EL TERRORISMO CIBERNÉTICO COMO ACTO QUE CRIMINALIZA LA LIBERTAD DE EXPRESIÓN: UNA MIRADA DESDE LA GEOINFORMATICA

LA LIBERTAD DE EXPRESIÓN AFECTADA CON EL CIBERTERRORISMO.

ROXANA ECHEVERRIA GOMEZ

UNIVERSIDAD CES
FACULTAD DE DERECHO
Medellín
2017

GLOSARIO

Amenaza Informática: La aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. Tal como lo informa el **CONPES 3854** sobre **Política Nacional de Seguridad Digital** de abril del 2016. (Departamento Nacional de Planeación & Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

Ciber: Del ingl. *cyber-,* acort. de *cybernetic* 'cibernético'.

1. elem. Compos. Indica relación con redes informáticas. *Ciberespacio, cibernauta.* Real Academia Española. (2014) Ciber. En Diccionario de la lengua española (23ª ed.)

Ciberespacio: Del ingl. *cyberspace,* de *cyber-* 'ciber-' y *space* 'espacio'.

1. m. Ámbito artificial creado por medios informáticos. Real Academia Española (2014). Ciberespacio, En Diccionario de la lengua española (23ª ed.)

Cibergeografía:

Puede definirse como un sub-campo de investigación de la geografía, en el que el énfasis está centrado en las implicaciones sociales y espaciales asociadas a la irrupción de las tecnologías digitales de la información y la comunicación. La relación entre técnica y territorio siempre ha sido estrecha, y por ello es relevante escudriñar en torno las múltiples implicaciones de la actual revolución tecnológica, originada desde mediados del siglo XX y basada en una nueva unidad de medida: El BIT. Puesto que la comunicación es la base de las formas de organización territorial, la mediación digital se constituye en un factor central transversal para comprender el mundo de hoy y sus tendencias. El medio digital está en proceso de instalación. ("Línea de investigación Geografía, Universidad Nacional.", 2017)

Internauta/cibernauta: m. y f. Persona que navega por el ciberespacio. Real Academia Española. (2014) Cibernauta. En Diccionario de la lengua española (23ª ed.)

Incidente Informático: Evento único o serie de eventos de seguridad de la informática inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de una entidad y amenazar la seguridad de la información. (Ministerio de Hacienda, 2016)

Terrorismo:

1. m. Dominación por el terror.

2. m. Sucesión de actos de violencia ejecutados para infundirterror.

3. m. Actuación criminal de bandas organizadas, que,reiteradamente y por lo común de modo indiscriminado,pretende crear alarma social con fines políticos. Real Academia Española. (2014) Terrorismo. En Diccionario de la lengua española (23ª ed.)

INTRODUCCION

La comunicación surgió desde los comienzos de la humanidad, como medio para transmitir las emociones, sentimientos, además de ser una forma de supervivencia, como lo son las señales de humo, los destellos con los espejos.

En el año 5000 antes de Cristo se inventa la ñescrituraò, antes de este año la comunicación era por signos gráficos que representaban alguna cosa, es desde este momento donde surge la necesidad del hombre de compartir información (FERRUCCIO ROSSI-LANDI & WILLIAMS, 1992)

Con la necesidad de compartir la información y que la comunicación se diera de manera rápida y sistemática es que el hombre inventa las tecnologías de la información a través de la Internet, convirtiéndose esta en la tecnología más revolucionaria hasta hoy vista, ya que es una herramienta indispensable y carente de límites del mundo globalizado.

El Internet se da gracias a un proyecto militar estadunidense con el fin de crear una red de computadores que unieran los centros de investigación de defensa en busca de información en caso de ataques y que esta siguiera funcionando a pesar de que fuera destruida parcialmente. ("Internet y la World Wide Web", 2008)

Luego de su creación esta red fue utilizada por el gobierno, universidades y otros.

En el año de 1980 aproximadamente los usuarios de la red eran científicos y curiosos, en el año de 1990 aproximadamente desaparece el proyecto del ministerio de defensa de los Estados Unidos (ARPANET) y se abre paso a las redes interconectadas de internet, en donde se establecen servicios como el correo electrónico, chats, web, acceso remoto de máquinas, trasferencia de archivos, creación de buscadores, entre otros. ("Internet y la World Wide Web", 2008)

Es una herramienta que ha brindado la oportunidad de difundir información de carácter global, siendo una forma de interactuar entre los individuos y las computadoras sin importar en qué lugar del mundo nos encontremos, a la que cualquier persona y en cualquier momento puede acceder. Hoy en día hay integración de nuevas redes y usuarios por lo que el dominio es más amplio y el aprovechamiento es mejor, como lo es el acceso a través dispositivos móviles que permiten conectarse al internet de manera inalámbrica. (UNESCO, 2005)

Es una realidad que al ser la internet una herramienta globalizada, no todos tenemos la cultura del buen uso y del respeto por el otro, y al estar esta red al alcance de millones

de personas, en ella podemos encontrar delincuentes que aprovechan este medio de comunicación para infundir terror y miedo sobre la población, el gobierno, u otros entes políticos. Conforme aumenta el acceso a la información en el ciberespacio también se ven disminuidos o afectados algunos de nuestros derechos y se ponen en peligro nuestras libertades, como lo es la libertad de expresión.

La internet ha modificado las relaciones humanas, tanto en el ámbito político, económico y social, porque también ha sido un mecanismo para infundir criminalidad en el ciberespacio, entonces hablamos de cibercriminal, ciberterrorismo, cibervïctima.

El objetivo de este trabajo investigativo es dar a conocer como se afecta la libertad de expresión con el ciberterrorismo.

MARCO DE REFERENCIA

1.1. Planteamiento del problema

Hoy en día el desarrollo de la tecnología ha permitido a la humanidad evolucionar ya sea de forma positiva o negativa, lo que se revela es que el mundo está pasando por una etapa gris referida a la seguridad online. Los ciberdelincuentes son personas que llevan acciones ilícitas con fines económicos, políticos o sociales.

El desarrollo y la evolucion de la economía ha dado a entender que hoy en día se pueden obtener fines de lucro de la misma, hay personas que utilizan sus medios de conocimiento para llevar a cabo acciones ilicitas y obtener un provecho monetario o idealista. Para evitar esto se necesitarían sistemas informaticos eficientes en cuanto a su seguridad para que el comun de los ciudadanos podamos confiar.

En estudio de CORONADO CONTRERAS, (2015) se explica las implicaciones de la libertad de expresión y su afectación por mal uso en las plataformas virtuales, a esto es a lo que se le ha venido llamando ciberterrorismo en cuanto a los actos criminales que han atemorizado a millones de usuarios de esta platafoma. En consecuencia ha sido necesario limitar el ejercicio de algunos derechos como lo es la libertad de expresión por el manejo social que se le ha estado dando a la internet, lo que genera la creación de nuevas figuras penales que van a criminalizar el uso de las redes sociales con diferentes finalidades. (CORONADO CONTRERAS, 2015)

Necesitamos la creación de sistemas de seguridad que garanticen el respeto por nuestros derechos sin menoscabar o disminuir los que ya tenemos, creando sistemas seguros, confiables, efectivos y adecuados, pues toda persona tiene derecho a la protección legal contra atraques ciberterorristas.

En este aspecto, explica CORONADO CONTRERAS, (2015) sobre las consecuencias del crecimiento de la red virtual que propicia a que se den estos actos ciberterroristas siendo ataques informaticos para la sociedad de hoy en día que esta fuertemente ligada a la tecnologia, ya que la podemos tener al alcance de nuestros hogares y lo que a esto

respecta la importancia de una regulación global al respecto. (CORONADO CONTRERAS, 2015)

El problema a tratar es el ciberterrorismo, la última modalidad terrorista proporcionada en el siglo XXI; el terrorismo cibernetico uno de los medios mas eficaces de atemorizar a una pluralidad de personas de manera inmediata. Es un problema ya que, en muchas ocasiones, aunque no se cumplan dichas amenazas terroristas, atemorizan al comun de las personas de manera expedita; sin fallas, ya que se difunden en el mayor medio de circulacion social del momento, la social media, la internet; hoy en dia los seres humanos, la gran mayoria necesitamos de este medio para continuar nuestro día a día. Para estar comunicados. (UNODC, 2013)

Existen hoy en día multiples casos documentados, desde los mas minimos hasta los mundialmente reconocidos y donde paises potencia han sido atemorizados y afectados en gran parte de su economía por estos actos terroristas. Con el grupo ISIS y su atentado en paris , en el libano y en bruselas, atemorizo en multiples plataformas de internet a la comunidad cibernauta y al mundo entero diciendo que iba a atacar a toda Europa y tambien a America; que acabaria con el cristianismo catolico y que ellos serian los unicos que quedarian vivos. Esto ha sido recopilado por Denning, D (2000)

1.2. Justificación

Gran parte de la sociedad de hoy en dia, desconoce el término de ñciberdelitosò o delitos cibernéticos, según Chicarro, A, (2009); en este caso en concreto el ciberterrorismo; ni si quiera le dan la importancia debida a estos delitos y es mas los pueden cometer en su diario vivir y puede no darse cuenta de su grave error. Estos delitos no transgreden fisicamente al individuo, pero si de una manera subjetiva, por tal razon esta investigacion trata de esa transgresion y hasta donde la libertad de la persona puede vulnerar de manera mental sin vulnerar la parte fisica de una persona a la misma.

Es importante porque muchas personas desconocemos el alcance que tiene el internet en nuestro medio y la clase de delitos que se pueden cometer, por eso se puede sostener que la informática es un forma de poder social.

Son delitos que se presentan de manera pasiva a la sociedad ya que aparentemente no causan daños físicos visibles, lo que significa que la sociedad le reste importancia a acciones que en la realidad son de importante cuidado por el riesgo que tienen las redes informáticas y la información que se maneja y circula por estas, ya que son utilizadas para cometer delitos que traspasan las fronteras desligando cual es el límite de los estados. (Chicarro, A, 2009)

Alimentando el poder de la ciberdelicuencia para poder obtener información y satisfacer sus propios intereses a expensas de las libertades individuales como lo es la libertad de expresión, reconociendo de igual manera los beneficios que los medios tecnológicos brindan a la sociedad y que por lo tanto requieren de una inminente regulación jurídica

con respecto al buen uso de manera que se evite conducta antisociales y delictivas. (UIT & Departamento de Infraestructura, Entorno propicio y ciberaplicaciones., 2014)

La sociedad de hoy en día tiene un grado de dependencia alto a la tecnologia y al mundo virtual como lo explica CORONADO CONTRERAS, 2015. En la que la gran mayoría hacen parte de nuestra cotidianidad, los avances tecnologicos han sido de gran ayuda para nuestra sociedad , pero también la realidad de que naciones, empresas y personas se ven afectados por estos actos es inminente. (CORONADO CONTRERAS, 2015)

Uno de los alcances que quiere lograr el ciberterrorismo es amplificar las consecuencias del ataque terrorista e infundir miedo, panico y confusion y repercutir en terceros de manera cibernetica.

El ciberterrorismo hoy en dia es de gran importancia estudiarlo y analizarlo ya que es la forma mas efectiva de ataque mundial a las personas, a veces es mas poderoso la atemorizacion de carácter virtual, llega mas al mundo que la atemorizacion de manera fisica y efectiva en contra de un ente particular, ya que las personas hoy en dia en las redes sociales viven en torno a eso, y lo que tenga mas ñboomò mas se le da importancia y revuelo mundial. El ciberterrorismo es un delito inminente a la humanidad, y muy subjetvo y relativo a la vez; cada quien puede tener una afectacion similar o diferencial a su par; tal vez por ese sentido le falta muchisima mas regulacion.

Esta investigacion tiene como fin esclarecer que es el ciberterrorismo, cuales son sus fuentes y porque se confunde la libertad de expresion con el ciberterrorismo, que para este documento es la base y lo mas importante del analisis. Toda persona tiene derecho a expresarse libremente, pero hasta donde este derecho se puede utilizar. La mejor manera de utilizar un derecho no se podria decir es hasta donde no vulnere el de mi igual; entonces el terrorismo cibernetico si sera una libertad de expresion vulnerando el derecho de mis semejantes.

1.3. Objetivos

1.3.1. Objetivo General

Establecer el alcance geo-político y geo-social del ciberterrorismo y hasta donde está afectando la libertad de expresión.

1.3.2. Objetivos Específicos

- Ampliar los conocimientos sobre el alcance que tiene la libertad de expresión en el mundo de la informática desde el ámbito legal.
- Analizar los riesgos que se aceptan una vez que se ingresa en el mundo de la informática.
- Ampliar el conocimiento sobre la línea que se traza sobre la libertad de expresión y cualquier información que amenace la seguridad.

1.4. Alcances

Dar a conocer como hoy por hoy la internet ha sido un mecanismo ideal para que la información llegue de manera oportuna, pero de igual forma se determine el valor que se vulnera cuando personas sin escrúpulos usan un medio para hacer valer un derecho con el cual afectan, violan y vulneran derechos fundamentales, criminalizando el derecho a la libertad de expresión.

CAPITULO I

MARCO LEGAL NACIONAL

Es una obligación de todo Estado soberano proteger su infraestructura cibernética. Cualquier deterioro en la misma, no sólo afectaría al ciudadano común, sino también numerosos aspectos gubernamentales, industriales y del comercio. (Álvarez Samaniego, 2009)

Ley 599 del 2000:

Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de ñviolación ilícita de comunicacionesò, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el ñAcceso abusivo a un sistema informáticoò, así:

ñArt. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.ò (Congreso de la Republica, 2000)

Ley 1273 del 2009

Esta ley creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.[1]

El 5 de enero del 2009, el Congreso de la Republica de Colombia promulgó la Ley 1273 por medio del cual se modifica el código penal y se introduce un nuevo tipo penal que se llama ñde la protección de la información y de los datosò

Hasta el año 1999 sólo había 3 delitos informáticos:

1. Sabotaje.

[1] (1) Durante el 2009 el salario mínimo legal en Colombia será de COP$496.900. Por lo tanto las multas serán de máximo COP$745.350.000.

2. Acceso abusivo a sistema informático.
3. Interceptación de acceso informático.

Antes de 1999 la investigación de delitos informáticos se hacía por analogía, lo que no es permitido porque en derecho penal no se puede investigar por la vía de analogía, entonces como no se podía investigar por analogía se crearon unos nuevos delitos que se encuentran en la ley 1273 de 1999, el titulo 7 B ï ñde la protección y de los datosò

La importancia de esta ley radica en que adiciona al Código Penal colombiano los delitos "De la Protección de la información y de los datos" que se divide en dos capítulos: ñDe los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticosò y ñDe los atentados informáticos y otras infraccionesò (Congreso de la Republica, 2009)

CAPITULO II

MARCO INTERNCIONAL

CONVENIO SOBRE CIBERDELINCUENCIA DEL CONSEJO DE EUROPA ï CCC (CONOCIDO COMO EN CONVENIO SOBRE CIBERCRIMINALIDAD DE BUDAPEST)

Este convenio es el primer tratado a nivel internacional que ha adoptado una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas, es decir, crimines cometidos a través de internet u otras redes informáticas, tales como pornografía infantil, violaciones a la seguridad de la red, fraude informático, infracciones a los derechos de autor, entre otros. Este convenio también adopta medidas para la búsqueda de redes informáticas y la interceptación. Se trata de un convenio con carácter prioritario de una política penal contra la ciberdelincuencia.

Único instrumento vinculante vigente sobre el tema en el ámbito internacional y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos. El Consejo considera que el delito cibernético exige una política penal común destinada a prevenir la delincuencia en el ciberespacio y en particular, hacerlo mediante la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional. Cabe resaltar que si bien el CCC tuvo su origen en el ámbito regional europeo por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004, es un instrumento abierto para su adhesión a todos los países del mundo. (Consejo de Europa, 2001)

DECLARACION UNIVERSAL DE DERECHOS HUMANOS:

ART. 19: Todo *individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir*

informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

Art. 29:

1. Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad.

2. En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática.

3. Estos derechos y libertades no podrán en ningún caso ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas.

La libertad de expresión es el derecho fundamental clave para el desarrollo, la dignidad de cada persona, desde el momento que se tenga la oportunidad de expresar sus ideas y sobre todo de ser oído, con el fin de debatir y establecer interrogantes, políticas de gobierno que aseguren el progreso social y económico de un Estado, dentro del marco de la democracia y del respeto por el otro.

Hoy, en el siglo XXI, los avances tecnológicos han servido para crear nuevas oportunidades para ampliar el marco de acción con relación de este derecho fundamental, por consiguiente promover la defensa de este al igual que establecer los límites cuando el derecho del otro se ve vulnerado, la información se transmite de manera rápida, casi de forma instantánea por todo el mundo, con la posibilidad de vernos afectados o ser víctimas de una guerra que se inicia a través de los teclados de una computadora, o desde un celular; utilizando la internet como medio de comunicación e información un arma que sirve para ataques complejos y hasta posiblemente inevitables, no es alejar al mundo de la posibilidad de obtener información de carácter masivo o censurar la red, se trata de controlar todo tipo de actividades ciberterorristas, donde la internet es el medio para llegar al fin.

Es importante reconocer que todas las personas somos diferentes y que debemos actuar de acuerdo con nuestra moral y ética para el ejercicio libre de nuestros derechos, garantizando el bien común, siempre respetando y reconociendo los derechos de los demás, ya que con el uso de la internet como medio masivo de información de carácter virtual se ha tenido la creencia errónea de que todo lo que está en la red es veraz, que toda persona es libre de ofender, denigrar, calumniar y ejercer acciones coactivas, refugiándose detrás de una pantalla de un dispositivo electrónico. (ONU, 1948

CAPITULO III

MARCO GEOPOLITICO

Hoy, siglo XXI surgen nuevos espacios de vigilancia y control, el ciberespacio, dándonos la posibilidad de navegación a través de Internet, por lo que se establece una contradicción entre la posibilidad de la navegación, los limites, los derechos fundamentales desde el ámbito de la libertad de expresión al igual que la libertad de circulación.

La ciberbiografia estudia las redes de comunicación computacionales, en la cual la Internet, los sitios Web, la World Wide, redes sociales, plataformas móviles, entre otros, es lo que comprende el Ciberespacio, el cual es un espacio geográfico hecho por el hombre, que está en constante cambio y que por lo tanto sus propietarios es cada persona que ocupe un lugar en el espacio, cuando se quiere causar daño o hacer terrorismo por este medio no se necesita movimiento físico para hacerlo simplemente se necesita de un espacio computacional en la esfera del universo.

La globalización implica un estado de poder donde su eje central es el comercio ï economía, utilizando un territorio virtual como lo es el espacio, dependencia creciente de este y junto a ello crecientes amenazas y vulnerabilidades.

Todo se gestiona a la velocidad de la luz en el espacio, por lo tanto se han venido gestionando durante los últimos años políticas de gobierno orientadas a garantizar la seguridad ciberespacial en el mundo y en el ámbito nacional Colombia, promoviendo la responsabilidad en cabeza del estado a través de las fuerzas armadas con un sistema de colaboración transparente apoyado en la recolección de información sobre amenazas potenciales.

CIBERVOLUCION

El 4 de febrero de 1957 satélite artificial soviético SPUTNIK hace normalmente su recorrido espacial, cuando de pronto Estados Unidos se da cuenta que la Unión Sovietica ha desarrollado la capacidad de explorar tecnología militar de una forma rápida, a su vez con este descubrimiento Estados Unidos inicia todos los proyectos en ese tiempo posibles para comenzar su carrera espacial organismo como lo son National Aeronautics and Space Admininistration (NASA) y el Advanced Research Project Agency (ARPA) organismo dependiente del Departamento de Defensa de dicho Estado, encargado principalmente de las comunicaciones. ("Internet y la World Wide Web", 2008)

En el año 1961 ARPA (Advanced Research Projects Agency) creada en respuesta a los desafíos tecnológicos y militares de Rusia, durante la Guerra Fría; pone en función sus actividades de defensa, debido a un sabotaje en las antenas de transmisión de Utah , con lo que se demuestra la debilidad del sistema de comunicaciones, el cual es utilizado por las fuerzas militares, significa un reto para la creación de comunicaciones en red con el fin de evitar posibles sabotajes. (CORONADO CONTRERAS, 2015)

En la guerra fría, Estados Unidos pone en marcha la red de comunicaciones sin centro, la cual corresponde a el desarrollo de nuevas tecnologías para uso militar y defensa de la seguridad nacional. ("Internet y la World Wide Web", 2008)

El ARPANET,es la red que dio origen a la Internet, con cuatro computadoras conectadas de diferentes puntos geográficos: Massachussets, Los Ángeles, Santa bárbara y Utah. Hoy por hoy es posible que millones de computadoras se conecten de manera simultánea y por consiguiente es la conexión de millones de personas en todo el mundo y todos con el objetivo de explorar el espacio cibernético. ("Internet y la World Wide Web", 2008)

CONTROL CIBERESPACIAL:

Hoy las potencias mundiales han utilizado al ciberespacio como un campo de guerra, en el enfoque de la dominación, pues quienes tengan la capacidad de dominio mayor tendrán por consiguiente mayor poder político y económico en el orden mundial elemento que propine la globalización actual. Este es un control basado en el espionaje por intermedio de la alta tecnología, es el hambre de dominar el espacio al costo ilimitable, las guerras futuras no son ni por aire, tierra o mar, son guerras basadas en conocimiento e información.

El ciberespacio es un mecanismo utilizado para conectar al mundo pero al mismo tiempo es un mecanismo de dominio el cual es utilizado desde dos ámbitos:

1. Modo de fomentar libertades individuales con el fin de brindar información de carácter oportuna e inmediata.

2. La libertad individual como primera instancia es lo que le constituye o corresponde a una persona para hacer respetar sus deberes y sus derechos fundamentales, obtener informacion de manera oportuna, inmediata de fuentes certeras es un derecho que no se les puede quitar ni minimizar a los ciudadanos y a los usuarios del ciber espacio para que puedan estar enterados de lo que pasa en el mundo día a dia.

Modo de ejercer un método represivo para con la población mundial en cuanto al manejo de la ubicación en tiempo real para cada persona, cuando se maneja la información de manera distorsionada. Se habla de represión en el sentido de que los ciudadanos no tengan al alcance dicha informacion y que esta no sea certera para que no puedan apreciar la realidad de hoy en día. Eso es lo que ocurre con muchas fuentes en la internet, distorsionan la informacion, dan noticias mentirosas haciendo que los usuarios no tengan una realidad o tambien muchos gobiernos no fan informacion mentirosa, si no que reprimen a los ciudadanos para que no sepan la realidad de otros paises del mundo.

COMISION COLOMBIANA DEL ESPACIO

La Comisión Colombiana del Espacio es el órgano intersectorial de consulta, coordinación, orientación y planificación. Orienta la ejecución de la política nacional para el desarrollo y aplicación de las tecnologías espaciales, y coordina la elaboración de planes, programas y proyectos en este campo. (Comisión Colombiana del Espacio, 2017)

Colombia tiene la misión de observar el territorio colombiano mediante la adquisición de tecnologías satelitales, así entonces, el Instituto geográfico Agustín Codazzi ï IGAC, el Centro Internacional de Física ï CIF, y COLCIENCIAS (Convenio 160), han realizado actividades de investigación sobre el estado del arte en tecnologías satelitales de observación de la tierra. Estas tegnologías satelitales buscan expandir el ciberespacio en colombia y posibilitar la mayor apuesta a las tegnologias ciberespaciales en el país, mejorando el desarrollo de este en el mundo. Tambien busca saber como se limita el ciberespacio, ya que el espacio real geografico territorial se encuentra limitado, ya que ha habido muchos intentos por colonizar este y han sido fallidos ya que como a la vez s puede estar muy cerca, asi mismo muy lejos.

LIBERTAD I

Es un satélite artificial que fue construido por la Universidad Sergio Arboleda, el cual fue lanzado el 17 de abril del 2007, es el primer satélite construido en Colombia con la ayuda y asesoría de los Estados Unidos, este satélite. (Portilla, 2012)

COLOMBIA ï DOCUMENTO CONPES 3701:

El cibercrimen o Ciberdelito conocido en Colombia como delitos informáticos se presenta en Colombia y en todo el mundo ya que la tecnología avanza cada día más y más y es por ello que en Colombia se refleja a través legislación penal.

Por ello Colombia está tomando medidas importantes para enfrentarse a las amenazas cibernéticas, las cuales representan un problema que está creciendo de manera vertiginosa, permitiendo de esta manera sentar bases para que nuestro país se apoye en un punto estratégico de modo que se alcance a mitigar el daño con respecto a los nuevos conflictos delictivos para el siglo XXI. Colombia por ejemplo, para el año 2000 tan solo el 2% de la población tenía acceso a Internet; actualmente el 40% hace uso constante de este medio Ministerio de Defensa Colombia, ubicando al país en el cuarto lugar en el ranking de usuarios de América Latina y en el puesto 24 del mundo(Departamento Nacional de Planeación, 2011).

Desde el año 2005, el Ministerio de Relaciones Exteriores creó un grupo intergerencial de trabajo para analizar y profundizar en los temas concernientes al ciberespacio. Posteriormente, el Ministerio de TICs, por medio de una consultoría, identificó las brechas y los vacíos que tiene la Nación en materia de Seguridad Informática. Teniendo

el resultado de esta iniciativa y el de múltiples discusiones en el grupo de trabajo, la Cancillería, el Ministerio del Interior y Justicia, el Ministerio de TICs, y otras entidades involucradas en el proceso, decidieron que el Ministerio de Defensa liderara los temas de Ciberseguridad y Ciberdefensa. Departamento Nacional de Planeación, 2011).

El Gobierno Colombiano en miras de establecer medidas urgentes para proteger la seguridad y la defensa cibernética y reforzar la seguridad de la información nacional, específicamente por medio de organizaciones oficiales creadas para este fin por medio de un documento, denominado CONPES 3701, en el cual combinan tres organizaciones paralelas con el objetivo de mantener la seguridad cibernética. Departamento Nacional de Planeación, 2011).

COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia):

El término CERT se deriva de las siglas en inglés "Computer Emergency Response Team" y está conformando por un equipo de personas que pertenecen al Ministerio de Defensa, dedicadas a la gestión de incidente con el objetivo de mitigar el riesgo y dar respuesta a incidentes de tipo cibernético.

Con relación a infraestructuras críticas del país, el COLCERT reconoce el concepto de incidente como la violación o amenaza inminente de las políticas de Seguridad Informática, las políticas de uso aceptable o las prácticas estándar de seguridad informática, criterios determinados en la página web del órgano (http://www.colcert.gov.co/), así:

- Intentos de obtener acceso no autorizado a un sistema o sus datos, ya sea fallido o exitoso.
- Interrupción no deseada o denegación de servicios.
- El uso no autorizado de un sistema que procese o almacene datos.
    - Cambios en el hardware del sistema, el firmware o las características de software sin el conocimiento del propietario, instrucción o autorización. (Departamento Nacional de Planeación & Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)
-

CCP (Centro Cibernético Policial:

Es una dependencia adscrita a la DIJIN, encargada de las labores de investigación y procesamiento anual de delincuentes informáticos.

Es una plataforma virtual -CAI virtual- encargado de la prevención de delitos en la Internet en temas como la pornografía infantil, la suplantación de sitios web, el hurto de contraseñas y el hackeo de correos electrónicos, entre otros. Tarea observable en su sitio web **(**www.ccp.gov.co)

CCP (Comando Conjunto Cibernético):

Es una dependencia adscrita al Comando de las Fuerzas Militares, el cual se encarga de coordinar la respuesta a incidentes de seguridad que afecten la seguridad nacional.

- Este Comando surge con el fin de atender todas la amenazas y ataques que puedan surgir al Estado, ya sea a la parte del gobierno, a la parte de las Fuerza Militares, y de acuerdo con el Documentos CONPES 3701 se crea esta unidad para que atienda todas estas emergencias las cuales son tema reciente y son el boom a nivel mundial (Departamento Nacional de Planeación & Ministerio de Tecnologías de la Información y las Comunicaciones, 2011)

El trabajo del gobierno colombiano está orientado a trabajar en los siguientes ejes temáticos:

- Fortalecimiento Jurídico e Institucional:

Adecuación y adopción de las medidas legislativas y judiciales para la ciberseguridad, a cargo del Ministerio del Interior y de Justicia.

- Asuntos Internacionales:

Seguimiento a tendencias internacionales e implementación de acuerdos asumidos por el Estado, a cargo del Ministerio de Relaciones Exteriores.

- Medidas contra el Delito Cibernético:

Implementación de medidas para la seguridad y defensa del Estado Colombiano y puesta en marcha del COLCERT, a cargo del Ministerio de Defensa Nacional (Presidencia de la República de Colombia, 2017)

Políticas del ciberespacio

Normatividad

Adjuntos:

Documento Conpes 3585 CCE.pdf

Documento Conpes 3080 CCE.pdf

Documento Conpes 3683 CCE.pdf

Decreto 3816 del 31 de diciembre de 2003.pdf

Circular No 001 - 2009 - COINFO.pdf

Convenio especial de cooperacion No 4093 - 2009 COLCIENCIAAS- CIAF-IGAC.pdf

Visión 2019 Consolidado ver 6 definitivo.pdf

CAPITULO IV.

EL CIBERTERRORISMO COMO COMO LÍMITE AL DERECHO A LA LIBERTAD DE EXPRESIÓN

¿Qué es Ciber?

- Según la RAE (Real Academia Española, 2014) es un prefijo referido al adjetivo *cibernético,* relacionado con el mundo de las computadores u ordenadores y de la realidad virtual.

Origen de la palabra ñCiberò

Palabra de origen griego ***ñ***κυβερνήτης***ò*** o en latín ***ñ****ciber****ò*** el cual significa ***ñ****timón****ò*** control, ***ñ****timonel****ò*** así lo han definido ("Etimología", 2001) como persona que gobierna una ñnaveòen un espacio virtual creado por medios informáticos.

¿Qué es Cibernauta?

Es la persona que se comunica con otros individuos a través de las redes informáticas. O según la RAE (Real Academia Española, 2014) es ñ*Persona que navega por el ciberespacio.****ò***

¿Qué es terrorismo?

Según la RAE (Real Academia Española, 2014) se considera como terrorismo a ñ3. m. Actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos.

¿Qué es Ciberterrorismo?

En 2015, "¿Qué es el Ciberterrorismo?" establece que por ciberterrorismo se debe entender la comisión de delitos e infracciones de terrorismo a través de medios y sistemas informáticos. Entre ellas se encuentra el cracking, Ddos, botnets, malware entre otras.

¿Ciberseguridad?

Se puede definir como una protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados. (CARVAJAL AZCONA, 2017)

Es la estrategia que se implementa para evitar fraudes y actividades ilícitas a través de la tecnología de la información asi como lso servicios de internet.

Informando a los usuarios de estas herramientas previniendo y capacitándolos para su adecuado uso.

¿CIBERDEFENSA?

Conjunto de meidas, técnicas, políticas organizativas enfocadas a proteger los sistemas de información, comunicaciones y control ante ciberataques de cualquier índole. (BATANERO, 2013)

CIBERGUERRA

Es un área en las agencias militares de los países que analizan, evalúan y realizan ataques sobre las vulnerabilidades técnicas de los sistemas o redes informáticas de los Estados enemigo. Entre los países inmersos en el concepto de ciberguerra se encuentra Estados Unidos, China, Rusa, Francia e Israel. (Sain, 2016)

CIBERCRIMEN

Se define como los delitos cometidos a través de internet por medio del uso de un computador o mecanismo análogo, existen términos emparentados como delito informático, *computer crime o high tech-crime.* (CASTILLO ARA, Alejandra, 2017)

CONCLUSIONES

En retrospectiva, este artículo presenta un panorama histórico-político de lo que hasta el momento se ha podido concebir como ciberterrorismo, sus repercusiones y la problemática que suscita hoy en día.

Esto no se puede desligar de un contexto plagado de amenazas que por una multicausalidad de elementos y factores se ha convertido en una amenaza real que como vimos ha afectado a naciones enteras, particulares, empresas y compañías. Así, que dado este punto este escrito plantea a su vez la necesidad de desarrollar

herramientas legales, procedimentales y virtuales en razón a la normativa y políticas ya dispuestas que tengan un carácter preventivo sobre lo que ha implicado el tratamiento del ciberterrorismo en la contemporaneidad.

Frente a los objetivos propuestos para este artículo, sobre el reconocer el alcance geo-político y geo-social del ciberterrorismo y su afectación de la libertad de expresión, se debe explicar que a lo largo del mismo se hizo un razonamiento dialéctico explicando lo que cada punto expone con sus implicaciones, para ello se tomaron de referencia las ideas de autores europeos y americanos que aportan a la discusión una doble visión del asunto, ya que a pesar de que el ciberterrorismo es un fenómeno global estos nos exponen como han abordado esta problemática en sus contextos.

Así pues, lo planteado dirime los propósitos del texto pero además nos permite realizar varias inferencias que a modo de conclusiones se recopilarán enumerándolas:

1. Existe una relación indivisible entre el aumento de riesgos jurídicos, políticos y sociales con el auge de los ataques ciberterroristas. Lo cual nos lleva a pensar sobre las herramientas y las necesidades de replantear las formas de combatir la cibercriminalidad

2. Por otra parte, al existir una vasta normativa tanto nacional como internacional explica la importancia social del control de los ciberespacios. Que de otra forma, se explicaría en razón a esto que los Estados y órganos de control tienen un deber frente a las acciones que deben ser ejecutadas para evitar que en espacios *ciber* ocurran acciones delictivas, que en los últimos tiempos se han vuelto habituales y normalizados.

3. Se observa una discusión natural entre las medidas, controles y actos delincuenciales en el *ciber espacio ï Ciber terrorismo-* y la afectación a la libertad de expresión inherente al ser mismo. Ello, como lo manifiesta CORONADO CONTRERAS, L. (2015) pone en medio discusiones que a su vez tocan asuntos álgidos en la sociedad como lo podrían ser la desregulación de los espacios virtuales como ejercicio de autonomía de los hombres, la prohibición como una forma *inconstitucional ï* En el caso colombiano- de proteger y evitar la *ciberdelincuencia*, el choque directo entre los valores de la seguridad nacional vs la paz pública entre otros.

4. Así, también queda la pregunta abierta sobre las formas de libertad de expresión y las ñformas efectivasò en las que los Estados se aseguran de su efectivo cumplimiento, puesto que con las variadas formas de libertad de expresión como lo son la libertad de pensamiento, la libertad religiosa, la libertad de medios de comunicación, la libertad de cátedra, enseñanza e investigación surgen inquietudes puntuales sobre cada uno, sin pormenorizar las dificultades en cada una de las necesidades que podrían suscitar la adecuada protección de tales libertades.

5. Tampoco se puede perder de vista que con las facilidades del acceso a la información y al internet, las formas delincuenciales se han vuelto más sencillas llegando al punto en el que las personas sin tener conocimiento o una falsa creencia (culpa) dan lugar a acciones ilícitas tanto en el país y proscritas en muchos de los Estados adscritos a convenciones internacionales sobre el asunto, aunado a que los niveles de impunidad en esto son desmesurados. Ergo se puede hablar de una

inefectividad de las normas que está acompañada del desconocimiento y facilidad sobre actos delincuenciales, especialmente ciberterroristas.

6. Al analizar la normativa, y políticas públicas en el caso colombiano se vuelve notable considerar que el tratamiento de esta situación se volca a un mediano y largo plazo, puesto que la mayoría de normativas son recinetes, no teniendo la mayoría de estas mas de 5 o 6 años. Lo que refiere que para poder revisar la efectividad de las medidas tomadas tanto en la protección de la libertad de expresión como en la penalización de las acciones ilícitas solo podrá tener algún sentido con el pasar de los años, por lo cual se deberá tener especial cuidado al momento de revisar esta información sin revisar con la perspectiva adecuada la ejecución de estos planes.

7. La pregunta respecto a la vulneración de la libertad de expresión frente a las medidas legales para evitar el terrorismo y ciberterrorismo ha tenido una respuesta condicionada a ciertos apartes, sin embargo la discusión en el asunto no ha finalizado considerando la envergadura del mismo, por lo que será necesario plantear discusiones respecto a las necesidades y protección de la libertad de expresión tal como se aduce de la conclusión 4.

Referencias

1. Departamento Nacional de Planeación, & Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Documento **CONPES 3854**, Política nacional de seguridad digital. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.

2. Real academia Española. *Diccionario de la Lengua Española (23ª Ed). Recuperado de* http://dle.rae.es/?id=98ULSyc

3. Real Academia Española. (2014) Ciber. En Diccionario de la lengua española (23ª ed.) recuperado de: http://dle.rae.es/?id=98ULSyc

4. Real Academia Española. (2014) Ciberespacio. En Diccionario de la lengua española (23ª ed.) recuperado de: http://dle.rae.es/?id=98Wdd57

5. Línea de investigación Geografía, Universidad Nacional. (2017, 24 de octubre) recuperado el 25 de octubre, 2017 de: http://www.humanas.unal.edu.co/geografia/investigacion/grupos/cibergeografia

6. Real Academia Española. (2014) Cibernauta. En Diccionario de la lengua española (23ª ed.) recuperado de http://dle.rae.es/srv/search?m=30&w=cibernauta UNESCO. (2005).

7. Ferrucio Rossi-landi & Williams, R. (1992) *Historia de la comunicación,* recuperado de http://www.elsarbresdefahrenheit.net/documentos/obras/2346/fichero

8. *Las tecnologías de la información y la comunicación en la enseñanza.* Recuperado de. http://unesdoc.unesco.org/images/0013/001390/139028s.pdf

9. UNODC. (2013). El uso de internet con fines terroristas. Recuperado de https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet

10. UIT, & Departamento de Infraestructura, Entorno propicio y ciberaplicaciones.. (2014). Comprensión del Ciberdelito: Fenómenos, dificultades y respuesta jurídica.. Recuperado de http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf

11. Ley 599 del 2000, Diario Oficial de la República de Colombia, Bogotá, Colombia, 24 de julio de 2000

12. Álvarez Samaniego, C. A. R. L. O. S. (2009, 1 octubre). [Ciberseguridad y ciberdefensa]. Recuperado de https://www.academia.edu/15316374/Ciberseguridad_y_ciberdefensa

13. [Internet y la World Wide Web]. (2008). Recuperado de http://www.paralibros.com/passim/p20-tec/pg2050ci.htm

14. Departamento Nacional de Planeación. (2011). CONPES 3701. Recuperado de http://www.mintic.gov.co/portal/604/w3-article-3510.html0xMJ8ZcbZlrHcgbG1PImEc

15. [Significado]. (s.f.). Recuperado de https://www.significados.com/ciber/

16. [Glosario]. (s.f.). Recuperado de http://tecnologiaedu.us.es/cursos/29/html/glosario_principal.htm

17. BUZAI, G. D. Solaris ï El océano tecnológico. Semanario Noticias y Protagonistas, Mar del Plata, n. 90, p. 12, 20 jun. 1999.

18. Convenio sobre la Ciberdelincuencia y delitos informáticos, Budapest, 23 de Noviembre de 2001. *Serie de tratados Europeos.* Recuperado en: https://rm.coe.int/16802fa41c

19. Ley 1273 de 2009, Diario Oficial de la República de Colombia, Bogotá, Colombia, 05 de enero de 2009.

20. Comisión Colombiana del Espacio, 2017. Tomado de https://www.cce.gov.co/.

21. Real Academia Española. (2014) Terrorismo. En Diccionario de la lengua española (23ª ed.) recuperado de: http://dle.rae.es/?id=Zd3L6Oc

22. Etimología [Conjunto de datos]. (2001). Recuperado de http://etimologias.dechile.net/?ciberne.tica

23. Real Academia Española. (2014) Terrorismo. En Diccionario de la lengua española (23ª ed.) recuperado de: http://dle.rae.es/?id=Zd3L6Oc

24. Castillo ara, A. La sistemática general de los delitos cibernéticos y los delitos cibernéticos propios en el Derecho penal alemán: la necesidad de una regulación diferenciada, publicado en: DPyC 2017 (agosto), 11/08/2017, 32; cita online: AR/DOC/1764/2017).

25. Denning, D. (2000). Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services of the U.S. House of Representatives, [en línea]. Disponible en: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.htm

26. Coronado Contreras, L. (2015). La libertad de expresión en el ciberespacio. Recuperado de http://eprints.ucm.es/33067/1/T36374.pdf

27. Chicarro, A. (2009). La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas, [en línea]. Disponible en:http://www.academia.edu/4924420/La_labor_legislativa_del_Consejo_de_Europa_frente_a_la_utilizacion_de_Internet_con_fines_terroristas [2014, 26 de febrero].

28. Real Academia Española. (2014) Ciber. En Diccionario de la lengua española (23ª ed.) recuperado de http://dle.rae.es/srv/search?m=30&w=ciber-

29. Carvajal Azcona, J. (2017, 11 julio). La Ciberseguridad y el riesgo.. Recuperado de https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

30. Portilla, G. (2012, diciembre). La órbita del satélite libertad 1.. Recuperado de http://www.scielo.org.co/pdf/racefn/v36n141/v36n141a02.pdf

31. Presidencia de la República de Colombia. (2017). Prevención cibernética. Recuperado de http://especiales.presidencia.gov.co/Documents/20170601-ataques-ciberneticos/sin-ciber-ataques.html

32. Sain, G. (2016). ¿Qué es la Ciberguerra? Recuperado de http://www.pensamientopenal.com.ar/system/files/2016/02/doctrina4295

33. Atanero, J. C. (2013, 6 marzo). Ciberdefensa. Recuperado de http://www.criptored.upm.es/descarga/ConferenciaJuanCarlosBataneroTA