LA OBTENCIÓN DE LA PRUEBA PENAL INTERNACIONAL EN MATERIA DE DELITOS CIBERNÉTICOS.

Jessica López

Mónica Sáenz Figueroa

Universidad Politécnico Gran Colombiano

Facultad de Derecho

Bogotá, 2018

LA OBTENCIÓN DE LA PRUEBA PENAL INTERNACIONAL EN MATERIA DE DELITOS CIBERNÉTICOS.

Jessica López

Mónica Sáenz Figueroa

Monografía de grado para optar por el título de abogado.

Universidad Politécnico Gran Colombiano

Facultad de Derecho

Bogotá, 2018

TABLA DE CONTENIDO

Contenido

CAPITULO 1. PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema de investigación

El índice Global de Competitividad del año 2017-2018 realizado por el Foro Económico Mundial (Schwab, 2017-2018) (p.1), señala que frente a este indicador, el cual calcula la facultad que tiene un país, para sostener un crecimiento continuo en el tiempo, identificando y comparando la capacidad de los países evaluados, para proveer oportunidades de progreso a sus ciudadanos -, Colombia perdió cinco posiciones frente a la evaluación del año anterior, ubicándose en la posición 66 entre 137 países estudiados (p. 13).

Lo anterior, en razón a que las instituciones que prestan un servicio a la sociedad no son lo suficientemente eficientes y competitivas, esto no es ajeno al sector justicia, ya que el país se ubica entre los cinco países con más alta impunidad, tal como se ha señalado en el Informe Nacional de Competitividad 2017-2018 (El Consejo Privado de Competitividad, 2017) (p. 8).

Dentro de este contexto, uno de los delitos que más ha aumentado en los últimos años en el país es el que tiene que ver con temas informáticos, ya que en promedio se producen 542.465 ataques informáticos diarios (Portafolio, 2017), lo que ubica a Colombia en el quinto lugar de las naciones más afectadas por este flagelo, en Latinoamérica.

Las cifras que revela el CAI Virtual de la Policía, en el informe sobre el balance del cibercrimen en 2017 (Policia Nacional de la Republica de Colombia, 2017), señala que en lo corrido de ese año se recibieron 11.618 denuncias por estos delitos, de estas denuncias menos del 2% llegan a juicio (p. 8).

Ante este panorama, se abre un abanico de posibilidades para abordar los delitos informáticos, lo anterior teniendo en cuenta la relevancia que ha tomado el tema no solo en el ámbito internacional, al interior del país, que las políticas que se tomen frente al tema van a influir directamente en el nivel de eficiencia de la justicia.

Por tal motivo, es necesario ahondar esfuerzos con el propósito de realizar análisis y estudios, a fin de generar propuestas para mejorar dichos indicadores, ya que esto está estrechamente ligado con las oportunidades de desarrollo del país.

Esta es la razón por la cual centraremos esta monografía, en el estudio de los delitos informáticos desde la óptica del derecho penal y la consecución de la prueba internacional.

1.2 Formulación del problema de investigación

El génesis de esta monografía lo encontramos en el concepto que conocemos hoy como globalización, entendido este como un proceso dinámico y estructural que cuenta con unas características especiales de interdependencia e interconexión a nivel mundial, las cuales catapultaron a la sociedad hacia una nueva era denominada de la tecnología, en la que el internet

se consolidó como su motor, gestando grandes cambios no solo a nivel político, sino también en lo social, económico y cultural.

Para iniciar esta contextualización es necesario precisar algunos conceptos, el primero de ellos es el internet, para este fin acudiremos a la definición de la Real Academia de la Lengua Española, que señala a este como una red de informática mundial, creada con el propósito del intercambio de información, a partir de la interconexión directa entre computadoras o dispositivos electrónicos y que cuenta con dos características especiales, una es su funcionamiento descentralizado y otra que manejan un lenguaje especial de comunicación.

Sobre el particular, vale la pena señalar que esta interacción entre dichos dispositivos a través del internet ha ido creciendo exponencialmente. Lo anterior se sustenta en el informe de la Unión Internacional de Telecomunicaciones UIT (ITU, 2017), que señala que de los siete millones de personas que habitan en la tierra, cuatro se conectan a esta red.

Todo ese flujo de información se aloja en un lugar denominado ciberespacio, el cual se concibe como una realidad a pesar de no poder ubicarse en un espacio físico. De hecho, se afirma que se encuentra al interior de cada uno de los módulos que se conectan a la red y tiene como peculiaridad que forma una proyección artificial y arbitraria del mundo real, lo cual es consecuencia de la masificación de estos dispositivos, (valenzuela).

Este espacio virtual al generar una realidad paralela a la nuestra creó una forma diferente de interacción entre las personas, empresas y gobiernos, la cual ha sido tan exitosa que cada vez existe un mayor grado de interdependencia entre ellos y de estos con la red. Este fenómeno no solo trajo

grandes beneficios a la sociedad, si no que por el contrario también abrió la puerta a un sinnúmero de problemas en diferentes estadios, de los cuales escogimos uno como marco central de nuestro estudio de investigación y es el del delito informático.

El informe de riesgos mundiales del año 2017 (Foro Económico Mundial, 2017), señala que, en el marco de la cuarta revolución industrial, - la cual tiene que ver entre otras cosas con la creciente interdependencia de las infraestructuras de comunicación- indica que el ciberespacio es algo tan real como los riesgos que conlleva (p. 16). Esta es la gran paradoja de la era de la información, en la medida en que la tecnología le ha dado al hombre poder para crear y construir, pero ese dominio lamentablemente también está al alcance de las personas que busca perturbar y destruir.

Al respecto, podemos afirmar que el ciberespacio generó un sitio propicio para la comisión de delitos, los cuales son denominados delito informático. Definidos estos, como conductas punibles que se configura a partir del mal uso del internet, se pueden dividir en dos grandes grupos, el primero los que se conforman a partir de la utilización de la red como medio para cometer un delito, como la interceptación de datos electrónicos y , y el segundo cuando la red es el fin del daño, es decir, que el propósito se concentra en de destruir o inutilizar cualquier dispositivo electrónico o el propio internet, ya sea utilizando un tipo de virus, troyano o gusano.

En un principio se creía que estas acciones eran ejecutadas solo por personas que tenían amplios conocimientos en el área de los sistemas. Sin embargo, esta afirmación se encuentra revaluada, en la medida en que el avance en la tecnología logró que el internet sea de acceso público.

Para dimensionar el problema del delito informático en el mundo, basta con señalar las cifras reveladas en un estudio de Cybersecurity Ventures (–Steve Morgan). Al día se presentan más de un millón de víctimas por algún tipo de ciberdelito, de ahí la importancia de que los países busquen contrarrestar este flagelo, no solo ajustando sus legislaciones internas, sino con acuerdos de cooperación internacional, teniendo en cuenta que estos delitos trasgreden las fronteras.

En Colombia el problema no es diferente al que se presenta en el resto del mundo, según la Policía Nacional (DIJIN), para el año de 2017 este tipo de delitos aumentaron 28 % respecto del año anterior, y causaron 50.000 millones en pérdidas, a la vez que se comenzaron a utilizar nuevas modalidades en este campo.

De lo anteriormente descrito, en esta monografía hemos limitado el estudio del mismo desde la óptica del derecho penal, enfocándonos en la obtención de la prueba jurídica internacional, en materia de delito informático. Así es como surge nuestro problema de investigación: ¿Cuáles son los desafíos que enfrentan los operadores de la justicia colombiana, para la obtención de la prueba penal internacional, en materia de delitos informáticos?

1.3 Objetivos del trabajo

1.3.1 *Objetivo General*

- Establecer los desafíos que enfrentan los operadores de la justicia colombiana, para la obtención de la prueba penal, en materia de delitos informáticos.

1.3.2 Objetivos Específicos

- Identificar los mecanismos y los instrumentos de cooperación internacional con lo que actualmente cuenta Colombia para la obtención de la prueba penal en materia de delitos informáticos.
- Determinar y establecer el proceso de obtención de la prueba, en materia de delitos informáticos, en el marco del sistema penal acusatorio colombiano.
- Identificar y establecer los problemas jurídicos de la obtención de la prueba penal, en materia de delitos informáticos en el marco de la cooperación jurídica internacional.

1.4 Justificación

La razón que nos lleva a realizar este estudio radica en la dificultad que tienen actualmente los operadores de justicia, a la hora de obtener pruebas trasnacionales cuando investigan un delito cibernético. Para ilustrar la anterior afirmación, utilizaremos un ejemplo en el cual se configuró el

delito de suplantación de sitios web para capturar datos personales, a raíz del envío de un correo electrónico masivo, que en su contenido tenía un enlace en el cual al darle doble clic solicitaba realizar una actualización de datos personales.

En el avance de la indagación, se estableció que el servidor desde el cual se envió el e- mail se encontraba en Suráfrica, es en este punto cuando se activan los mecanismos de cooperación judicial, con el fin de obtener información sobre el posible autor de la conducta punible. Sin embargo, en la actualidad Colombia no tiene acuerdos con este país, que permita la obtención de la prueba penal en un tiempo razonable.

Otro ejemplo, es el caso de un niño contactado mediante un chat por parte de un adulto, el cual se camufla bajo la identidad de un menor de edad, con el fin de generar empatía y así lograr que el niño le envíe fotografías desnudo, para luego amenazarlo con distribuirlas en internet si no le enviaba más. En el proceso investigativo se estableció que la IP desde la cual se conecta el victimario se halla en México, y este delito llamado grooming, no se encuentra configurado en ese país.

Estos son algunos ejemplos de los desafíos a los cuales se enfrentan los operadores de justicia, cuando tienen un caso de delitos informáticos y necesitan activar los mecanismos de cooperación judicial, con el fin de obtener pruebas internacionales.

En este contexto, hemos dividido este estudio en tres grandes capítulos, en el primero abordaremos los delitos cibernéticos realizando una conceptualización en general junto con su clasificación, para luego llevar a cabo un estudio de este tema en la legislación colombiana.

En el segundo capítulo, nos enfocaremos en todo lo relacionado con la obtención de la prueba internacional en materia penal en delitos cibernéticos, para este propósito iniciaremos con una introducción de la generalidad la obtención de la prueba en materia penal, para luego llevar a cabo un análisis detallado en materia de delitos cibernéticos y sus limitaciones actuales.

Por último, en el tercer capítulo buscaremos desarrollar la solución a la hipótesis base de esta monografía, a través del tema cooperación jurídica internacional, profundizando en sus herramientas, los convenios aplicables en este tema, para luego realizar una recomendación para la solución de la hipótesis planteada.

Al respecto, se plantea un estudio de carácter socio-jurídico donde es necesario realizar una verificación empírica de la hipótesis, en atención a ello, el tipo de investigación entra en un proceso de explicación y descripción, enfocándonos en la parte conceptual del problema jurídico.

Lo anterior se desarrollará por medio de un estudio documental teórico y doctrinario, realizando un barrido jurisprudencial, que nos va a ayudar a esclarecer si a nivel internacional y en Colombia existen pronunciamientos por parte de las corporaciones judiciales, en el tema de interés. Así mismo, se pretende medir el nivel de eficiencia y eficacia de la legislación encontrada a través de la realización de entrevistas y estudios de casos, con el fin de poder responder la pregunta de investigación y hacer las recomendaciones pertinentes.

CAPITULO 2. DELITOS INFORMATICOS

Con el propósito de enmarcar la importancia de los delitos informáticos en el ordenamiento jurídico actual, es necesario entender que para poder abordarlos se ha acudido a varias corrientes de pensamiento, por un lado están los autores que afirman que basta con renovar antiguas formas delictivas, otros señalan que es necesario crear nuevas modalidades criminales, y los demás advierten que no es imperioso realizar una diferenciación entre los delitos informáticos y los tradicionales, ya que los primeros son los mismos que los segundos, solo se diferencian porque son consumados a través de otros medios.

2.1 Definición

En este contexto, iniciaremos delimitando el concepto de delito informático, para este propósito acudiremos a revisar el desarrollo de esta noción en la academia. Por ejemplo, para el profesor mexicano Julio Téllez Valdés (Valdéz, 2006) afirma que los delitos informáticos son formas de actuación ilícitas, en las cuales el computador puede ser un mero instrumento o por el contrario es el fin de la acción (p. 104).

Dicho autor a su vez describe una serie de características para poder identificarlos, entre las que se encuentran; conductas ejecutadas por determinadas personas que tienen conocimientos avanzados en tecnología, o que cuentan con unas características especiales dentro de la sociedad como la

honorabilidad y respetabilidad, vinculando estos delitos dentro de los denominados de cuello blanco.

Así mismo, señala que son “acciones ocupacionales” en la medida en que se realizan en muchos casos, desde el lugar de trabajo del sujeto que las ejecuta, también describe que son “acciones de oportunidad” ya que se producen debido a la creación de escenarios en el ámbito de la economía y la tecnología.

Otras particularidades señaladas por este autor, advierten que estas acciones antijurídicas provocan grandes pérdidas económicas, se efectúan sin la necesidad de que la persona que ejecuta se encuentre físicamente en el lugar donde se produce el daño, así mismo indica que es difícil confirmar el perjuicio ocasionado, ya que faltaría probar la intencionalidad, también afirma que facilita la comisión de acciones delictivas en menores de edad y que cada vez este tipo de delitos se incrementan más.

Por su parte, para los catedráticos Norberto J. de la Mata y Leyre Hernández Díaz (Díaz, 2009), señalan que en la actualidad existen nuevas maneras de trasgredir los derechos tanto los colectivos, como los individuales, esto ha llevado a que el derecho penal se ajuste a este nuevo contexto, incorporando el concepto de daño al sistema informático o su contenido (p. 311). Sobre el particular, realizan la siguiente apreciación, el concepto tradicional del daño sostiene que el objeto sobre el cual insiste la conducta típica debe ser corpóreo o material, mueble o inmueble, económica y material, cosa propia o ajena, susceptible de deterioro o destrucción, y estas características no se cumplen en un sistema informático, los cuales físicamente son impulsos electromagnéticos.

Dichos autores, introducen el concepto de daño informático cuando la consecuencia de una conducta es la invalidación, destrucción, inutilización, desaparición entre otras, de los componentes de un sistema tecnológico, que se traduce en la inoperancia de los programas, aplicaciones o el acceso a sus datos.

Otro autor es Felipe Villavicencio Terreros (Terreros, 2014) quien señala que los delitos informáticos en la comunidad internacional son asociados a la ejecución de infracciones a la ley por medio del computador y la red, pero indica que este pensamiento no es del todo cierto en la medida que estos son solo medios que facilitan
la acción, pero no es el determinante de la comisión de delito (p. 286).

Por último, Carlos Sarzana (Sarzana, 1979), indica que las infracciones realizadas por computador abarcan diversas actuaciones criminales, en las cuales este dispositivo ha estado implicado como medio u objeto de la acción (p. 16).

Nuestro concepto sobre la definición de los delitos informáticos sería; Cualquier comportamiento delictivo, en el cual el computador es el medio o el fin de la acción.

2.2 Delitos informáticos en el mundo

Ahora bien, en el ámbito internacional a través de múltiples organismos multilaterales se ha buscado definir y delimitar los citados delitos, la primera legislación que se conoce del tema fue realizada por la OCDE (Organización de Cooperación y Desarrollo Económico) en el año de 1983, titulado Delitos de Informática: análisis de la normativa jurídica (Unidas, 2010).

Dicho escrito reseñaba la legislación existente en ese momento y realizaba algunas recomendaciones para que los Estados Miembros las siguieran, las cuales se plasmaron en una lista que contenía ejemplos del uso indebido de la tecnología. Como por ejemplo la falsificación y el fraude electrónico, la reproducción de programas electrónicos, espionaje informático, utilización no autorizada de computadores entre otros, los cuales deberían estar prohibidos y sancionados en la legislación penal interna de cada país.

En el año de 1996 el Comité Europeo para los Problemas Criminales (CDPC), creó una comisión de expertos en materia de delitos cibernéticos. Su decisión se cimentó en aspectos tales como el vertiginoso desarrollo en el sector de la tecnología de la información, la compenetración de los sistemas de telecomunicación, y por último la facilidad en el acopio y transmisión de comunicación a través de redes y superautopistas de la información (Consejo Europeo, 2001) .

En este contexto, se empezó a dilucidar el concepto de delitos cometidos en el ciberespacio, los cuales contienen actividades que transgreden la confiabilidad, disponibilidad e integridad tanto de las redes , esto llevó a que en el año 2001 se suscribiera en la ciudad de Budapest, el Convenio sobre la Ciberdelincuencia del Consejo de Europa en el cual se definió el delito informático como

todo suceso encaminado a abusar o violar la disponibilidad, confidencialidad e integridad, de los datos, redes y sistemas informáticos (p. 6).

2.3 Características

Los delitos informáticos cuentan con los siguientes rasgos;

- Son difíciles de demostrar, debido a los obstáculos que se presentan en la consecución de las pruebas.
- Evolucionan y se expanden rápidamente
- Pueden ejecutarse de manera rápida y sin estar físicamente desde el lugar donde se realiza la acción.
- Se consideran delitos de Cuello Blanco, en la medida en quienes los ejecutan tienen conocimientos específicos en el área tecnológica.
- En la actualidad no existe paridad entre los casos por estos delitos, las denuncias por estos hechos, y las condenas debido a la falta de regulación en las legislaciones internas de los países.

2.4 Evolución de los delitos informáticos en Colombia.

Hacia la década de los años noventa en Colombia durante el gobierno del presidente Cesar Gaviria se dio la apertura económica, la cual trajo consigo un cambio importante en la sociedad, ya que el país abrió sus puertas al mundo. Esta nueva interacción facilitó el ingreso al país de compañías de

telecomunicaciones internacionales, las cuales facilitaron el servicio de internet permitiendo que cada vez más personas tuvieran acceso a este medio.

De hecho, hoy en día Colombia maneja cifras relevantes frente a otros países de Latinoamérica en cuanto al acceso de conexión de internet. Lo anterior se sustenta según las cifras reveladas por último informe del Ministerio de la Tecnología de la Información y Comunicación (Revista Dinero, 2018), que señala que el 61% de la población nacional tiene acceso a la red, esto como lo hemos visto anteriormente no solo ha traído beneficios para la sociedad en general, sino que también ha favorecido la comisión de delitos.

El primer indicio para la reglamentación de estas conductas al margen de la ley se produce en el año de 1989, cuando se crea la primera ley que busca proteger las nuevas creaciones tanto de aplicaciones, como de soluciones informáticas. Lo anterior, se materializó a través del decreto 1360 del citado año, el cual insta a que el software sea inscrito en el Registro Nacional de Derechos de Autor, con el ánimo de proteger la propiedad intelectual.

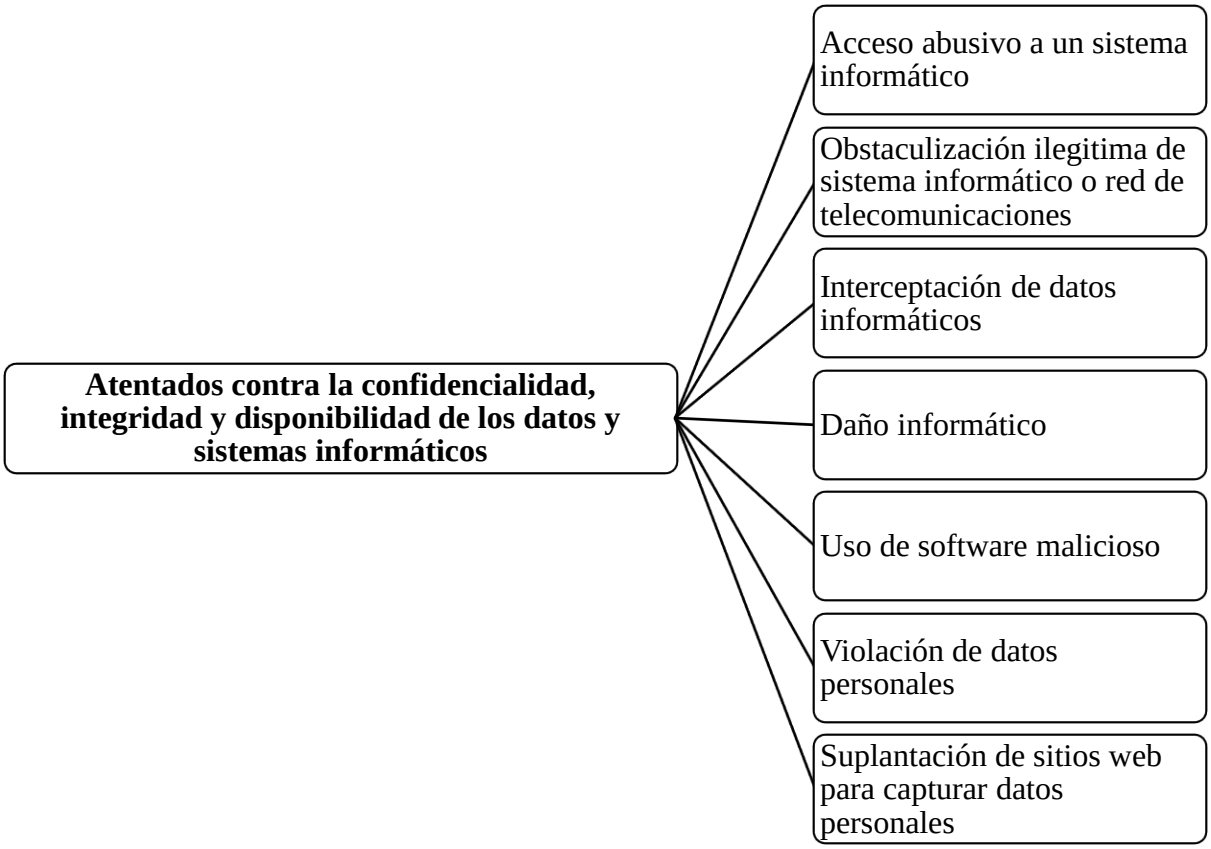
Luego en el año 2000 se realiza la reforma al Código Penal Colombiano, en esta se introduce la penalización a la violación de los derechos de autor, los cuales se tipifican en el Título VIII, titulado delitos contra los derechos de autor, entre los que se encuentran la violación a los derechos morales, defraudación a los derechos patrimoniales de autor, la violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.

Así mismo en el Título III se delimitan los delitos contra la libertad individual y otras garantías, los cuales abarcan la interceptación de comunicaciones, violación a la intimidad, daño en obra o

servicios de comunicaciones, utilización ilícita de equipos de comunicación, comunicaciones, correspondencia de carácter oficial y acceso abusivo a un sistema informático.

Después, en el año 2001 mediante la ley 679 (Diario Oficial No. 44.509 de 4 de Agosto, 2001), se conforma el Estatuto para prevenir y contrarrestar la pornografía y el turismo en menores de edad, en el cual se prohíbe para los administradores, proveedores, servidores, usuarios de la red en general, albergar documentos o archivos que contengan material con actitudes sexuales o pornográficas en las cuales se encuentren menores de edad. Luego, el anterior estatuto, se penaliza mediante la ley 1336 de julio de 2009.

Posteriormente con la ley 1273 de 2009, se establece un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos, el cual es considerado como la ley contra los delitos informáticos en el país, pues contempla lo siguiente:



2. 5 Estructura penal de los Delitos Informáticos

El doctor Almanza (Altamira, 2010) define los dos tipos de sujetos que se encuentran en el tipo penal (pp. 71-78). Al respecto, el delito por ser el producto de un hecho realizado por el hombre, siempre tiene un autor, ya sea debido a que la persona realizó u omitió una acción esperada, a esto se le conoce como sujeto activo (p. 71). Por su parte, la persona quien tiene el interés del bien jurídico lesionado es el sujeto pasivo (p. 74).

Ahora bien, para conceptualizar sobre el bien jurídico, en estos delitos acudiremos a la doctora Mayer quien en su artículo sobre este tema (Lux, 2017), hace la siguiente aclaración sobre la

utilización del término delitos informáticos. Al respecto, señala que este término ha sido utilizado en dos sentidos, uno amplio el cual serían los delitos tradicionales cometidos por medio de un computador o el internet y uno estricto, que delimitaría solo los delitos cometidos en contra de sistemas informáticos.

Así mismo, realiza una aclaración entre el software y hardware, el primero lo define como el sistema lógico, por medio del cual la maquina puede realizar tareas específicas, el componente físico que ejecuta las ordenes que le envía el software. En este contexto se indica que no toda conducta delictiva que recae sobre un sistema informático constituye un delito informático. Estrictamente, el delito recae sobre el software o soporte lógico, cuando la acción recae sobre el hardware pueden ser subsumidas por los delitos clásicos, como el daño.

CAPITULO 3. LA OBTENCION DE PRUEBA PENAL INTERNACIONAL, EN LOS DELITOS INFORMATICOS.

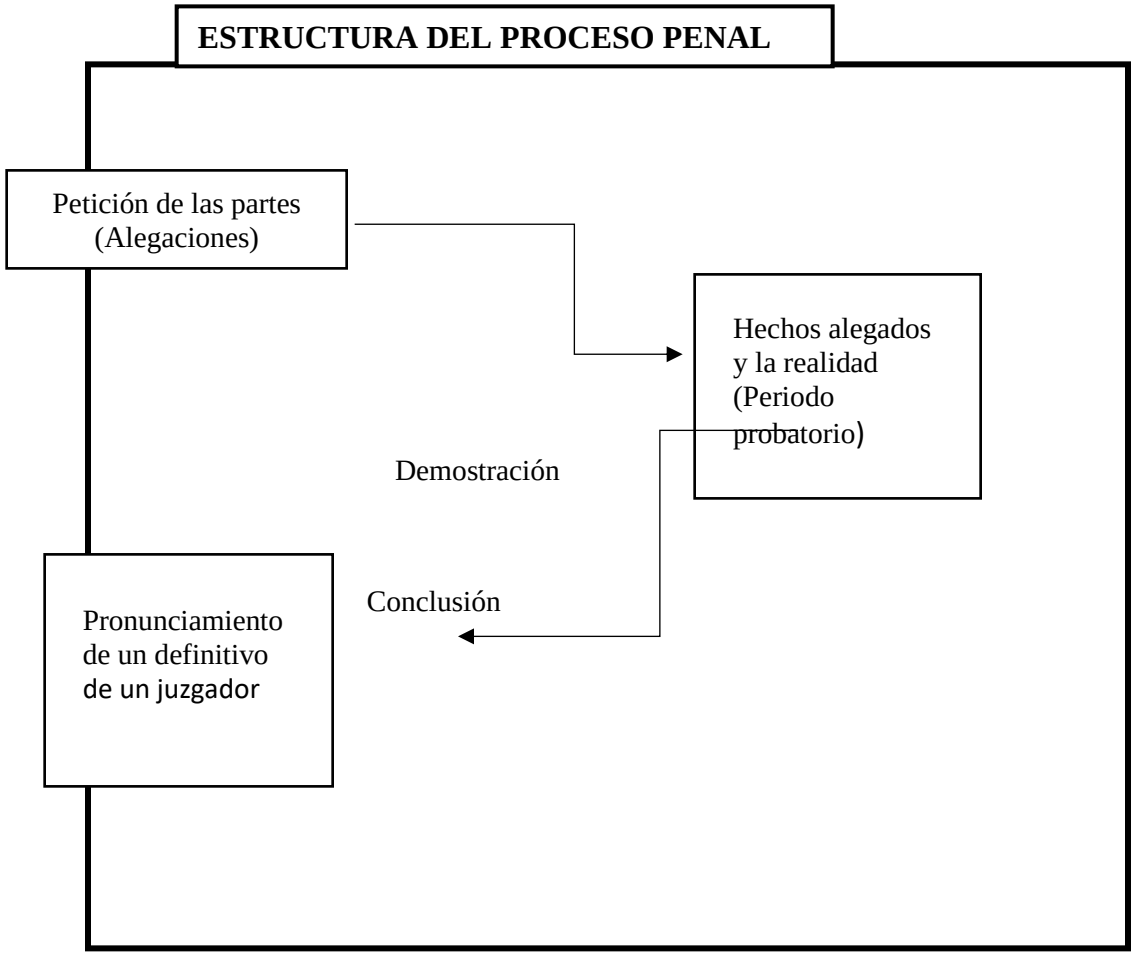
En el marco normativo de la legislación colombiana los derechos, garantías y deberes al que son sujetos todos los ciudadanos en ejercicio de los mismos están enmarcados en el Titulo II de la carta magna, es allí donde nace el desarrollo del derecho fundamental base del proceso penal en Colombia, el debido proceso.

Tal como se desarrolla en el artículo 29 (Constitucion politica de la Republica de Colombia, 1991), toda persona se presume inocente hasta que no sea vencido en Juicio, proceso en el cual tiene derecho a la defensa y asistencia de un abogado, a un debido proceso sin ningún tipo de dilaciones, a presentar o controvertir pruebas presentadas en su defensa o en su contra, a poder controvertir la decisión o sentencia y sobre todo a no ser juzgado 2 veces por el mismo hecho punible.

Es así como desde la constitución política se vislumbra como columna vertebral del derecho fundamental al debido proceso, el derecho de las partes procesales de aportar o controvertir pruebas judiciales, derecho que es insustituible para cada una de las partes principalmente en función del principio de igualdad de oportunidades. (Rodriguez Choconta, 2014), aunque adicionalmente este derecho no puede ser ejercido de manera arbitraria y con desconocimiento del ordenamiento jurídico ya que siempre debe atender el límite de la generalidad del debido proceso en sí (p. 62).

El Sistema Penal Acusatorio por el cual se rige el país desde la implementación de la ley 906 de 2004, se caracteriza por el enfrentamiento de dos partes, los cuales se someten a la decisión de un tercero.

El desarrollo del proceso judicial se presenta de la siguiente forma:



En contexto anterior, la prueba es el mecanismo por medio del cual se busca que el juez se convenza de los hechos que aportan cada una de la partes, esto es percibido desde dos frentes, la parte acusadora y la defensa.

Lo anterior se encuentra ampliamente legislado tanto en el ámbito internacional en el Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea de las Naciones Unidas en el año de 1966, el cual establece el derecho que tiene cualquier persona a ser escuchada, con las debidas garantías por parte de un tribunal, esas garantías conciben proponer y practicar pruebas a su favor.

Por su parte, la Convención Americana de Derechos Humanos de 1969, en el artículo 8 se refiere a las garantías judiciales con las que cuenta todo ser humano, y en el primer parágrafo señala que toda persona tiene derecho a ser oída por un juez o tribunal competente, dentro de un proceso penal, en igualdad de condiciones esto es lo que se conoce como el derecho general de defensa o igualdad de armas.

En nuestra legislación interna los derechos, garantías y deberes a los cuales se encuentran sujetos los ciudadanos del país, se enmarcan en el Titulo II de la constitución, es allí donde se establecen las bases del proceso penal en Colombia y del debido proceso.

El artículo 29 de la carta política establece el debido proceso, el cual se aplicará en todas las actuaciones jurídicas y administrativas, así mismo invoca la presunción de inocencia, la cual establece que toda persona se presume inocente hasta que no sea vencido en juicio, proceso en el cual tiene derecho a la defensa y asistencia de un abogado, a un debido proceso sin ningún tipo de

dilaciones, a presentar o controvertir pruebas presentadas en su defensa o en su contra, a poder controvertir la decisión o sentencia y sobre todo a no ser juzgado dos veces por el mismo hecho punible.

3.1 Definición de prueba

A través de la academia se ha buscado desarrollar este concepto, por lo anterior es importante hacer mención algunas de estas definiciones. Etimológicamente la prueba se precisa como todo aquello que busca mostrar la certeza de cualquier verdad o falsedad (Martinez Garnelo, 2010) (p. 1). Por su parte, en un sentido amplio se relaciona con los elementos que buscan confirmar o desvirtuar una hipótesis. En el campo penal, busca ser un mecanismo por medio del cual, se descubre la verdad de los hechos objeto de investigación (Arocena, Balcarce y Cesano, 2009) (p. 3).

Otro autor, delimita a la prueba como las razones, instrumentos, escritos, etc. que son llevados a una audiencia, con el propósito de que el Juez designado para el caso pueda obtener certeza de los hechos en disputa, (Varga Vargas, 2005) (p.3). Para Giacomette la prueba puede puntualizarse como la demostración de las aseveraciones presentes que tienen relación con hechos ya sucedidos. (Giacomette Ferrer, 2015) (p. 64).

En el sistema penal acusatorio, la prueba es el objeto material probatorio sometido a divulgación y refutación en el proceso penal (USAID, 2014). En este contexto, es importante señalar que existen una serie de cimientos rectores los cuales garantizan que todos los intervinientes en un proceso

penal, tengan las mismas garantías y oportunidades, las cuales son fundamentales en un Estado social de derecho.

3.2 Fin de la prueba

Teniendo ya claro el concepto general de prueba y su acercamiento al ejercicio del Derecho, es necesario establecer y delimitar el fin de la prueba judicial enfocándonos en el desarrollo de la generalidad de la práctica del derecho y su acercamiento y profundización en el área penal.

En el derecho procesal el fin fundamental de la prueba es la producción de conocimiento que sustenten los hechos y la verdad procesal correspondiente a los mismos, adicionalmente no se puede dejar de lado que este fin se ver complementado por lograr el convencimiento del juez sobre la existencia de los hechos y la implicación jurídica de los mismos con el objetivo de lograr una motivación de la decisión (Ramirez Carvajal, 2013) (p. 61)

Aunque profundizando un poco más y delimitando la función de la prueba en el proceso penal se puede establecer que el fin de la prueba es soportar la reconstrucción de los hechos históricos que están siendo sometidos a decisión del juez y los cuales deben estar relacionados con el cometimiento de un tipo penal (Arocena, Balcarce, Cesano, 2009) (p. 3)

Logrando ya un entendimiento general del concepto de prueba y su fin en el macro contexto del derecho procesal y penal, podemos desarrollar su aplicación, alcance y limitaciones dentro del contexto de los delitos informáticos, tema objeto de investigación en este escrito.

3.3 Diferencias entre de los medios de prueba, la prueba y la fuente de prueba

Antes de avanzar en todo lo relacionado con el análisis de la prueba en el proceso penal, es necesario realizar una aclaración frente a estos tres términos con el fin de comprender mejor el tema de investigación.

- *Fuente de prueba:* existen antes del proceso, son independiente, solo las partes las conocen.
- *Medios de prueba:* surgen del proceso, medio de valoración actuaciones judiciales.
- *Prueba:* Resultado de las actuaciones judiciales que buscan obtener una convicción de un hecho.

3.4 Principios de la prueba

- *Principio de presunción de inocencia:* Garantía al debido proceso, la cual se encuentra estipulada en la Constitución de Colombia, en el artículo 29 señalando "Toda persona se presume inocente hasta que se demuestre lo contrario". Por su parte la (Corte, Constitucional de Colombia, 2012), en sentencia C-289/12, determina que dicha garantía cobija a la persona investigada en un proceso penal, hasta el momento en que un Juez dicte un fallo, por tal motivo, quien asume completamente la carga de la prueba, es al ente acusador .

- *El derecho a guardar silencio y no auto incriminarse:* El no auto incriminarse es un derecho que está determinado en el artículo VIII, parágrafo g, de la Convención Interamericana de Derechos Humanos, y en el artículo 33 de la Constitución Colombiana, indica que nadie tiene la obligación a declarar contra el mismo o sus allegados de su círculo familiar, ni declararse culpable. Así mismo señala que tiene el procesado tiene derecho a guardar silencio, sin que eso traiga consecuencias negativas para la persona.

- *Principio de legalidad:* La Corte Constitucional en la sentencia C-710/01 (Triviño, 2001), señala que el citado principio es la columna vertebral del ejercicio del poder y del derecho sancionador, en la medida en que las facultades, funciones y actos que ejecutan los funcionarios públicos todos están contemplados en la ley, lo que se deduce que su actuar siempre este sujeto bajo esos lineamientos prestablecidos.

- *Principio de libertad probatoria:* Señala que la prueba puede realizar de acuerdo con lo establecido en la ley. Así mismo permite que se utilice cualquier medio técnico o científico para conseguirla siempre y cuando esto no se vulnere los derechos humanos (USAID, 2014).

- *Principio de Contradicción:* En la sentencia C-371/11 (Corte Constitucional de Colombia, 2011), una de las garantías del debido proceso es la del derecho de contradicción y controversia probatoria, en donde intervinientes y sujetos procesales controvierten en igualdad de condiciones, sin embargo estos no son derechos absolutos, si no que por el

contrario puede verse limitado por el legislador, siempre y cuando estos se acojan a criterios como el de razonabilidad y proporcionalidad.

- *Principio de Inmediación:* Se define como la interacción que tiene el juez, con las partes que participan en el proceso penal. Este principio establece que para que una prueba sea tomada en cuenta dentro del proceso, debe reunir dos requisitos; por un lado ser incorporada de manera pública, oral y concentrada y sujeta a contradicción. La Corte Suprema de Justicia en la Sentencia T-205/11 (Pinilla, 2011), argumenta que la inmediación de la prueba, en el sistema penal acusatorio, permite que el juez obtenga de manera directa acceso a la prueba.

- *Principio de Concentración:* La actividad procesal denota que tanto la práctica probatoria como el debate argumentativo se realice en una misma audiencia de ser posible en un mismo día. El artículo 454 del código de procedimiento penal, señala que la audiencia de juicio oral deberá ser continua salvo que se presenten hechos graves que impidan avanzar en la misma. Lo anterior con el fin de que el juez tenga una visión global del proceso y no fraccionada.

- *Doble instancia:* Es un principio de rango constitucional ya que se encuentra consagrado en el artículo 31, que determina que cualquier sentencia puede ser apelada, lo que se traduce en una garantía dentro del proceso ya que con esto se tiene una nueva oportunidad para la defensa contra posibles errores o arbitrariedades. Tanto la a Convención Americana sobre

Derechos Humanos como el Pacto Internacional de Derechos Civiles y Políticos, establecen que la doble instancia garantiza el debido proceso.

3.5 Medios de prueba en el Sistema Penal Acusatorio

Los medios de prueba, como señalamos anteriormente se definen como los mecanismos por medio de los cuales se busca constatar, los hechos objeto de investigación. Dentro de este contexto tenemos tres grandes grupos que son; la prueba testimonial, documental, referencial y pericial.

- *Prueba Testimonial*: Esta definida como la narración que realiza un tercero ante un juez, sobre los hechos que directa o indirectamente se relacionan con el delito investigado (RAVE, 2006). El artículo 404 del Código de Procedimiento Penal consagra los juicios de apreciación del testimonio entre los que están los conocimientos científico- técnico, los procesos de el tercero en recordad, el comportamiento del testigo durante el interrogatorio, entre otras cosas.

- *Prueba Documental*: Son todos aquellos instrumentos en diferentes formatos que son presentados ante un juez, con el propósito de apoyar los hechos objeto de investigación, estos constan de un amplio abanico entre los que encontramos; los textos (manuscritos, impresos, mecanografiados), grabaciones magnetofónicas, mensajes de datos, ecografías, electro gramas entre otros.

- *Prueba referencial*: Toda declaración realizada fuera del juicio oral la cual persiga probar o excluir elementos del delito, grado de intervención, circunstancias de atenuación entre se considera como prueba de referencia.

- *Prueba Pericial*: Cuando en un proceso es necesario realizar la valoración de una persona que tenga conocimientos científicos, técnicos, artísticos o especializados, se procede a realizar una prueba pericial.

Sin embargo, tal y como explicamos anteriormente en la era de la tecnología existen una serie de datos que quedan registrados en algún medio tecnológico ya sea un computador, celular, ipad, o cualquier dispositivo electrónico, los cuales en determinado momento se convierten en medio de prueba, cuando estos dispositivos electrónicos, son utilizados como medio o fin, en la comisión de un delito (delitos informáticos). Esos elementos de prueba, han planteado un nuevo paradigma para la justicia, ya que existen muchos vacíos en la legislación actual, debido a que la regulación de su obtención, conservación y presentación es muy escasa.

Aunado a esto, la mayoría de estos datos están almacenados en servidores ubicados en diferentes partes del mundo, en empresas privadas que se rigen por la legislación interna de cada país y que para poder tener acceso a ellos, es necesario que los operadores de justicia acudan a los mecanismos de cooperación jurídica internacional.

El anterior contexto abre una nueva puerta a lo que se denomina la prueba electrónica en el proceso penal, la cual se define como:

- *Prueba electrónica penal*: Cualquier clase de información que tenga un valor probatorio, ya sea porque fue trasmitido, producido, almacenado o contenido en un medio electrónico, y que este pueda ayudan a acreditar un hecho dentro de un proceso penal (Borges, 30 de junio de 2017).

  Lo más importante de este tipo de pruebas es que aunque son físicas, poseen un carácter de intangibilidad debido al lugar donde se producen y se conservan que es la red.

Este tipo de prueba se allega al proceso de las cuatro formas que ya explicamos anteriormente, es decir, de forma pericial, referencia, documental o testimonial.

3.6 Características de la prueba electrónica penal

Las pruebas electrónicas, poseen una serie de características que son importantes de analizar, con el fin de tener un mejor contexto sobre el tema.

- *Parciales:* En algunas de las circustancias, los medios electrónicos que contienen evidencias, se encuentran en poder de las personas que quieren presentarlas como pruebas (Perez, 2016).

- *Destruibles:* Una prueba electrónica se puede destruir con un solo clic y para poderla recuperar se debe contar con la ayuda de un perito calificado.

- *Transgresivas:* La obtención de material probatorio electrónico puede trasgredir derechos y libertades fundamentales como el de la libertad, intimidad protección de datos etc.

- *Intangibles:* Por el solo hecho de estar en el ciberespacio, tienen esta característica, recordando que el mismo se encuentre en números binarios.

3.7 Acceso a la prueba electrónica.

Como resultado de este estudio se logro analizar la forma como se accede a la prueba electrónica internacional. Para esto, hay que tener en cuenta el lugar donde se aloja, es decir, ya sea contenida en aparatos informáticos, como los es un celular, tableta, computador, etc. O almacenado en un servidor de alguna de las empresas que prestan servicios de mensajería o redes sociales, tales como Yahoo, Hotmail, WhatsApp, Twiter, Facebook, entre otros, dichos equipos informáticos se ubican en diferentes partes de mundo, en su gran mayoría en los Estados Unidos de América.

Para el primer caso, la prueba se puede obtener una vez realizada la incautación del elemento electrónico por parte de la autoridad competente, cumpliendo con los requerimientos de ley. O que una de las partes lo allegue voluntariamente.

En el segundo caso, se debe acceder al mecanismo de cooperación jurídica internacional, el cual es el tema que se abordará en nuestro último capítulo.

3.8 Normativa penal de la prueba electrónica.

Actualmente no existe una regulación específica frente al tema, porque tal como lo señalamos en el primer capítulo, la tecnología y por ende los delitos cibernéticos avanzan más rápido de lo que puede hacerlo el derecho penal.

Ante este hecho, se utilizan normas que contienen material análogo, y el cual se esboza continuación:

- Decreto 2150 de 1995: El propósito de esta ley fue lograr la utilización de sistemas electrónicos de archivo y trasmisión entre entidades de administración pública, para que los usuarios reciban y envíen información dentro de su trabajo.

- *Ley 527 de 1999* ((Ley 527, 1999): Se define y reglamenta el mensaje de datos, comercio electrónico, firma digital, firma digital, intercambio electrónico, sistemas de información, uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y otras disposiciones. Su objetivo es crear un marco normativo para que entre otras cosas se le dé valor jurídico a los mensajes electrónicos.

    - ✓ Para que un documento electrónico pueda tener una equivalencia frente a un documento tradicional, debe cumplir con los requisitos de ley que le otorgan validez jurídica y probatoria. Estos son: “La confiabilidad de la forma como se

generó archivo, como se comunicó el mensaje y la manera como se conservó la integridad de la información.

CAPITULO 4. COOPERACION JURIDICA INTERNACIONAL.

4.1 Cooperación Jurídica Internacional.

La cooperación jurídica internacional, es la asistencia que los Estados se prestan entre sí en materia judicial, siguiendo los principios rectores de las relaciones internacionales como son reciprocidad, cooperación, equidad, respeto, igualdad y autodeterminación de los pueblos.

Lo anterior, se materializa a través de la firma de acuerdos bilaterales y multilaterales, los cuales tienen como propósito actuar conjuntamente frente a un tema, creando acciones de control y represión con el ánimo de enfrentar las formas de actividad delictiva trasnacional, ya que a través de la experiencia se ha reconocido que este es un mecanismo efectivo y eficaz de lucha contra los delitos (Klor, 2010).

4.2 Marco Jurídico

La ley 600 del año 2000 establece en su artículo 500 que el Fiscal General de la Nación, puede celebrar con homólogos de otros países, intercambio de tecnología, experiencias, entregas vigiladas, controladas, agentes encubiertos, cooperación judicial etc.

Por su parte la ley 906 de 2004, indica en su artículo 484 y 485, la forma como las autoridades competentes, podrán solicitar y realizar intercambio de información en procesos judiciales, siempre y cuando cumplan con los requerimientos previstos para realizar el mismo.

De igual forma se fundamenta en la Constitución Colombiana, los Tratados Multilaterales y Bilaterales, Costumbre Internacional, Principios de Derecho Internacional aceptado por Colombia, Memorandos de entendimiento.

4.3 Objetivo

El objetivo de la cooperación jurídica internacional es proporcionar ayuda entre las autoridades homólogas competentes con el fin de obtener elementos materiales probatorios, evidencia física o pruebas dentro de un proceso (Ministerio de Relaciones Exteriores, 2018).

4.4 Estructura

En cada convenio los Estados partes fijan una autoridad central que puede ser el Ministerio Público o la Fiscalía, y a su vez en cada una de estas Entidades existe un punto de contacto directo que suele ser la oficina de asuntos internacionales que es el ente encargado de recibir, analizar, direccionar y devolver las asistencias de cooperación internacional.

4.5 Instrumentos

Los instrumentos de cooperación jurídica internacional se encuentran establecidos en el Manual de Cooperación Jurídica Internacional, expedido por el Ministerio de Relaciones Exteriores y la Fiscalía General de la Nación, indican que en la práctica judicial se utiliza la Carta Rogatoria o Asistencia judicial, el exhorto o la nota suplicatoria.

Lo anterior, se explica en el siguiente gráfico que indica la autoridad a quien debe ir dirigirla la petición, cuál debe ser el contenido, que parámetros debe cumplir y los requisitos de ley.

4.6 La obtención de la prueba internacional y los delitos cibernéticos.

Según lo señalado anteriormente en el contexto de la cooperación jurídica internacional, existe un procedimiento especial para la obtención de la prueba internacional relacionada con delitos cibernéticos, lo anterior se ha ido ajustando en la práctica teniendo en cuenta que la mayoría de solicitudes que salen de la Fiscalía General de la Nación, se direccionan hacia a las autoridades homólogas en los Estados Unidos de América, debido a que allí se encuentran los principales servidores de las empresas Yahoo, Hotmail, Facebook, Instagram entre otros.

Para entender mejor este proceso se ilustrara el siguiente caso: El Fiscal X recibe una denuncia interpuesta por la señora Y, en contra de personas indeterminadas manifestado que según información obtenida en internet y la red social de Facebook, se evidencian perfiles falsos y grupos de personas que usurpan la identidad, imagen, marca y símbolos que identifican legítimamente a la entidad a la cual representa la señora Y, dichos elementos son utilizados con el fin de calumniar e injuriar a personas pertenecientes a la citada empresas, distorsionando la información destinada al público en general. Estos hechos se vienen estructurando de manera sistemática desde el año 2014.

Ante estos hechos, el fiscal de conocimiento tipifica los delitos de relacionados con hostigamiento por raza, religión, ideología, política u origen nacional, étnico o cultural y calumnia e injuria y activa los mecanismos de cooperación judicial requiriendo a las autoridades homólogas en los Estados Unidos, que suministre información que permita establecer la identidad de las personas administradoras de los grupos de Facebook, identificando la IP desde donde fueron creadas, así como el historial de las IP mediante las cuales se accedió al perfil de administrador para el periodo

de tiempo 2013-2015. Así mismo, requiere eliminar o bloquear a los grupos y usuarios anteriormente descritos

Para estos casos, lo procedente es que el fiscal de conocimiento eleve una carta rogatoria dirigida a las autoridades homologas en los Estados Unidos, la cual se canaliza a través de la Dirección de Asuntos Internacionales de la Fiscalía General de la Nación, la cual debe además de cumplir con los lineamientos anteriormente señalados, es indispensable que solicite al Proveedor de Servicios de Internet (ISP), la preservación de los datos de la cuenta desde la cual se están enviando las amenazas, para ser analizados posteriormente en la investigación. Así mismo, deberá solicitar al Proveedor de Servicios de Internet, los datos registrados en la cuenta a analizar y la ubicación de la misma.

4.7 Dificultades en la consecución de la prueba internacional en materia de delitos cibernéticos.

En este aparte, señalaremos algunos de los obstáculos a los que que se enfrenta en la obtencion de la prueba internacional en materia de delitos cibernéticos, estos son:

- Que no exista convenio aplicable con el país del cual se requiera obtener la información. Por ejemplo, que en una investigación se haya evidenciado que los servidores se encuentran ubicados en Nigeria.

- Que los delitos con los cuales se fundamenta la solicitud de asistencia judicial, no sean castigados por la legislación del país receptor. Por ejemplo, en el caso que describimos anteriormente, el Fiscal de conocimiento fundamentó la petición a los Estados Unidos, bajo la comisión de los delitos de injuria y calumnia. Y en este país la Primera Enmienda de la Constitución, ofrece una sólida protección impidiendo la judicialización penal basada en la libertad de opinión y expresión.

- El tiempo de respuesta de una asistencia judicial por los canales de cooperación judicial oscila entre los 6 y 10 meses, lo cual genera que el operador de justicia no tenga la información en el momento oportuno.

4.8 Cooperación Internacional frente a los delitos cibernéticos

Como ya lo hemos señalado anteriormente el continuo crecimiento de los delitos informáticos, con sus principales características de tecnificación y tras nacionalidad, ha generado que los Estados es su afán por luchar en este flagelo, se unan en busca de nuevas formas de combatirlo, desde todos los frentes posibles.

Este esfuerzo generó que en el año de 2004 entrara en vigor el Convenio de Budapest que se conoce también como el Convenio sobre la Ciberdelincuencia.

- **Convenio de Budapest**

Fue elaborado por el Consejo de Europa en la ciudad de Estrasburgo, en el cual participaron como invitados países como Filipinas, Costa Rica, Chile, Japón, Estados Unidos, Canadá, en calidad de observadores.

- ✓ El objetivo del presente convenio es aplicar una política penal, la cual busca proteger a la comunidad internacional de los delitos cibernéticos, por medio de la conjunción de las leyes de los Estados Partes, la optimización de las técnicas de investigación, y el aumento en la cooperación entre los países firmantes.

- ✓ Lo anterior, se materializa por medio de medidas consensuadas por los países intervinientes, las cuales cada Estado que desee adherirse debe adoptar a nivel nacional.

- ✓ En este contexto el primer eje del citado convenio indica que en el derecho penal sustantivo de cada país parte, se deben crear los siguientes delitos:

    - La tecnología como un fin, entre estos se encuentran los que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; Acceso ilícito, Interceptación ilícita, Ataques a la integridad de datos, de los sistemas, abuso de los dispositivos.

- La tecnología como medio; Fraude informático, falsificación informática.

- De contenido: Pornografía infantil.

- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

- ✓ El segundo eje, indica las normas procesales que deben ser adoptadas por los países parte, señalando entre otros aspectos la conservación de los datos almacenados, por medio de la creación de medidas legislativas necesarias para conservar rápidamente los datos, cuando se piense que estos pueden ser susceptibles de pérdida o modificación.

- ✓ Así mismo indica que se debe facultar a las autoridades competentes a ordenar a personas y proveedores tanto de telefonía como de datos informáticos que presten el servicio en su territorio que comunique datos que ejecuten en su poder o bajo su control relativo a los usuarios.

- ✓ Finalmente el tercer eje se concentra en las normas de cooperación internacional tendientes a investigar, localizar, recolectar material probatorio y sospechosos de cometer delitos cibernéticos.

Resumiendo el presente convenio es hasta la fecha el mas importante esfuerzo de la comunidad internacional, en la lucha contra los delitos cibernéticos, a través de la conjunción del derecho

penal, la búsqueda del establecimiento de medidas procesales y cautelares y el lineamiento de una cooperación internacional más efectiva.

5. Conclusión

Colombia en junio de la presente anualidad, aprobó la ley 1928 de 2018 que señala la adhesión del Estado Colombiano al Convenio de Budapest, se une a los 56 países que han firmado la principal herramienta a nivel mundial, con la cual cuentan los países para combatir los delitos informáticos y todas sus implicaciones.

Este paso es indudablemente beneficioso para el tema que desarrollamos en la presente monografía, ya que como explicamos anteriormente, el tercer eje de este convenio se centra en establecer normas que entre otras cosas, coadyuven a localizar y recolectar material probatorio.

Lo anterior, es un tema de la mayor relevancia en el ámbito jurídico nacional, teniendo en cuenta que los delitos cibernéticos son un flagelo que en el país crece exponencialmente, tal y como lo señalan las cifras que reporta la Policía Nacional y la Fiscalía General, las cuales indican un incremento del 28.30 por ciento, frente al año anterior, tal como figura en el reporte del Centro Cibernético Policial.

Por lo tanto, en este contexto se hace más necesario implantar medidas que ayuden en todo el proceso de judicialización con el fin de que estos delitos no queden en la impunidad.

Bibliografía

(s.f.).

Altamira, F. A. (2010). *Teoría del Delito (Manual Práctico para su aplicación en la Teoría dle caso).* Peru: Editorial Nomos & Thesis E.I.R.L.

Arocena, Balcarce y Cesano. (2009). *Prueba en materia Penal.* (E. A. Depalma, Ed.) Buenos Aires, Buenos Aires, Argentina: Editorial Astrea.

Arocena, Balcarce, Cesano. (2009). *Prueba en materia penal.* (E. Astrea, Ed.) Buenos Aires, Argentina: Editorial Astrea.

Barceló, r. o. (2016). *La prueba electrónica , validez y eficacia procesal.* juristas con futuro E Book. Obtenido de https://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf

Bedoya Sierra, L. F. (2008). *La prueba en el proceso penal Colombiano* (Primera ed.). Bogota D.C., Bogota D.C., Colombia: Republica de Colombia, Fiscalia General de la Nacion.

Borges, R. (30 de junio de 2017). *La Prueba Electrónica en el Proceso Penal y el Valor Probatorio de Conversaciones Mantenidas Utilizando la Menjaseria Instantaneas* . españa: Rev. Boliv. de Derecho Nº 25.

Callegari, N. (julio -septiembre de 1985). delitos informaticos. *revista de la faculatd de derecho y ciencias policticas de la UPB*(70).

Castells, M. (1996). *La era de la información.* México: Economía, sociedad y cultura.

Consejo Europeo. (2001). *CONVENIO SOBRE LA CIBERDELINCUENCIA.* Bruselas, Bélgica: Consejo Europeo. Obtenido de https://rm.coe.int/16802fa403

Constitucion politica de la Republica de Colombia. (1991).

Corte Constitucional de Colombia. (2011). *Sentencia C-371/11*. bogota. Obtenido de Sentencia C-371/11

Corte, Constitucional de Colombia. (2012). Sentencia C-289/12. colombia. Obtenido de http://www.corteconstitucional.gov.co/relatoria/2012/C-289-12.htm

Diario Oficial No. 44.509 de 4 de Agosto. (2001). Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. *LEY 679*. Obtenido de https://www.icbf.gov.co/cargues/avance/docs/ley_0679_2001.htm

Díaz, N. J. (diciembre de 2009). El delito de daños informatico: Una tipificación defectuosa. (S. d. Compostel, Ed.) *Estudios penales y criminalisticos volumen XXIX*, 311-362. Obtenido de http://hdl.handle.net/10347/4149

El Consejo Privado de Competitividad. (2017). *Justicia, Informe nacional de competitividad.* bogota. Obtenido de https://compite.com.co/informe/informe-nacional-de-competitividad-2017-2018/justicia/#cpc_breadcrumb

Foro Económico Mundial. (2017). *Informe de riesgos Mundiales 2017.* Foro Economico Mundial, Cologny/Ginebra. Obtenido de http://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/jan/Global-Risk-Report-2017_ES.pdf

Giacomette Ferrer, A. (2015). *Teoria General de la prueba.* (E. Temis, Ed.) Bogota D.C., Bogota D.C., Colombia: Editorial Temis.

Gonzalez Navarro, A. L. (2011). *La prueba en el sistema penal acusatorio.* (L. Editores, Ed.) Bogota D.C., Bogota D.C., Colombia: Leyes Editores.

Grupo de Estudios en internet, comercio electronico, telecomunicaciones e informatica. (2011). *Derecho & TIC 10.0.* (E. T. S.A., Ed.) Bogota D.C., Cundinamarca, Colombia: Editorial Temis S.A.

julio. (s.f.).

Klor, A. D. (2010). La cooperacion juridica internacional: Instrumento imprescindible para la integración. *Instituto de Investigaciones Jurídicas de la UNAM* , 264.

Ley 527. (1999). Bogota: Diario oficial No. 43.673 del 21 de agosto de 1999. Obtenido de https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

Lima Malvido, M. d. (Mayo de 1981). Los delitos electronicos. *Revista Señal*.

Lopez Polando, H. A. (2004). *El documentos electronico como titulo valor* (1ª Edicion ed.). Popayan, Cauca, Colombia: Felipe Garcia Quintero.

Lux, L. M. (Abril de 2017). El bien juridico protegido en los delitos informaticos. *Revista chilena de derecho. vol.44 no.1*. Obtenido de http://dx.doi.org/10.4067/S0718-34372017000100011

Martinez Garnelo, J. (2010). *La prueba iniciaria presuncional o circustancial en el nuevo sistema penal acusatorio.* Mexico D.F., Mexico D.F., Mexico: Editorial Porrua.

Ministerio de Relaciones Exteriores. (17 de octubre de 2018). *Cancilleria*. Obtenido de http://www.cancilleria.gov.co/tramites_servicios/cooperacion_judicial

Miniwats Marketing Group. (2017). *http://www.internetworldstats.com/stats.htm*.

Perez, J. E. (2016). *la prueba electrónica.* cataluña: universidad de cataluña. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf

Pinilla, N. P. (2011). T-2830810. bogota: Corte Suprema de Justicia, Sala de Casación Penal. Obtenido de http://www.corteconstitucional.gov.co/relatoria/2011/T-205-11.htm

Policia Nacional de la Republica de Colombia. (2017). *Balance Cibercrimen en Colombia 2017.* Policia Nacional de la Republica de Colombia, Direccion de Investigacion Criminal e Interpol. Bogotá: Centro cibernetico Policial. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Portafolio. (27 de Septiembre de 2017). *Colombia registró 198 millones de ataques cibernéticos en el 2017*. Recuperado el 16 de Junio de 2018, de http://www.portafolio.co/tendencias/colombia-es-uno-de-los-paises-mas-afectados-por-ataques-ciberneticos-510128

Ramirez Carvajal, D. M. (2013). *La prueba en el proceso, una aventura intelectual.* (L. J. Ltda, Ed.) Medellin, Antioquia, Colombia: Libreria Juridica Sanchez R. Ltda.

RAVE, G. M. (2006). *PROCEDIMIENTO PENAL.* bogota: EDITORIAL TEMIS S. A. Obtenido de http://www.editorialtemis.com/Temis/Contenidos/10-000-0028.pdf

Revista Dinero. (5 de 4 de 2018). Así está Colombia conectada a Internet. *Revista Dinero*. Obtenido de https://www.dinero.com/pais/articulo/conectividad-de-colombia-a-internet-en-abril-de-2018/258047

Rodriguez Choconta, O. A. (2014). *Prueba ilicita penal derechos y garantias constitucionales* (Segunda ed.). (E. d. S.A., Ed.) Bogota D.C., Bogota D.C., Colombia: Ediciones doctrina y ley S.A.

Sarzana, C. (1979). *Criminalitá e tecnologia: Il caso dei computer-crimes.* Roma.

Schwab, K. (2017-2018). *The Global Competitiveness Report.* World Economic Forum. Geneva, Switzeland: World Economic Forum. Obtenido de file:///C:/Users/monsaenz/Desktop/TheGlobalCompetitivenessReport2017%E2%80%932018.pdf

SEMANA. (2017). El cibercrimen en 2017: la amenaza crece sobre Colombia. *SEMANA*. Obtenido de https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979

Terreros, F. V. (2014). Cybercrimen. *ius et veritas*, 208-304.

Torres, A. (2018). Se disparan estadísticas de delitos en Colombia. *CMI Noticias*. Obtenido de https://canal1.com.co/noticias/se-disparan-estadisticas-de-delitos-en-colombia/

Triviño, J. C. (2001). *C-710/01*. bogota: Corte Constitucional de Colombia. Obtenido de http://www.corteconstitucional.gov.co/relatoria/2001/c-710-01.htm

Unidas, N. (2010). *12° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.* Salvador (Brasil). Obtenido de https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf

USAID, D. D. (2014). *La prueba en el sistema penal.* bogota: Defensoria del Pueblo. Obtenido de https://litigacionoral.com/wp-content/uploads/2017/03/Modulo-de-Pruebas.pdf

Valdes, J. T. (2003). *Derecho Informatico.* Mexico: Mc-Graw Hill.

Valdéz, J. T. (2006). *Derecho Informaático.* mexico : Mc Gray Hill.

Varga Vargas, P. P. (2005). *Las pruebas en el sistema Penal Acusatorio Colombiano.* (E. D. S.A., Ed.) Bogota D.C., Bogota D.C., Colombia: Ediciones Doctrina y Ley S.A.