FALENCIAS EN EL SISTEMA LEGISLATIVO EN LA UNIFICACION DE LAS INFRACCIONES INFORMATICAS EN COLOMBIA

Medina Ramírez Edison Giovanni
Quintero Bayona Nereyda Johana
Silva Rincón José Iván

UNIVERSIDAD SIMON BOLIVAR SEDE CUCUTA
FACULTAD DE CIENCIAS JURIDICAS SOCIALES
PROGRAMA ACADEMICO DE DERECHO
SAN JOSE DE CUCUTA
2018-2

FALENCIAS EN EL SISTEMA LEGISLATIVO EN LA UNIFICACION DE LAS INFRACCIONES INFORMATICAS EN COLOMBIA

Medina Ramírez Edison Giovanni
Quintero Bayona Nereyda Johana
José Iván Silva Rincón

Producto de Trabajo de investigación presentado como prerrequisito para optar título de Abogado

Docente:
Dr. Andrea Johana Aguilar Barreto

UNIVERSIDAD SIMON BOLIVAR SEDE CUCUTA
FACULTAD DE CIENCIAS JURIDICAS SOCIALES
PROGRAMA ACADEMICO DE DERECHO
SAN JOSE DE CUCUTA
2018-2

CONTENIDO

Pág.

TITULO

FALENCIAS EN EL SISTEMA LEGISLATIVO EN LA UNIFICACION DE LAS INFRACCIONES INFORMATICAS EN COLOMBIA

RESUMEN

La globalización y el progreso de la tecnología han desencadenado fenómenos que actualmente mueven masas, al punto de ser indispensables en la cotidianidad del ciudadano promedio, se trata de la internet en especial los portales brindados por todos los sistemas digitales y las redes sociales; ya que ha generado importantes avances creando una proyección y un desarrollo en toda la población moderna.

Con este desarrollo se busca traspasar las barreras que existían frente a la necesidad de comunicación, pues antes eran necesarios utilizar el traslado de los hombres o manejar medios de información como las cartas a través del correo, que generalmente demoraban semanas y meses para llegar a su destino; por tal razón la innovación y la evolución de estos medios trae grandes beneficios en optimización de tiempo y otros elementos, también comporta serios riesgos como lo es la presencia de delitos informáticos; el presente artículo aborda los delitos y el cómo el mundo, ha tenido que avanzar en la normatividad jurídica para hacer frente a esos ciberdelitos.

Además, se buscó analizar la evolución de estos sistemas de comunicación pero enfocándose en el marco conceptual y jurídico necesario para incluir las infracciones informáticas teniendo en cuenta los planteamientos y estudios realizados por diferentes juristas nacionales e internacionales quienes han establecido la base jurídica y normas sobre este tema en Colombia, por tal razón se planteó y creó la ley 1273 de 2009, con la cual se buscó que nuestro país se equipare con las normativas internacionales sobre la ciber criminalidad que ha venido infringiendo las distintas áreas de sectores tan esenciales e importantes como el de las comunicaciones personales, las empresariales e incluso institucionales.

TITULO

FALENCIAS EN EL SISTEMA LEGISLATIVO EN LA UNIFICACION DE LAS INFRACCIONES INFORMATICAS EN COLOMBIA

Autor: *Medina Ramírez Edison Giovanni*
Silva Rincón José Iván
Quintero Bayona Nereyda Johana

Fecha: 27 noviembre de 2018

Resumen

Con la elaboración de este artículo pudimos conocer a fondo la situación a la que estuvieron expuestas algunas víctimas de delitos informáticos en diferentes situaciones que tenían como elementos principales la utilización de medios electrónicos y un alto conocimiento en programación y decodificación de información guardada en bases de datos por parte de quienes pudieron identificar como posibles autores de estos tipos de delitos, los cuales afectaron a las víctimas en diferentes formas como desfalcos económicos, afectando a su buen nombre.

Por otra parte tuvimos la oportunidad de estudiar a fondo las leyes que fueron reformadas y diseñadas para enmarcar o tipificar este tipo de conductas como un delito de tipo penal con una sanción económica o privativa de la libertad para quien fuese condenado como autor material o intelectual de este. Asimismo fue como pudimos definir las rutas que debían aplicar en cada una de los diferentes situaciones en las cuales las víctimas se le vulneraron sus derechos constitucionales protegidos de acuerdo a las condiciones o situación en las que se debe presentar la querella o denuncia ante la autoridad competente, tener en cuenta el material probatorio y que este cumpliera con los requisitos necesarios para ser tenidas en cuenta en el proceso judicial a iniciar contra el victimario; para lograr llegar a entender esta problemática utilizamos una metodología hermenéutica la cual nos permitió establecer lo difícil que es ser víctima de un delito informático y a la hora de denunciar sea tipificado por la autoridad competente como otro bien jurídico protegido

Palabras Claves: Delitos informáticos, medios electrónicos, hermenéutica, ruta jurídica.

1. PROBLEMA

1.1. Planteamiento y Formulación del Problema

La tecnología a lo largo de la historia ha traído progreso, brindándonos la libertad para movernos y permanecer comunicados y conectados por redes con diversos países a nivel mundial. Nos dan la posibilidad de aprender, enseñar, jugar, trabajar hasta de intervenir en infinidad de procesos ya sean políticos, médicos, culturales, deportivos, económicos y sociales; estos avances tecnológicos demuestran la evolución que ha tenido el hombre en las diversas modalidades informáticas siendo evidente que por medio de ellas han encontrado solución a problemáticas presentes en cada etapa de su vida y le ha permitido estar un poco más cerca de esos seres queridos que se encuentran lejos cumpliendo sueños y realizándose profesionalmente.

En el momento de acceder a internet, redes sociales, correos electrónicos y chats hay que establecer claridad frente a los contenidos que presentan cada uno de estos espacios de interacción y participación, ya que en muchas ocasiones se encuentran perfiles ocultos que pueden dañar a las personas por medio de invitaciones a compartir su información personal como direcciones, números telefónicos, cuentas bancarias, fotografías con la finalidad de vulnerar datos personales; para después ser utilizados para hostigar y sobornar a estas víctimas sino acceden a sus pretensiones. Las Tecnologías de la Información y la Comunicación con la implementación de vive digital y zona de wifi gratis en centros públicos como: colegios, parques, bibliotecas, a nivel regional han transformado la educación, la convivencia social, el entorno familiar, por el mal manejo que se le da a los contenidos al que acceden las personas, y no ser utilizados para el propósito que fueron creados que era afianzar sus conocimientos, estar actualizados en los diferentes programas incluyentes del Estado y su legislación para evitar la vulneración de derechos fundamentales, se ha visto en peligro la integridad personal de las mismas.

El presente artículo aborda los delitos y el cómo el mundo, ha tenido que avanzar en la normatividad jurídica para hacer frente a esos ciberdelitos, además, se buscó analizar la evolución de estos sistemas de comunicación pero enfocándose en el marco conceptual y jurídico necesario para incluir las infracciones informáticas teniendo en cuenta los

planteamientos y estudios realizados por diferentes juristas nacionales e internacionales quienes han establecido la base jurídica y normas sobre este tema en Colombia, por tal razón se planteó y creó la ley 1273 de 2009, con la cual se buscó que nuestro país se equipare con las normativas internacionales sobre la ciber criminalidad que ha venido infringiendo las distintas áreas de sectores tan esenciales e importantes como el de las comunicaciones personales, las empresariales e incluso institucionales.

Por otro lado a medida que va generando más impacto las tecnologías; más expuestos estamos a peligros que estas traen por la mala utilización de las mismas como: Sexting, Ciber Acoso, Phishing, Ciberdependencia, robos extorciones, trata de personas, entre otras; quedando en anonimato muchas de estas por no denunciar y otras por falta de pruebas que sean relevantes para una investigación. Los delitos informáticos se presentan de manera progresiva ya que es difícil suponer que un delito se pueda cometer sin empuñar un arma, pero la realidad es distinta ya que con solo hacer un clic acompañado de unos cuantos pasos más sea para el atracador virtual la posibilidad de atentar con la información, el bolsillo de la gente o las arcas empresariales, entre algunas modalidades reconocidas como delito informático; un ejemplo es la definición de Camacho Losa, que nos dice que el delito informático es “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas.”

Con lo anterior podemos diferir que esta problemática se ha hecho más evidente en nuestro país por lo cual nuestra legislación judicial debe buscar la manera más apropiada para contrarrestar y dar un castigo ejemplar para aquellas personas que vienen cometiendo esta clase de delitos. Es ahí donde la transformación social basada en el crecimiento tecnológico trajeron consigo conductas negativas que van en contra de la normatividad y el desconocimiento de muchos sectores frente a su tratamiento, podría verse reflejado en el incremento significativo de sucesos, con un panorama de impunidad, aun cuando existan herramientas y normas jurídicas que sancionan estas conductas. Con este desarrollo se busca traspasar las barreras que existían frente a la necesidad de comunicación, pues antes

eran necesarios utilizar el traslado de los hombres o manejar medios de información como las cartas a través del correo, que generalmente demoraban semanas y meses para llegar a su destino; por tal razón la innovación y la evolución de estos medios trae grandes beneficios en optimización de tiempo y otros elementos, también comporta serios riesgos como lo es la presencia de delitos informáticos.

1.2.Justificación

Hasta el momento el estudio por parte de la doctrina del fenómeno de la criminalidad o delincuencia informática y la búsqueda de una verdadera implementación o reacción legal frente a esta; se ha centrado en los casos que han llegado a los tribunales y juzgados en nuestro país que se han dedicado al análisis jurisprudencial y sobre una perspectiva clásica del derecho penal en donde la vinculación con lo informático y con la acción abusiva o ilícita ha venido tratándose como una complementación a la protección de un bien jurídico tradicional en la correspondiente rama del derecho penal; causando con esto su punibilidad o impunidad legal. Esto ha causado que en los últimos años haya aumentado considerablemente no solo los perjuicios y daños efectivos en el ámbito personal o de la intimidad, sino económicos y patrimoniales que colocan en peligro y riesgo de quebranto los bienes jurídicos sociales o colectivos vinculados a la informática.

Según estadísticas del grupo de investigación de Delitos Informáticos de la dirección Central de Policía Judicial (DIJIN), el cual se dedica a la investigación de conductas delictivas derivadas del uso de la tecnología y telecomunicaciones, el hurto a través de internet es uno de los mayores delitos que se presentan en Colombia (Grupo Investigativo de Delitos Informáticos- GRIDI, 2009). Lo que se considera que los delincuentes cuentan con un sofisticado recurso técnico que les permiten estar en anonimato razón por la cual se deben adoptar medidas para garantizar la seguridad física y económica de las personas que acceden a medios electrónicos sin una debida precaución.

La ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico tutelado a partir del concepto dela protección de la información y los datos, este marco jurídico se ha convertido en una importante contribución y un instrumento para que las

entidades públicas y privadas puedan enfrentar los delitos informáticos; de igual forma también contamos con el convenio internacional sobre la ciberdelincuencia firmado en Budapest el 23 de noviembre de 2001 el cual se reconoce el problema de la ciberdelincuencia y la necesidad de una cooperativa transnacional para abordarlo, lo que se ve en la necesidad de crear mecanismos idóneos para la protección de unos de los activos más valiosos como lo es la información y con la promulgación de esta ley junto con el convenio internacional podremos combatir esta ciberdelincuencia presente en cada rincón de nuestro país que causa tantos inconvenientes en el aspecto social, familiar, empresarial, económico, educativo y personal que genera tanta impunidad por no denunciar y otras veces porque el ente encargado de suministrar justicia se equivoca al momento de tipificar el delito por falta de pruebas que demuestren el delito informático cometido.

2. MARCO REFERENCIAL

2.1. Estado del arte

Para la realización de dicho artículo se investigó e indago en documentos, leyes, jurisprudencias y revistas jurídicas, de igual manera en páginas Web: Ley 1581 de (2012). Disposiciones generales para la protección de datos personales, Manual de derecho informático (1996), Sentencia T-277/15 (2013). Derecho a la intimidad y al debido proceso, Informe de ponencia para primer debate al proyecto 281 de 2008, Ley sobre protección a la vida privada o protección de datos de carácter personal, Diccionario Jurídico Elemental, Revista de información, tecnología y sociedad No. 18, Manual de Derecho Penal. Tomo II Ediciones Doctrina y Ley.

2.2. Marco Conceptual:

En la actualidad, la sociedad post moderna busca crear una comunicación rápida acortando las distancias; en ese sentido el internet ha contribuido al avance acelerado de las Tecnologías de la información y la comunicación permitiendo con la misma premura los delitos informáticos; por ello desde la apertura de la era tecnológica también los gobiernos vieron la necesidad de tipificar y sancionar la apropiación ilícita de la información íntima de las quienes utilizan las redes sociales, y esta debe ser considerada para precautelar la integridad y la intimidad personal que en muchas circunstancias las transgresiones a la seguridad informática no solo afectan la intimidad de una persona sino que pueden afectar a un colectivo en general.

En Colombia, aún existen vacíos legales para la tipificación del delito informático como la apropiación de la información y la privacidad en la red social y debe considerarse acto antijurídico, además debe ser causa de sanción debido a que lesiona los derechos constitucionales y de pertenencia; siendo las redes sociales un medio de interacción entre personas, que pueden o no compartir los mismos gustos, estas plataformas permiten una comunicación asertiva entre los usuarios pero también es un medio para cometer delito y la poca idea que se tiene del contenido que se propaga en las tecnologías de la información y comunicación es la principal causa que impide salvaguardar los derechos, pues es allí

donde los futuros abogados deben reformar la legislación en materia penal, para fortalecer algunos elementos más contundentes en caso de llevarlos ante los jueces del gobierno.

En este orden de ideas existe la posibilidad que también pueda verse afectado los sistemas de hospitales, aeropuertos, parlamentos, sistemas de seguridad, sistemas de administración de justicia, entre otros; por el uso indebido que se le dan a los medios electrónicos ya que puedan ser manipulados permitiendo la comisión de conductas delictivas de distintas características, lo que hace necesario que la Corte en cumplimiento de su deber constitucional y legal adopte medidas para garantizarle a la sociedad una efectiva protección de aquellos datos que son suministrados por los usuarios para la integra prestación de sus servicios y no lleguen a ser alterados o difundidos de forma irregular donde se vulnere la dignidad humana.

Al Estado se les imposible en muchas ocasiones conocer la verdadera magnitud de los delitos informáticos, ya sea por la falta de denuncias o las falencias que presenta el sistema al investigar y aplicar el procedimiento jurídico adecuado a esta problemática; y en otras ocasiones existe el temor de las entidades de denunciar estos ilícitos por el descrédito que esto les puede ocasionar y las consecuentes pérdidas económicas que les genera lo que hace que este tipo de conductas se mantenga bajo la llamada cifra oculta o cifra negra quedando en la impunidad y permitiendo que se acrecenté cada día las diferentes infracciones que se cometen desde un sistema informático, dispositivo móvil o cualquier avance tecnológico que requiera de internet para su continuo funcionamiento y pueda acceder a información de bases de datos que al no tener las respectivas formas de seguridad puedan ser manipulados vulnerando la privacidad e información confidencial.

3. OBJETIVOS

3.1. Objetivo General

Analizarla aplicabilidad del proceso judicial frente a los delitos informáticos en casos donde se vulnera la intimidad, en el Ordenamiento Jurídico Colombiano.

3.2. Objetivos Específicos

Conocer desde la norma las implicaciones procesales, para los casos donde se vulnera la intimidad personal por los delitos informáticos.

Estudiar los elementos de manejo probatorio frente a casos de delitos informáticos que vulneran la intimidad en el Ordenamiento Jurídico Colombiano.

Aplicar una ruta de acceso jurídica, que facilite el manejo probatorio en casos de delitos informáticos que vulneran la intimidad en el Ordenamiento Jurídico Colombiano.

4. METODOLOGIA

En el presente artículo se plantea el paradigma interpretativo o método cualitativo en donde se utiliza el diseño hermenéutico, y la decisión de los lineamientos existentes del Derecho Penal, para los casos en donde se presentan delitos informáticos y se hace necesario la defensa del bien legal de la información y los datos personales.

Este método también se puede caracterizar como método documental, ya que para ello se debe realizar una revisión documental tanto de la norma como del análisis relacionados con el tema propuesto, donde se tiene en cuenta algunas categorías como la ciberdelincuencia analizada desde un punto de vista que se ha definido como fenómeno actual de afectación de derechos, en ese sentido se pretende analizar las falencias en portales digitales para la aplicación o amparo de los derechos con lo ofrecido en el ordenamiento penal actual.

5. RESULTADOS DE LA INVESTIGACION

Para Rodríguez A. (2002) nos dice que: “La ciber delincuencia son aquellas conductas que ponen en peligro o lesionan la integridad, confidencialidad y/o disponibilidad de los datos y sistemas informáticos, sin perjuicio de que además puedan suponer una puesta en peligro o lesión de bienes jurídicos distintos".

Por lo anterior se pude diferir que el ciberdelito se puede entender como la ejecución de una operación que reuniendo las particularidades que definen el concepto de delito, se lleva a cabo utilizando un dispositivo informático, o quebrantando los derechos del titular de un aparato informático ya sea hardware o software. Para que un delito sea configurado dentro de los ciber delito es estrictamente necesario que en su realización o en alguna de sus partes sea utilizado algún mecanismo electrónico, para que esta conducta sea considera punible y como resultado dicha acción es traducida o entendida como la violación a un método informático. Los tipos de delitos más frecuentes son la creación y utilización indebida de información que se halla recopilada en operaciones informáticas, y se presenta en otros como la transformación y destrucción de estos en sistemas informáticos.

De acuerdo a lo anteriormente expuesto, el bien jurídico que se protege se encarga de tipificar y puntualizar las amenazas informáticas para que la ley que lo reglamenta lo considere como un bien jurídico nuevo, con una característica esencialmente virtual pero orientada hacia la protección de la información sensible y la confiabilidad de datos personales recopilados en los sistemas de información virtual. Dentro de la delincuencia cibernética el fraude informático es considerado como estafa y establece que: “esta consiste en la transmisión no consentida de activos a través de la manipulación o alteración de datos informáticos”. Rodríguez, A. (2002).

Por consiguiente según los criterios doctrinales se está ante un comportamiento simultaneo a una conducta enmarcada como estafa, en donde el actuar del sujeto activo se encuentra guiado hacia un fin lucrativo y se dirige al usufructo patrimonial en donde el fraude es un desafío mediante engaño lo cual no se debe a un error de la víctima sino a la estafa que se hace mediante un sistema informático. Además se encuadra dentro de los ciberdelitos, la clonación de las tarjetas débito, crédito o de cualquier sistema de pago

similar con tarjetas magnéticas o con chips, ya que esta acción en años posteriores ha tenido un aumento progresivo en la frecuencia con la que denuncia o detecta estas actividades, por lo cual se revelan la existencia de organizaciones criminales especializadas en el encargo hacia este tipo de delitos; por tal motivo los establecimientos bancarios sean visto abocados a realizar las correspondientes previsiones en sus sistema informáticos de manejo financiero, para bloquear y restringir al máximo el acceso a estos datos.

Desde una perspectiva más enfocada a la legislación penal actual las conductas conocidas como el phishing y pharming se encuentra tipificadas en la nueva modalidad de estafa a través de medio informático; las jurisprudencias buscan principalmente definir que todas estas acciones son destinadas a duplicar páginas web con la conclusión de atraer de esta manera la información financiera de los usuarios para con esta hacer transferencias, compras o avances en efectivo lo cual hace una disminución patrimonial no autorizada y de este modo están perjudicando a un tercero, produciendo un engaño en el titular de la cuenta mediante el envío de mensajes falsos que les termina generando pérdidas económicas.

La forma más usada por los delincuentes en estos casos es la elaboración de un sitio web falso o la réplica de un Ciberespacio pero cuya finalidad es engañar al usuario y es por esta razón que esta labor se considera como delito de falsedad documental, y a su vez es tipificado como delito de recepción de información íntima y personal de datos en medios informáticos y esto pretende precisamente la creación de toda una estructura criminal que generalmente la mayor parte de los casos se propagan internacionalmente, lo cual incrementa la pena para quien realiza este tipo de actos fraudulentos de acuerdo a lo establecido en cada normatividad territorial actual, en Colombia, la ley 1581 de 2012 que recientemente ha entrado en vigor y con la cual a través de esta se protegen los datos sensibles. Al estar en ella bien especificado y tipificando los delitos y con esto volviéndolos punibles y sancionándolos con multas económicas e incluso de acuerdo al daño causado con prisión.

En Colombia se viene presentando un preocupante aumento en la denuncias por falsificación de documentos digitales que son usados como instrumentos de pago electrónicos debido a esto ha tenido que ser determinado como un delito del ciber espacio,

provocando que este sea considerado dentro de las conductas delictivas de tipo penal y entendido como uno de los nuevos delitos adoptados por las cortes como delitos punibles y juzgables. En general todo documento donde se incluyan características electrónicas podría incluirse dentro de los ciber delitos o delitos informáticos; y con la sentencia T-277/15 la Legislación Colombiana contempla sustancialmente salvaguardar el derecho a la intimidad personal y familiar, donde se vea afectado su imagen, la dignidad y el pleno ejercicio de sus derechos.

Asimismo para darle aplicación al ejercicio del derecho colombiano, el habeas data es una vía de acceso al reajuste y rectificación de la información dentro del proceso del método dado en medios electrónico ya sea con un carácter público o solamente privado que tiene todo ciudadano en Colombia no sólo las personas naturales se ven directamente afectadas por los delitos informáticos, también las empresas se convierten en víctimas diariamente y lamentablemente la preparación para contrarrestar estos delitos o ataques es mínima llevando consigo que los datos de millones de usuarios sean vulnerados pero el gobierno busca crear en este momento dentro de los organismos judiciales unidades especializadas las cuales hacen énfasis sobre la seguridad actuando en la prevención, corrección, detección efectiva en los casos o violaciones a la intimidad a través de su información.

El criminólogo Edwin Sutherland, (1943) fue “el primero en manejar el término delitos de cuello blanco además presentó dos puntos exactos para incluir al autor del delito: primero que el sujeto activo del delito debe ser un individuo de cierto estatus social y económico; segundo que el cometido nunca podrá justificarse en la falta de medios económicos, carencia en la educación, poco conocimiento al contrario son individuos con una gran especialidad en informática que conocen muy bien las particularidades de la programación de sistemas computados, de esta manera es como logran un manejo técnico de las herramientas necesarias para quebrantar la seguridad de un sistema automatizado”.

Por otro lado en los niveles corporativos la confidencialidad opera de manera que dependiendo del usuario y el rol dentro de la organización se le otorgan diversos permisos, por ejemplo en un banco se denotaría diferentes niveles de acceso que se le otorgan a cada usuario dependiendo de la labor que ejerza dentro del banco ya que la información

financiera tiene un tratamiento confidencial. Para el caso específico de las corporaciones financieras esto depende del rol que tiene el autor del delito dentro de esa organización ya que se les otorgan diversas claves, accesos o permisos, a cada usuario dependiendo de la labor que desempeñe dentro del banco ya que como es bien sabido la información financiera tiene un tratamiento muy confidencial.

Por consiguiente para lograr este propósito estas corporaciones financieras hacen uso de diversas herramientas de seguridad informática, como las aplicaciones y programas los cuales permiten encriptar toda esa información para reducir al máximo la debilidad de los datos confidenciales de los beneficiarios; en estos casos la información es sensible por tal motivo no todas las personas tienen acceso a la información y en los procesos de que esta sea extraída por terceros son manejadas con fines delictivos. Por esta razón el Estado colombiano vio la necesidad de derogar ciertos artículos de la ley 1273 de 2009 para proteger derechos y con la elaboración de la ley 1581 de 2012 permitió salvaguardar los datos íntimos y reglamentar los derechos que tienen los Colombianos al habeas data y la importancia que se tiene del mismo.

De igual manera mediante la sentencia 748 de 2011 se establecieron controles Constitucionales a la ley 1581, buscando que todos los antecedentes asentados en cualquier base de datos sean protegidos y permitan efectuar operaciones, recolección, acaparamiento, circulación, uso o supresión por parte de entidades de carácter privado y público. Es por esto que la Corte Constitucional anunció el habeas data como garantía del derecho fundamental a la intimidad, y por ello la defensa de los datos hace referencia a la vida familiar y personal lo cual se considera específicamente impenetrables pues son entendidos como fundamentales para efectuar su proyecto de vida y ningún otro particular puede interferir o apoderarse de estos ya que se evita el desarrollo normal de los ciudadanos colombianos e incluso extranjeros dentro de nuestro territorio.

En la actualidad el hábeas data es un derecho independiente, combinado por la independencia económica e independencia informática; este derecho se considerado fundamental y debe ser eficaz al momento de la protección se deben generar los mecanismos que la garanticen los cuales, no sólo deben ser reafirmado solo por jueces, sino por también por parte de una institución administrativa que además de controlar y

vigilar a todos los sujetos aplicando y aplicarles tanto a el derecho público como al privado, obedeciendo que cada caso en particular desempeñe su función de una manera efectiva, buscando siempre el resguardo de datos en razón de su carácter técnico, y que estas tengan la capacidad de instaurar políticas públicas encaminadas a esta factor, pero sin el preámbulo del carácter político para el acatamiento de estas disposiciones.

Así mismo, la Ley obliga a todas las entidades ya sean públicas o privadas a revisar y mantener mecanismos de seguridad sobre el uso y manejo dado a toda la información de carácter personal contenidos en sus bases de datos, para con ello cumplir lo expuesto por Rodríguez (2015). “Al promover un sistemas de información en donde está, no presente fugas que puedan fortalecerse de manera puntual utilizando herramientas dadas por la ley haciendo que estas entidades, definan la forma y la manera pueden darse los tratamientos y cuáles son los fines y medios esenciales para el tratamiento de estos, solicitando a los usuarios o titulares quienes deben fungir como responsable y qué tipo de datos pueden transferirse a otras entidades respondiendo así a los principios de la administración de datos y a los derechos a la intimidad y el hábeas data del titular del dato personal".

Según otro autor nos dice que: "existe una clasificación de delitos informáticos, la cual está dada por el Convenio de Ciberdelincuencia del Consejo de Europa firmado en noviembre de 2001 en Budapest". (Pabón 2013).

Por dicha clasificación se puede deducir que los delitos informáticos, se dividen en cuatro grandes grupos: acceso ilícito a sistemas informáticos, interceptación ilícita de datos informáticos, interferencia en el funcionamiento de un sistema informático, abuso de dispositivos que faciliten la comisión de delitos; se debe tener claro que esta clasificación se encuentra fundamentada en tres pilares muy necesarios para la seguridad informática que son: la confiabilidad, la integridad y la disponibilidad de los datos en sistemas informáticos, al respecto también estos pilares solo pueden ser alterados por expertos con un alto conocimiento sobre el tema de programación y seguridad informática los llamados hackers pero incluso estos también tiene una clasificación definida ya que hay algunos hackers de cuello blanco que son expertos programadores orientados a violar la información de un sistema informático con libertad, con el único fin de evidenciar las

fisuras de una determinada red ya que la mayoría de veces son en realidad trabajadores de los sistemas de una entidad que deben estar velando por la seguridad informática.

Además encontramos otra categoría de Hackers de sombrero negro los cuales descargan y violan los sistemas sin autorización con pedido legal o formal ya sea que este le pertenezca a una empresa o entidad del gobierno, pero estos lo hacen es con otros fines encaminados más a la monetización esta se da cuando el hacker debe realizar ataques a la red del banco con el fin de obtener información clasificada, como por ejemplo cuentas bancarias y números de tarjeta (atenta contra la confidencialidad) o tumbar páginas para que no puedan ser visitadas o redirección ando al usuario (atenta contra la disponibilidad) esto se lo realizan no solo a las personas naturales sino también a las jurídicas para realizarle desfalcos; pero también se da por el solo hecho de alcanzar algún nivel de popularidad mediante el reconocimiento mediático como incluso como activista enfocado o defensor de sus ideales mediante el campo digital llamado hacktivismo.

Por todo lo anterior estos ataques se están dando con mayor frecuencia, debido a la forma acelerada con la que se maneja demasiada información en estas bases de datos o sistemas digitales de registro financiero lo cual a su vez ha provocado que mucha de esta información recorra el mundo moviéndose a una velocidad impresionante y haciendo que muchas veces no sea posible la protección total de esta, en especial los datos de carácter más personal; como lo manifiesta Segu.info (2016) expone que: "la instrucción de los derechos en los titulares de la información, deben entender que el manejo de la información, se puede disponer del anuncio como tal, a partir de un tiempo prudencial (a los cinco días siguientes de la comunicación), a partir de ahí el titular, puede allegar una carta, en donde comunique a la Superintendencia de Industria y Comercio, sobre las causales de la queja. Seguidamente, debe anexar el formato de autorización diligenciado para poder recolectar los datos y así determinar el canal electrónico y físico para recibir las autorizaciones".

Otros juristas explican el delito informático en forma típica y atípica, entendiendo como típica las conductas antijurídicas y culpables que se realizan en las computadoras como herramienta para la comisión del delito, actitudes ilícitas, y la capacidad o conocimiento que tiene quien comete el delito a través de la computadora o sistemas informáticos; así

mismo la responsabilidad del acceso a esos datos recae en los que fueron autorizados para manejar este tipo de información y son ellos quienes deben definir las finalidades y los métodos que se utilizarán con cada grupo de acuerdo al interés o sensibilidad la información, pues para esto se debe mostrar la política de tratamiento ajustada a la normatividad creada para este propósito ya que por ellos cuentan con esa autorización.

En Colombia los que pueden manejar la información digital de personas tanto naturales como jurídicas deben ser asentados en sistemas bien protegidos, pues que sobre ellas recae la disposición de la base de datos que de ser accedida sin autorización genera unas sanciones para quienes hayan sido responsables del cuidado y tratamiento de información personal ya sean personas naturales o jurídicas, dichas sanciones son impuestas por la superintendencia de industria y comercio y comprenden multas de carácter institucional o personal hasta por dos mil S.M.L.M.V., además se pueden suspender la autorización que tenía para hacer las actividades ligadas a esta información hasta por seis meses y puede llevarse a cabo un cierre inmediato y definitivo de la actividad que esté ligada a estos datos.

En pocas palabras las empresas, corporaciones o entidades bancarias son la únicas responsables de la información que acorde con el principio de la buena fe depositan en ellos los clientes, y los convierte en únicos responsables de los daños o robos virtuales de que lleguen a ser víctimas sus clientes es por ello que se ha querido dejar claro cuáles son las leyes que las regulan y generan obligaciones sobre estas entidades, entonces es bueno pasar a establecer cuál es la ruta jurídica que debe seguir quien sea víctima de cualquier conducta punible y sancionable por el ordenamiento penal colombiano; lo primero que se debe hacer al enterarse que está siendo o fue víctima de algún robo suplantación o estafa a través de medios electrónicos es utilizar este mismo medio a su favor y notificar a la entidad, corporación o banco de lo que está sucediendo para que este de forma inmediata suspenda, apague o bloque la tarjeta o evite la realización de más descuentos de la cuanta ya sea crédito o débito. Segundo cuando la estafa o el robo es por un valor que se encuentre entre 10 y 150 S.M.L.M.V. ($7´377.170 y $110´657.550) deben demostrar una querella ante la Fiscalía en cualquiera de sus oficinas más cercanas en todo el territorio nacional por parte del titular de la cuenta.

Si la estafa es mayor a 150 S.M.L.M.V., no solo puede denunciar la victima sino cualquier persona que tenga conocimiento del caso, se pueden presentar en forma verbal o por escrito y sin la necesidad de un abogado ya sea en los diferentes centros de atención dispuesto para este propósito como las salas de atención al usuario (S.A.U.), la unidad de reacción Inmediata (U.R.I.) los centros de atención a víctimas y las casas de justicia. Ya cuando este caso se presenta en un municipio o corregimiento donde no existen ninguna oficina lo puede hacer ante la policía nacional; debe presentar la cédula de ciudadanía y la mayor cantidad de material probatorio posible, que permita la demostración de la estafa o del engaño ya sean: unas facturas, algunos folletos de la empresa o entidad que le pidió sus datos, material fotográfico en físico o en un dispositivo, testimonios, comprobantes de pago o facturas, entre otros.

Asimismo, la Fiscalía hará la indagación de los hechos y los presentara ante un juzgado penal para establecer el autor material del delito, teniendo en cuenta que las entidades bancarias son responsables pero hasta cierto monto y este varía de acuerdo a las políticas propias del banco. El siguiente segmento que se quiere analizar está relacionado a algo muy común y actual es la información ya sea que esta esté en texto o en imágenes que puede almacenar un dispositivo móvil en su memoria interna o externa y se trata de los computadores portátiles, las memoria U.S.B, una Tablet o un celular ya que como lo han demostrado diferentes estudios estamos en la época en que sean hecho videos y tomado más fotografías que en todo el tiempo trascurrido desde la aparición de estos dispositivos en la humanidad, lo otro que se demostró es que esto como es apenas lógico se ha debido a la accesibilidad que se tiene para adquirir y disfrutar estos aparatos, como dichos dispositivos tiene un uso privado los textos e imágenes también almacenadas en ellos terminan siendo sensibles para su propietario, ya que pueden contener contenidos muy íntimos o comprometedores.

Además, es allí donde la legislación colombiana promulgo la ley 1273 del 2009 y creó otros bienes protegidos por el Estado, para velar por el buen nombre o Habeas Data del artículo 15 de nuestra Constitución Colombiana el cual en estos casos es el bien intangible que puede verse afectado por el uso o manejo prohibido de la información personal almacenada en equipos móviles; esto también puede convertirse a su vez en un concurso de

hechos punibles al presentarse extorsiones, abusos sexuales todo lo se puede presentar por el solo hecho que la víctima no quiere que se rebele o se dé a conocer algunas imágenes o información que tiene en su poder el victimario. Lo complicado de eso es que muchas personas no tienen conocimiento de que las autoridades cuentan con muchas herramientas para colaborarle a estas personas en la solución pronta y efectiva para esta situación y es entonces cuando por querer evitarse un escándalo público terminan es convirtiéndose ellos mismos en los creadores del mismo.

Así mismo es muy importante tener claro las formas como la información es obtenida por victimario porque si esta se dio por confianza en él y ella se le entrego de forma voluntaria pero este ya sea por represaría, venganza o buscando beneficio económico decide publicarla eso no exime de responsabilidad al culpable o en los casos en que cometiendo un delito este conlleva a otro como puede ser el hurto de un teléfono móvil o celular que al lograr ser desbloqueado por el victimario descubre una imágenes de un contenido sexual explícito y valiéndose de artimañas pretende extorsionar o acceder sexualmente a la propietaria para no publicarlas en la WEB esa información. En estos dos casos hipotéticos pero muy comunes estamos ante el delito de sexting pero para que se configure este se debe presentar el material probatorio como: fotos, videos y mensajes de contenido sexual que son enviados a través de sistemas electrónicos ya sean dispositivos móviles o computadoras; y hacer la respectiva denuncia ante la unidad de delitos sexuales de la Fiscalía en donde narre los hechos que fundan el delito.

También podrá dirigirse a realizar la denuncia ante el cuadrante de la Policía Nacional o la Comisaria de Familia más cercana a su residencia, donde será enviada a la autoridad competente; durante el transcurso del proceso la Fiscalía deberá solicitar al Ministerio de las Tecnologías de Información y de las Comunicaciones y por medio del proveedor de servicios de internet bloquee la página web donde aparecen las imágenes del menor para darle un manejo adecuado a las pruebas para que puedan ser válidas y tenidas en cuenta en un futuro proceso penal.

Por otro lado, durante un coloquio celebrado en Wurzburgo la Asociación Internacional de Derecho Penal (1992) adoptó “diversas recomendaciones respecto a los delitos informáticos, estas contemplaban que en la medida en que el derecho penal tradicional no

sea suficiente deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad)".

Por consiguiente, los delitos informáticos son difícilmente manifiestos ya que estos delincuentes actúan discretamente y poseen equipos capaces de borrar todo rastro de infracción y fabricación del delito, y desafortunadamente el país no cuenta con personal altamente calificado para indagar dichos hechos ya que al momento de ser denunciados son tipificados como otros bienes jurídicos constituidos en el código penal colombiano; además se debe tener en cuenta que la ley penal de cada Estado solo es aplicable dentro de su territorio lo que genera un escenario donde mayormente se configura este delito llamado ciberespacio ya que en este no existen fronteras territoriales.

En conclusión, los infractores que cometen esta clase de delitos se mantienen en anonimato como forma de evitar su responsabilidad ya que no emplean sus propios equipos electrónicos para que no puedan ser detectados utilizando múltiples virus o en ocasiones se pueden valer de un tercero para hackear la información de usuarios que no tienen las medidas de seguridad adecuadas convirtiéndose en presa fácil de estos criminales que cometen toda clase de trasgresiones vulnerando la intimidad y la privacidad de sus datos.

REFERENCIAS BIBLIOGRAFICAS

- OJEDA, J. RINCÓ, F. ARIAS, M. y DAZA MARTÍNEZ, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia, recuperado de: http://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176.

- LAUDON, C. y GUERCIO, C. (2009), Delitos informáticos y entorno jurídico vigente en Colombia. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=3643404.
- RODRÍGUEZ, G. (2002). Derecho penal e Internet, y CREMADES, J. Régimen jurídico de Internet, La Ley, Madrid, pág. 261.

- DAVARA RODRÍGUEZ, M. (1997). Manual de derecho informático, aranzadi, Pamplona, (p. 288).

- OXMAN, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del phishing y el pharming. Recuperado de: https://scielo.conicyt.cl/scielo.php?pid=S0718-68512013000200007&script=sci_arttext&tlng=en.

- recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

- Sentencia T-277/15 (2013). Derecho a la intimidad y al debido proceso. Recuperado de: http://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm.

- MARTÍNEZ, R. (2006). Hackers blancos y negros, mismo trabajo, distinto objetivo. Recuperado de: http://ntrzacatecas.com/2016/04/24/hackers-blancos-y-negros-mismo-trabajo-distinto-objetivo/

- Cuellar P. (2008) Informe de ponencia para primer debate al proyecto 281 de 2008. Bogotá, Mayo 14 de 2008, p. 5. AA.

- CASTRO, S. (2002) Ley sobre protección a la vida privada o protección de datos de carácter personal, en: http://www.sernac.cl/leyes/ La información como bien jurídico y los delitos informáticos en el nuevo Código Penal Colombiano. Universidad Externado de Colombia, Bogotá, julio 15 de 2002. Vía Internet.

- BURNEO, R. E. (2010). Derechos y Garantías Constitucionales en el Ecuador, Evolución y Actualidad. Quito: Corporación de Estudios y Publicaciones.

- Caballenas de las Cuevas, G. (2008). Diccionario Jurídico Elemental. Buenos Aires: Editrorial Heliasta. Carpio, D. S. (2013). El Delito Informático, Prueba pericial informático.

- LOJA FLOREZ, C. (2013): Universidad Técnica Particular de Loja, tipos de hackers, Revista de información, tecnología y sociedad No. 18.
- GANDINI, I. (2016), Ley de los delitos informáticos en Colombia {En línea} {29 de Abril de 2016} Disponible en http://www.deltaasesores.com/articulos/autoresinvitados/otros/3576-ley-de-delitos-informaticos-en-colombia.

- GARCÍA, C. (2010). Hacking ético. Hablemos de Spoofing {En línea} {19 de Noviembre de 2016} Disponible en https://hackingetico.com/2010/08/26/hablemos-de-spoofing/

- GUZMÁN, A. (2011). Seguridad Informática, confidencialidad e integridad {En línea} {29 de Abril de 2016} Disponible en http://seguridadanggie.blogspot.com.co/2011/11/confidencialidad.html.

- MARTÍNEZ, B. (2006). La filosofía hacking & cracking blog.capacityacademy.com/2012/07/11/7-tipos-de-hackers-y-sus-motivaciones/32.

- McClure, S.; Scambray, J.; Kurtz, G. (2000) Hackers: secretos y soluciones para la seguridad de redes.

- McGraw-Hill, N. (2016). Bots y botnets: una amenaza creciente {en línea} {2 de noviembre de 2016} disponible en https://es.norton.com/botnet .

- OJEDA, J., RINCÓN, F., ARIAS, M. y DAZA, L. (2010), Delitos informáticos y entorno jurídico vigente en Colombia. Cuaderno de contabilidad.

- PABÓN, P. (2013). Manual de Derecho Penal. Tomo II Ediciones Doctrina y Ley.

- POSADA MAYA, R. (2006). Aproximación a la criminalidad informática en Colombia. Revista de derecho, comunicaciones y nuevas tecnologías (2), págs. 11- 60.

- RIQUERT, M. (2014). Convenio sobre Cibercriminalidad de Budapest y el Mercosur Propuestas de derecho penal material y su armonización con la legislación regional sudamericana.

- RODRÍGUEZ, J. (2015), Revista Derecho Penal, año III N° 7, análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación, facultad de derecho, Universidad Javeriana, Bogotá.

- Cámara de Comercio de Bogotá (2013). ABC para proteger los datos personales, Ley 1581 de 2012, decreto 1377 de 2013, Recuperado de: https://colombiadigital.net/publicaciones_ccd/anexos/certicamara_proteccion_datos_ago28.pdf.

- CAMACHO LOSA, L. (1996), El Delito Informático, Madrid, España, Manual de Informática Jurídica, Editorial Astrea.

- LEY 599 DEL 2000 Código Penal Colombiano.