ÁNALISIS CRIMINOLÓGICO DEL CIBERCRIMEN

KAREN MILENA CRISTIANO CRISTIANO

MARILUZ MAYORGA ORTIZ

Universidad la Gran Colombia

Facultad de Postgrados

Programa de Especialización de Derecho Penal y Criminología

Bogotá

2015

Resumen

Este documento investigativo realiza un análisis descriptivo del término Cibercrimen desde el ámbito criminológico, comienza con una breve presentación de su inicio en la historia a través de los medios de comunicación; acto seguido, se hace una breve presentación de los posible sinónimos como son: delito de los computadores, delito informático, delito de redes e internet, que finalmente resultaran erróneos frente a la conducta punible y luego se determinará su ámbito de acción, es decir, la arquitectura del ciberespacio. Luego se dará paso a mostrar que el cibercrimen tiene como característica principal las TIC, que es de corte transnacional y que la víctima tiene gran importancia respecto a facilitar la comisión de este delito al omitir las recomendaciones para mitigar el riesgo del ciberdelincuente, esto si es persona natural o usuario común, mientras que si es una persona jurídica y/o un Estado debe tener un fuerte sistema de prevención del riesgo y ataque al cibercrimen. Y se muestra que a la fecha el ámbito normativo se queda corto en posibles situaciones tipológicas de cibercrimen, por tanto la jurisprudencia de la Corte Constitucional aún es tímida al utilizar este término, sus pronunciamientos sigue siendo únicamente respecto a la protección de la intimidad, libertad y datos personales, respecto a los casos en que el cibercrimen es el ámbito de ejecución del delito, y de forma insólita no se pronuncia ni se cita el termino.

Palabras claves

Cibercrimen, tipología, normativo, ciberespacio, cibercriminalidad, ciberdelincuente, víctimas, TIC, Internet, redes sociales, delito informatico, riesgo, seguridad.

Abstract

This research paper makes a descriptive analysis of the term cybercrime from the criminological field, begins with a brief presentation of his home in the story through the media; Then, a brief presentation of possible synonyms such as is done: crime of computers, computer crime, crime networks and the Internet, which eventually turn out wrong against the criminal offense and then its scope is determined, ie, the architecture of cyberspace. Then it gives way to show that the main characteristic cybercrime ICT, which is transnational court and the victim is of great importance with respect to facilitating the commission of this crime to ignore the recommendations to mitigate the risk of cyber criminals, that if individual or common user, while if it is a legal entity and / or a state must have a strong system of risk prevention and cybercrime attack. And it shows that to date the policy level falls short of potential typological situations cybercrime, so the jurisprudence of the Constitutional Court is still timid to use this term, his pronouncements remains solely with respect to privacy, freedom and personal information concerning cases in which cybercrime is the area of execution of the crime, and so no position insolita the term cited.

Keywords

Cybercrime, typology, regulatory, cyberspace, cybercrime, cyber criminals, victims, ICT, Internet, social networks, computer crime, risk, safety.

Tabla de Contenido

Proyecto de Investigación

Teniendo en cuenta la época actual en la que vivimos, la cual se podría denominar como la era de las TIC, y con el uso común y frecuente de carácter internacional del ciberespacio, surge el interrogante, ¿todas las posibles conductas punibles que se comenten en el ciberespacio estarían tipificadas dentro del código penal colombiano?, para llegar a una posible respuesta el objeto de estudio es analizar desde el aspecto criminológico el término Cibercrimen, de lo cual se desprenden dos posturas, una tipológica de ámbito criminológico que estudia causas sociales, de contexto cibernético, de interacción de los sujetos que determina o no esta forma de delito y por otra se encuentra la postura normativa que hace referencia a los posibles de tipos penales donde se podría entender como tipificado este delito. Sin embargo, en ningún tipo penal se utiliza el término cibercrimen.

Por consiguiente encontramos una pequeña muestra del uso de las herramientas tecnológicas de la información y de la comunicación, la cual, se extrae de la página web de la Fiscalía General de Colombia, donde se evidencia cifras en las cuales se refleja que Colombia no es la excepción en la investigación y judicialización de conductas punibles del "Cibercrimen":

> En 2014, la entidad llevó a cabo 851 investigaciones en las que fueron utilizados medios informáticos para la comisión de delitos: 159 por violación a la protección de la información y los datos; 124 por punibles contra la administración pública; 101 por afectaciones a la libertad individual; 80 por patrimonio económico; 73 por seguridad pública; 70 por delitos contra el orden económico y social; 25 por hechos que atentaron contra la vida y la integridad personal; 12 por conductas contra personas y bienes protegidos por el derecho

> internacional humanitario; 34 por afectaciones a la libertad, integridad y formación sexual; 21 contra la integridad moral y 16 por atentados a los derechos de autor; las restantes se adelantan por delitos contra la fe pública; los recursos naturales y el medio ambiente; la salud pública; la participación democrática; la eficaz y recta impartición de justicia; y el régimen constitucional y legal.(Fiscalia General de la Nacion, 2015)

Lo anterior ratifica que el estudio criminológico del término Cibercrimen, no puede dejarse pasar por alto en el acompañamiento del derecho penal, teniendo en cuenta el impacto social, económico y el incremento de este tipo de delincuencia común y organizada, tanto en Colombia como en el resto del mundo.

Frenar el Cibercrimen es un asunto de todos: del sector público, de las empresas y de los usuarios que tienen un papel fundamental para contrarrestar este delito que deja billonarias pérdidas en el mundo, como prueba, la Fiscalía General de Colombia, en su página web oficial, el pasado 26 de febrero de 2015 informa que:

> De acuerdo con el *Norton Report*de 2013 más de 400 millones de personas son víctimas del Cibercrimen en el mundo, lo que genera pérdidas por 113 billones de dólares, incluso un estudio del IDC de ese mismo año estimó que los usuarios gastaron 22 billones de dólares y por lo menos 1.5 billones de horas solucionando problemas de seguridad relacionados con software falsificado. En el ámbito empresarial, una de cada 5 pymes fue perjudicada por cibercriminales según el *NationalCyber Security Alliance* y cerca del 53 por ciento de los

> intercambios realizados en la bolsa fue atacado durante 2012. (Fiscalia General de la Nacion, 2015)

Comprender el fenómeno del Cibercrimen, desde su tipología, es el primer objetivo de esta investigación, puesto que se debe confirmar criminológicamente que encierra el Cibercrimen, que es un término inglés, frente a su traducción al español como delito informático; es de anotar que este término puede estudiarse desde un primer ámbito tipológico y otra que se denominaría normativo.

En el primer caso, el termino Cibercrimen describiría conductas como la consistente en acceder ilícitamente a un sistema informático ajeno, o la del adulto que propone a través de Internet un contacto con un menor con la intención de consumar posteriormente un abuso sexual. En el segundo, el termino Cibercrimen describiría tipos penales como el del nuevo art. 197.3 que sanciona el acceso informático ilícito, o el del art. 183 bis que castiga el denominado online childgrooming. (Miró, 2012, pág. 40)

Luego, identificar su espacio de comisión, como lo es el ciberespacio y su interacción permanente con las TIC, puesto que después de comprender que es una conducta catalogada como Cibercrimen, se debe señalar el lugar y su temporalidad de comisión del punible, es el segundo escalón que se abordará.

Al fin al cabo todo evento social es distinto en Internet, un nuevo ámbito estructuralmente distinto al físico en el que sucedían las cosas hasta el momento. Y el crimen es un evento social que cambia en Internet. De hecho, la criminología no ha negado nunca que el ámbito incide en el delito. Si, como señalaran hace ya más de tres décadas Cohen y Felson, el crimen se produce cuando se unen en el espacio y el tiempo un objetivo adecuado,

un delincuente motivado y la ausencia de un guardián capaz de darle protección al primero, es evidente entonces que los especiales caracteres del ciberespacio en los que se ven modificados los parámetros espacio temporales, pueden incidir en una modificación de los condiciones del delito. (Miró, 2012, pág. 144)

Por último, aprender como el Cibercrimen tiene su eje de acción trasnacional, y la importancia que juega la víctima en este ámbito. Es algo novedoso, porque aquí no existen fronteras, es un sitio multicultural y nace con la victima la obligación de salvaguardar su propio riesgo. Es decir, universalmente todos y cada uno de los usuariosson víctimas potenciales y deben blindarse cada vez más un posible ataque cibernético, entre otros.

No creemos que se deba exagerarse la amenaza, pues si bien es cierto que los ataques han ido aumentado a lo largo de los años, también lo es que los procedimientos de seguridad también han ido mejorando, y conforme vayan surgiendo ámbitos de criminalidad irán desarrollándose estrategias preventivas que limitaran los efectos de los mismos.(Miró, 2012, pág. 294).

Esta es una investigación cualitativa de la cual se debe decir que, en este contexto, como técnica "indirecta" «el análisis de contenido es una técnica de investigación que consiste en el análisis de la realidad social a través de la observación y el análisis de los documentos que se crean o producen en el seno de una o varias sociedades. Lo característico del análisis de contenido, y que lo distingue de otras técnicas de investigación sociológica, es que se trata de una técnica que combina intrincadamente, y de ahí su complejidad, la observación y el análisis documental» (López-Aranguren 1986 : 366). En términos generales, el análisis de contenido es un método que busca descubrir la significación de un mensaje, ya sea este un discurso, una

historia de vida, un artículo de revista, un texto escolar, un decreto ministerial, etc. (Revista de Ciencias Humanas - UTP N°20, 2000)

De lo anterior, se infiere que la hipótesis de este documento, no es descubrir una nueva posición, sino por el contrario comprender el significado del término cibercrimen desde su tipología y concluir si efectivamente este tipo de crimen en las TIC se encuentra correctamente tipificados en el ordenamiento jurídico colombiano y comprobar que son múltiples las posibles situaciones punibles que pueden presentarse desde el ciberespacio que aún están por fuera de la jurisprudencia.

Siendo una investigación jurídica, también de corte dogmático, para el cual las fuentes primarias son las siguientes obras: El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Ponds y el libro Sistemas Penales y problemas sociales. Los mass media y el pensamiento criminológico. Las demas fuentes podran ser halladas en las referencias y en las citas que tienen gran relevancia para este estudio criminologico.

De este documento se tendrá la posibilidad de comprender desde la dogmática jurídica una conducta delictiva en el ciberespacio para los estudios criminológicos establecidos para los delitos comunes, entre lo normal, es una divergente dentro de esta disciplina, el: *Cybercrime*. Y mucho más cuando se habla que la víctima es la mayor responsable respecto a su vulneración de derechos por no guardar las recomendaciones de seguridad midiendo unos posibles riesgos. Esto quiere decir que efectivamente es una tipología donde convergen varios derechos tutelados vulnerados por medio de las TIC y que aún la tipificación normativa confunde el cibercrimen de carácter tipológico con delitos informáticos.

Desarrollo sobre el concepto de Cibercrimen y la Delincuencia informática desde la perspectiva Criminológica.

En el último tercio del siglo XX se empieza a dar una mirada periodística al delito y a comienzos del siglo XX se presentan los primeros trabajos desde la teoría de la comunicación.

En los años setenta se da una nueva mirada a la criminología y al tratamiento del crimen en la prensa desde la teoría de la comunicación y se habla de la Mass Media (prensa de masas) y para hablar de esta nueva mirada es necesario traer a colación cómo se originó este suceso en la sociedad y encontramos los Pliegos de Cordel, también conocidos como la literatura de los pobres, los cuales hacían referencia a la relación de sucesos y a la expresión escrita del suceso delictivo, de una manera obsesiva, donde se anunciaban los crímenes de forma sangrienta y de la Justicia implacable.(Baratta, 2003, págs. 489, 490)

Los Pliegos de Cordel difundieron una visión romántica del bandido y gracias a esto la "literatura de bandidos" fue estudiada por los impulsores del saber criminológico, entre ellos el positivista Enrico Ferri, quien aseguraba que el bandido representaba la rebeldía contra los abusos de los tiranos; permitiendo que la narración tuviera una parte monstruosa cuando se trataba de crímenes y asesinatos y una parte fantástica cuando se hacía referencia a hechos que no tenían una explicación.(Baratta, 2003, pág. 492)

Aparece una cultura mediática del delito, donde se expresan unas formas narrativas renovadas, se ofrece un espacio de difusión de las ideas en torno al crimen y se da una herramienta que mueve el sentir social, en la cual se debería expresar una narrativa

modernizada, ofreciendo un espacio de difusión de ideas en torno al crimen y utilizando una herramienta que moviera el sentir social. (Baratta, 2003, págs. 498, 499)

A principios y a mediados del siglo XX aparecen medios de comunicación como el cinematógrafo, la radio y las tiras de comic entre otras, pero se vislumbra una nueva posición de alarma frente a los efectos nocivos de los mismos, teniendo en cuenta que se empieza a presentar un aumento de criminalidad por los mensajes que eran copiados por los jóvenes y adolescentes vulnerables mentalmente, dichos planteamientos estaban influenciados por la Teoría de la Asociación diferencial impuesta en Estados Unidos por Sutherland y Cressey Psicólogos, que lograron determinar que el comportamiento criminal será siempre un comportamiento aprendido, resaltando la exposición directa e indirecta a los medios de comunicación, para lo cual y frente a esta posición los mismos medios de comunicación controvierten lo anteriormente dicho dando a entender que "los medios simplemente reflejan la realidad tal y como es" .(Baratta, 2003, págs. 502, 503)

Posteriormente la televisión entra a jugar un papel muy importante en la emisión de ficción criminal, estas emisiones fueron estudiadas por varios investigadores interesados en ampliar el conocimiento de la sociología de la criminalidad y aparece la Teoría del Cultivo desarrollada por George Gerbner, proyecto al que denomino "Indicadores Culturales" los cuales sugirieron como resultado indicando que "la principal influencia de la televisión radica en su capacidad para comunicar ideas acerca de la conducta, las normas y las estructuras sociales". (Baratta, 2003, págs. 507, 508)

Con lo anterior vale la pena resaltar que para la Criminología los medios de comunicación se generaron con el fin de informar a la población de los hechos ocurridos en su

entorno social, precisamente porque se hacía necesario hacer públicas las conductas que iban en contra de las normas y las decisiones que los órganos judiciales tomaban respecto de los individuos que las infringían, pero a medida que la tecnología iba avanzando los medios de comunicación empezaron a aprovechar su grandiosa aceptación por parte de los espectadores, entre ellos los que leían diarios, veían películas, escuchaban la radio, veían la televisión etc., para enviar mensajes con información que difícilmente iba a ser entendida y asimilada, y que por el contrario incitó al público a querer imitar aquellas conductas criminales descritas

De la Delincuencia Informática a la Cibercriminalidad.

Es de importancia, en primer plano conocer el término informática y su entorno de acción, si bien es cierto, viene a la mente, computadores, internet, correos electrónicos, no se puede pasar por alto que también corresponde a este grupo los medios masivos de comunicación como lo son la radio y la televisión. Todos producidos por un procesador de datos que ha venido evolucionando a través del tiempo.

La palabra española informática deriva del vocablo francés *informatique*, que a su vez es un compuesto contacto de información y *automatique*. La informática alude directamente al tratamiento automático de la información. Así es, El diccionario de la Real Academia Española de 1984 definía la voz informática como "el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de calculadora electrónicas". Actualmente, con el avance de la técnica, ha sido preciso cambiar las palabras calculadoras electrónicas por computadores, manteniendo intacta el resto de la definición.(Larrea, 2004, pág. 13)

Siendo así las cosas, el término fue lo de menos, puesto que a la velocidad del cambio de las inmensas maquinas procesadoras a un pequeño puerto extraíble donde se lleva el internet en un bolsillo. Es decir la red y la tecnología al alcance de la mano de todos los seres humanos, que cada vez están más ligadas al uso común de un estilo de vida post-moderno, siendo mucho más fácil la comisión de delitos con solo la pulsación de una señal, correo electrónico o uso de redes sociales.

La categoría de los delitos informáticos, como constructo doctrinal y que se usó por la doctrina penal alemana y española durante los años setenta, ochenta, noventa y al principio de este nuevo siglo, sigue usándose por parte de la doctrina, no se concibió por quienes lo utilizan en el sentido de grupo autónomo de infracciones penales con caracteres sistemáticos, o de contendió material de protección, homogéneos que exigirán una metodología distinta al resto de grupos o de una valoración político-criminal común al tutelar intereses sociales de idéntica naturaleza. De acuerdo con la caracterización sobre el que recaía el ataque, que conlleva que formasen parte de la misma tanto aquellos comportamientos delictivos realizados a través de procesos electrónicos, como aquellos delitos tradicionales que recaían sobre bienes que presentaban una configuración especifica o bien sobre nuevos objetos como el hardware y el software, difícilmente podía decirse que los tipos que la conformaban tuvieran problemas dogmáticos idénticos o, cuenta menos, distintos a los de otras figuras delictivas. Tampoco la doctrina se empeñaba en buscar algún tipo de identidad de bienes jurídicos en todos los delitos económicos. Siguiendo la caracterización del ciber, el patrimonio y el orden económico, bienes personalísimos como la intimidad o la libertad sexual, y otros bienes supraindividuales o difusos, se consideraban protegidos por los delitos informáticos.(Miró, 2012, pág. 34)

Por lo tanto, ya no solo se trata de una herramienta, como el celular cuando es usado como detonador de un explosivo, sino mucho más allá, el constreñir a alguien en su entorno personal y moral, un posible acoso sexual a una usuaria menor de edad en Facebook, por alguien que bien puede ser aceptado en su perfil como amigo, o aquellos que intentan por medio Firewall ingresar a su cuenta para obtener información de contacto con ella.

La categoría de los delitos informáticos, o quizá mejor, de la criminalidad o delincuencia informática, no definía un bien jurídico protegido común a todos ellos, sino más bien un ámbito de riesgo, el que derivaba de la expansión social de la tecnología informática, común a muchos bienes jurídicos cuya tutela completa por parte del legislador parecía requerir una modificación de los tipos penales existentes para su adaptación a las nuevas realidades informáticas o la creación de tipos distintos que respondiesen a las nuevas necesidades de protección.(Miró, 2012, pág. 36)

En lo actual, podría entenderse que este despliegue de interacción en la sociedad y sus individuos cada vez es más veloz, mucho más constante y popular entre las personas. Por tanto se refiere al alcance de comprensión preventiva de la política criminal para prevenir el riesgo de eficacia de este tipo de delitos como la posible adecuación del tipo penal existente en las conductas delictivas desplegadas en el Ciberespacio.

Relativo al riesgo informático, lo común a infracciones penales como el fraude informático, el sabotaje o daños informáticos, la sustracción de servicios informáticos, el espionaje informático, o la piratería informática de obras de ingenio, tipologías de conducta especifica que la doctrina penal considera merecedoras de la respuesta penal y sobre las que se analizaba su posible incardinación en los tipos penales tradicionales o la reforma de los

mismos, e incluso la creación de tipos nuevos, para una mejor protección de los intereses dignos de tutela.(Miró, 2012, pág. 36)

Aquí cabe señalar, entonces que sucede con los tipos que no contienen en su estructura el termino informática(o), pues deja por fuera el comportamiento criminológico de otros delitos, que si bien no tienen este componente lingüístico si lo tienen en su comisión, medio y conducta delictiva.

En este cambio de denominación esta la evolución, desde una perspectiva criminológica, de los comportamientos ilícitos en la Red y la preocupación legal en relación con ellos, concretamente, el hecho de que pasara de ser el centro de riesgo la información del sistema informático, a serlo las redes telemáticas a las que los sistemas empezaron a estar conectados y los intereses personales y sociales que se ponen en juego en las mismas.(Miró, 2012, pág. 37)

Entonces ahora si después de ver el concepto de delito informático a cibercriminalidad, se entiende que las conductas delictivas son aúnmás diversas y comunes que un solo termino, en la que si bien se refiere al uso de la información, de equipos informáticos también viene conexo la Internet como espacio de comisión. De aquí el salto de concepción criminológica de delitos informáticos a cibercriminalidad.

Al fin y al cabo, si bien Internet, la Red más popular y a través de la cual se realizaran prácticamente todas estas infracciones, es en sí misma un medio informático y, por tanto, todos los ciberdelitos podrían entrar dentro de la categoría de delitos informáticos, con la utilización del términocibercriminalidad se pone de manifestó que sus implicaciones de riesgo van másallá de la utilización de tecnologías informáticas y se relacionan en la actualidad a

redes telemáticas, con los particulares problemas político-criminales que ello plantea en la actualidad. (Miró, 2012, pág. 38)

Descripción criminológica del termino Cibercrimen.

En pleno siglo XXI el ciberespacio es la forma de comunicación más usada por los habitantes del planeta tierra, sin embargo, aún no ha sido en pleno el estudio de lo que distingue este término a la luz del derecho penal y de la criminología. A lo que atañe esta muestra, desde la criminología.

Este punto de vista, que desvincula la criminología de las definiciones legales del delito (desde luego sin dejar de apreciar críticamente el catalogo legal de las conductas punibles), y que la aproxima a conceptos de lo divergente y lo desviado, parece ser el más adecuado para la construcción de un logo criminológico.(Fontalvo, 2014, pág. 12)

Es decir, la evolución del término cibercrimenes de origen de una tipología social divergente al orden común aprobado por las mayorías, es decir, como calificativo de conductas delictivas ejecutadas por medio del uso de la internet y las TIC, que han pasado por varias concepciones, donde inicialmente se trataba de un sujeto que delinquía usando para ello un ordenador, por lo tanto el termino también fue considerado en inglés como *computercrime*, sin embargo para la modernidad esto ha cambiado y ahora se requiere que se cometa en lo que se conoce como ciberespacio.

En la raíz de este cambio de denominación esta la evolución, desde una perspectiva criminológica de los comportamientos ilícitos en la Red y la preocupación legal en relación con ellos, concretamente el hecho de que pasara de ser el centro del riesgo la información del

sistema informático, a serlo las redes telemáticas a las que los sistemas empezaron a estar conectados y los intereses personales y sociales que se ponen en juego en las mismas.(Miró, 2012, pág. 37)

El que se pueda lograr una compresión de las posible conductas punibles que den origen a la comisión de delitos en el ciberespacio es el fin de este documento, para la generación de la internet y las TIC es importante conocer más allá de un posible tipo penal que se adecue a una conducta punible y entender cuál es el lugar o mejor aún el medio que se usa para consumar el acto.

Para entrar al tema es necesario entender el termino ciberespacio o espacio cibernético, el cual se entiende como "el espacio virtual en el cual usuarios y los programas conectados entre ellos a través de una red telemática (por ejemplo: internet) pueden moverse e interactuar con propósitos diversos…" (Guerrero, 2004).

El delito en sentido normativo y el delito en sentido tipológico, como hecho concreto con relevancia social. A partir de aquí, pues, hay que reconocer que podemos utilizar el término Cibercrimen para referirnos a un comportamiento concreto que reúne una serie de características criminológicas (también podrían ser legales) relacionadas con el ciberespacio (sentido tipológico).(Miró, 2012, pág. 40)

De aquí surge, que se den dos componentes, uno que la conducta criminal se da a través de las TIC y otro que tenga un elemento esencial del delito. A su vez, se da el uso del término cibercriminalidad, que significa el Modus Operandi de la comisión de delitos usando las TIC y el cambio Cibercrimen para una conducta especifica.

Ciberespacio y Cibercrimen, en una conducta transnacional.

La acción tradicional de realizar negocios, y de cometer delitos, como aquel que realiza una venta de acciones de su empresa en subasta electrónica o las prohibiciones penales como aquel que matare a otro, o aquel que constriña para obtener algo, o bien falsifique un documento, está enmarcado en una prueba tangible y material, sin embargo, las herramientas informáticas y las TIC han abierto la puerta a la desmaterialización.

En la medida en que se ha ido generalizando masivamente las comunicaciones realizadas con el apoyo de medios electrónicos como teléfonos, videos, redes internas, redes mundiales, etc., los negocios, las transacciones financieras y todo el tráfico mercantil han ido perdiendo, poco a poco, ese soporte "material" tradicional, aquel texto plasmado en el papel con tinta indeleble y firmado con nuestro puño y letra, que aún hoy nos deja sentir el sabor de la seguridad. Es lo que conocemos técnicamente como la desmaterialización de las comunicaciones.(Larrea, 2004, pág. 6)

Y no para menos, que se trate de enmarcar algunos punibles, que para las alianzas inter estatales, busquen proteger la vida, la economía y la seguridad mundial, su fuerte aún sigue basado en los factores de poder, el libre comercio y su protección tiene un ámbito de desarrollo normativo diferencial, donde lo primer que hace es reglar el valor probatorio de los documentos electrónicos.

Los esfuerzos de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional han generado cuantiosos frutos. En todo el mundo se van sancionando normas que regulan el tratamiento de la prueba electrónica y, especialmente, de la firma electrónica.

El primer país europeo en tener una ley específica sobre la materia fue Alemania. La comunidad Europea, entre tanto, ha aprobado múltiples decisiones acerca del comercio electrónica, como la 1692/96/CE, la 92/242/CEE, la 99/93/CE, la 94/445/CE y la 91/385/CEE.(Larrea, 2004, pág. 9)

Bueno, y para el ámbito penal y su corte criminológico, para entrar en contexto se requiere recordar a grandes rasgos algo sobre la arquitectura del ciberespacio y los principios jurídicos de las TIC.

Es decir, analizar en que cambia el ciberespacio con respecto al espacio físico, cuales son las singularidades de ese nuevo espacio que conllevan que cualquier evento social en él se caracterice de forma distinta a como lo es en el otro espacio de comunicación social. Obviamente no se pretende realizar una definición antropológico-social del ciberespacio como ámbito espacial o físico en el que tradicionalmente se han cometido infracciones.(Larrea, 2004, pág. 145)

Simplemente el concepto de en qué lugar se cometen las conductas cibercriminales, en qué lugar tienen su consumación los ataques cibernéticos, la usurpación de los datos personales, o el montaje fotográfico de pornografía donde las víctimas no han aceptado el uso de su imagen en estos videos.

Concepto de ciberespacio, frente a la arquitectura del mismo, es aquel que asevera que son metáforas geográficas o sociales, como la del propio ciberespacio, sitio web, comunidad virtual o autopista de la información, ayudan a visualizar, en términos de funcionalidad social,

lo que, en última instancia, no son más que circuitos de señales electrónicas que contienen información codificada. (Miró, 2012, pág. 146)

Sin embargo, donde comienza y donde termina el ciberespacio, seria sencillo de comprenderlo si únicamente estuviese dado en el contacto de dos personas, pero los usos de las TIC´s es a nivel mundial, con sujetos que pueden estar o no presentes en una comunicación abierta por medio del internet, que la interacción puede ser obtenida desde uno, dos o millones de usuarios, conectados virtualmente en la nube.

El ciberespacio es un espacio porque en él las personas se encuentran y relacionan, pero mientras que el espacio físico existe antes y seguirá existiendo después de que termine la relación (al menos mientras exista un observador), el ciberespacio agota su existencia en cuanto el mismo sirva para la comunicación entre los sujetos, dado que sin interacción no hay red. Así, frente al espacio geotécnico como la tierra, que existe independientemente de los actos de la gente que tengan lugar en ella, y que solo puede ser ocupado a la vez por un mismo ente, el ciberespacio existe en cuanto en él se interacciona y es posible que sea ocupado por muchos entes al mismo tiempo.(Miró, 2012, pág. 146)

Por tanto se debe comprenden que el ciberespacio, es el lugar donde existe múltiples comunicaciones simultaneas, que no deja de existir por el hecho que el delincuente cibernético no se conecte hoy a su red social favorita, o por el contrario, este lugar no deja de existir si la oficina de seguridad de la naciones unidas lo interviene para realizar una búsqueda selectiva en bases de datos.

El ciberespacio, en todo caso, convive con el espacio físico o terrestre, y también tiene, en algunos aspectos, una relación directa con él que no debe ser obviada: las redes telemáticas que conforman el ciberespacio vienen a unir, de forma virtual pero también física, terminales o sistemas informáticos que están ubicado en espacios terrestres concretos en países nacionales determinados con contextos sociales de facilitación del acceso a Internet específicos, así como regímenes jurídicos distintos que pueden afectar, por ejemplo, a las obligaciones de los prestadores de servicios respecto a la identificación de los titulares de las direcciones IP. (Miró, 2012, pág. 147)

Un ejemplo, en el sistema financiero, que se supone es la forma segura para los ciudadanos de administrar su dinero, y además la manera que tiene el estado de controlar el flujo dinerario de sus miembros, con el fin de evaluar la cuota de ingresos y endeudamiento, el comportamiento de la economía y la efectividad en la prevención de lavado de dinero y financiación del terrorismo. Resultado de la apertura y globalización económica que nace junto con la constitución política de 1991 en Colombia, los establecimientos bancarios abre sus servicios en Redes Sociales, Banca Móvil (desde el teléfono celular) y por internet con obtenga su clave segura para transacciones "online" en línea, todo lo anterior con el fin de llevar los servicios más cerca del cliente, lo que muestra que el desplazamiento físico deja de ser un requisito para realizar sus transacciones con éxito.

Es por lo anterior, como una pequeña muestra que, la distancia deja de ser un obstáculo, por tanto, para la comunicación en el ciberespacio, de modo que esté donde esté el sujeto al que va dirigida la acción en Internet, el coste de realización es exactamente el mismo, dado que la distancia física no tiene relevancia en el ciberespacio.(Miró, 2012, pág. 148)

En línea con la globalización económica, se incentiva el uso de la tecnología y de las transacciones virtuales, la mejora constante y facilidad que brindan los establecimientos bancarios a sus clientes es el fuerte de la competencia, más allá de las tasas de interés, es necesario evitar a los clientes las largas filas para realizar sus transacciones bancarias, el internet y la masificación de esta herramienta no solo como una red social para amigos, sino para la perfección de contratos, compras y ventas, pago de servicios públicos; también hace que la mente criminal use este medio para la comisión de delitos sin usar su cuerpo en un espacio físico determinado donde se encuentra el objeto de su crimen.

Y después de hacer un recorrido por un lugar intangible, ahora bien es necesario comprender que principios jurídicos rigen las TIC, en las cuales según lo dice Cárdenas:

> La neutralidad Tecnológica. Este principio propende, porque las normas puedan abarcar las tecnologías que propiciaron su reglamentación, así como las tecnologías que se están desarrollando y las que están por desarrollarse. En tal sentido constituye una parte importante del segundo pilar de interpretación legal, por cuanto, e la concreción real y necesaria del entorno dentro del cual la ley va ase aplicada.
>
> Buena Fe. Este principio es simplemente una reafirmación del fundamento que informa a nivel general todo el derecho, en especial cuando se hace referencia al intercambio nacional o internacional de bienes y servicios. Cuando hablamos de comercio electrónico este principio adquiere especial relevancia por cuanto las características del intercambio que se realiza por medio de los

soportes tecnológicos están fundamentadas en la confianza entre los contratantes.

Libertad contractual. Esto es más una manifestación o consecuencia necesaria del principio sobre la inalterabilidad del derecho preexistente, frente a las TIC, siendo este un derecho que se debe contextualizar en el marco de la libertada de empresa, de la autonomía privada y de la libertad de competencia. La innovación tecnológica persistente respecto de la facilitación del acceso a Internet ha auxiliado a la expansión de las nuevas tecnologías y la actividad comercial por vías electrónicas, haciendo que la población tenga la posibilidad de participar de las ventajas de transacciones comerciales electrónicas y que las empresas – entre ellas las pequeñas y medianas – puedan compenetrarse en el proceso virtual con aumento de competitividad y escala. Ante esta realidad, como operadores jurídicos estamos obligados a asumir esta realidad, como nos es dada, para que hagamos algo con ella.

No modificación del régimen del derecho de las obligaciones y los contratos privados. El comercio electrónico no implica una modificación sustancial del actual derecho de las obligaciones y los contratos, esto teniendo en cuenta que la electrónica y su aplicabilidad jurídica sobre todo tipo de transacciones, es simplemente un nuevo soporte y medio de transmisión de voluntades negóciales o prenegociables. Por ello no puede modificarse el derecho preexistente referente a la perfección, desarrollo y ejecución de los contratos.

> Sin embargo no se puede negar que la generalización en la utilización del comercio electrónico en relación con determinados contratos, ha determinado un cambio en el derecho aplicable, y esto como consecuencia, en muchas oportunidades, del vacío jurídico que se presenta al momento de identificar los problemas y soluciones de los aspectos más destacables del comercio electrónico.
>
> Equivalencia funcional de los actos electrónicos. El principio de la equivalencia funcional de los actos jurídicos celebrados a través de medios electrónicos respecto de aquellos actos jurídicos suscritos en forma manuscrita, e incluso oral, constituye el principal fundamento de la interrelación del derecho con las nuevas tecnologías. Dicho principio se puede simplificar de la siguiente forma: la función jurídica que cumple la instrumentación escrita y autógrafa respecto de todo acto jurídico, o su expresión oral, la cumple de igual forma la instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, extensión, alcance y finalidad del acto así instrumentado.
>
> Es así como, este principio constituye la base fundamental para evitar la discriminación de los mensajes de datos electrónicos con respecto a las declaraciones de voluntad expresadas de manera escrita o tradicional.(Rincon, 2015, págs. 81-84)

Lo anterior, permite que se tenga un mínimo de garantía jurídica frente a las TIC, se observa un fuerte desarrollo en el ámbito del derecho comercial electrónico y no se nota un despliegue en el ámbito penal, pero es una gran herramienta, que se debe contemplar como los

principios mínimos y garantías para los que ejercen este tipo de contactos por medio del ciberespacio, por tanto, se infiere que la globalización económica si se ha preocupado por garantizar unos mínimos círculos de aplicación y se ha pronunciado sobre qué condiciones de aplicación del derecho privado se manejan igual. Un gran ejemplo la buena fe, que para el ámbito penal podría ser similar a actual sin dolo.

Entonces después de conocer los principios jurídicos de las TIC y su aplicación se pude llegar a la afirmación, que el ciberespacio es un nuevo espacio, estamos anticipando la respuesta sobre la incidencia del ámbito en la otra dimensión, el tiempo. Internet también cambia el tiempo, su percepción social, así como la forma en la que el mismo tiempo se organiza. La contradicción del espacio conlleva, en primer lugar, un aumento de la importancia del tiempo, y en segundo lugar, una comprensión del tiempo necesario para la comunicación social. El tiempo necesario para la comunicación entre dos personas separadas pro un espacio físico también se contrae ante la ausencia de la distancia y la aparición de un espacio virtual de intercomunicación inmediata.(Miró, 2012, pág. 148)

Entonces las conductas punibles consumadas en el ciberespacio se trataran bajo el estirpe de condonación Cibercrimen, si bien es cierto no con el suficiente desarrollo criminológico y normativo de la creciente oleada de las comunicaciones masivas e internacionales que se envuelven el termino Cibercrimen.

Por esto, el Cibercrimen o ciber delito se define como aquel delito cuya característica esencial es el rol central que las TIC juegan en su comisión. El mero hecho que el delito se ejecute utilizando internet, dota la conducta de unos caracteres de riesgo delictivo y riesgo penal distintos a los de las infracciones penales ejecutadas en el espacio físico-real, entonces

debe entenderse, como aquí se hace que la categoría debe abarcar a todas ellas: sean las infracciones nuevas en su esencia o tan solo en los medios; sean las TIC el objetivo, el medio o el lugar de ejecución; y sean los bienes jurídicos afectados tan dispares como el patrimonio, la seguridad nacional o la indemnidad sexual de los menores.(Miró, 2012, pág. 148)

Respecto a lo que atañe esta investigación se hablara de la comisión de delitos informáticos como se ha llamado clásicamente, pero ahora se sobre entiende que va más allá de ser un sistema informático, también es telemático y de la información, el Cibercrimen.

Puede pretenderse que se configure delitos bajo esta tipología como un ejemplo a continuación: se entiende como delitos contra el patrimonio económico, las posibilidades de fraude informático que podría concretarse en el tipo penal que se configura como el daño en bien ajeno, el abuso de confianza, la estafa, el hurto simple o calificado y de peculado entre otros, los cuales deben ajustarse a un tipo de conducta "ilícita informática". Los perjuicios eminentemente materiales serán en favor de la persona natural o jurídica que haya resultado perjudicada y desde luego por quien ha sido declarado penalmente responsable.(Santos, 1993, pág. 56)

Al pasar del tiempo la lucha contra la comisión de delitos cometidos en el ciberespacio han abarcado marcos normativos nacionales e internacionales, sin embargo al parecer aún se queda corta la importancia del estudio criminológico de esta conducta en el margen de lo transnacional, como un sujeto desde un Estado puede interactuar con la información de otro Estado que se encuentre al otro lado del hemisferio.

Es por esto que, la transnacionalidad del ciberespacio se traduce, a los efectos que nos interesan, en la total ausencia, para la comunicación e interacción entre individuos, de barrera que no sean impuestas o configuradas por el propio sujeto. Desde cualquier Estado nacional es posible acceder a cualquier Estado nacional, y un contenido vertido en una página web localizada en un servidor de un Estado concreto y colgada por un sujeto de un determinado Estado, puede ser vista por cientos de personas en cientos de sitios distintos en el mundo. (Miró, 2012, pág. 154)

Siendo así las cosas, en la era de las TIC, también surge el término de riesgo delictivo, para lo cual desde las políticas internas de los países como tratados de estirpe internacional han tratado de poner un grado prevención y de punibilidad a un posible daño causado que se origina a través de la cibercriminalidad.

Así, y bien podemos encontrar en los últimos diez años interesantes estudios de criminología aplicada a la cibercriminalidad en las que se manejan teorías como la del autocontrol, la decisión racional, la del aprendizaje social, el control social o el etiquetamiento, gran parte de los estudios criminológicos que tratan de comprender el crimen en Internet y de, incluso, definir los caracteres particulares de este evento por el hecho de llevarse a cabo en el ciberespacio, toman en consideración para su estudio, tal y como he analizado un trabajo reciente, la teoría de las actividades cotidianas de Choen y Felson.(Miró, 2012, pág. 163)

Es decir que no se escapa del Cibercrimen un hogar común, un usuario de internet móvil desde su equipo celular, las empresas, los conglomerados internacionales, las ONG, y los estados, todos los que interactúen en el ciberespacio están a la distancia de un clic de

cometer un ciber delito o ser víctimas de ellos, en un entorno universal con diferentes normatividades y múltiples culturas, lo que para algunos es permitido para otros es condenable.

Lo anterior porque como lo dice Miro:

> Internet no está sometido a las leyes nacionales de un único país, ni unas normas propias aceptadas por todos los que la conforman, y esto conlleva que los controles gubernamentales resulten poco efectivos, al existir variadas formas de evitar los que va imponiendo los Estados Nacionales. Es obvio, sin embargo, que la existencia de este espacio trasnacional, neutro y distribuido, con las consecuencias que conlleva, produce una tensión, en este caso en el plano jurídico, con la casi contradictoria existencia de Estado nacionales con legislaciones distintas reguladoras de este u otro fenómeno. Si bien no existe un control global de la Red, los gobiernos nacionales han comenzado a tratar de regular Internet ante el potencial riesgo que supone y su popularización en todas las escalas sociales. Estos controles van desde el propio acceso a Internet hasta el responsabilizarles de lo publicado en este gran medio de comunicación, y sobre las que trataremos más adelante. En todo caso, la adopción de decisiones nacionales apenas soluciona el problema, como es obvio. El potencial riesgo que supone la transnacionalidad del Cibercrimen y que le convierte en uno de los mayores desafíos planteados en la actualidad, deriva de lo complejo que resulta responder localmente a riesgos globales. Y mientras que el mundo parece encogerse y el crimen cometido desde “el edificio de al lado” se perpetra

> hoy desde otro continente, los Estados, sus normas y las instituciones que las aplican aún se diferencian entre sí y no logran conjugar lo que no se puede más que considerarse un “problema común”.(Miró, 2012, págs. 155,156)

La Importancia de quien es víctima en el Ciberespacio y la prevención del Crimen

Como se conoce, el derecho penal ampara a las personas, quienes son poseedores de derechos fundamentales, sin embargo, cuando se expone a la ampliación de la cobertura a personas jurídicas, se observa que el concepto de un delito penalizado en la última ratio pasa a ser de un uso común. Frente a las organizaciones de macro infraestructura tecnológica que determina políticas de prevención de riesgos a sus usuarios, frente a un delincuente común individual o que también puede pertenecer a organizaciones estructuradas de criminalidad.

Entonces aparecen los riesgos propios de la actividad electrónica. Garantizar la seguridad en medios electrónicos, es quizá el problema más significativo para las personas interesadas en efectuar operaciones de comercio electrónico. En un enfoque más amplio, la confidencialidad, la autenticidad, la integridad, la disponibilidad y el no repudio son los principales problemas que afectan a los documentos electrónicos.(Rincon, 2015, pág. 129)

Lo anterior para delimitar un trozo de las potenciales víctimas, aquellos que se dedican al comercio, sin embargo, aquellos que son usuarios de redes sociales, y otros tantos que únicamente están obligados a transitar en las TIC como caminar por la calle de las grandes urbes para entrar en contacto con su contexto.

Es decir que, en el mundo podemos hablar de aproximadamente mil millones de usuarios y por tanto, de millones de objetivos sobre los que pueden actuar los criminales. Y es que si bien hubo un momento en que los sistemas informáticos era únicamente utilizados por empresas o instituciones públicas, y el acceso a los mismos era muy limitado, en las últimas décadas se ha producido una popularización de la informática, un aumento de las facilidades

para adquirir o acceder a terminales y, muy especialmente, la interconexión entre todas ellas en un espacio de comunicación global que también se ha generalizado.(Miró, 2012, pág. 157)

Es de comprender que el derecho penal protege en primera instancia a los seres humanos víctimas directas y pero el desarrollo de los delitos informáticos son proclives a la protección de personas jurídicas. Sin embargo, para cual fuese el caso, respecto a la judicialización del delincuente que cometiere un Cibercrimen, existe una difícil identificación en virtud de la colaboración de la Internet para conservar el anonimato, y/o aceptar seudónimos para usar y crear cuentas de acceso a información.

Es por esto que, pese a que desde algunos sectores se está intentando construir algún tipo de sistema que permita la identificación de los usuarios en la Red, parece, al menos de momento, difícil de imaginar un ciberespacio en el que todos o la mayoría de los que intervienen en el estén identificados. Tal y como lo conocemos en estos momentos, el ciberespacio es un ámbito que favorece el anonimato del sujeto que interviene en el por lo menos en comparación con el otro ámbito de comunicación social, el físico.(Miró, 2012, pág. 158)

No es de desconocer que el desarrollo tecnológico y preventivo por parte de los Estados y de las empresas, en búsqueda de minimizar las condiciones de anonimato, no son las óptimas, si bien es cierto se habla de cuentas autenticadas y de la dirección IP de los usuarios, los café internet, el acceso wifi y los Smartphone superan estas condiciones de identificación fehaciente a la material.

Aunque se diga que, el anonimato no es ya una característica de Internet al ser cada vez más sencilla la identificación de las direcciones IP, lo cierto es que sigue siendo en la actualidad más compleja, pese a los rastros digitales del delito, la identificación de los autores de esta conductas que la de otros sujetos que cometen similares infracciones per en el mundo real. Y todas las teorías criminológicas aseveran, que la percepción de que la actuación se realiza en el anonimato conlleva un aumento de la sensación de impunidad y esta, a su vez, un incremento del riesgo de que el agente acabe por ejecutar el delito.(Miró, 2012, pág. 158)

Es por lo anterior, que todos temen al ciberdelincuente anónimo, el hecho de pensar que difícilmente se encontrara el verdadero rostro del receptor o emisor, hace que la víctima juegue un papel importancia en su propio cuidado. Es decir, toma fuerza la frase de: "no te metas en mi facebook".

Generalmente, se alude a la diferenciación entre los mecanismos de prevención del delito de tipo estructural, psicológico y circunstancial, según se atienda respectivamente a las consideraciones económicas, sociales y políticas que condicionan la delincuencia, a los elementos conductuales y cognitivos relacionados con el sujeto que puede llevar a cabo el crimen. (Miró, 2012)

Es un poco contradictorio, puesto que toma bastante relevancia el hecho de que la víctima obre en debida diligencia de prevención y acepte o no ciertos estamentos de interacción en el ciberespacio. Algo así como para que no le hurten el celular en la calle no lo saque mientras camina por ella.

Son tres factores que hacen que la víctima adquiera una especial importancia para la explicación y prevención del delito en el ciberespacio. El primero,… gran capacidad para

dejar fuera del ámbito de riesgo aquello que no quiere que se vea afectado…; segundo: define su interacción en el ciberespacio el grado de visualización de sus objetivos y, por tanto, las posibilidades de contacto con un agresor…. Tercero: la víctima es la única que puede incorporar guardianes capaces para su autoprotección. (Miró, 2012, pág. 192)

Y como en los delitos de masa, se selecciona un grupo de personas, que aunque ostenten derechos individuales, también se segrega en la eficacia y el fin de comisión del delito contra ellas, es decir en el Cibercrimen también opera una selección de víctimas.

En, los estudios analizados ponen de manifestó que hay factores demográficos también relevantes a la hora de la mayor o menor victimización: en los Estados Unidos se confirma que las personas de raza blanca tienen un mayor riesgo de victimización, y lo mismo ocurre en general con los varones frente a las mujeres, lo cual, por otra parte, de nuevo acercándonos a la TAC, se corresponde con la frecuencia de uso de Internet y la duración del tiempo pasado en el ciberespacio, que son mayores en los varones, como se muestra en la tabla basa en el estudio de Alshalan. Es cierto, sin embargo, que la diferencia entre el tiempo de uso de Internet entre hombres y mujeres…. Por lo cual debiese tenerse en cuenta el tipo de actividad cotidiana online. (Miró, 2012, pág. 193)

Y no se puede pasar por alto, que de las víctimas más selectas son los Estados, bien sea por interés de datos de seguridad nacional, espionaje y simplemente competencia económica.

El concepto de ciberdefensa como modalidad distinta. Tomado como definición la contenida en el documento Conpes 3701 de 2011, se entiende como ciberdefensa la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. Por tanto si ciberseguridad y la ciberdefensa se encargan de

proteger y garantizar que la información no se vea afectada por ningún tipo de amenazas informáticas, entendidas como la aparición de una situación potencial o actual donde una agente externo tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política de un Estado.(Rincon, 2015, pág. 428)

El desarrollo tecnológico para el Estado Colombiano, se espera que sea más versátil que otros modelos de competencia, la seguridad soberana está en manos ya no solo de grupos armados al margen de la ley que empuñan sus fusiles por los campos, o por aquellas organización de delincuencia común que trafican con narcóticos en las calles, sino que estos mismo y otros, pueden buscar un ataque directo al presupuesto nacional y además filtran todos los sectores financieros con transacciones de comercios indebidos.

Desarrollo Normativo Colombiano y aportes Jurisprudenciales a las conductas Cibercriminales.

En nuestra legislación colombiana (Ley 599 de 2000) encontramos el Título VII, en el cual aparecen los Delitos contra el Patrimonio Económico, pero para ser más precisos y haciendo referencia a los Delitos Informáticos, los cuales son objeto de esta investigación se puede evidenciar que el Título VII BIS denominado "De la Protección de la Información y de los datos", adicionado por el artículo 1 de la Ley 1273 de 2009, fue agregado con la finalidad de preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (Código Penal Colombiano, 2015)

A continuación nos permitimos relacionar los artículos consignados en el Título VII BIS del Código Penal:

- Art. 269A - Acceso Abusivo a un sistema informático: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- Art. 269B – Obstaculización ilegítima de sistema informático o red de telecomunicación: El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a

1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- Art. 269C – Interceptación de datos informáticos: El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
- Art. 269D – Daño Informático: El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- Art. 269E – Uso de Software malicioso: El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- Art. 269F – Violación de datos personales: El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa

y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Art. 269G – Suplantación de sitios de web para capturar datos personales: El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

  En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

  La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.
- Art. 269H – Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

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

  2. Por servidor público en ejercicio de sus funciones.

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

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

5. Obteniendo provecho para sí o para un tercero.

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

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

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

- Art. 269I – Hurto por medios informáticos y semejantes: El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.
- Art. 269J – Transferencia no consentida de activos: El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

> Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Para la época actual en Colombia y en el mundo se debe reconocer, que el Derecho debe ir de la mano con los avances tecnológicos que día a día van teniendo un gran impacto en la sociedad, precisamente por convertirse en elementos esenciales de comunicación y de manejo de la información. Dentro de estos avances encontramos Internet, que como lo asegura (Prada, 2012, pág. 17), nació en el ámbito militar para garantizar la seguridad y la continuidad de las trasmisiones, utilizando inicialmente un sistema de conexiones entre ordenadores, lo cual con el transcurrir del tiempo evolucionaria hasta convertirse en una inmensa Red compuesta de servidores, clientes, nodos, redes locales, cables, satélites entre otros. Con lo anterior podríamos concluir que Internet hace parte de esta nueva tecnología digital, que se mueve en el Ciberespacio donde precisamente actúa el mundo digital y mundo físico, pero al tratarse de un medio tan amplio, que no tiene principio ni fin, se hace necesario reglamentar de manera específica cada conducta que vaya en contravía del bien jurídico tutelado.

La criminalidad informática como lo menciona (Prada, 2012, págs. 22, 23, 25), es uno de los efectos generados por las nuevas tecnologías de la comunicación, que han creado una nueva dimensión del espacio que no es tangible o sensorial sino virtual, donde circula información a través de canales informáticos, pero para entender esta nueva modalidad delincuencial es necesario mencionar tres presupuestos; el primer presupuesto se refiera a la interactuación entre el espacio virtual y el real, donde aparece la fuerza de Internet y su

potencialidad ofensiva sobre los bienes jurídicos protegidos por el espacio real, pero sensibles a ataques de un espacio nuevo y poco conocido; el segundo presupuesto se basa en la vulnerabilidad de bienes jurídicos como consecuencia de la interconexión entre espacio virtual y real, por lo tanto se necesita regular el uso del ciberespacio con normas técnicas y jurídicas que garanticen los principios y valores de los modernos ordenamientos jurídicos y como tercer presupuesto parte de la dificultad de tipificar penalmente las conductas que deben ser sancionadas en el ciberespacio.

De la jurisprudencia, hasta el momento no se ha encontrado el termino Cibercrimen, como un factor de consideración previa. Sin embargo se citará algunas sentencias en las cuales se hace referencia a algunos derechos fundamentales y posible vinculación de medios de comunicación de la información.

Derecho a la protección de datos personales unido al derecho fundamental de la intimidad. Magistrado Ponente Alejandro Martínez Caballero:

> El artículo 15 de la constitución relativo al derecho a la intimidad, contiene una zona de reservar para la propia persona, de la que quedan excluidos los demás, a menos que la persona protegida decida voluntariamente compartir dicho ámbito. Contiene dicho artículo, entre otros, los derechos a la intimidad personal y familiar, al buen nombre, al habeas data y a la inviolabilidad de la correspondencia y demás formas de comunicación privada. Todos estos derechos están unidos por su finalidad, cual es la de aislar a la persona de las injerencias de terceros, así como proteger su imagen.(Caballero, 1992)

Ahora, se tomara una parte de la Sentencia del Magistrado Ponente Ciro Angarita Barón, que habla sobre el derecho a la protección de datos personales unido al derecho fundamental a la libertad:

> Se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad. Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extra patrimonial, inalienable e imprescriptible y que se pueda hacer valer erga omnes, tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Esta Sala no vacila en reconocer que la prevalencia del derecho a la intimidad sobre el derecho a la información, es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial, a la vez, del Estado social de derecho en que se ha transformado hoy Colombia, por virtud de lo dispuesto en el artículo 1 de la Carta de 1991.(Barón, 1992)

Se evidencia que el fuerte del desarrollo jurisprudencial es el Derecho Fundamental del Habeas Data, como lo expresa también la Sentencia del Magistrado Ponente Alex Julio Estrada, donde la corte resume tres supuestos básicos para tutelar o no este derecho:

Tanto para la autodeterminación de la información, como para el principio de libertad, el consentimiento es el punto de identidad y relevancia que determinará la vulneración o no del derecho fundamental al habeas data. Ahora bien, en materia de autorización, el

consentimiento otorgado al encargado del tratamiento de autorización, el consentimiento debe ser previo, expreso e informado y, por el contrario, la publicidad indiscriminada de la información sobre datos personales sin el cumplimiento de los requisitos antes descritos configura una finalidad ilegal y/o inconstitucional que facilita la vulneración de derechos fundamentales. En este orden de ideas, cabe destacar que el consentimiento del titular de la información sobre el registro de sus datos se encuentra ligado a la necesidad de que aquel cuente con oportunidades reales para ejercer sus facultades de rectificación actualización durante las diversas etapas de dicho proceso, que resultan vitales para salvaguardar los derechos a la intimidad y al buen nombre. En conclusión, compete a los jueces, en cada caso, analizar el contenido de la autodeterminación y el principio de libertad así como el cumplimiento de los requisitos dispuestos en la ley y la jurisprudencia, a fin de no incurrir en alguna violación de derechos fundamentales. Dichos requisitos se pueden sintetizar en: (i) obtener el consentimiento del titular de la información, (ii) tal consentimiento debe ser calificado, es decir, expreso, informado y previo, (iii) el tratamiento de la información se debe realizar para las finalidades informadas y aceptadas por el titular del dato, (iv) el responsable del tratamiento le corresponde obtener y conservar la autorización del titular.(Estrada, 2013)

Situaciones paradigmáticas, típicos modelos, para comprobar los límites del manejo y desarrollo del concepto Cibercrimen.

En un posible ejercicio de simulación de hechos punibles cometidos en el ciberespacio a continuación algunos casos donde se reflejan las conductas que usualmente podrían afectar de una u otra forma bienes jurídicamente tutelados por medio del cibercrimen:

1. Uno de los autores, es el titular de una tarjeta de crédito que aprovecha la confianza depositada por el banco al expedirle debidamente dicha tarjeta para retirar avances en efectivo a través de varios cajeros automáticos, en complicidad de un funcionario de la red bancaria (segundo autor) que desbloqueo la tarjeta en más de 50 oportunidades para facilitar los retiros, haciendo uso de todas la claves genéricas que se le habían confiado para borrar toda la información relacionada con las transacciones. Conducta que podría relacionarse al tipo penal de Hurto Calificado y Agravado.
2. A una persona se le encuentran 15 microfichas de la relación diaria de saldos para autorizaciones, 69 microfichas de extractos de las tarjetas que corresponden a la información de los cuentahabientes de la entidad financiera defraudada, 668 tarjetas involucradas, con las cuales se hicieron retiros en efectivo en 6000 ocasiones y en tan solo un fin de semana, clonando así la información en la banda magnética con datos reales y permitiendo establecer que dicha información fue proporcionada por personal de la entidad bancaria.
3. El sujeto activo de la conducta tramito la apertura de dos cuentas de ahorro y procede a efectuar retiro con volantes de la oficina bancaria en cajeros automáticos,

transfiriendo fondos a otras cuentas de las que no era titular. Presentándose una falsedad material de cedulas y tarjetas débito alterando las pistas magnéticas.

4. En la jerga de la red el Hacker es un intruso o pirata informático que posee conocimientos a fondo de sistemas informáticos, lenguajes de programación y protocolos de Internet a los cuales acude navegando en los mares de Internet, su conducta consiste en desplegar una seria de comportamientos con la finalidad de obtener acceso o interferencia no autorizada a un sistema informático o una red de comunicación electrónica de datos(Prada, 2012, pág. 66). Con lo anterior vale la pena reflexionar sobre la siguiente conducta que a la vista pública no sobrepasa los esquemas del delito: el alumno que con intenciones de variar sus calificaciones, accede a los sistemas de información de su universidad sin estar autorizado, este alumno posee grandes conocimientos en la materia y sabe cómo se puede ingresar y como se puede modificar dicha información.
5. Con la expansión de Internet ha incrementado en cantidades alarmantes los delitos contra la libertad sexual de menores, teniendo en cuenta que estos menores ahora tienen más acceso a la tecnología y a las redes sociales, lo cual permite que los rangos de comunicaciones sean más amplios e inseguros, porque en algunos casos los intervinientes no siempre están debidamente identificados con información real. (Prada, 2012, págs. 238, 239), de acuerdo a lo anteriormente señalado, que nos garantiza que no se esté utilizando material pornográfico en la red con la intensión de que un menor ingrese y llegue a realizar conductas sexuales, como la exhibición lasciva de los genitales.

Conclusiones

Siendo así las cosas, se considera que aún existe confusión al nombrar Cibercrimen, puesto que generalmente se asocia con delitos informáticos y no es correcto, se concluye que el término Cibercrimenes mucho más amplio que la tipificación de hoy en el ordenamiento jurídico, teniendo en cuenta que desde los datos personales hasta la seguridad nacional de un estado es vulnerado por esta conducta realmente divergente dentro de la tradicional, lo cual afecta directamente la política criminal del Estado, puesto que si no sabe que debe tipo de punibles debe prevenir tampoco sabrá cómo debe de penalizarlos.

Que el lugar y la temporalidad del ámbito de la comisión de conductas punibles dentro de lo conocido como Cibercrimen, corresponde a una arquitectura de ciberespacio inmaterial y de comisión inmediata, puesto que rompe los supuesto de un lugar tangible y la temporalidad es casi invisible, se ajusta a la comisión del acto, en muchos casos anónimo, mediante una Red y el abarcamiento de la TIC, que facilita al ciberdelincuente alcanzar su objetivo a cientos, miles o millones de kilómetros de distancia.

Además que no solo con un buen cuidado por parte de la víctima, (persona natural, jurídica, ONG y Estados), es decir valorando los riesgos y previniéndolos por medios de técnicas de seguridad, se podría llegar a excluir el comportamiento criminal del ciberdelincuente de su ámbito de acción.

Se observa que aun el desarrollo legal y jurisprudencial respecto al término, es corto por su amplio ámbito de comisión, por lo difícil de probar, y lo difícil de ubicar, realmente es una latente de temor entre los usuarios que conocen de los riesgos, como los son las oficinas de seguridad de los Estados, los emporios financieros y todos aquellos que utilizan las TIC

para mantenerse en comercio y en contacto gubernamental y diplomático. Pero aún falta mucho por implementar sobre todo a aquellas personas naturales que solo como usuarios y ciudadanos de una comunidad transitan libremente desconociendo los riesgos reales que está corriendo y por tanto tampoco cuenta con el desarrollo tecnológico para poder asegurar su conexión contra ciberdelincuentes.

Con lo citado en este párrafo, se comprueba que el aún es desconocido el carácter tipológico del termino cibercrimen, puesto que no saben aún el abanico de punibles que pueden cometerse en el ciberespacio y prueba de esto, es la jurisprudencia sigue omitiendo el uso de este término.

Referencias

Baratta, F. (2003). *Sistemas Penales y problemas sociales. Los mass media y el pensamiento criminológico.* Valencia: Tirant Lo Blanch.

Código Penal Colombiano. (2015). Bogotá: Legis.

Fiscalia General de la Nacion. (26 de 02 de 2015). Recuperado el 10 de 09 de 2015, de www.fiscalia.gov.co: http://www.fiscalia.gov.co/colombia/noticias/destacada/cibercrimen-cuesta-mas-de-usd113-billones-al-ano-a-los-usuarios/

Fontalvo, J. R. (2014). *Criminología - Un enfoque humanistico.* Bogotá: Temis S.A.

Francesc, B. (2003). *Sistemas Penales y problemas sociales. Los mass media y el pensamiento criminológico.* Vaencia: Tirant Lo Blanch.

Guerrero, M. F. (2004). *La ciberdelincuencia.* Bogotá: Instituto de estudios del ministerio público.

Larrea, J. (2004). *La prueba electronica.* Bogotá: Temis.

Miró, F. (2012). *El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.

Prada, I. F. (2012). *Criminalidad Informática.* Valencia, España: Tirant Lo Blanch.

Revista de Ciencias Humanas - UTP N°20. (05 de 2000). Recuperado el 20 de 09 de 2015, de Revista de Ciencias Humanas - UTP N°20 Análisis de contenido cualitativo y cuantitativo: http://www.utp.edu.co/~chumanas/revistas/revistas/rev20/gomez.htm

Rincon, E. (2015). *Derecho Electronico y de Internet.* Bootá: Legis S.A.

Santos, J. E. (1993). *Fraude Informatico en la Banca.* Bogotá: Lerner Ltd.

Sentencia T-058, 085 (Corte Constitucional 2013).

Sentencia T-412, 412 (Corte Constitucional 1992).

Sentencia T-414, 414 (Corte Constitucional 1992).