APORTE INTERNACIONAL FRENTE A LOS DELITOS INFORMÁTICOS EN COLOMBIA Y SU EJECUCIÓN POR PARTE DE LAS AUTORIDADES COMPETENTES

ALEJANDRA CANO CUERVO

JUAN MANUEL DIAZ HEREDIA

CRISTIAN CAMILO MENDIETA VARGAS

CRISTIAN CAMILO RIVAS SANCHEZ

NICOLAS FERNANDO SANCHEZ CARVAJAL

UNIVERSIDAD LIBRE DE COLOMBIA

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

CENTRO DE INVESTIGACIÒNES SOCIO-JURIDICAS

BOGOTA D.C. 2014

APORTE INTERNACIONAL FRENTE A LOS DELITOS INFORMÁTICOS EN COLOMBIA Y SU EJECUCIÓN POR PARTE DE LAS AUTORIDADES COMPETENTES

ALEJANDRA CANO CUERVO

JUAN MANUEL DIAZ HEREDIA

CRISTIAN CAMILO MENDIETA VARGAS

CRISTIAN CAMILO RIVAS SANCHEZ

NICOLAS FERNANDO SANCHEZ CARVAJAL

Monografía De Grado Para Optar El Titulo De Bogotá

Docente Asesor:

José Rodríguez

UNIVERSIDAD LIBRE DE COLOMBIA

FACULTAD DE DERECHO Y CIENCIAS POLITICAS

CENTRO DE INVESTIGACIÒNES SOCIO-JURIDICAS

BOGOTA D.C. 2014

DEDICATORIA

Dedicado a nuestra familia,

por la colaboración y ayuda

forjándonos en la academia.

AUTORIDADES ACADEMICAS

PRESIDENTE NACIONAL

VICTOR HERNADO ALVARADO ARDILA

RECTOR NACIONAL

NICOLAS FERNANDO ZULETA HINCAPIE

CENSOR NACIONAL

ANTONIO JOSÉ LIZARAZO OCMAPO

SECRETARIO GENERAL

PABLO EMILIO CRUZ SAMBONI

PRESIDENTE SECCIONAL

EURIPIDES DE JESUS CUEVAS CUEVAS

RECTOR SECCIONAL

RAUL ENRIQUE CARO PORRAS

DECANO

JESUS HERNANDO ALVAREZ MORA

SECRATARIO ACADEMICO

ALVARO ALJURE MORENO

DIRECTOR CENTRO DE INVESTIGACIONES

JOSÉ HELVERT RAMOS NOCUA

COORDINADOR AREA DE INVESTIGACION

JOSUE OTTO DE QUESADA

NOTA DE ACEPTACIÒN

_____

_____

_____

_____

Presidente Del Jurado.

_____

Jurado.

_____

Jurado.

AGRADECIMIENTOS

Agradecemos a nuestros familiares, quienes siempre están presentes para ayudar y motivar nuestros logros académicos.

En primera instancia agradecemos a nuestros padres, los cuales han sido un pilar para fomentar nuestra educación. A nuestros hermanos quienes han sido apoyo.

CONTENIDO

CAPITULO II

2. CONCEPTO DELITO INFORMÁTICO

CAPITULO III

3. TIPOS PENALES INFORMÁTICOS

CAPITULO IV

4. PROPUESTA TRATAMIENTO DERECHO PENAL FRENTE A LOS DELITOS INFORMÁTICOS

INTRODUCCIÓN.

La globalización junto con el desarrollo acelerado de la ciencia, la tecnología y la información, han cambiado las costumbres de los individuos ya que la mayoría de transacciones e interacciones con los demás se realizan a través de medios electromagnéticos; está actividad ha logrado que se aceleren las comunicaciones y sean más eficaces, pero también ha conseguido fomentar el riesgo de algunos bienes jurídicos expuestos por este medio.

A través de esta interacción se puede delinquir, por ello se han creado nuevas tipologías del delito que han hecho que el Código Penal modifique y adicione diferentes conductas desviadas que son ejecutadas a través de medios electrónicos.

Por tal motivo es necesario iniciar la presente investigación que consta de cuatro pilares fundamentales para el conocimiento y comprensión de esta investigación.

Como primera referencia, se plantea el problema de investigación teniendo en cuenta los tipos penales informáticos en Colombia y el incremento de estas conductas en la sociedad, se identifica la difícil tarea que enfrentan las autoridades al investigar los delitos cometidos a través de la internet; el segundo punto, se reflejará la falta de capacitación de las autoridades frente a los delitos informáticos; en tercer punto se verificará la falta de seguimiento de las autoridades conforme a los comportamientos irregulares tecnológicos e informáticos y el cuarto punto consta de la educación frente al manejo de las redes tecnológicas para evitar el daño a los bienes jurídicamente tutelados de las personas que pueden estar en riesgo en la internet.

Realizar este tipo de investigación motiva al estudiante de derecho, porque es un tema novedoso, atiende a la protección de derechos constitucionales, la manera de sancionar aquellas conductas que amenacen o vulneren los bienes jurídicos expuestos en redes informáticas, observar la necesidad de regular los delitos de

acuerdo a las conductas desviadas observadas por las autoridades competentes que se presentan a nivel nacional e internacional.

Como objetivos se plantean analizar los delitos informáticos a nivel nacional e internacional, informar los conceptos que se plasman en la doctrina e identificar las características y elementos de los delitos informáticos en la ley 1273 de 2009 que establece la protección de la información y los datos como bienes jurídicamente tutelados.

Es importante resaltar las diferentes formas que la tecnología ha determinado los hechos constituidos para delinquir, aquellas conductas las cuales infringen el tipo penal establecido y que ha tenido que ser reformado a través de la historia debido al desarrollo de la tecnología y la globalización.

Estos tipos de delitos en nuestra sociedad se han incrementado en los últimos tiempos, por diferentes motivos, el primero lo podemos identificar de acuerdo a la difícil tarea de investigar los delitos cometidos a través de la internet, el segundo, la falta de capacitación de las autoridades frente a estos delitos y tercero, la falta de seguimiento de las autoridades ante estos comportamientos irregulares tecnológicos e informáticos.

La ciberdelincuencia merece un trato especial frente a los demás delitos en cuanto a la investigación y ejecución de pruebas, la falta de restricción en las actividades en internet y diferentes medio informáticos ha permitido el detrimento de los bienes de las personas y de la Nación.

Los datos de las personas tanto personales, como patrimoniales han sido expuestos en los medio informáticos, sin que se haya ideado algún tipo de protección de los mismos, cualquier clase de manipulación puede violentar y divulgar información estrictamente privada, o violar ciertas restricciones que nuestros derechos imponen para mantener la seguridad de nuestro bienes jurídicamente tutelados.

Es menester tener en cuenta el tratamiento de las diferentes naciones frente a estos delitos informáticos, las sanciones proporcionales de acuerdo al daño causado y las investigaciones que se llevan a cabo por parte de las autoridades encargas de vigilar el comportamiento de las personas conforme a los lineamientos normativos.

Se analizaran diferentes estudios de los delitos informáticos, tomados como manuales, actualizando al profesional del derecho en los distintos delitos tecnológicos, *"(…) no puede ser indiferente a ninguna persona cuya vida se encuentra condicionada por los parámetros sociales y estatales cada vez más inclinados hacia la virtualidad. Contiene reflexiones fruto de la experiencia personal en este campo, que en Colombia no ha sido ampliamente abordado salvo contadas excepciones, y representa un aporte, con el objeto de sensibilizar sobre una materia cuya relevancia se incrementa de forma incesante por el fenómeno que representa la convivencia con las nuevas tecnologías de la información y las comunicaciones.[1]"*

[1] PALOMA PARRA. Luis Orlando. "Delitos informáticos en el ciberespacio doctrina y análisis de casos reales". Ediciones jurídicas Andrés Morales. Bogotá. 2012. Pág. 23

CAPITULO I

1 PLANTEAMINTO DEL PROBLEMA SOCIO – JURIDICO DE LA INVESTIGACION

1.1 IDENTIFICACION DEL PROBLEMA SOCIOJURIDICO

Dentro del proyecto de investigación se hace necesario resaltar la problemática objeto del tema de delitos informáticos regulado en Colombia, los ataques al sistema tecnológico y de seguridad que han sido incrementados en los últimos tiempos obteniendo como resultado la vulneración de derechos de las personas en aspectos económicos y personales.

Las leyes en Colombia no han sido suficientes para la seguridad en el mundo cibernético, falta crear criterios mundiales que efectivicen los sistemas de seguridad en las redes, respetando los espacios virtuales cumpliendo con los deberes y libertades que cada persona cuenta en el uso de estos medios electrónicos.

Los cambios sociales que ha sufrido la población Colombiana frente a los cambios tecnológicos y la mutación de los delitos cibernéticos.

"No obstante, como todo gran desarrollo técnico humano, de forma paralela con las bondades suscitadas en este escenario, se han manifestado practicas negativas con la incursión de nuevas modalidades de conductas susceptibles de tipificarse como delitos, las cuales han proliferado gracias a la dependencia tecnológica del ciudadano del nuevo milenio, registrando un nuevo capítulo en la antigua historia del derecho penal y la defensa de los pilares de la sociedad"[2].

[2] PALOMA PARRA. Luis Orlando. "Delitos informáticos en el ciberespacio doctrina y análisis de casos reales". Ediciones jurídicas Andrés Morales. Bogotá. 2012. Pág. 25

Conforme lo anterior es necesario verificar la restricción y la falta de control de las autoridades competentes frente al incremento de los delitos informáticos, ya que estos son los que tienen la responsabilidad de garantizar la seguridad y el bienestar de la comunidad.

1.2 DELIMITACION DEL PROBLEMA SOCIO JURIDICO

1.2.1 TIEMPO

El problema socio jurídico lo establecemos con posterior a la promulgación de la ley 1273 – 2009. Enfatizando en los periodos 2013 – 2014. Los cuales se ven incremento de conductas punibles de bandas organizadas a nivel de los delitos informáticos.

1.2.2 ESPACIO

El estudio socio jurídico que se va hacer frente al aporte internacional de los delitos informáticos es a nivel nacional, el cual es donde se ve afectado la territorialidad de nuestra legislación. Ya que es donde las bandas delincuenciales y los sujetos de acción realizan sus conductas.

1.2.3 SUJETOS

Son las personas que ejecutan la acción de la conducta de delitos informáticos, como aquellos sujetos activos, y los sujetos pasivos, los cuales se comprenden entre las edades de 12 a 24 años. De los que se hablara en las tablas indicadas por el DANE, en el Capítulo IV de la investigación.

1.3 DESCRIPCION DE LA SITUACION PROBLEMICA SOCIO – JURIDICA DE LA INVESTIGACION.

LOS ATAQUES DE LOS CIBERDELINCUENTES A LA SOCIEDAD

En Colombia se ha regulado sobre los ataques cibernéticos, los cuales al paso del tiempo y el desarrollo tecnológico, son cada día más complejos para garantizar la protección de la información.

Estos ataques como eje esencial buscan desestabilizar la seguridad del estado y existen otros que tienen la finalidad de combatir la seguridad personal, como lo hemos visto actualmente existen hackers con intención de perturbar la información e intimidad de las personas.

Es así que Colombia ha regulado y tipificado a los delitos informáticos en nuestro Código Penal, para poder judicializar a estos vándalos. Pero como el problema socio jurídico existente es que los jueces no tienen conocimiento para adecuar esa tipificación en nuestra legislación. Ni las autoridades tienen el conocimiento sobre ataques y protección a los datos.
Se hace necesaria la implementación de políticas educativas para capacitar a las autoridades ejerciendo un control automático; como es vista nuestras fuerzas armadas, han sido sobresalientes en políticas de guerra civil, pero se hace necesario que tengan conocimiento sobre ataques cibernéticos para controlar y contrarrestar las acciones delincuenciales.

De esta manera manifestando al Estado y sociedad que se encuentran seguros y protegidos en sus derechos a la seguridad e integridad personal.

1.4 FORMULACION DEL PROBELMA SOCIO – JURIDICO DE LA INVESTIGACION.

¿Qué impacto tiene la ausencia del control de las autoridades competentes nacionales frente a los delitos informáticos que se ejecutan en Colombia?

1.4.1 SISTEMATIZACION PROBLEMA SOCIO – JURIDICO DE LA INVESTIGACION

- ¿Cuáles son las políticas implementadas por las autoridades frente a los delitos informáticos y sus falencias?
- ¿Por qué las autoridades competentes para legalizar la captura de los delincuentes no implementan esta tipificación?
- ¿Cuál es la forma idónea para regular e informar a los integrantes de la red?
- ¿Cómo probar que los presuntos delincuentes han cometido dicho delito?

1.5 JUSTIFICACION DE LA INVESTIGACION

La importancia del estudio propuesto es en primera medida la novedad de los delitos informáticos en el derecho penal, la adición y modificación de diferentes tipos penales conforme a la evolución del delito a través de las redes.

Es pertinente identificar en qué momento de la historia se dio inicio a la ejecución de estos delitos informáticos y la evolución en la tipificación de los mismas, los medios probatorios o el seguimiento que hacen las autoridades como cuerpo especial de policía que debe estar acorde con la alta tecnología.

Así mismo, la viabilidad de las investigaciones en la utilización de herramientas idóneas que prevengan, identifique y pongan fin a los delitos informáticos, para

hacer efectiva la seguridad de los bienes jurídicamente tutelados de las personas que usan los medios electromagnéticos y que entran al ciberespacio.

Por ello, es importante identificar los aportes internacionales aplicados en la normatividad en Colombia frente a los delitos informáticos, los derechos que se pueden afectar con las mismas conductas y la importancia en la educación frente a la manipulación de medios tecnológicos, que pueden dar como resultado conductas desviadas de fácil ejecución que deben ser sancionadas por la jurisdicción penal y otro tipo de responsabilidades donde el garante es el Estado frente a los derechos de la colectividad limitando aquellas potestades que amenazan o vulneran.

Son muy pocos los estudios que cuestionan la utilización de los medios informáticos dentro del ciberespacio y las modalidades de cibercrimen, distinguiendo la falta de vigilancia por las autoridades o los administradores de las redes ofrecidas por internet, es importante reflejar a través de la presente investigación que este sistema contiene unos límites para su utilización y que su mal uso puede engendrar algún tipo de responsabilidad penal y un desmedro de algún derecho personal o colectivo.

Es necesario observar las diferentes herramientas que utilizan los delincuentes cibernéticos, para poder identificarlas, prevenirlas y denunciarlas a tiempo para que con ayuda de todos los ciudadanos pueda erradicarse esta manera de delinquir que pone en riesgo derechos personales, familiares, económicos, etc.

1.6 OBJETIVOS

1.6.1. Objetivo General

Debatir el impacto de los delitos informáticos por la ausencia de control de las autoridades competentes en Colombia.

1.6.2 Objetivos Específicos.

- Examinar los diferentes conceptos que se encuentran en la doctrina sobre delitos informáticos
- Identificar las características y elementos de los delitos informáticos
- Analizar la normatividad y los límites existentes de los delitos informáticos a nivel nacional e internacional.
- Establecer el impacto de los delitos informáticos en la sociedad
- Determinar la educación y los retos de la investigación de los delitos informáticos para prevenirlos en Colombia.

1.7 HIPOTESIS.

Como variable inicial, determinamos que el impacto generado por la falta de control de las autoridades frente a los delitos informáticos que se presentan en Colombia tiene efectos negativos en la sociedad, ya que no se identifican a tiempo las bandas delincuenciales que cada día crecen más, observando que la ruptura original es la falta de actualización de las autoridades frente a los medios tecnológicos, empeorando gravemente la lesión de los bienes jurídicamente tutelados de los usuarios en la ciberespacio.

Por ello es necesario que las autoridades competentes creen estrategias eficaces para poder prevenir o descubrir a tiempo las conductas que se configuran dentro de los delitos informáticos.

El Estado ha capacitado a la autoridad competente ampliando sus conocimientos basados en tecnologías aplicadas que tienen como fin la protección de los bienes jurídicamente tutelados, en el orden económico, político, social y cultural con el cumplimiento de los fines de la Nación; pero estas mismas no han sido suficientes, es necesario que se lleve a cabo una actualización a nivel internacional, adquirir equipos de última tecnología que coadyuven con la tarea de

erradicar el crimen en los medios electromagnéticos y se genere seguridad en las redes.

Algunas de las trampas que han ideado los ciberdelincuentes han tenido con preocupación a las autoridades del Estado Colombiano, según comunicado por parte de La Dirección de Investigación Criminal e Interpol (DIJIN), ya que estos deben generar seguridad en todas las actuaciones de las personas en la sociedad y permitir que se creen estrategias que permitan hacer seguimiento oportuno a las personas que realizan conductas desviadas.

Es importante tener en cuenta la legislación nacional e internacional verificando el proceso que se lleva a cabo para la protección de la información que se expone en los medios electromagnéticos, la reserva que debe tener de la misma, la confidencialidad, las restricciones, etc., conforme a los derechos que pueden ser vulnerados o amenazados por estos medios tecnológicos.

Es tarea de los usuarios en compañía de las autoridades denunciar a tiempo cualquier irregularidad en los medios tecnológicos, ya que es un medio que se facilita para el delinquir donde se hace más difícil su investigación y seguimiento al delincuente

1.8 ESTRATEGIA METODOLOGICA.

1.8.1 Población

Se manejara una población que se encuentra entre las edades de 12 a 24 años, en las cabeceras municipales a nivel nacional, según informe del DANE la cual se informara más adelante en los Capítulos siguientes.

1.8.2 Formas de Investigación.

1.8.2.1 Básica

1.8.2.1.1 Jurídica

Aporte internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes

Este título se complementa ya que para los lectores infiere que se toman los aportes internacionales y la regulación existente en Colombia frente a la tipificación de los delitos informáticos.

1.8.2.2 Aplicada

1.8.2.2.1 Socio – Jurídica

Será la investigación socio jurídica, teniendo en cuenta los hechos acontecidos en la sociedad de acuerdo a las tecnologías manejadas en la actualidad y los delitos que emergen de esta actividad.

Estudia el derecho en la vida social, en su práctica social, en el mundo material las investigaciones socio jurídicas están orientadas a estudiar la condicionalidad social del derecho, a los efectos de éste en la sociedad y a su eficacia como norma reguladora de relaciones sociales.[3]

1.8.3 Tipo de Investigación.

1.8.3.1 Explicativa

Tiende a exponer los eventos de la sociedad y la regulación que se le ha dado por parte del Estado a través de las normas reguladoras de los delitos informáticos y su incidencia en el comportamiento de las personas conforme a la tecnología aplicada en la actualidad.

Este tipo de investigaciones “están dirigidas a responder a las causas de los eventos físicos o sociales. Como su nombre lo indica, su interés se

[3] BALLEN. Rafael. Guía para la elaboración de proyectos de investigación. Universidad Libre de Colombia. Facultad de derecho. Bogotá. 2010. Pág. 50-60

centra en explicar por qué ocurre un fenómeno y en qué condiciones se da éste, o por qué dos o más variables están relacionadas".[4]

1.8.4 Método de Investigación

1.8.4.1 Teórico

Utilizando el método teórico, partiendo del análisis y síntesis, descomponiendo el objeto investigado en todas sus partes, relacionando el delito informático y sus características no solo en Colombia sino a nivel mundial ya que la globalización transportó la tecnología a diferentes comportamientos que pueden verse desviados debido a la falta de control por las autoridades.

> El fin del análisis es el de llegar al conocimiento de las partes como elementos de un todo complejo, en ver que nexos se dan entre ellos y las leyes a que está sujeto el todo en su desarrollo. Por su parte, la síntesis es la unión que forma un todo íntegro de las partes, propiedades y relaciones delimitadas por medio del análisis, pasando de lo esencial a lo múltiple, uniendo lo general a lo singular, la unidad y la multiplicidad en un todo concreto, vivo. La síntesis completa al análisis y forma con él una unidad indisoluble, relacionada con el mundo circundante, exterior y la actividad práctica del hombre.[5]

[4] Ibíd. Pág. 50-60
[5] Ibíd. Pág. 50-60

CAPITULO II

2 CONCEPTO DELITO INFORMÁTICO

Los delitos informáticos han evolucionado y han sido objeto de investigación de muchos doctrinantes, de los cuales partimos para comprender y así realizar un concepto práctico para nuestra sociedad.

Según Henry William Torres autor del libro "derecho penal de la informática" el delito informático es:

> "(…) una estrecha relación con las actividades criminales que en una primera instancia los diferentes tratadistas y doctrinales han tratado de encuadrar en figuras típicas de carácter tradicional, dado que mucho de ellos no constituyen una nueva categoría delictiva sino que son los mismos delitos que ya se vienen castigando, delitos contra las personas, el honor, la libertad, la seguridad pública, la nación, tales como robo, hurto, fraude, falsedad, sabotaje, espionaje, terrorismo, narcotráfico. Pero no se puede negar que entre, el conocimiento, la información, los computadores y los sistemas han originado nuevos enfoques, conductas, incluidas las marginales y su dificultad de control. El desarrollo en las tecnologías informáticas ha creado nuevas posibilidades al uso indebido de los sistemas informáticos lo que ha propiciado a su vez a la necesidad de regulación por parte de los legisladores, gobiernos y administraciones, unificación en la perceptibilidad y globalización de criterios, esfuerzos, normas, control y aplicaciones."[6]

Lo anterior explica que, los delitos informáticos atentan contra cualquier derecho constitucional reconocido en la carta magna y los derechos humanos, por ello es importante que se legisle de manera idónea para asegurar los derechos inalienables, imprescriptibles e inviolables.

Los delitos informáticos han venido tipificándose, pero quedando algunos otros por fuera del marco normativo, entonces, es importante analizar aquellos que

[6] TORRES TORRES. Henry William. Derecho penal de la informática. Edición jurídica Gustavo Ibáñez. Medellín- Colombia. 2002. Pág. 21

están regulados y las conductas que en el diario continúan ilustrándose en la lesión de los bienes jurídicamente tutelados.

Según Julio Téllez Valdés miembro del instituto de investigaciones jurídicas de la Universidad Nacional Autónoma de México define el delito informático "como la comisión de verdaderos actos ilícitos en los que se tengan a las computadoras como instrumento o fin.[7]

En cuanto nos refiere María de la Luz Lima[8], abogada y tratadista del delito informático el delito tecnológico es "cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[9]

Cada uno de ellos han concluido que referirse a los delitos informáticos cada vez ha sido más complejo, debido al dinamismo y evolución de las Tecnologías de la Información y Comunicación (TIC) siendo conductas innovadoras, pues en esta materia especializada y técnica que no es de mayor entendimiento para los profesionales en derecho, legisladores y juristas, deben adquirir y conocer la caracterización de las conductas informáticas ilícitas.

Armonizados en lo anterior se crea un concepto practico, donde es de vital importancia comprender al delito; como aquella conducta que va en contra vía de los bienes jurídicamente tutelados de las personas, aquella conducta que es típica, antijurídica y culpable; ahora bien, definamos que es informática, es una ciencia que estudia las diferentes tecnologías, o mejor definido por el diccionario de la real Academia Española es "conjunto de conocimientos científicos y técnicas

[7] VALDES TELLES. Julio. Derecho informático. Edición McGraw-Hill/Interamericana. México. 2008. Pag. 163
[8] LIMA. de la LUZ María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero-Julio 1984.
[9] Ibíd. Pág. 87

que hacen posible el tratamiento automático de la información por medio de ordenadores"[10]

Entonces haciendo un concepto técnico el delito informático, es aquella conducta típica, antijurídica y culpable realizada en medios informáticos u ordenadores que hacen posible el tratamiento automático de la información.

2.1 TRATAMIENTO DELITOS INFORMÁTICOS EN EL MUNDO.

Quienes se encuentran regulando este delito a nivel mundial, ha sido a través de distintas organizaciones, como la Organización de las Naciones Unidas (ONU), la Unión Internacional de Telecomunicaciones (UIT), Organización de Cooperación y Desarrollo Económico (OCDE); cada una ha realizado aportes de información y descubriendo cada tipificación por parte de los ciberdelincuentes, de igual forma hacen convenciones para determinar y actualizar la ejecución de los delitos informáticos.

Al indagar se dispuso que a nivel mundial los países han reglamentado y legislado de manera preventiva, ejecutado políticas de protección para esta tipología (como distinguiremos más adelante), según el profesor Pedro J. Montano, del área de Derecho Penal de la Universidad de la República de la ciudad de Montevideo – Uruguay "se han adoptado textos especiales, en muchos casos multiarticulados y orgánicamente estructurados, como si fuesen códigos ad hoc[11] refiriéndose a la técnica que se implementa en diversas naciones.

2.1.1 ORGANIZACIÓN DE NACIONES UNIDAS (ONU).

[10] RAE. Significado informática. Consultado el día 20 de Enero del año 2014 en la página web http://lema.rae.es/drae/srv/search?key=inform%C3%A1tica
[11] MONTANO, Pedro J. "Nuevos desafíos en Derecho Penal Económico". Editorial B de F. Montevideo – Buenos Aires. 2012. Pág. 188.

Esta organización ha desarrollado investigaciones sobre temas de prevención y control de los delitos informáticos, a lo cual realizó un Manual donde contiene un capítulo sobre seguridad de la información y la prevención de los delitos cibernéticos.[12]

En el congreso número 12 de las Naciones Unidas sobre la Prevención del Delito y Justicia Penal realizado en el año 2010, se debatieron las diferentes conductas en el panorama mundial, pues se demostró que al avanzar la tecnología, los delitos y las prácticas de igual forma evolucionan, convirtiéndose en un reto para las autoridades regularlo antes que se vea disminuido el patrimonio de las personas.

La ONU en su preámbulo sobre la delincuencia y el delito informático informa que desde el año de 1960 hasta el año de 1980, los Estados tuvieron que hacer frente a nuevos actos, tales como la manipulación informática y el espionaje de datos, para los que no había legislación penal. En esos años, el debate se centró en la elaboración de una respuesta jurídica.[13]

Al analizar dicho documento, se alcanza inferir que el incremento de usuarios en la internet desde los años en que dicha práctica era utilizado por pocos, hasta la década de los noventa donde se incrementó potencialmente el intercambio de información y la agilidad para llegar a otro país, fue uno de los grandes retos para dicha organización, ya que los inescrupulosos se aprovechan de tal situación

[12] Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente Viena, 10 a 17 de abril de 2000. http://www.uncjin.org/Documents/congr10/10s.pdf (consultado el día 27 de agosto de 2014)

[13] 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal Salvador (Brasil), 12 a 19 de abril de 2010. https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf (Consultado el día 27 de Agosto de 2014)

para delinquir con espacios transnacionales, a través de ello determina la ONU que la soberanía de los países y las relaciones internacionales, juegan un papel importante para perseguir a ciberdelincuentes, demostrando así que se han generado fraudes a nivel internacional a través de la herramienta de internet.

En el primer decenio del siglo XXI han predominado los métodos nuevos y sofisticados para delinquir (tales como la "pesca de datos" o "*phishing*" y los ataques con redes zombi o *"botnets*" y el uso de tecnologías que resultan aún más difíciles de controlar para los funcionarios encargados de las investigaciones (tales como las comunicaciones con transmisión de voz sobre protocolo de internet *(VoIP*) y la informática en nube *("cloud computing*").[14]

2.1.2 UNION INTERNACIONAL DE TELECOMUNICACIONES (UIT)

Este es un agencia con especialidad en las tecnologías de la información y comunicación (TIC) perteneciente a las Naciones Unidas. La cual ha colaborado en guías y foros para países en desarrollo en temas del ciberdelito, el cual atiende a problemáticas y repercusiones de los delitos informáticos.

Esta agencia ha nutrido sobre temas importantes en nuestra sociedad como el ciberdelito y la ciberseguridad, fue ente regulador en la cumbre mundial de la sociedad de la información, realizada en Ginebra y Túnez

[14] 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal Salvador (Brasil), 12 a 19 de abril de 2010. https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf (Consultado el día 27 de Agosto de 2014)

respectivamente, donde se argumentó la internacionalización de la información.

En dicha cumbre se reglamentaron e implementaron criterios para la ayuda internacional de los estados en la cual concibieron:

C5. Creación de la confianza y seguridad en la utilización de las TIC. La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información. [15]

> b) Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel internacional para la prevención, detección y recuperación de estos incidentes; y alentando la educación y la sensibilización.[16]

2.1.3 ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLO ECONÓMICO (OCDE).

Este organismo publicó un informe sobre los delitos de la informática, de sus normas vigentes, colaborando con los países estudiando reformas que pudieran aportar a la prohibición del fraude, alteración de datos, sabotaje, interceptación y demás delitos que invaden la seguridad de las personas.

El tratamiento que se ha dado fuerte con la lucha en contra del ciberterrorismo, globalización y ciberespacio la ha dado Estados

[15] El Ciberdelito Guía Para Los Países En Desarrollo. Pág. 101. http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf (Consultado el día 28 de Agosto de 2014)
[16] Ibídem. Pág. 102

Unidos, con la ley patriótica en el año de 2011, la cual origina un precedente mundial, mejorando la seguridad en los sistemas de las oficinas oficiales y privadas.

(…) *Las decisiones tomadas por el organismo coordinador de los recursos se basaran primordialmente en fortalecer la infraestructura tecnológica informativa y telemática con los más avanzados sistemas que utilizan la inteligencia artificial, para determinar las tendencias del trafico informacional y los comportamientos al interior de las redes de comunicación, con el objeto de descubrir situaciones anómalas que pongan en riesgo la estabilidad mundial. Estos sistemas son básicamente modelos proactivos y no reactivos y sus objetivos son las distintas modalidades de ciberterrorismo incluidos los ataques con armas químicas y biológicas*.[17]

Los sistemas de inteligencia de los gobiernos se han visto invadidos sin darse cuenta, de allí se derivan intereses políticos, económicos y culturales, no es un secreto que Estados Unidos ha interferido en la regulación de conflictos de otros países, invadiendo la soberanía y originando diversas conductas que ponen en riesgo la vida y la integridad de las personas, de acuerdo con actos terroristas de los que ha sido víctima este país.

La expedición de la ley patriótica genero toda suerte de efectos, involucrando de esa manera todas las actividades económicas que de forma directa se sirve de internet para interactuar en un esquema económico global. Ciertamente la red de redes no puede hoy catalogarse como un simple “instrumento” y/o como un “novedoso canal alterno de distribución y negociación”. Es ante todo un dinámico espacio

[17] GUERRERO. Mateus María Fernanda. La ciberdelincuencia La ley patriótica y los efectos globales en las regulaciones nacionales y en particular en el caso Colombiano. Editorial Imprenta Nacional de Colombia. 2004. Pág. 24

de comunicación universal donde todos estamos acompañados. Es un espacio en el que interactúan de manera directa los agentes participantes de distintos mercados, así como aquellos participantes cuya actividad principal está en ser operadores o facilitadores de la comunicación en internet.[18]

Aunado en lo anterior, se expone el artículo 362 de dicha ley para conocer sobre las medidas implementadas por los legisladores de los Estados Unidos.

Artículo 362. Establecimiento de una red de alta seguridad.

(a) En general. El Secretario establecerá una red de alta seguridad en la Red de Juzgamiento de Delitos Financieros, que:

(1) permita a las entidades financieras presentar los informes exigidos en virtud del Título 31, capítulo 53, sub-capítulo I ó II del U.S. Code, el capítulo 2 de la Ley Pública 91-508, o el Art. 21 de la Ley Federal de Seguro de Depósitos, a través de dicha red de alta seguridad; y

(2) brinde a las entidades financieras alertas y demás información relativa a actividades sospechosas que justifiquen una vigilancia inmediata y más estrecha.

(b) Rápido desarrollo. El Secretario tomará medidas destinadas a asegurar que la red de alta seguridad prevista en el inciso (a) precedente se encuentra totalmente operativa antes de transcurridos nueve meses a partir de la fecha de dictado de la presente Ley.[19]

Dentro del resumen de leyes que se tipificaron por medio de esta ley se caracterizan por sancionar toda aquella conducta que ponga en riesgo

[18] Ibíd. Pág. 26.
[19] Ley patriótica de los Estados Unidos. http://www.interamericanusa.com/articulos/Leyes/US-Patriot%20Act.htm#A301 (Consultado 05 de Junio de 2014)

el patrimonio de las personas y del Estado. Adicionalmente, se juzga a los servidores que tengan acceso a información secreta, donde cualquier irregularidad en el procedimiento dará de inmediato a su investigación, regula todas las actuaciones financieras, el uso de la moneda y evita a todo lugar la corrupción y los actos terroristas.

La globalización ha generado que la herramienta de la internet sea utilizada para vulnerar los límites de la soberanía de otros países y violar o quebrantar los derechos constitucionales de las personas.

La forma en que se define y explica el patriotismo ciudadano por la ley patriótica nos permite apreciar allí tres manifestaciones fundamentales; la primera hace referencia a la necesidad de una ética universal que permita establecimiento de responsabilidades por el futuro de la humanidad y, particularmente, por las consecuencias del progreso técnico, donde la ausencia de esa ética impedirá un ordenado y justo desarrollo de la globalización informática y financiera abriendo abismos insalvables y, por ende, no propiciaría el gran anhelo de la ciudadanía multicultural y cosmopolita. Para explicar esta primera manifestación se cuenta, dentro de los modelos establecidos para llegar a la ética universal, con el modelo que, basado en la argumentación, sostiene el carácter obligatorio de una ética universal, que se presenta como una ética de corresponsabilidad por las consecuencias de las acciones colectivas.[20]

Para María Fernanda Guerrero Mateus, se encuentran métodos para combatir la delincuencia por medio de un procedimiento "estratégico preventivo" como aquellas técnicas que implementó el gobierno de los Estados Unidos con apoyo del FBI, de un programa llamado "carnívoro". Este programa trabaja sobre un sistema de información

[20] GUERRERO. Mateus María Fernanda. La ciberdelincuencia La ley patriótica y los efectos globales en las regulaciones nacionales y en particular en el caso Colombiano. Editorial Imprenta Nacional de Colombia. 2004. Pág. 31.

particularizada, intercepta comunicaciones, a través de claves que permiten el acceso a correos electrónicos, Messenger y chat.[21]

Es así que al FBI se le instauro como ente regulador y protector del mencionado programa, a través de ello, recauda distintas pruebas que requieren por internet y son de carácter importante en el desarrollo de procesos de delitos graves; de acuerdo con distintos proveedores de internet, trabajan de la mano asumiendo que es una tarea de orden judicial y que requiere de la atención de los proveedores para que a con estos programas no se generen alguna clase de delitos ya que podrían tener alguna responsabilidad por no suministrar los límites y auditorias necesarias para mantener la seguridad de sus usuarios.

De esta manera se puede inferir que las medidas tomadas por medio de la ley Patriótica dan un ejemplo del cual los Estados toman precauciones y prevenciones a raíz de los actos cometidos por los ciberdelincuentes al amenazar el orden público y defender los intereses particulares.

2.2 DELITO ELECTRÓNICO EN COLOMBIA.

Como antecedente podemos estipular que la primera regulación y definición establecida en Colombia frente al uso de los mensajes de datos, del comercio electrónico y de las firmas digitales fue la ley 527 de 1999[22], sancionada por el Presidente Andrés Pastrana Arango. En la cual informa y estableces los requisitos jurídicos de carácter procedimental.

[21] Ibídem. Pág. 65.
[22] COLOMBIA, Congreso de la Republica. Ley 527 de 1999. DIARIO OFICIAL Santafé de Bogotá, Sábado 21 de agosto de 1999 Año CXXXV No. 43.673.

Estructuralmente se estudió el delito electrónico en el año de 2006 cuando el Gobierno Nacional, distinguió la necesidad de legislar sobre esta materia junto con la Universidad de Cali.

Se realizó el primer foro sobre fraude en la contratación electrónica en el año 2007, en la Universidad Santiago de Cali, abriendo un debate a nivel nacional e internacional, acto seguido en el año de 2008 se realizó un congreso mundial de derecho informático, donde participaron varias personas ilustres en el derecho, consultando a su vez con representantes de la cámara y del senado,

Se propuso el proyecto de ley llamado "por medio del cual se crea el bien jurídicamente tutelado, denominado de la protección de la información y datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones", siendo aprobado este entendiendo su necesidad.

De las precisiones iníciales en la exposición de motivos del proyecto de ley anteriormente mencionado, se tomaron en cuenta los riesgos al utilizar los computadores y las amenazas que sufren las personas y las empresas al exponer su información, "la proliferación de estos instrumentos que se han constituido en la principal herramienta de funcionamiento en casi todos los niveles de convivencia, así como la creación de la red global, ha provocado que cada vez más personas se las ingenien para lucrarse, hacer daño o causar perjuicios a través del uso de estos instrumentos"[23]

El proyecto de ley tenía un fin y era regular aquellas conductas que habían quedado por fuera de la regulación penal e imponer sanciones para los que infringen el mundo del ciberespacio en pro de intereses individuales.

[23] RINCON. Ríos Jarvey. delito electrónico en Colombia. editorial universidad Santiago de Cali. Aseuc. 2009. pág. 22.

Para el debate fue necesario validar los documentos electrónicos y su legitimidad, estableciendo lo que se configura como un delito informático y una conducta punible usando medios electrónicos para la consumación del delito.

Lo anterior sumamente importante para destacar futuras diferencias de los que se configura como delitos informáticos y la manipulación de sistemas electrónicos para consumar un delito establecido ya en la ley penal ósea típico.

Para que los legisladores pudieran hablar de delitos informáticos se vio en la entera necesidad de verificar dos presupuestos.

a) Que la conducta constitutiva del mismo este tipificada en la ley.
b) Que mediante sentencia condenatoria en la cual el funcionario judicial, haya declarado probada la existencia concreta de una conducta típica, antijurídica y culpable del delito informático.

Precisando lo que se constituye como bienes jurídicamente tutelados y determinar si dicha ilicitud se encuadra en alguno tipo penal de nuestra legislación. Con el fin primordial de que la sociedad Colombiana, no se encuentre afectada por la interacción del ciberespacio y garantizar a todos las personas que utilizan movimientos por medio de la internet, que sus derechos se encuentran protegidos.

El derecho penal, pues, tiene su razón de ser en un Estado Social, porque en el sistema que garantiza la protección de la sociedad a través de la tutela de sus bienes jurídicos, en su calidad de intereses muy importantes para el sistema social y, por ello, protegibles por el Derecho Penal. Sin embargo, no debe olvidarse que existen bienes jurídicos, que no son amparados por el derecho penal, por ser de interés solo morales, por lo cual, no todos los bienes jurídicos son bienes jurídico- penales[24].

[24] RINCON RÍOS. Jarvey. Delito Electrónico en Colombia. Editorial universidad Santiago de Cali. Aseuc. 2009. Cali - Colombia. Pág. 22. pág. 27

En el derecho penal se busca la protección de esta clase de bienes ya que interesa salvaguardar los intereses de la comunidad sin restricción alguna, así haya otro medio para su protección, el derecho penal conserva esa función proteccionista, coercitiva y sancionalista para el que vulnere aquellos estándares o límites que impone la ley.

Se ha expuesto que se discuten las diferentes polémicas particulares que se han generado del tema investigativo, es por ello necesario resaltar que el bien jurídicamente tutelado de la información ha sido motivo de disputa en cuanto a su exposición en los medios electrónicos, lo cual pueden inferirse tres circunstancias:

a. Que por estar expuesto en las computadoras y ordenadores dicha información no está protegida y por ello la violación a este bien no existiría.
b. Otros opinan, que dicho delito es propio y conserva sus características.
c. Dicha información puede ser objeto de manipulación, convertir la información, utilizado como una herramienta al delito y puede servir también como un medio de prueba en la comisión de actos delictivos.

2.3 LOS DISPOSITIVOS ELECTRÓNICOS COMO MEDIOS DE ACCIÓN.

Es importante conocer cuáles son los medios con los cuales afectan y vulneran los derechos de las personas que se encuentran en el ciberespacio. Como lo hemos dicho en el transcurso de esta investigación, al hablar de los delitos informáticos, se debe conocer el medio por el cual se afectan o nos atacan los ciberdelincuentes.

2.1.1 USB.

Denominada así como por sus siglas en inglés (bus serial universal), es una herramienta que sirve para compartir cualquier tipo de información transportada previamente almacenada, permite conectar hasta 127 dispositivos, este es un medio utilizado por muchas personas y manejan una alta confidencialidad de la información allí guardada.

A través de esta herramienta el usuario permite compartir información de datos que contienen fotografías, procesador de DVD, reproductor de CD, etc.

Las entradas o puertos USB están fabricadas para transportar energía eléctrica al punto de conexión que se encuentra conectado; de esta manera no se necesita de un cable adicional para enlazarse a una toma de corriente.

2.3.2 Ps2.

Este punto de conexión es denominado por una serie de ordenadores creados por la multinacional IBM en el año de 1.987 a través de ella se puede conectar el mouse y teclados de ordenadores.

2.3.3 SKIMMING.

Se refiere al hurto de información de cualquier clase de tarjetas de crédito o débito utilizadas en el momento de ejecutarse una transacción, con la finalidad de reproducir, copiar o clonar la tarjeta de crédito o débito, para su posterior uso fraudulento es decir, es el procedimiento de copiado de toda la información personal de las Cibervíctimas en la banda magnética de una tarjeta(Crédito, débito, etc.), que luego es utilizada en diferentes escenarios de tipo comercial como almacenes de cadena, restaurante, bares, bombas de gasolina o en ATM, huelga, cajeros electrónicos donde un coparticipe de la acción contraria a derecho, que es parte de la empresa criminal, está

en posesión de la tarjeta débito o crédito de la víctima o en un lugar en el que se ha instalado un dispositivo que puede copiar la información[25].

2.3.4 OPERATIVA

Consiste en el empleo de una red inalámbrica o línea telefónica a la que conecta un dispositivo especializado, se conectan a través de ella entidades bancarias o comerciales con los centros de datos de entidades financieras, permite controlar las operaciones de ventas por medio de tarjetas de crédito o débito.

Para estas formas de pago se cuentan con herramientas como el datafono que generaba trámites innecesarios pero esta herramienta permitía sobre pasar los límites de los créditos que realmente una persona podía obtener.

Entonces, se vio la necesidad de operar con redes inalámbricas y equipos telefónicos que permitían, trabajar en tiempo real, usar un teléfono o red convencional y autorizar, controlar y capturar diferentes transacciones derivadas de las consultas instantáneas con los bancos de datos financieros que manejan bases de datos personales.

2.3.5 PIN PAD.

Es un sistema electrónico que se utiliza en las tarjetas de crédito, débito o tarjetas inteligentes, para permitir transacciones de entrada y permitir que ellos se han registrados por medios de PIN o contraseña. Para que el usuario pueda acceder al manejo de esta herramienta se requiere de un PASSWORD (contraseña) para que se utilice de manera segura el sistema evitando que crezca el mundo de la Ciberdelincuencia asegurando los bienes patrimoniales de las personas.

[25] PALOMA. Parra Luis Orlando. “Delitos informáticos en el ciberespacio doctrina y análisis de casos reales”. Ediciones jurídicas Andrés Morales. Bogotá 2012 pág. 5

Posteriormente los delincuentes virtuales reclutan todo un ejército de personas que venden su consciencia y su voluntad y, despojan de los dineros de las cuentas de las victimas sin hacer pasar el más mínimo escalofrio, pues mientras están laboran, descasan o pernoctan en cualquier parte del país o del mundo, sus cuentas están siendo atacadas por los delincuentes que solo les interesan extraer el dinero que tienen depositado en los diferentes bancos que existen en Colombia. Con esta acción desde luego ya están en los linderos del hurto, y como lo llama el codificador, son los denominados hurtos por medios electrónicos o semejantes.

2.4 DERECHO PENAL EN LA INFORMÁTICA

Acordando que nuestra legislación a instaurado que "el derecho penal tendrá como fundamento el respeto a la dignidad humana"[26] y como lo hemos acordado en el transcurso de la investigación que la informática es el conocimiento científico y técnico ejecutado por medio de ordenadores. Al fusionar y establecer el eje central de estos dos significados. Podemos definir que el Derecho Penal en la informática esencialmente es encontrar la conducta típica, antijurídica y culpable por parte del sujeto activo, definido como aquel agente o persona que ejecuta la acción, definido como autor implementando los medios electrónicos para elaborar y llevar acabo el delito sobre el sujeto pasivo, refiriéndonos aquel como personal natural o jurídica. Ya sea actuando por medio de alguna de las Modalidades de la conducta punible.

Modalidades de la conducta punible. La conducta es dolosa, culposa o preterintencional. La culpa y la preterintención sólo son punibles en los casos expresamente señalados por la ley.[27]

[26] COLOMBIA. Congreso de la Republica. Código Penal (Ley 599 de 2000). Artículo 1.
[27] Ibídem. Artículo 21.

Dolo. La conducta es dolosa cuando el agente conoce los hechos constitutivos de la infracción penal y quiere su realización. También será dolosa la conducta cuando la realización de la infracción penal ha sido prevista como probable y su no producción se deja librada al azar.[28]

Culpa. La conducta es culposa cuando el resultado típico es producto de la infracción al deber objetivo de cuidado y el agente debió haberlo previsto por ser previsible, o habiéndolo previsto, confió en poder evitarlo.[29]

La conducta es preterintencional cuando su resultado, siendo previsible, excede la intención del agente.[30]

Acción y omisión. La conducta punible puede ser realizada por acción o por omisión.[31]

Como hemos visto, el investigador Julio Téllez Valdés clasifica en dos a los delitos Informáticos, "como **instrumento o medio** y como **fin u objetivo**".[32] Varios autores han tomado a dicho investigador como su eje fundamental para describir la problemática y tomar sus lineamientos para clasificar a los delitos informáticos, en nuestra investigación, lo tomaremos para referenciar y desde ese punto descubriremos nuestra clasificación.

Como Instrumento o Medio se configuran las conductas ilícitas que se valen de los ordenadores como método, medio o símbolo en la comisión del ilícito.

Como Fin u Objetivo: Se configuran las conductas ilícitas que van en contra de los sistemas informáticos o programas.

A lo largo de nuestra investigación podemos clasificar a los delitos informáticos en dos:

---

[28] Ibídem. Artículo 22.
[29] Ibídem. Artículo 23.
[30] Ibídem. Artículo 24.
[31] Ibídem. Artículo 25.
[32] TELLEZ VALDES. Julio. Derecho informático. Edición McGraw-Hill/Interamericana. México. 2008. Pág. 190.

A. Como aquellos que afectan el patrimonio, la integridad e intimidad de la persona.

Cuando nos referimos a los delitos informáticos que buscan afectar el patrimonio, la integridad y la intimidad de la persona, nos referimos aquella conducta del sujeto activo sin tener autorización ni facultado para acceder, interceptar, destruir o sustraer información del sujeto pasivo, colocando en peligro aquellos derechos protegidos por la Constitución Política de Colombia.

B. Aquellos con el fin de afectar los medios informáticos.

Estos son acaecidos directamente sobre los objetos informáticos ya sea sobre software o sobre el sistema operativo de algún elemento electrónico.

Para identificar la necesidad de regular los delitos informáticos en el derecho penal a nivel nacional sino internacional, se identificaron ciertas conductas que amenazaron o vulneraron los bienes personales o patrimoniales de las personas expuestos en un ordenador de internet.

Es importante presumir de la buena fe de las personas en las acciones realizadas en la internet, pero también, hay que lograr determinar que algunas personas debido a su agilidad en la manipulación de programas informáticos se aprovechan para enriquecerse o poner en desventaja a las personas víctimas de estos delitos.

A partir de estos hechos se ha logrado poner en alerta de cualquier irregularidad en los dispositivos usados, teniendo en cuenta que la denuncia a tiempo de las mismas puede evitar y capturar a los delincuentes que usan este tipo de conductas desviadas.

Estas conductas ilícitas son investigadas a diario por la policía judicial, por orden de la fiscalía, asumiendo el control y la impartición de administración de justicia resguardando los intereses de la colectividad.

“Es difícil elaborar estadísticas sobre este tipo de delitos (la cifra negra), que es como se llama la cantidad de conductas o delitos que son denunciados o reportados por los que no se incluyen en las estadísticas, es muy alta; los perjuicios económicos son altísimos; existen un creciente reconocimiento de la opinión pública sobre los daños ocasionados a la sociedad; algunos sectores no consideran delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos consideran a sí mismos (respetables) e incluso despiertan cierta simpatía. Algunos tipos de estos delitos, en muchos países son objeto de simples medidas o sanciones de carácter administrativo y no privativos de la libertad, todo esto en el mejor de los casos, ya que por regla general quedan totalmente impunes.”[33]

Es por eso que la Nación ha tenido la necesidad de implementar políticas para proteger la seguridad en el ciberespacio de los continuos ataques de dichos ciberdelincuentes. Es así que el Ministerio de Defensa Nacional, debe preocuparse no solo por la seguridad territorial y mantener el orden de la nación en los campos aéreos, acuáticos y terrestres, sino también del ciberespacio.

Pero no solo podemos inferir que el Ministerio de Defensa Nacional dentro de sus implementaciones para proteger los derechos de los ciudadanos, es la completa seguridad a la cual nos debemos someter. Ya que si en nuestra Nación no existe una regulación fuerte sobre aquellos sujetos que actúan y accionan delitos contra la seguridad personal y del Estado Colombiano. O se tipifican delitos frente a las operaciones delincuenciales en la red. Dichas estrategias van a ser atacadas y como consecuencia nos encontraremos ante una problemática de cibercriminalidad.

CAPITULO III

[33] TORRES TORRES. Henry William. Derecho penal de la informática. Ediciones jurídicas Gustavo Ibáñez. Medellín – Colombia. 2012. P. 32

3 TIPOS PENALES INFORMATICOS.

Para el profesor HENRRY WILLIAM TORRES TORRES en su libro (Derecho Informático) y la doctora YOLANDA GUERRA GARCÍA autora del libro (Delitos Informaticos), nos instruyen LOS TIPOS DE DELITOS INFORMATICOS que fueron reconocidos por las NACIONES UNIDAS, a lo cual según la indagación aportada por ellos realizamos en 3 cuadros para representar lo que dichos autores y Naciones unidas han tipificado.

Cuadro 1

CARACTERISTICAS	**A. FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS**	
	DELITOS	• **MANIPULACIÓN DE LOS DATOS DE ENTRADA**
		Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
		• **LA MANIPULACIÓN DE PROGRAMAS**
		Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
		• **MANIPULACIÓN DE LOS DATOS DE SALIDA**
		Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la

		computadora en la fase de adquisición de datos. tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
		• **FRAUDE EFECTUADO POR MANIPULACIÓN INFORMÁTICA**
		Aprovecha las repeticiones automáticas de los procesos de computo es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles de transacción financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Cuadro 2

CARACTERISTICAS	**B. FALSIFICACIONES INFORMATICAS**	
	DELTIOS	**COMO OBJETO**
		Cuando se alteran datos de los documentos almacenados en forma computarizada
		COMO INSTRUMENTOS:
		Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando

		empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos laser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.

Cuadro 3

CARACTERISTICAS	**C. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS**	
	DELTIOS	**SABOTAJE INFORMÁTICO**
		Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
		VIRUS: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legitima de soporte lógico que ha quedado infectada, así como utilizando en método del Caballo de Troya.
		GUSANOS: Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
		BOMBA LÓGICA O CRONOLÓGICA: Exige conocimientos especializados ya que requiere la programación de la destrucción o

		modificación de datos en un momento dado del futuro. Ahora bien al revés de los virus o de los gusanos las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se halla marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.
		ACCESO NO AUTORIZADO A SISTEMAS O SERVICIOS: Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático.
		PIRATAS INFORMÁTICOS O HACKERS: El acceso se efectúa a menudo desde un lugar exterior situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede utilizar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencias en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
		REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

La información anteriormente recopilada se encuentra en los libros de Delitos informáticos página 92 autora GUERRA GARCÍA YOLANDA y HENRRY WILLIAM TORRES TORRES autor del libro Derecho Informático página 26 ss.

3.1 REGULACION INTERNACIONAL SOBRE LOS DELITOS INFORMATICOS

Ha sido necesario comprender e implementar las medidas de protección por parte de los Países que han contrarrestado la forma delincuencial de los ciberdelincuentes. Por lo cual hablaremos de los países más importantes como ALEMANIA – CHILE – ESPAÑA – ESTDOS UNIDOS – FRANCIA. Por tal motivo es necesario ilustrar la situación internacional.

- **ALEMANIA.**

Según el Código Penal de Alemania en la sección decimoquinta la cual protege la intimidad personal y al ámbito del secreto personal se encuentra el artículo 202a, se remite a la piratería informática, en la sección vigesimosegunda en la cual tipifica la estafa y deslealtad se encuentra el artículo 263a que nos dispone a la Estafa por computador. En la Sección Vigesimoséptima referente al daño material, el artículo 303a nos determina la Alteración de datos y el 303b el sabotaje de computadoras.

Actualmente se ejecuta el Centro Nacional de Ciberdefensa, con políticas como el Plan Nacional para la protección de infraestructuras de información.

Alemania ya había creado en 1986 la ley contra la criminalidad económica, protegiendo así mismo los bienes tutelados de las personas que se encuentran en los ordenadores informáticos. Esta ley reformó el Código (art. 148 del 22 de diciembre de 1987) y contempló los siguientes delitos:

- Espionaje de datos
- Estafa informática
- Falsificación de datos probatorios
- Alteración de datos
- Sabotaje informático
- Destrucción de datos de especial significado
- Utilización abusiva de cheques o tarjetas de crédito

En la legislación Alemana, no se castiga al intruso sin autorización o la sola sagacidad no autorizada en sistemas ajenos de computadoras sino que tampoco sanciona el uso no autorizado de aparatos de procesos de datos.

- **CHILE.**

Este país se resalta por ser el primero en Latinoamérica en aprobar una ley contra los delitos informáticos, esta se dio en el año de 1993, protege el bien jurídico de la información contenida en programas automatizados y los productos que se obtengan del manejo de ellas.

La ley contiene cuatro artículos que sanciona a la persona que destruya o inutilice un sistema de tratamiento de información o sus componentes, o el que impida, obstaculice o modifique su funcionamiento. O sanciona a la persona que tenga el ánimo de a apoderarse o indebidamente use la información que este dentro de un sistema informático u ordenador. Sanciona también al que altere, dañe o destruya los datos dentro de un sistema de información y por último, sanciona a que maliciosamente revele o difunda los datos dentro de un sistema de información.

- **ESPAÑA.**

Este país en el año de 1995, regulo los delitos informáticos en el artículo 197 de la ley orgánica 10 plasmo lo siguiente:

- El que para descubrir los secretos o vulnerar la intimidad de otro sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepten sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de 1 a 4 años y multas de 12 a 24 meses.

- Las mismas penas se impondrán al que, sin estar autorizado se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos o a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
- Se impondrá la pena de prisión de 2 a 5 años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Sera castigados con las penas de prisión de 1 a 3 años y multa de 12 a 24 meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior[34].

En resumen, esta ley sanciona a aquellos que vulneren los derechos de carácter personal que violen la integridad o intimidad para fines lucrativos espionaje, revelación de secretos, o que pretendan cometer a través de los medios informáticos delitos que expongan el grave daño de los bienes jurídicamente tutelados.

- **ESTADOS UNIDOS.**

Creo la Estrategia Internacional para el Ciberespacio, la cual tiene como principal eje la libertad en el ciberespacio y la seguridad para quienes la utilizan.

Este país en el año de 1994 modifico el acta de fraude y abuso computacional de 1986. Sanciona los actos de transmisión de virus, la transmisión de un programa, información, códigos o comandos que causan daño a los sistemas informáticos u ordenadores. La pena será hasta los 10 años de prisión acompañado de una multa pecuniaria.

[34] PALOMA. Parra Luis Orlando. “Delitos informáticos en el ciberespacio doctrina y análisis de casos reales”. Ediciones jurídicas Andrés Morales. Bogotá. 2012.

- **FRANCIA.**

Este país señalo como delitos informáticos el fraude informático en el año de 1.988.

- Acceso fraudulento a un sistema de elaboración de datos
- Sabotaje informático
- Destrucción de datos
- Falsificación de documentos informatizados
- Uso de documentos informatizados falsos

3.2 ALCANCE JURIDICO DE LA LEY 1273 DEL AÑO 2009.

Para el análisis de la siguiente ley fue importante el estudio de la legislación en distintos países y comprender el desarrollo tecnológico e informático de los ordenamientos normativos jurídicos que apelan a las necesidades de protección de las personas que desenvuelven su información a través de medios electrónicos u ordenamientos que contienen base de datos que generan intereses patrimoniales necesarios para su desarrollo legal.

La mayoría de información de las personas se encuentra por necesidad o por gusto propio en las redes de internet, su acceso es de manera fácil, permitiendo que se elaboren herramientas de acceso a toda la comunidad con algunas restricciones. Esas restricciones son las que permiten se proteja el bien jurídico de otros que así mismo guardan intereses personales, económicos, culturales y / o sociales.

Cabe anotar, que en la evolución de las sistematización de información en base de datos privados o públicos a generado intereses de organizaciones criminales encargados de violar cualquier tipo de seguridad a tentando contra el patrimonio de las personas, la vida, la integridad, dignidad y demás derechos conexos.

En la historia de la humanidad han existido organizaciones criminales que han causado enormes daños no solo a la sensibilidad de los seres humanos en su vida, en su patrimonio moral, sino también menoscabo en sus patrimonios económicos y de ellos de predica en toda clase de asuntos delictivos en el mundo, por ello, en la hora actual y ante el descomunal crecimiento de quienes navegan ilegalmente en los mares y carreteras virtuales, convirtiéndose en auténticos piratas informáticos, vienen ocasionando deterioros no solo pecuniarios sino zozobras, angustia, sufrimiento a quienes afectan a través de la red, como también a toda la colectividad que ven fuertemente amenazados sus intereses patrimoniales y morales con el uso súper necesario de las computadores[35]

Como antecedente de la ley 1273 del 2009 se tiene el proyecto de ley 281 del 2008 en el senado, y 42 y 123 del 2007 en la cámara de representantes; estos debates tuvieron distintas posturas teniendo en cuenta que para un sector no era necesaria esta ley porque en la ley 599 del 2000 sancionaba a aquellas conductas punibles que se presentaban en los proyectos de ley mencionados. Para otro sector, los delitos informáticos debían ser regulados ya que en otros países habían aprobado distintas legislaciones que protegían los datos de información y aquellos productos o servicios que provienen de los ordenadores informáticos.

Se buscaba con la nueva regulación penal colombiana quedar en igualdad de condiciones con el convenio sobre la cibercriminalidad suscrito en Budapest en el año del 2.001 , proponiendo lo siguiente" prevenir los actos atentatorios de la

[35] PALOMA. Parra Luis Orlando. "Delitos informáticos en el ciberespacio doctrina y análisis de casos reales ediciones jurídicas". Ediciones Jurídicas Andrés Morales. Bogotá. 2012 pág. 228

confidencialidad, la integridad y la disponibilidad de los sistemas informáticos de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente convenio, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detención, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable.[36]

La ley 1273 del 2009 modificó el código penal, estableciendo como nuevo bien jurídico tutelado, *la protección de información y datos*. Como primera medida, adiciona el *Título VII BIS denominado De la Protección de la información y de los* datos, el cual contiene dos CAPITULOS denominándose de la siguiente forma: **CAPITULO I** *De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*. **CAPITULO II** *De los atentados informáticos y otras infracciones.*

Respaldando lo anterior se hace un caracterización del Código Penal Colombiano, resaltando la parte en que se adiciono y reformo por medio de la ley 1273 de 2009, anexando la tipificación de los delitos de dicha ley.

Es decir que nuestro Código Penal Colombiano se encuentra de la siguiente forma:

Cuadro 4

CODIGO PENAL COLOMBIANO LEY 599 DE 2000
LIBRO PRIMERO
PARTE GENERAL
TITULO I
De Las Normas Rectoras De La Ley Penal Colombiana

[36] REMOLINA. Angarita Nelson. Anotaciones sobre la ley 1273 del 2009. pág. 240

TITULO II
De La Aplicación De La Ley Penal
TITULO III
De La Conducta Punible
TITULO IV
De Las Consecuencias Jurídicas De La Conducta Punible
LIBRO SEGUNDO
PARTE ESPECIAL
De Los Delitos En Particular
TITULO I
Delitos Contra La Vida Y La Integridad Personal
TITULO II
Delitos Contra Personas Y Bienes Protegidos Por El Derecho Internacional Humanitario
TITULO III
Delitos Contra La Libertad Individual Y Otras Garantías
TITULO IV
Delitos Contra La Libertad, Integridad Y Formación Sexuales
TITULO V
Delitos Contra La Integridad Moral
TITULO VI
Delitos Contra La Familia
TITULO VII
Delitos Contra El Patrimonio Económico
TITULO VII BIS
ADICONADO POR LA LEY 1273-2009
DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS
TÍTULO VII-A
De Delitos Contra El Patrimonio Cultural Sumergido
TITULO VIII
De Los Delitos Contra Los Derechos De Autor
TITULO IX
Delitos Contra La Fe Pública
TITULO X
Delitos contra el orden económico social

TITULO XI
De Los Delitos Contra Los Recursos Naturales Y El Medio Ambiente
TITULO XII
Delitos Contra La Seguridad Pública
TITULO XIII
De los delitos contra la salud pública
TITULO XIV
Delitos Contra Mecanismos De Participación Democrática
TITULO XV
Delitos Contra La Administración Pública
TITULO XVI
Delitos Contra La Eficaz Y Recta Impartición De Justicia
TITULO XVII
Delitos Contra La Existencia Y Seguridad Del Estado
TITULO XVIII
De Los Delitos Contra El Régimen Constitucional Y Legal
TITULO XIX
Disposiciones Generales

Adicionado por la ley 1273 de 2009.

De igual forma anexamos por medio del cuadro 5 los tipos penales que adiciono la ley 1273 de 2009.

Cuadro 5.

TIPOS PENALES LEY 1273 DE 2009		
ARTÍCULO	**CONTENIDO**	**DESCRIPCIÓN DEL TIPO PENAL**
	El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un	**Tipo subjetivo:** Dolo. **Tipo objetivo:**

Artículo 269A *Acceso abusivo a un sistema informático.*	sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.	Verbo rector:Acceder. Sujeto activo: puede ser uno o varios autores. Objeto Material: Sistema informático. Objeto jurídico: Intimidad o privacidad.
Artículo 269B *Obstaculización ilegítima de sistema informático o red de telecomunicación.*	El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.	**Tipo subjetivo:** Dolo. **Tipo objetivo:** Verbo rector: impedir u obstaculizar. Sujeto activo: puede ser uno o varios autores. Objeto Material: Sistema informático, datos o red de telecomunicaciones. Objeto jurídico: privacidad, acceso a la información.

Artículo 269C *Interceptación de datos informáticos.*	El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.	**Tipo subjetivo:** Dolo. **Tipo objetivo:** Verbo rector: interceptar. Sujeto activo: puede ser uno o varios autores. Objeto Material: Sistema informático o emisiones electromagnéticas. Objeto jurídico: Intimidad, privacidad, seguridad personal, integridad.
Artículo 269D *Daño Informático*.	El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales	**Tipo subjetivo:** Dolo. **Tipo objetivo:** Verbo rector: Destruir, dañar, borrar, alterar y suprimir. Sujeto activo: puede ser uno o varios autores. Objeto Material: Sistema informático, partes o

	mensuales vigentes.	componentes lógicos del mismo. Objeto jurídico: Acceso a la información.
Artículo 269E *Uso de software malicioso.*	El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.	**Tipo subjetivo:** Dolo. **Tipo objetivo:** Verbo rector: Producir, traficar, adquirir, distribuir, vender, enviar, introducir y extraer. Sujeto activo: puede ser uno o varios autores. Objeto Material: Software malicioso o programas de computación con efectos dañinos. Objeto jurídico: privacidad, seguridad personal, acceso a la información.
	El que, sin estar facultado para ello, con provecho propio	**Tipo subjetivo:** Dolo. **Tipo objetivo:**

Artículo 269F *Violación de datos personales*.	o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.	Verbo rector: Obtener, compilar, sustraer ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar modificar o emplear. Sujeto activo: puede ser uno o varios autores. Objeto Material: códigos o datos personales, bases de datos ficheros o archivos. objeto jurídico: Intimidad o privacidad, secreto profesional, seguridad personal, acceso a la información.
Artículo 269G *Suplantación de sitios web para capturar*	El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena	**Tipo subjetivo:** Dolo. **Tipo objetivo:** Verbo rector: Diseñar, desarrollar, traficar vender, ejecutar, programar.

datos personales.	de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.	Sujeto activo: puede ser uno o varios autores. Objeto Material: Páginas electrónicas, enlaces, ventanas emergentes de sitios web. Objeto jurídico: Derechos de autor, seguridad personal, acceso a la información.
Artículo 269I *Hurto por medios informáticos y*	El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[37] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un	**Tipo subjetivo:** Dolo. **Tipo objetivo:** Verbo rector: Apoderar. Sujeto activo: puede ser uno o varios

[37] HURTO: El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro, incurrirá en prisión de treinta y dos (32) a ciento ocho (108) meses.

semejantes.	usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.	autores. Objeto Material: Sistema informático red de sistema electrónico o telemático. Objeto jurídico: privacidad, seguridad personal, acceso a la información.
Artículo 269J *Transferencia no consentida de activos*.	El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de	**Tipo subjetivo:** Dolo. **Tipo objetivo:** Verbo rector: Conseguir. Sujeto activo: puede ser uno o varios autores. Objeto Material: Transferencia no consentida de activos. Objeto jurídico: privacidad, seguridad personal, acceso a la información.

	computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.	

Artículo 269H: *Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Fuente: Ley 1273 de 2009

3.3 MANEJO DE LA INFORMACION (SEGURIDAD Y CALIDAD)

La superintendencia Financiera de Colombia, respecto a diversos ataques y delitos cometidos hacia los ciudadanos frente a la información financiera recolectada por entidades y medios de distribución. Ha obligado a las entidades a proteger la información confidencial, la cual toda aquella "información amparada por la reserva bancaria V. gr. número de cuenta; número de identificación personal (PIN); número de tarjeta física; información sobre depósitos o inversiones de cualquier tipo, créditos, saldos, cupos y movimientos de cuenta, siempre que vayan acompañados del nombre o número de identificación del cliente"[38].

Dicha superintendencia se creó en el año 2005, por medio del decreto 4327 de 2005, al fusionar la Superintendencia Bancaria de Colombia con la Superintendencia de Valores, creando la Superintendencia Financiera de Colombia, con la intención de vigilar el control financiero, manteniendo la confianza y protegiendo los derechos de inversionistas.

Por lo cual se puede referir que nuestro sistema financiero ha sido protegido desde la incorporación de la Constitución política de Colombia, ya que se puede evidenciar que le dio la potestad al Congreso de la Republica "expedir las normas a las cuales debe sujetarse el Gobierno para el ejercicio de las funciones de inspección y vigilancia que le señala la Constitución.[39]

Esto evidencia que por parte de los Organismos Fiscales, la protección a la información ha sido prioridad para la regulación y supervisión al sistema financiero, demostrando que la protección a la intimidad personal.

Dispuesto en el documento del Consejo Nacional de Política Económica y Social (Conpes 3701 de 2011), en la cual determina y argumenta políticas y estrategias

[38] COLOMBIA. Superintendencia financiera de Colombia. Circular 052 de 2007. Bogotá. Pág. 98
[39] COLOMBIA. Congreso de la Republica. Constitución Política de Colombia. Legis 2013. Articulo 150 parágrafo 8.

para prevenir y examinar la ciberseguridad en Colombia según su fuente se incluye en el Plan Nacional de Desarrollo, establecido en el periodo 2010 a 2014. Como objetivos específicos dispuestos por dicha entidad, han solicitado implementar una comisión intersectorial, la cual se encargar de conocer y regular los fundamentos en tecnología y ciberdefensa.

Según comunicado del Ministerio de Defensa del 14 de Julio de 2011, se crearon 3 grupos importantes para proteger y contrarrestar los sistemas de información nacional ColCERT, el Comando Conjunto Cibernético de las Fuerza Militares y la Comisión Intersectorial conformada por el Gobierno Nacional; cabe aclarar que estos fueron aprobados por el CONPES por medio del documento anteriormente expuesto.[40]

El Grupo de Respuestas a Emergencias Cibernéticas de Colombia, denominado ColCERT, atendiendo las emergencias que vulneren los servicios y las bases de la defensa nacional en ciberseguridad.

El Comando Conjunto Cibernético de las Fuerza Militares, su función es de fortalecer, defender y desarrollar políticas para defender la seguridad nacional.

Según el documento CONPES la estructura de los 3 grupos anteriormente nombrados serán de la siguiente forma:[41]

[40] COLOMBIA. Ministerio de Defensa. https://www.mindefensa.gov.co/irj/go/km/docs/documents/News/NoticiaGrandeMDN/60a20bd2-8890-2e10-7dab-8a117a5461d8.xml (Consultado el día 29 de Agosto de 2014)
[41] COLOMBIA. Consejo Nacional de Política Económica y Social. Documento 3701 de 2011 Lineamientos De Política Para Ciberseguridad Y Ciberdefensa. Bogota. 2011. http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf (Consultado 29 de Agosto de 2014)

Grafica 1 Modelo de Coordinación

Fuente: Documento CONPES 3701 de 2011

CAPITULO IV

4. PROPUESTA TRATAMIENTO DERECHO PENAL FRENTE A LOS DELITOS INFORMÁTICOS

Como propuesta para impedir que la defraudación por delitos penales se incremente y afecte el patrimonio del Estado y las personas naturales o jurídicas, a nivel individual o colectivo.

Para ello se han hecho estudios de educación en la manipulación de información en las redes de internet o procesadores informáticos. Y algunos métodos para la investigación de los actos delictivos informáticos.

4.1 EDUCACIÓN PARA EL USO ADECUADO DE LA TECNOLOGÍA.

En nuestra investigación hemos podido comprender que la forma de combatir directamente los atentados y acciones contra la integridad personal e intimidad y seguridad en el ciberespacio es promoviendo la educación en el uso adecuado de la tecnología, siendo importante ejercer control de la información expuesta en los medios informáticos, fortalecer el respeto a la intimidad, los derechos patrimoniales y económicos de las personas en los medios electrónicos.

El conocimiento de términos, uso, ventajas y desventajas de las TIC´s (Tecnología de información y comunicación) debe hacer parte del conocimiento general de todo educador, padres, docentes, con el fin de disminuir la brecha generacional existente por la nueva cultura generada por el uso de manera tal que sea responsabilidad de todo usuario estar en capacidad de discernir sobre las herramientas de la web y el adecuado uso del poder tecnológico.[42]

En este punto la doctora Yolanda Guerra, permite contextualizar en el derecho y la tecnología la aplicación de la ética, haciendo que el espacio de internet se genere para compartir información, opiniones, conversaciones y espacios abiertos que permitan el desarrollo, social, económico y cultural de las personas.

De las leyes que deben aplicarse en el uso de la tecnología y el internet, se ilustran las del profesor y filósofo Luciano Floridi quien ha transmitido conocimiento y expuesto sobre la filosofía de la información, tales son:

[42] GUERRA. García Yolanda M. Derecho y tecnología. universidad Santo Tomas. editorial Ibáñez. Bogotá. 2012. pág. 80.

- Internet ha de servir para aumentar el conocimiento, por lo tanto deberían ser censuradas las informaciones que no contribuyeran a ello.
- Ha de servir para desarrollar el conocimiento útil: más y mejores conocimientos.
- La entropía (desorden) ha de ser combatida. también hay que tener en cuenta el principio de responsabilidad, de Hans Jonas que merece un apartado propio, nos viene a decir que "el hombre ha de tener una responsabilidad a la altura de su poder de cambiar el mundo.[43]

Aquellos alcances tecnológicos hacen parte de la objetividad de desarrollarlos hasta que los límites de los derechos del otro me lo permitan, no puedo llegar a invadir con fines de alterar el marco legal los derechos jurídicamente tutelados de las personas, ni sobrepasar los estándares normativos que el legislador ha propuesto.

Los ciudadanos deben saber que la manipulación de aquellos sistemas informáticos tiene un uso bueno y otro malo, y esta información por ser usuario debo entenderla para correr riesgos en la lesión de los bienes jurídicamente tutelados dentro del Estado Social de Derecho.

Enfocándonos en el análisis de dicha información, se deben comprender que al entrar al ciberespacio se encuentran con la posibilidad de acceder a información personal de los demás y engendrar una tipificación de delito, ya sea tan solo al dirigirse algún enlace de la web; tal como lo comenta Manuel Gomez Tomillo, autor del libro Responsabilidad Penal y Civil por Delitos Cometidos a través de Internet, "la conducta del proveedor de enlaces tan solo puede ser calificada como complicidad, necesaria o no, en el delito de otro que debe ser calificado como autor no equivale a afirmar la absoluta impunidad de tal sujeto".[44]

[43] Ibíd. p. 81
[44] GOMEZ TOMILLO. Manuel. "Responsabilidad Penal y Civil por Delitos Cometidos a través de Internet" Editorial Aranzandi S.A. Navarra - España. 2006. pág. 166.

Observando que al ingresar a la red podemos estar expuestos a artículos o enlaces que nos lleven a proporcionar nuestra identidad en la red y que aquellos que se encuentren conectados puedan utilizarla para fines delictivos.

La globalización y el avance tecnológico trae a la personas alcances que maravillan el intelecto, el poder compartir información valiosa dentro de la academia, pero así mismo, puede invadir, manipular o dejar expuesta información que debe ser reservada para los que adquieran en algún momento derechos sobre la misma.

Como lo indica Gustavo Balmaceda Hoyos, Abogado de la Universidad de Chile y Doctor en Derecho Penal de la Universidad de Salamanca – España, al remitirse sobre las víctimas que podemos afirmar que las características comunes de este tipo de víctimas son las siguientes: son personas nuevas en la red; son sujetos inocentes por naturaleza; son individuos que son codiciosos, solitarios, o que tienen necesidades de carácter emocional; con frecuencia existen personas que informan haber sido atacadas pero en verdad no lo han sido; y en último lugar se trata de personas que simplemente son desafortunadas por estar en el lugar (virtualmente) equivocado en el momento equivocado."[45] Enfatizando que ess importante para los estudiantes y académicos que la invasión o manipulación inadecuada de información contrae sanciones penales de carácter grave de acuerdo al daño causado.

La presencia de las TIC´s en la vida moderna tiene una importante incidencia en la educación. La sociedad de la información, abre las puertas a un sin número de oportunidades para que las personas accedan a datos que antes eran difícil o imposibles de conseguir. Esto implica una serie de ventajas y desventajas en el proceso de formación moral e intelectual de niños y jóvenes.[46]

[45] BALMACEDA HOYOS. Gustavo. "El Delito de Estafa Informática". Ediciones Leyer. Bogotá. 2009. pág. 61 y ss.
[46] Ibíd. p. 84

La herramienta de la internet propone espacios de educación y desarrollo académico, trae oportunidades de trabajo, de brindar posibilidades de abrir los mercados, mejorar en la economía, cultura y sociedad de acuerdo a las herramientas que se ofrecen a través de los medios informáticos, su aprovechamiento debe ser de manera tal, que permita verificar el correcto manejo por parte de los usuarios a través de la red de apoyo informático y las autoridades encargadas por ley.

La tecno ética es una combinación de la mente con la tecnología y su objetivo es establecer principios que procuren controlar el alcance arrasador de la información, pretendiendo el control de una sociedad de conocimiento gestionada con reglas éticas. Esto llevado a todas las tecnologías aplicadas en la actualidad, muestra lo lejos que estamos de su cumplimiento y lo cerca que nos encontramos de sus fatales consecuencias.[47]

4.2 RESPONSABILIDADES DE INSTITUTOS DE FORMACIÓN EDUCATIVA.

Un análisis frente a las conductas efectuadas por los ciudadanos frente a los delitos informáticos se fomenta en invitar y realizar diseños pedagógicos por parte de las Instituciones Educativas, que hagan seguimiento a los alumnos en el tratamiento de ellos con los medios informáticos, las páginas consultadas y la restricción que sus padres hacen de la consulta.

La responsabilidad frente al manejo de las herramientas de internet genera más preocupación en la actualidad ya que no hay una preocupación en la enseñanza del manejo idóneo de los mismos.

Es así que el DANE realizo una investigación en medición de la cobertura y aprovechamiento de las TIC, en los hogares.

[47] Ibíd. P. 85.

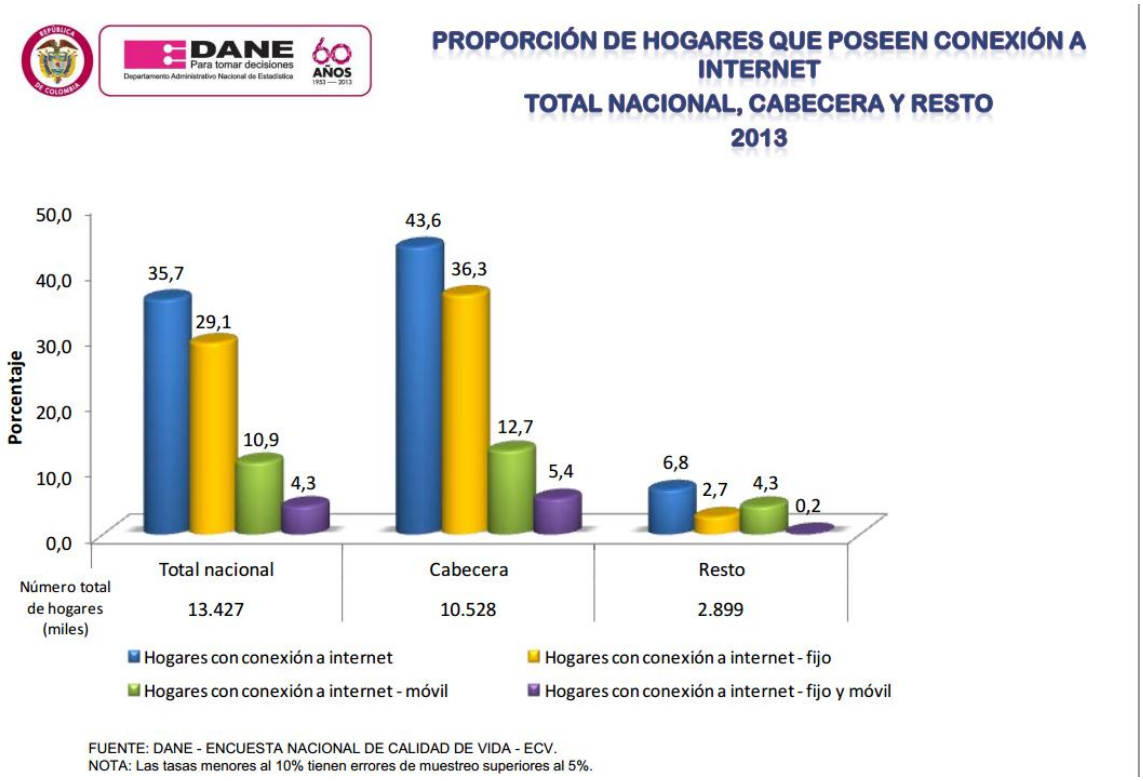
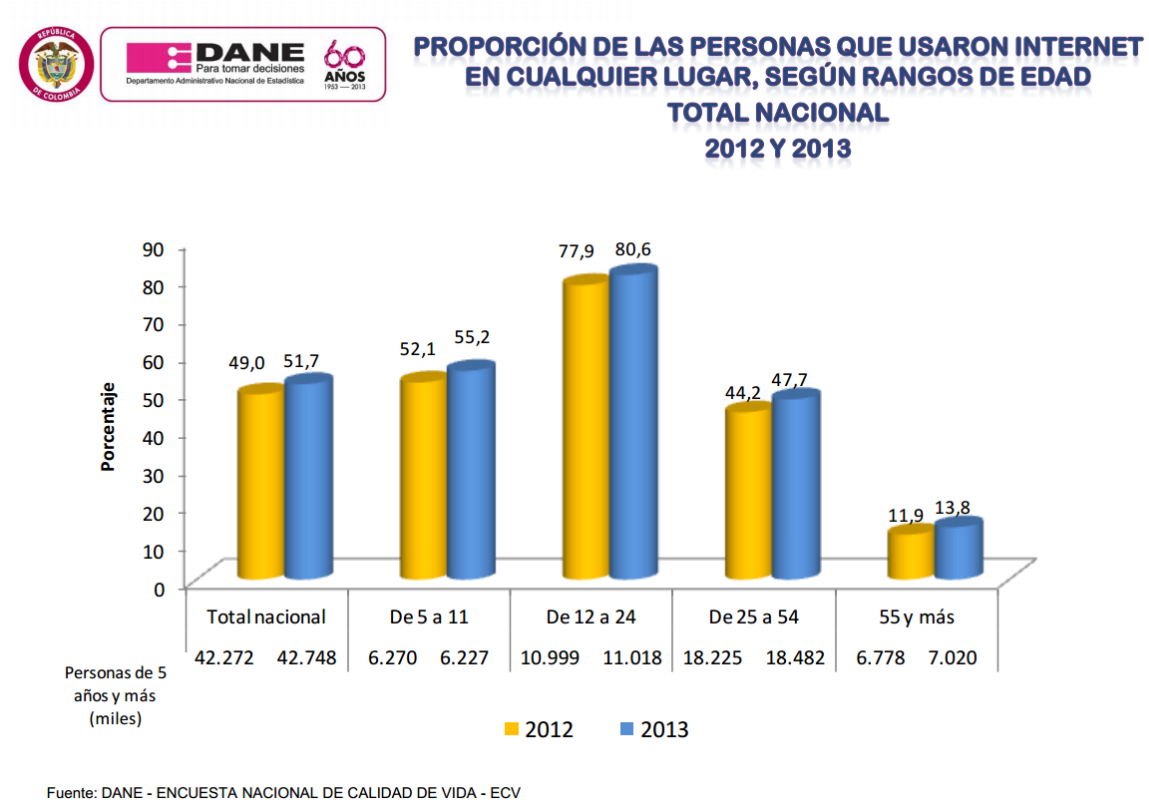


Figura N° 1

Según informe del DANE sobre indicadores del uso de la tecnología y la información y comunicación sobre personas de 5 o más años de edad podemos inferir que la población de la cabecera se encuentra con mayor acceso a internet, lo cual para las instituciones, sus políticas deberán iniciar en las cabeceras municipales. Lo cual indica que se debe contar no solo con el apoyo del Gobierno Nacional, sino también se debe tener conexión con las Alcaldías Municipales.



Fuente: DANE - ENCUESTA NACIONAL DE CALIDAD DE VIDA - ECV

Figura N° 2

Referente a la encuesta del DANE sobre la proporción de personas que utilizaron internet por rangos de edad, nos lleva a enfatizar que nuestra investigación y procedimiento frente a las políticas por parte de las Instituciones de formación Educativa y el Estado, deben ejecutarse primordialmente en las personas entre las edades de 12 a 24 años, ya que según la Figura N°2 son los que mayor porcentaje tienen que usan internet, cabe destacar que dicha figura muestra que con el año anterior se encuentran en aumento esta práctica, lo cual muestra que es indispensable la educación y formación sobre estos temas en nuestra sociedad.

En los últimos años, se han arrojado cifras de víctimas de hurto, homicidios, víctimas de trata de personas, drogadicción, *bullying* a causa del mal manejo de

estos instrumentos e inocencia de los que creen que las personas al otro lado de la pantalla no tienen intenciones de hacer daño.

No es solamente una realidad que tenga intensión de hurtar, sus dimensiones van más allá, hasta quitar la vida y la integridad de las personas, sobre todo quedan más expuestos los menores de edad que no tiene un control frente a las redes sociales.

Es necesario mirar la virtualidad desde el punto de vista educativo con otros ojos distintos a la modalidad que esto representa y la amplitud de los programas generados a través del *e-learning*. la comercialización de la educación, sea esta o no una consecuencia de la mundialización o de la globalización, hace referencia a la internacionalización de la educación y la aparición de oferta educativa a través de diversas modalidades que difieren de los tradicional y regulado por el Estado a la educación como servicio a la orden de la OMC mercadeada por proveedores externos que se pierden bajo el control de un Ministerio Educativo que garantice su calidad para ser vigilados por estamentos de industria y comercio que regulen su transaccionalidad (importación, exportación, comercialización) dejando en dudas su aporte al desarrollo de un país o su resultado debilitador para aquellos que su estructura gubernamental y presencia de Estado no logran tener el control que garantice su éxito.[48]

4.3 RETOS PARA LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS.

Para la investigación de delitos informáticos se requiere que aquellos investigadores competentes de la investigación de los mismos, requieren de nuevas tecnologías y avances a nivel académico, para encontrar los medios de prueba para la imputación de estos delitos.

[48] GUERRA. García Yolanda M. Derecho y tecnología. Universidad Santo Tomas. Editorial Ibáñez. Bogotá. 2012

Es importante hacer un seguimiento constante de los usuarios de las redes sociales más comunes y ver cualquier alteración en la creación de distintos usuarios, no solo basta con ello, sino que debe estar en contacto con entidades financieras que podrían detectar cualquier uso irregular en las cuentas bancarias de las personas, que manejan virtualmente su cuenta o el sistema reconoce algún tipo de violación a los *passwords* o contraseñas establecidas por el cliente.

Los investigadores deberán tener en cuenta ciertos aspectos manejados a nivel internacional, tales son:

4.3.1 Rastros En Ambientes Virtuales.

Son aquellos incrementos de las plataformas virtuales, la virtualización de servidores y del almacenamiento, comprende un ambiente dominado por archivos e infraestructura manejada por memoria de disco o bases de datos.

Estos llamados "entornos virtualizados", son escenario de alta capacidad en memoria, soportan distintas actividades dinámicas, con elementos de seguridad propios del acceso a sus objetos.

En este escenario virtual encontrar rasgos de un ataque o incidente de seguridad exige del investigador comprender en detalle el funcionamiento de las máquinas virtuales, su utilización de la memoria y el disco, los archivos que ayudan al manejo de cada entorno y sus relaciones entre sí. Luego de esto, establecer qué tipo de rastros podrían haber quedado en las máquinas virtuales, la identificación de los usuarios y las posibles estrategias que ha utilizado el atacante para desvirtuar las trazas identificadas.[49]

[49] CANO. Martínez Jeimy José. El peritaje informático y la evidencia digital en Colombia. Concepto, retos y propuestas. Universidad de los Andes. Facultad de derecho. 2010.

4.3.2 Informática forense en bases de datos.

Las bases de datos es un sistema de recopilación de información que llevan muchas de las empresas a nivel mundial y manejan un volumen acorde a su experiencia y mercado dentro de la legalidad y constitución de la misma.

Habría distintas clases de bases de datos públicas y privadas según la experiencia de las empresas, unas de obligatoria divulgación y otras de reserva en la estrategia de negocios, productos o servicios.

Las bases de datos, o mejor, los sistemas manejadores de bases de datos, son un gran reto para la informática forense dado que las herramientas que se han de utilizar para su análisis (a la fecha) deben ser propias del fabricante de ellas, pues no se cuenta con herramientas generales que puedan revisar y analizar los datos o información residente dentro de estas.[50]

Estas estrategias de práctica de análisis forense o aspectos probatorios que se tienen en cuenta dentro de la investigación según Fowler, son:

- Probar o no la ocurrencia de una brecha de seguridad en los datos.
- Determinar el alcance de la instrucción en a base de datos.
- Reconstruir las operaciones de Data Manipulación *Language (DML) y data definition lenguaje (DDL)* efectuadas por un usuario.
- Identificar las transacciones pre y *postintrusion*.
- Recuperar (en la medida de los posible) loa datos borrados de la base de datos.[51]

[50] Ibíd. P. 345
[51] Ibíd. P. 345

Estos datos de reserva del sumario o no, deben ser de constante auditoria por las autoridades competentes de acuerdo a los movimientos extraños, o denunciados por la comunidad, hay empresas que se encargan de manejar datos personales sin autorización. En la actualidad deben las personas otorgar autorización a las empresas con las que ha contratado algún producto o servicio y las que el futuro puede originarse algún tipo de contrato.

La manipulación errónea e irregular de esta información da lugar a obtener sanciones pecuniarias y penas privativas de la libertas desde el año a diez años por la gravedad de la conducta y las intenciones que se hayan podido probar en la conducta punible.

Nuestra legislación de acuerdo a la innovación y la tecnología aplicada en la realización de toda una labor investigativa, es importante, ha sido una legislación novedosa y completa de acuerda a las anteriormente expuestas, pero es importante que para la valoración de la prueba se genere presupuesto en la implementación de aparatos especializados para el rastreo de aquéllas conductas ya descritas.

> *De igual forma, se requiere que la Administración de Justicia y los entes de policía judicial avancen de manera coordinada con el legislador para entrar en una dinámica de entrenamiento técnico y ajuste de las regulaciones que les facilite tanto a los investigadores de campo como a las organizaciones construir marcos de acción confiables y validos tanto desde el punto de vista jurídico y tecnológico. Es importante anotar que la integración de la tecnología y el ordenamiento jurídico es un proceso que exige desaprender de cuanto conocemos, para abrir la mente hacia las posibilidades y limitaciones que brindan los nuevos desarrollos tecnológicos, así como aprovecharnos de lo expuesto en las regulaciones actuales para potenciar los procedimientos tecnológicos actuales y futuros*[52]*.*

[52] Ibíd. P. 347.

CONCLUSIONES

El desarrollo de distintas tecnologías ha traído consigo múltiple conductas que atentan contra los derechos personales, económicos, patrimoniales y seguridad de las personas, también ha sido víctima el Estado en la defraudación no solo de recursos sino también de aquellas conductas que sus servidores han ejecutado a través de información secreta registrada en servidores informáticos.

Es de manera importante resaltar la tarea que los organismos internacionales advierten para el cuidado permanente de los bienes jurídicamente tutelados y conforme a ello han realizado también, estrategias de seguimiento y rastreo de delincuentes que atentan contra los derechos individuales y grupales.

Los países también han tenido que unirse en la lucha contra los delitos informáticos ya que tantas pérdidas cuantiosas en el detrimento de los bienes patrimoniales de la Nación, a partir de los actos terroristas e información cifrada de las estrategias secretas de seguridad para a partir de burlar el sistema informático puedan hacer de las suyas por motivos, políticos, económicos, étnicos o sociales.

La regulación en Colombia de los delitos informáticos y su regulación, ha demostrado la actualidad de las leyes en este país, pero no se ha permitido avanzar mucho de acuerdo a la tecnología necesitada para la investigación de estos delitos que requieren de tiempo, capacitación y conocimiento especial de programas irregulares o ilegales.

Se requiere de la participación del gobierno, entidades públicas, privadas, instituciones de educación y financieras para la erradicación de estas conductas que ponen en un hilo los intereses de la sociedad.

La administración de justicia debe globalizarse en el entendido de los estándares cambiantes de la sociedad, importante tener en cuenta las nuevas estrategias para delinquir, pero también, las estrategias para darse cuenta que se está

haciendo víctima de delitos informáticos, evitarlos o informar a tiempo para la detención correspondiente.

La violación a la intimidad por algunas personas ha sido objeto de burla por los mismo amigos, compañeros o conocidos de las personas a través de las redes sociales, como *Facebook, MySpace, twitter*, etc., están diseñadas para facilitar la información y control sobre los bienes de las personas, la divulgación de información personal puede afectar directamente los derechos tutelados de las personas y ser víctimas de personas que están pendientes de invadir e infringir la ley penal.

Para los profesionales en derecho es necesario que este tipo de conductas se regulen ya que toda la información de las personas se encuentra expuesta en estos medios de internet, se contratan servicios o productos para los cuales es fundamental suministrar información que después estas mismas entidades dejan a la deriva, sin ser conscientes del riesgo que se tiene en la manipulación de información que registre la actividad personal, profesional y/o económica.

GLOSARIO

1. **CIBERDELINCUENCIA**: Se trata de ataques contra sistemas y datos informáticos, usurpación de la identidad, distribución de imágenes de agresiones sexuales contra menores, estafas relacionadas con las subastas realizadas a través de Internet, intrusión en servicios financieros en línea, difusión de virus, *botnets* (redes de ordenadores infectados controlados por usuarios remotos) y distintos tipos de estafas cometidas por correo electrónico, como el *phishing* (adquisición fraudulenta de información personal confidencial)**.**[53]

2. **CLOUD COMPUTING:** Es el desarrollo y la utilización de capacidad de procesamiento computacional basado en Internet (la "nube"). El concepto es un cambio de paradigma, a través del cual los usuarios ya no necesitan contar con conocimientos, experiencia o control sobre la infraestructura tecnológica que se encuentra "en la nube", la misma que soporta sus actividades. Este concepto involucra típicamente la provisión de recursos fácilmente escalables y casi siempre virtualizados, tratados como servicios sobre Internet[54]**.**

3. **Voz sobre protocolo de internet *(VoIP*)**:** es la tecnología que posibilita el uso de redes IP como medio de transmisión de voz. El concepto es simple y consiste en convertir los paquetes de voz, analógicos, en paquetes digitales y hacerlos transitar por internet[55]**.**

4. **DELITOS INFORMÁTICOS:** Es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o

[53] INTERPOL. Disponible en: http://www.interpol.int/es/Criminalidad/Delincuencia-inform%C3%A1tica/Ciberdelincuencia

[54] CLOUD COMPUTING AMERICA. Disponible en: http://cloud-america.com/?page_id=257

[55] Informática Hoy. Entender sobre Voz de IP. Disponible en: http://www.informatica-hoy.com.ar/voz-ip-voip/Entender-VoIP-Voz-sobre-IP.php

manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera[56]**(ROMEO, 1987).**

5. **CIBERTERRORISMO:** Es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos[57]**.**
6. **CIBERESPACIO:** Ámbito artificial creado por medios informáticos.
7. **Tecnologías de la información (TIC´S):** Las TIC se definen colectivamente como innovaciones en microelectrónica, computación (hardware y software), telecomunicaciones y optoelectrónica - microprocesadores, semiconductores, fibra óptica - que permiten el procesamiento y acumulación de enormes cantidades de información, además de una rápida distribución de la información a través de redes de comunicación[58]**.**
8. **PASSWORD (contraseña):** Seña secreta que permite el acceso a algo, a alguien o a un grupo de personas antes inaccesible**. Real Academia**

[56] ROMEO CASABONA, Carlos María. "Poder informático y Seguridad jurídica". Editorial Fundesco 1987

[57] MANSANA, Sebastían. "El Ciberterrorismo : ¿una amenaza real para la paz mundial?" Disponible en: http://www.argentina-rree.com/documentos/ciberterrorismo.pdf (Consultado el 30 de Agosto de 2014)

[58] COBO ROMAN, Juan Cristobal. "El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento". Septiembre de 2008. Disponible en: http://www.ehu.es/zer/hemeroteca/pdfs/zer27-14-cobo.pdf (Consultado el 13 de Agosto de 2014)

9. **Hacker:** Término para designar a alguien con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionadas con las operaciones de computadora, redes, seguridad, etc[59]**.**

10. **Caballo de troya:** Los Troyanos Informáticos o Caballos de Troya (en inglés Trojan) es una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos legítimos/benignos (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño[60]**.**

11. ***e-learning:*** El concepto de e-learning (o de otros similares como teleformación, educación virtual, cursos on line, enseñanza flexible, educación web, docencia en línea, entre otros.) es una modalidad de enseñanza-aprendizaje que consiste en el diseño, puesta en práctica y evaluación de un curso o plan formativo desarrollado a través de redes de ordenadores y puede definirse como una educación o formación ofrecida a individuos que están geográficamente dispersos o separados o que interactúan en tiempos diferidos del docente empleando los recursos informáticos y de telecomunicaciones[61]**.**

12. **Bombas lógicas (*logic bombs*):** Se entiende por bomba lógica (en inglés denominado time bombs), aquel software, rutinas o modificaciones de programas que producen modificaciones, borrados de ficheros o

[59] Seguridad PC. Disponible en: http://www.seguridadpc.net/hackers.htm (Consultado el 15 de AGOSTO DE 2014)

[60] Seguridad PC. Disponible en: http://www.seguridadpc.net/troyanos.htm (Consultado 20 de Agosto de 2014)

[61] AREA, M. y ADELL, J. (2009): —eLearning: Enseñar y aprender en espacios virtuales. En J. De Pablos (Coord): Tecnología Educativa. La formación del profesorado en la era de Internet. Aljibe, Málaga, pags. 391-424.

alteraciones del sistema en un momento posterior a aquél en el que se introducen por su creador[62].

BIBLIOGRAFIA.

CANO MARTÍNEZ. Jeimy José. El peritaje informático y la evidencia digital en Colombia. Concepto, retos y propuestas. Universidad de los Andes. Facultad de derecho. 2010.

FERNANDEZ. CALVO. Rafael. El tratamiento del llamado delito informático. Proyecto de ley orgánico penal: reflexiones y propuestas de la CLI Comisión de libertades e informática, en informática y derecho.

GUERRA GARCÍA. Yolanda M. Derecho y tecnología. Universidad Santo Tomas. Editorial Ibáñez. 2012.

GUERRERO MATEUS. María Fernanda. La ciberdelincuencia: la ley articulo ganador del XV concurso Nacional José Ignacio Marques sobre derecho económico. La ley patriótica y los efectos globales en las regulaciones nacionales y en particular en el caso Colombiano. 2003.

PALOMA PARRA. Luis Orlando. Delitos informáticos en el ciberespacio doctrina y análisis de casos reales. Ediciones jurídicas Andrés Morales. Bogotá. 2012.

REMOLINA ANGARITA. Nelson. Anotaciones sobre la ley 1273 del 2.009.

RINCON RÍOS. Jarvey. Delito electrónico en Colombia. Editorial universidad Santiago de Cali. Aseuc. 2009.

[62] Delitos Informáticos. Disponible en: http://www.delitosinformaticos.com/10/2013//danos-informaticos/ataque-informatico-mediante-bomba-logica-o-bomba-de-tiempo#.UolnR_n3FJs (Consultado el 09 de Agosto de 2014)

UNIVERSIDAD LIBRE DE COLOMBIA. Guía para la elaboración de proyectos de investigación. 2013.

TORRES TORRES. Henry William. Derecho panal de la informática. Edición jurídica Gustavo Ibáñez. Medellín- Colombia. 2002

NORMATIVIDAD.

COLOMBIA. Congreso de la Republica. Ley 1473 de 2009.

COLOMBIA. Congreso de la Republica. Ley 1288 de 2009.

COLOMBIA. Congreso de la Republica. Ley 599 de 2000.

PAGINAS WWW.

12° congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Salvador (Brasil) 12 a 19 de Abril de 2010. www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf

Ley patriótica de los Estados Unidos. http://www.interamericanusa.com/articulos/Leyes/US-Patriot%20Act.htm#A301

Cada segundo hay dieciocho victimas de ciberdelitos. http://www.eltiempo.com/archivo/documento/CMS-12326635

Policía Nacional de Colombia. Delitos Informáticos. http://www.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones

_tipo_Operativas/Direccion_Seguridad_Ciudadana/Planes_de_Seguridad/Recomendaciones_de_seguridad/delitos_informaticos

Delitos informáticos. http://www.delitosinformaticos.com/10/2013/noticias/robo-de-datos-bancarios-phishing#.UlHxb5oQvIU