venezolano cuyo principal objetivo es la prevención, detección y gestión de los incidentes generados en los sistemas de información de toda la Administración Pública Nacional y Sectores Públicos a cargo de la gestión de Infraestructuras Críticas de la nación.

Los servicios de VenCERT permitirán proteger y garantizar la defensa y seguridad de la Nación, así como la suprema vigilancia de los intereses generales de la República, la conservación de la paz pública y la recta aplicación de la ley en todo el territorio nacional, conforme a las competencias establecidas en la Constitución de la República Bolivariana de Venezuela, para el Poder Público Nacional.

Laboratorio Nacional de Informática Forense (CENIF)

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) como una forma de apoyo a los distintos entes auxiliares de Justicia y a los entes Judiciales creó el Laboratorio Nacional de Informática Forense (CENIF) el cual, orienta sus actividades en cuanto a la ilustración de los usuarios y sus derechos, tal como lo reseña en su, pagina web.

Ante la necesidad, por razones de servicios, debido a las labores de asesoramiento, de prevención y detección, surge la creación del Laboratorio de Informática forense (CENIF), que viene a servir de apoyo al sistema judicial en el estudio de pruebas en esta materia.

¿Qué es la informática Forense?

Es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten realizar los procesos de Preservación, Colección, Análisis y Presentación de evidencia digital, de acuerdo a procedimientos Técnico-Legales preestablecidos, como apoyo a la Administración de Justicia en la resolución de un caso Legal.

Es una unidad netamente científica, que sirve de apoyo a los entes judiciales en el estudio de evidencias, bajo procedimientos técnicos.

¿Cuál es la principal misión de la Informática Forense?

Auxiliar a los abogados, fiscales y jueces a identificar, preservar y analizar datos almacenados en medios magnéticos y transacciones electrónicas en un litigio judicial o extrajudicial.

Esta función en Venezuela, es novedosa, porque anteriormente se apoyaba en los laboratorios científicos de los cuerpos de seguridad del estado directamente y solo en casos Judiciales, pero en este caso, se crea un laboratorio con este perfil, única y exclusivamente para esta materia y tiene la relevancia que puede ser solicitada su labor de forma extra-judicial.

¿Qué es un delito informático?

Es un crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar computadores, medios electrónicos y redes de Internet. Los delitos informáticos están contemplados en la Ley Especial contra los Delitos Informáticos

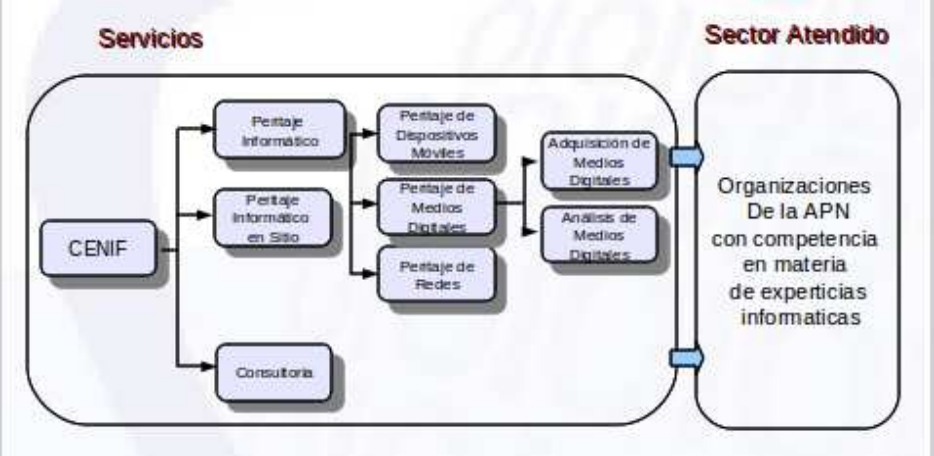
En términos normales un delito informático, de acuerdo al presente concepto señalado por el Laboratorio Nacional de Informática Forense (CENIF) viene a constituirse cuando a través de acciones ilegales en internet, se plantea el objetivo de causar un daño , abarcando redes , datos personales contenidas en las redes .

¿Qué es el CENIF?

El Centro Nacional de Informática Forense (CENIF), es un laboratorio de informática forense para la adquisición, análisis, preservación y presentación de las evidencias relacionadas a las tecnologías de información y comunicación, con el objeto de prestar apoyo a los cuerpos de investigación judicial órganos y entes del Estado que así lo requieran.

El Centro Nacional de Informática Forense es una iniciativa de la Superintendencia de Servicios de Certificación Electrónica y producto del trabajo en conjunto de diferentes instituciones del Estado que tiene por intención conformar un modelo de servicio para el apoyo técnico de todos los cuerpos y órganos del Estado con competencia en materia de experticias digitales.

¿Cuáles son los servicios que presta el CENIF?



Fuente: http//www.Suscerte.gov.ve .Venezuela .

Es resaltante entre todas las criticas que puede tener el Estado Venezolano, por no impulsar las acciones adecuadas para lograr una legislación ideal para proteger el derecho a la intimidad, así como los derechos inherentes a la dignidad humana pero si es reconocible el intento por adecuarse con los recursos que cuenta de inmediato, por ello, se crean todas las entidades, van naciendo las instituciones llevando adelante una serie de formas de aplicar las normas en esta materia.

Esto debido a que se tiene una Ley, unas normas, pero el escaso interés de implementar todo el proceso para seguridad del usuario, conllevó a un vacío legal, perfeccionándose nuevas maneras de delinquir, de realizar ofertas engañosas, de traficar con el uso del Dominio Electrónico, de los Mensajes de Datos y de la Firmas Electrónicas, la entrega de datos y actividades personales, configurándose los Delitos Informáticos, es decir que cuando se aplique, la Ley será obsoleta en cuanto a las nuevas tecnologías.

En el mismo orden de ideas la Ley contempla en su contenido las garantías para hacer un contrato más seguro desde su óptica, pero no protege el tráfico de los datos personales con otros fines:

Artículo 41.

> El proveedor de los servicios electrónicos deberá especificar las garantías que cubrirán la relación que surja entre éste y los consumidores y usuarios, las cuales deberán ser lo suficientemente claras y extensas para cubrir los inconvenientes que puedan derivarse.

En este caso, le otorga al proveedor toda la discrecionalidad para que él ofrezca garantías. De esta Ley se puede deducir en cuanto a los Artículos referidos, que son de aplicación directa en esta materia, aún con sus imprecisiones y generalidades pero está más cercana a criterios que permitan ciertas bases a los usuarios en el momento de realizar una contratación, adaptándose al término de electrónicos, asumiendo el peso de dichas negociaciones en defensa del consumidor, sin profundizar en el Mundo de la Informática.

El basamento legal que tienen los Contratos Electrónicos, en la medida que se analiza, van apareciendo una serie de disyuntivas, donde el Legislador, fue eficiente, hizo las previsiones del caso, pero, sencillamente, las nuevas tecnologías y su desarrollo van a grandes pasos y en el avance de las mismas han ido quedando atrás las normas existentes, teniendo que acudir a la vía supletoria para resolver conflictos, por lo que sería de gran beneficio para la Economía Venezolana la necesidad de unificar el Derecho y hacer uso de él, acorde con los nuevos tiempos.

Nuestra Legislación, se vio en la necesidad de crear una Ley que combatiera los delitos informático, así creo la denominada Ley Especial Contra los Delitos Informáticos publicada en Gaceta Oficial Nº 37313 de fecha 30/10/2001.

Esta Ley contra Delitos Informáticos, significa un gran avance en materia penal para Venezuela, visto que permitirá la protección de la tecnología de la información, persiguiendo todas aquellas conductas antijurídicas que se realicen en este campo. Es importante que se señalen los aspectos más importantes de la ley:

Objeto de la Ley.

El objeto de la Ley se encuentra consagrado en el artículo 1 el cual establece:

Artículo 1:

> La presente ley tiene por objeto la protección 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.

De la norma transcrita anteriormente se puede inferir que la ley tiene como objetivos principales:

1) La protección de los sistemas de tecnologías de información;
2) La prevención y sanción de los delitos cometidos contra tales sistemas;
3) los delitos cometidos mediante el uso de dichas tecnologías.

En este articulo se resume el objeto real de la Ley, siendo bastante amplia en su aplicación, donde establece la protección de los sistemas de tecnologías de información, busca prevenir la perpetración de delitos y al mismo tiempo , considera la sanción contra el el mal uso de las tecnologías.

La Extraterritorialidad.

La previsión de la Extraterritorialidad se encuentra tipificada en su artículo 3, y el cual es de gran importancia en razón de la dimensión transnacional del problema pues se trata de hechos que pueden cometerse de un país a otro.

En esta norma, protege la figura de una tecnología sin fronteras , por ello debe perseguir la red o la perpetración desde donde salga o donde se ejerza.

Sanciones.

En el aspecto de las sanciones se adopto simultáneamente el sistema binario, esto es, pena privativa de libertad y pena pecuniaria. Con relación a esta última se fijan montos representativos calculados sobre la base de unidades tributarias por considerarse que la mayoría de estos delitos, no obstante la discriminación de bienes jurídicos que se hace en el proyecto, afecta la viabilidad del sistema económico, el cual se sustenta, fundamentalmente, en la confiabilidad de las operaciones.

Cabe destacar que el legislador tomó en cuenta las deficiencias de otras leyes donde no se preveían las penas accesorias. Así, en la ley encontramos que las penas para los hechos punibles que se encuentran tipificados son principales y accesorias.

Las Penas accesorias las siguientes:

- El decomiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos.

- El trabajo comunitario.

- La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión industria, o para laborar en instituciones o empresas del ramo.

- La suspensión del permiso, registro o autorización para operar el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información.

- Divulgación de la sentencia condenatoria.

- Indemnización civil a la víctima por los daños causados.

Responsabilidad de las personas jurídicas

Algunos de los hechos punibles previstos en la ley pueden ser perpetrados por intermedio de una persona jurídica o con el fin que ésta reciba sus efectos o beneficios, se establece los supuestos que harían procedente su responsabilidad, es así que los gerentes, administradores, directores o dependientes, actuando en su nombre o representación, responderán de acuerdo con su participación en el hecho punible.

Los Delitos Informáticos se clasifican en:

La ley clasifica los delitos informáticos de acuerdo al siguiente criterio:

1) Delitos contra los sistemas que utilizan tecnologías de información;

2) Delitos contra la propiedad;

3) Delitos contra la privacidad de las personas y de las comunicaciones;

4) Delitos contra niños, niñas o adolescentes;

5) Delitos contra el orden económico.

Delitos que se encuentran tipificados dentro de cada una de estas categorías.

Delitos contra los sistemas que utilizan tecnologías de Información:

- Acceso indebido. (Pena: Prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).

- Sabotaje o daño a sistemas. (Pena: Prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).

- Sabotaje o daño culposo. (Pena: se revisa el caso en concreto y se aplica una reducción entre la mitad y dos tercios).

- Acceso indebido o sabotaje a sistemas protegidos. (Pena: las penas previstas anteriormente se aumentarán entre una tercera parte y la mitad cuando los hechos recaigan sobre un componente que utilice tecnología de información protegido con alguna medida de seguridad).

- Posesión de equipos o prestación de servicios de sabotaje. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).

- Espionaje informático. (Pena: prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).

- Falsificación de documentos. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).

Delitos contra la propiedad:

- Hurto. (Pena: prisión de 2 a 6 años y multa 200 a 600 Unidades Tributarias).

- Fraude. (Pena: prisión de 3 a 7 años y multa de 300 a 700 Unidades Tributarias).

- Obtención indebida de bienes y servicios. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

- Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. (Pena: prisión 5 a 10 años y multa de 500 a 1000 Unidades Tributarias).

- Apropiación de tarjetas inteligentes o instrumentos análogos. (Pena: prisión de 1 a 5 años y multa de 10 a 50 Unidades Tributarias).

- Provisión indebida de bienes o servicios. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

- Posesión de equipo para falsificaciones. (Pena: prisión de 3 a 6 años y multa de 300 a 600 Unidades Tributarias).

Delitos contra la privacidad de las personas y de las comunicaciones:

- Violación de la privacidad de la data o información de carácter personal. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

- Violación de la privacidad de las comunicaciones. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

- Revelación indebida de data o información de carácter personal. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

Delitos contra niños, niñas o adolescentes:

- Difusión o exhibición de material pornográfico. (Pena: prisión de 2 a 6 años y multa de 200 a 600 Unidades Tributarias).

- Exhibición pornográfica de niños o adolescentes. (Pena: prisión de 4 a 8 años y multa de 400 a 800 Unidades Tributarias).

Delitos contra el orden económico:

- Apropiación de propiedad intelectual. (Pena: prisión de 1 a 5 años y multa de 100 a 500 Unidades Tributarias).

- Oferta Engañosa. (Pena: prisión de 1 a 5 años y multa de 100 a 500 Unidades Tributarias).

Es importante destacar otras Normas que se encuentran plasmada en esta Ley son las siguientes

Violación de la privacidad de la data o información de carácter personal:

Artículo 20.

> El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de

información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

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

Se fortalece la necesidad de proteger la intimidad personal cuando se manifiesta la sanción y cuando se usa la información por algún interesado con otros fines, siendo un castigo significativo.

Violación de la privacidad de las comunicaciones.

Artículo 21.

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

Es publico y notorio, la intención de cometer este hecho punible con fines delictivos, de espionaje, de intromisión, por ello se establece esta sanción , como hecho punible y repudiable en la sociedad. .

Revelación indebida de data o información de carácter personal.

Artículo 22.

> El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
> Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Se ha venido hablando de la necesidad de proteger con mayor fortaleza el derecho a la intimidad, a la dignidad humana, por ello existe una sanción ejemplarizante, ante la perpetración de este hecho punible .

En Venezuela la única vía que se tiene de ejercer el Derecho fundamental de rango Constitucional, es a través de la anterior Ley, dejando los medios de prueba de igual manera, pero considerándose insuficientes, por cuanto en muchos casos es difícil la comprobación de hechos punibles por esta vía, aún cuando las experticias sobre los equipos sea muy diligente. De allí parte los constantes abusos, en tarjetas de créditos, de debito, en cajeros automáticos y en cualquier otro delito con esta característica.

En todo caso, puede apreciarse en Venezuela se ha dado un paso importante en la legislación penal que regula los delitos informáticos pero que

debe continuar con su evolución para enfrentar la exigencias de un mundo en proceso de globalización.

En este proceso de globalización, conlleva una serie de adaptaciones legales por lo extenso de los comportamientos humanos, donde la ciencia y la tecnología, es señal de progreso y desarrollo a los pueblos, teniendo la necesidad de tener un soporte que sea capaz desarrollar las nuevas formas de crecimiento económico y social, por ello, en Venezuela comenzó con la aprobación de la Constitución de la República Bolivariana de Venezuela, que establece en su artículo 110 lo siguiente:

> Artículo 110. "El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía".

Teniendo como base este articulo constitucional, avanza Venezuela en la promulgación de la Ley Orgánica de Ciencia, Tecnología e Innovación, que tiene por objeto tal y como lo señala su artículo 1:

Artículo 1:

> El presente Decreto-Ley tiene por objeto desarrollar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela, organizar el Sistema Nacional de Ciencia, Tecnología e Innovación, definir los lineamientos que orientarán las políticas y estrategias para la actividad científica, tecnológica y de innovación, con la implantación de mecanismos institucionales y operativos para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para generación, uso y circulación del conocimiento y de impulsar el desarrollo nacional.

Reconociendo el esfuerzo que hace Venezuela en su intención de adaptarse a los nuevos tiempos, pero también debe ser el punto de partida para que de una manera ordenada , pueda , en su conjunto, aminorar los abusos y en su lugar se tenga una tecnología con seguridad y masiva al mismo tiempo, dentro de un marco de respeto y consideración.

Conclusiones

El Proceso Globalizado ha traído consigo una enorme responsabilidad para los dirigentes y lideres del mundo, para enfrentarse ante un decidido avance tecnológico, aún cuando ese proceso es generado por la inteligencia humana, los lideres y dirigentes, en el caso Venezolano, medianamente han iniciado la preocupación para asumir el reto que ha puesto en el camino de la sociedad moderna las nuevas tecnologías.

En primer lugar la valoración jurídica del Derecho a la Intimidad y de los derechos inherentes a la dignidad humana, desde un punto de vista procesal y probatorio, esta sujeto al código de procedimiento civil pero no se desarrolla en una Ley especial en materia Penal que sea mas coherente y con mas fortaleza para otorgarle mayor valoración jurídica, que permita su eficacia probatoria y su validez legal.

Las desventajas que presenta la indiferencia, tiene como resultado tres vertientes, la falta de confianza que tiene el usuario al momento de celebrar cualquier contratación por vía electrónica, pero excesiva confianza, cuando se trata de incorporarse a las redes sociales y por otra parte, es obligante cuando se tiene que aportar información y datos personales por razones tributarias.

La Intimidad personal, como un derecho que tienen los ciudadanos en Venezuela, se concluye que no ha sido desarrollada de manera directa, junto al derecho al honor y los derechos inherentes a la dignidad humana, porque se puede observar que existe la dispersión de criterios, por lo dinámico del tema pero se debe tratar de concentrar en un solo instrumento jurídico, a fin de que sea mas efectiva su protección y mas inmediato.

En el estudio se puede apreciar la regulación de la figura del Habeas Data para la protección de los datos personales, regulación realizada por la vía Jurisprudencial, ante la inexistencia de una ley que haya desarrollado el artículo 28 de la Constitución de la República Bolivariana de Venezuela.

En Venezuela se cuenta para proteger a los usuarios con las leyes de delitos informáticos y la ley sobre mensajes y firmas electrónicas, pero no son suficientes ni eficientes, por la dinámica de la misma revolución informática, aún cuando trata de abarcar toda la tipología penal.

Existe en Venezuela un sistema de Certificación Electrónica, que permite acceder a su servicio para obtener paginas y operaciones seguras, dependiente del ministerio del poder popular para la ciencia y tecnología

Debe involucrarse el usuario en la información e incentivo que debe tener para tener operaciones seguras, para obtener la certificación electrónica, producto de que no existe labores de divulgación de manera masiva.

El Ordenamiento Jurídico Venezolano, cuenta con la Analogía para resolver en parte los problemas que puedan derivarse de la contratación electrónica, de la violación de derechos a la intimidad , aún cuando, cuenta con Leyes que, en forma generalizada, hablan sobre el tema; el Estado Venezolano necesita a través de sus Instituciones la sinceración o regular la actividad contractual y obtención de datos personales por vía electrónica, a fin de ofrecer mayor confianza, evitando el fraude y el manejo inadecuado de los datos y firmas personales.

Al mismo tiempo, no existe un marco regulatorio o de obligatorio cumplimiento que lleve a la actividad electrónica, producto de la informática

y de la digitalización, a acceder a las certificación electrónica, dejando a discreción de los usuarios, buscando la protección del usuario y reflejándose con visión futurista, tomando en consideración que la Revolución Informática, no descansa, a diario aparecen nuevas y mejores versiones en ese campo de la Tecnología.

REFERENCIAS BIBLIOGRAFICAS

- Ballestrini Acuña, M. *Como se elabora el Proyecto de Investigación*. Caracas: BL Consultores Asociados. Servicio Editorial. (2002)

- Código Penal de Venezuela

- Código Orgánico Procesal Penal

- Constitución de la República Bolivariana de Venezuela (1999)

- Declaración Universal de los Derechos del Hombre, de 10 de Diciembre de 1948

- *Delitos informáticos: Qué son y cómo se previenen*. (visita: 5 de Diciembre de 2011). <http://www.estarinformado.com.ar/pag%20tecnologia/TECNOLOGIA-2.htm>.

- El Convenio para la protección de los Derechos Humanos y las Libertades fundamentales de Roma, o Convenio de Roma de 1950

- El Pacto Internacional de Derechos Económicos, Sociales y Culturales.ONU 1966.

- El Pacto Internacional de Derechos Civiles y políticos, o Pacto de New York. ONU 1966.

- Jiménez, L. *La Ley y el Delito*. Buenos Aires: Sudamericana. (1980).

- La Convención Americana Sobre Derechos Humanos o Pacto de San José de Costa Rica. 1969

- Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001)

- Ley especial contra los Delitos Informáticos publicada en gaceta oficial nº 37313 de fecha 30/10/2001.

- Ley Orgánica de Ciencia, Tecnología e Innovación, Gaceta Oficial Nº.37.291, miércoles 26 de septiembre de 2001.

- Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales. Caracas. Fondo Editorial de la Universidad Pedagógica Experimental Libertador. FEDUPEL.

- Mendoza, J. *Curso de Derecho Penal Venezolano*. Caracas: Empresa el cojo. (1986).

- Orta Martínez, R. *Efectos Jurídicos del Cambio de Clausulas legales en Facebook*. (2009)

- Pérez Luñio, A. *Derechos Humanos, Estado de Derecho y Constitución.* Editorial Tecnos. Madrid.España. (2003)

- Peñaranda, J. *Fiabilidad y Prueba del Documento Electrónico.* Caracas: www.monografias .com (2001)

- Rico, M. *Comercio Electrónico Internet y Derecho.* Colombia: Legis Editores, S.A. (2005)

- Rivera Morales, R. *Actividad Probatoria y Valoracion Racional de la Prueba.* Venezuela. (2010)

- Ruiz Jiménez, j. *El Derecho a la Intimidad, un cuaderno para el dialogo*. España. (1969)

- Superintendencia de Servicios de Certificación Electrónica www.suscerte.gob.ve Visita: lunes 16 de abril de 2012.Hora: 6:30 pm

- Toffler, A. *La Transformación Mundial y sus Implicaciones para Venezuela*. Caracas. Ponencia ante Conindustria. (1999)

- Obando Peralta, J. *Los Contratos Electrónicos y Digitales*. España: Revista de Derecho Informático Alfa –Redi. (2004) www.alfa-redi.org

.