CIBERCRIMEN
UNA APROXIMACIÓN A LA DELINCUENCIA INFORMÁTICA

Por:

Amir Nayi Abushihab Collazos

Universidad Santo Tomás.

CYBERCRIME
AN APPROACH TO CYBER CRIME

By:

Amir Nayi Abushihab Collazos

Santo Tomás University

Resumen.

La educación, las entidades financieras y bursátiles, la administración e, incluso, la seguridad social, son sectores que no podrían funcionar sin las tecnologías que representan los sistemas informáticos. Esta importancia, es la que le da a las tecnologías de la información y la comunicación la legitimidad de ser protegidas mediante el derecho penal.

Abstract.

Education, financial and securities institutions, administration and even social security, are sectors that could not function without the technologies that represent computer systems. That importance is what gives to the information and communications technologies the legitimacy of being protected by the criminal law.

Palabras clave.

Derecho Penal; Informática; Telemática; Delito Informático; TIC; Sistema Informático; Bien Jurídico.

Key words.

Criminal law; Computing; Telematics; Cyber Crime; ICT; Information system; Legal asset.

Contenido

I. INTRODUCCIÓN. PLANTEAMIENTO DEL PROBLEMA.

Siglo XXI, nos encontramos en una época en donde la tecnología está en todos lados, en nuestras casas, en las calles de nuestras ciudades, en nuestros colegios, universidades, y en prácticamente todos las ámbitos de la sociedad moderna. Su influencia es mayor en la medida en que transcurre el tiempo, convirtiéndose en un elemento fundamental, básico e irremplazable, el cual le agrega un valor inusitado al desarrollo de nuestras actividades cotidianas. A través de la tecnología podemos obtener todo tipo de información; encontramos diversas maneras de entretención y esparcimiento; nos permite relacionarnos de un modo en el que hace solo algunas décadas era impensable; nos habilita para realizar todo tipo de trámites ante todo tipo de personas; adquirimos y vendemos bienes y servicios; trabajamos y aprendemos; en la tecnología descansa la forma en que las empresas operan y funcionan, tanto en el sector privado así como las entidades públicas; es a través de la tecnología que encontramos la forma de suministrar servicios básicos como son el de electricidad, agua, telefonía y cómo funcionan los hospitales que garantizan la salud y la vida de todas las personas[1].

[1] Al respecto, Vasquez A. (2.012), recurre a Nicholas Negroponte para describir al ser humano inmerso en una nueva era digital a través de lo que este último denomina como *"Homo Ciber Sapiens"* e indica como la era digital se sobrepone al ser humano. Específicamente indica: "Si volteamos a nuestro alrededor, **no es difícil advertir, que nos encontramos inmersos en un mundo digital, totalmente diferente, plagado de avances tecnológicos que facilitan la vida del hombre pero a la vez, lleno de retos, que nos obligan al conocimiento y a la vez genera nuevos cambios y mayores transformaciones, entre las cuales, definitivamente se encuentran las de tipo jurídico** y hay autores que plantean la posibilidad de contemplar al ser humano ya no únicamente como el Homo Sapiens Sapiens, sino como **el Homo Ciber Sapiens, término acuñado por Nicholas Negroponte, en su obra "Ser Digital", para catalogar al ser humano inmerso en la era digital.**

Ahora bien, pensemos, ¿Qué ocurriría si los semáforos colapsaran y una ambulancia no llegara a tiempo?, ¿Qué pasaría si alguien robara nuestra información y se hiciera pasar por nosotros sin que lo sepamos?, ¿Es esto posible?, ¿Podría ocurrir esto? Y lo cierto es que en la actualidad no es algo meramente posible, sino que es una realidad y un riesgo de constante ocurrencia.

Estos riesgos son perfectamente posibles en una sociedad tecnológica como en la que nos encontramos y esto puede afectar desde a una persona, una familia, un organismo público, una empresa, una entidad financiera, un hospital y hasta a una planta de energía nuclear. Esto mismo, lo afirma Negroponte (1.995) cuando desde décadas anteriores logró describir con perfecta exactitud el fenómeno en el cual nos encontramos actualmente. En el maravilloso epilogo de su obra afirmo:

*"Soy optimista por naturaleza. Sin embargo**, toda tecnología o avance científico tiene su lado menos positivo**, y ser digital no es una excepción. **La***

Las Nuevas tecnologías se entrelazan con la modificación de distintos componentes del régimen jurídico, de valores, principios, conceptos, normas reguladoras; con la aparición de nuevas modalidades en la creación del derecho y con cambios de puntos de vista sobre sus fuentes, su naturaleza y contenido, sus modos de organización y funcionamiento.
Asimismo, se debe tener presente que una de las aportaciones más importante en materia digital, es la Internet, a través del correo electrónico, páginas web, negocios cibernéticos, redes sociales y redes en general en todo el mundo entre otros muchos usos. Un aspecto que debe destacarse, es que los usuarios de la Internet, o conocidos también como cibernautas, en un inicio, fueron empíricos en el uso de las nuevas tecnologías, pero actualmente, se recibe instrucción en esta materia en las escuelas desde la educación básica." (P. 37)(Resaltado propio).

próxima década será testigo de un sinnúmero de casos de abusos de los derechos de propiedad intelectual y de invasión de nuestra intimidad. Habrá vandalismo digital, piratería del software y robo de información. Y lo peor de todo, mucha gente se quedará sin trabajo debido a los sistemas automatizados y las oficinas cambiarán tanto como lo han hecho las fábricas. *La noción de tener el mismo trabajo toda la vida ha empezado a desaparecer. La transformación radical de la naturaleza de nuestros mercados de trabajo, puesto que trabajamos con más bits y menos átomos, ocurrirá al mismo tiempo que la conexión a la Red de los 2.000 millones de personas que integran la fuerza laboral en India y China. (...) Las compañías norteamericanas han empezado a desarrollar hardware y a producir software en Rusia y la India, no por la mano de obra barata sino para asegurar una fuerza intelectual muy bien preparada dispuesta a trabajar más, más deprisa y porque es más disciplinada que la de su propio país. A medida que se globalice el mundo de los negocios e Internet crezca, se producirá un lugar de trabajo sin fisuras. Mucho antes de que se encuentren soluciones políticas o el GATT llegue a algún acuerdo respecto a las tarifas y al comercio de átomos (recuerden: el derecho de vender agua Evian en California),* ***los bits no tendrán fronteras y se almacenarán y manipularán independientemente de las barreras geopolíticas***. *De hecho, las zonas horarias desempeñarán un papel más importante en nuestro futuro digital que las zonas comerciales. Puedo imaginar algunos proyectos de software que literalmente atraviesen el planeta de este a oeste en*

veinticuatro horas y vayan de persona en persona o de grupo en grupo; uno trabaja mientras el otro duerme. Microsoft necesitará abrir sucursales en Londres y Tokio para producir software en tres turnos. ***A medida que nos acerquemos a ese mundo digital, todo un sector de la población será o se sentirá desplazado.*** *Cuando un trabajador siderúrgico de cincuenta años pierda su trabajo, lo más seguro es que, a diferencia de su hijo de veinticinco años, le sea imposible adaptarse al mundo digital. Sin embargo, si un secretario pierde su trabajo, al menos estará familiarizado con el mundo digital y poseerá habilidades transferibles. Los bits no se comen; en ese sentido no pueden calmar el hambre. Los ordenadores tampoco son entes morales; no pueden resolver temas complejos como el derecho a la vida o a la muerte. Sin embargo, ser digital nos proporciona motivos para ser optimistas. Como ocurre con las fuerzas de la naturaleza, no podemos negar o interrumpir la era digital. Posee cuatro cualidades muy poderosas que la harán triunfar:* ***es descentralizadora, globalizadora, armonizadora y permisiva****."(Subrayado fuera del texto) (P. 139).*

Concluye el autor en cita:

"El acceso, la movilidad y la habilidad para propiciar el cambio son los factores que harán que el futuro sea diferente del presente. ***La superautopista de la información puede estar de moda ahora, pero subestima el futuro. Se extenderá más allá de lo que nadie haya sido capaz de predecir****. En la medida en que los niños se apropien de un recurso de*

información global y descubran que sólo los adultos necesitan permiso para aprender, podremos encontrar nuevas esperanzas en lugares donde antes había muy pocas. No soy optimista porque me anticipe a alguna invención o descubrimiento. Encontrar la cura del cáncer o del sida, una manera digna de control de la población o inventar una máquina que pueda respirar nuestro aire, beber nuestros mares y que sus deshechos no contaminen el ambiente, son sueños que pueden o no ser realizables. Ser digital es diferente. ***No se trata de una invención, sino que está aquí y ahora. Podríamos decir que es genético por naturaleza, ya que cada generación será más digital que la que la precede. Los bits que controlan ese futuro digital están cada vez más en manos de los jóvenes.*** *Nada podría hacerme más feliz."* (P. 140) (Subrayado fuera del texto).

Ante este panorama, que desde hace 2 décadas pronosticaba y describía de forma visionaria y totalmente acertada el profesor Negroponte, es necesario tomar una actitud responsable frente al uso de las tecnologías en el rol que cada uno de nosotros ocupa en la sociedad, pues como indica Amador (2.016), para referirse en forma determinante y acertada a la implicación de las nuevas tecnologías como mecanismos de control y vigilancia social, afirmando:

"Cada nuevo invento, cada progreso tecnológico trae implícito un problema y este respecto de la vigilancia y la seguridad conllevan a la actualización de un modo de proceder del poder que ha actuado ya durante varias décadas, siendo las disciplinas estudiadas por Foucault un comienzo en el

cuál el poder experimentó un manejo sobre el cuerpo, el tiempo y la ortodoxia en pro de la producción." (P. 34).

Siguiendo la idea del autor mencionado anteriormente, es necesario entender que el ocuparse de la seguridad informática debe ser una prioridad, todos debemos tener una participación activa en la misma, antes que la agenda sea ocupada por los problemas de seguridad. La tecnología está en todos lados, en todo momento y en todo contexto y es deber de todos nosotros conocer sus riesgos.[2]

Pues bien, siendo conscientes de este panorama y de la necesidad de brindar una alternativa desde el derecho penal, en el presente texto, se buscará dar solución a un interrogante inicial respecto de la influencia de las comunicaciones para el derecho penal. Es decir, nos preguntaremos si **¿Mediante el derecho penal debe protegerse o no a los sistemas informáticos?** Cuestionamiento este que no es de fácil solución y precisamente para dar respuesta a este, será necesario entonces conocer el contexto en el que el derecho penal se encuentra actualmente a la luz de las Tecnologías de la información y de la comunicación (De ahora en adelante TIC)[3]; el impacto de estas últimas en la cotidianeidad de

[2] Tomado de: Jose2News (2.012-octubre-12). "SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN". (Archivo de video).
Recuperado de https://www.youtube.com/watch?v=m7bnF7XkqnU

[3] El termino Tecnologías de la información y de la comunicación (TIC), ha sido definido de varias formas, así es como por ejemplo Cabero (1.998) lo conceptualiza afirmando que *"En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las*

los individuos y de las sociedades, lo que a la postre, las convierten en un verdadero factor autónomo de riesgos y vulnerabilidades que debe ser razón suficiente para considerar a las TIC como un elemento generador de criminalidad y que de esta forma se le permita al derecho penal entrar a regular las eventuales conductas criminales que surjan como consecuencia del uso de estas nuevas herramientas.

Una vez que se determine el fundamento para que el derecho penal actué, se darán unas luces respecto de lo que implica, o de lo que ha de entenderse por DELITO INFORMÁTICO, concepto éste, que debemos indicar desde este momento, no ha sido definido con unanimidad, sino que por el contrario, es una categoría que se encuentra en desarrollo y sobre la cual hay muchas posiciones en conflicto, es sin duda un tópico nada pacífico y sobre el cual aún hay mucho por decir al respecto.

Con posterioridad, una vez que se ha hecho alusión a las distintas concepciones que existen sobre estas categorías jurídico-penales, será necesario abordar en la discusión respecto del bien jurídico tutelado, para determinar si basta con los bienes jurídicos creados y tradicionalmente considerados (patrimonio económico, propiedad intelectual, intimidad, etc.) para proteger a las personas

---

que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas" (P. 198)

de los eventuales atentados que se puedan ocasionar con las TIC, o si, por el contrario, es necesario crear un interés jurídico nuevo (Los sistemas informáticos y la información y los datos contenidos en los mismos) y el alcance que debería tener este bien jurídico.

Pese a la imposibilidad de determinar con exactitud y de forma unánime los elementos que componen esta categoría de delitos, será necesario elegir una posición al respecto, para lo cual, existen algunas herramientas que permitirán delimitar un campo de acción el cual avale la intervención del derecho penal sobre unos elementos mínimos (Principios transversales del derecho penal como son Fragmentariedad, Necesidad, Ultima Ratio) y así asegurar una protección jurídica adecuada.

Finalmente, haremos referencia a la categoría de delitos informáticos en Colombia, describiendo el panorama de esta temática en nuestro país, la legislación existente al respecto y el futuro de la discusión en nuestro contexto, para concluir con un análisis breve de los elementos constitutivos de estas infracciones penales para de esta forma, poder advertir las características que en nuestro país tienen estos tipos legales.

De esta manera, al final de nuestro recorrido, será posible responder al cuestionamiento planteado inicialmente, para con ello, indicar no solo la pertinencia, sino la absoluta necesidad de que el derecho penal proteja el bien

jurídico naciente de los sistemas informáticos y de los datos e información contenidos en estos sistemas y que con ello se logre desde el derecho en general y el derecho penal en particular, contribuir al sostenimiento de las sociedades modernas con las inmensas bondades y todos los beneficios que los sistemas tecnológicos representan para la humanidad.

Tras abordar estas discusiones en el orden metodológico propuesto, no subsistirá duda alguna acerca de la importancia y trascendencia de los sistemas informáticos en la sociedad actual y mucho menos, de la necesidad de proteger los mismos con las herramientas que el derecho penal ofrece. La vida misma como la conocemos sería impensable e inimaginable sin los aportes que nos realizan las tecnologías de la información y de la comunicación.

II. EVOLUCIÓN DE LAS TIC, SOCIEDAD DE LA INFORMACIÓN Y DEL RIESGO.

La post-modernidad ha traído consigo una serie de novedades que han implicado el avance constante del ser humano en prácticamente todos los aspectos de las relaciones sociales.

El permanente desarrollo de las tecnologías, la ciencia, la búsqueda incesante de nuevos conocimientos por parte del hombre, han llevado a las sociedades a un

nivel en el cual el tiempo es la única limitante para logar un sinfín de conocimientos y con ello generar un mundo nuevo de relaciones, una ***nueva sociedad del conocimiento.***[4]

Con la aparición de las TIC y la influencia que las mismas tienen en la vida de las personas, estas se han convertido sin duda en la base de muchas de las estructuras sociales de la modernidad. La civilización ha llegado al punto de sistematizarlo prácticamente todo mediante la tecnología[5]. Las formas básicas de comunicación que anteriormente se realizaban de forma directa y personal, hoy día han perdido dicho carácter y se han sistematizado por medio de las redes sociales, siendo estas los nuevos espacios de interacción social; por su parte, los centros de negocios que actualmente y gracias a los mecanismos tecnológicos pueden concretarse mediante redes virtuales que permiten la agilidad de los acuerdos y así mismo la posibilidad de realizarlos desde distintas partes del mundo; las fuentes de conocimiento también se han visto copadas por las tecnologías, las universidades y bibliotecas de todo el mundo, están promoviendo la cultura digital en la medida en que se propende por la creación

[4] Al respecto, Anarte (2.001), indica en la introducción a su texto lo siguiente: *"Las innovaciones tecnológicas apoyadas en la informática y en las redes de comunicación mundial, así como su expansión en las últimas décadas, han derivado en un nuevo paradigma sociológico nominado* ***Sociedad de la Información y/o del Conocimiento****. En este sentido, el conocido Informe Bangemann habla de una «nueva revolución industrial, basada en la información, que se puede procesar, almacenar, recuperar y comunicar de forma ilimitada e independiente de…, tiempo y distancia». Se trataría, según esto, de nuevos sistemas sociales basados en los servicios, cuyos principios axiales dejarían de ser el capital y el trabajo para* ***centrarse en el "conocimiento teórico****" (Pág. 1*) (Resaltado fuera del texto).

[5] Según la RAE, tecnología es el *"Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico".* (2012).

de bases de datos informáticas que evitan los mecanismos tradicionales de consultas en las bibliotecas; los documentos de papel van desapareciendo rápidamente a manos de los documentos digitales; los sistemas de salud e inclusive la administración de justicia que de a poco sistematiza todos los procedimientos ante las diferentes autoridades públicas, son solo algunos de los aspectos básicos que se han abocado hacia los beneficios de las nuevas tecnologías[6].

De lo anterior, se desprende necesariamente que las TIC se han convertido en un elemento no solo común, sino esencial para el sostenimiento de las sociedades actuales. En el presente es muy difícil, tal vez imposible, imaginarse un mundo en el que las comunicaciones, los sistemas informáticos[7] y las redes telemáticas[8] no sean parte fundamental de la vida de cada una de las personas.[9]

---

[6] En este sentido, Mata y Martin (2.003) afirma que "*Los servicios públicos (sanidad, regulación del tráfico rodado, aéreo o marítimo), la producción industrial, el comercio, la defensa de un país o la enseñanza, van integrándose inexorablemente en el entramado de las tecnologías de la información y Telecomunicaciones."*

[7] Según la RAE (2012), ha de entenderse por informática, el *"Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".*

[8] Según la RAE (2012), la telemática es la *"Aplicación de las técnicas de la telecomunicación y de la informática a la transmisión a larga distancia de información computarizada".*

[9] Sobre el particular, Amador (2.016), afirma *"Las celdas han desaparecido, los ideales de transparencia se han materializado y los vigilantes fantasma que creó el panóptico en sus comienzos se han alojado en lo más profundo del ser, la arquitectura circense invertida con la que se esquematizaba el panóptico ha perdido su espacialidad; ya no existe el tiempo, ni el espacio; estas herramientas de medición que algún día delimitaron lo que podríamos llamar nuestra existencia en el mundo, ya no tienen relevancia alguna ya, que allí en la web, todo existe por siempre y para siempre, nada envejece y por esto nada muere.* ***Es ahora allí en el hogar de lo digital "el ciberespacio" a donde trasladamos el interés por demostrar nuestra existencia****. Allí se encuentra el panóptico digital"* (P. 53) (Subrayado fuera del texto).

Vivimos entonces en una sociedad colmada por las bondades de las distintas formas de tecnología por cuanto estas representan beneficios en ahorro de tiempo; disminución de costos; aminoración de esfuerzos innecesarios; brindan una forma de generar, almacenar y transportar todo tipo de información, entre muchas más funciones, pero que pese a ese gran beneficio que representan, se debe ser consciente de la gran cantidad de riesgos que también generan, mediante estos medios novedosos, es altamente probable que se den afectaciones a bienes jurídicos, pues su utilización se ha masificado y mundializado, al punto tal, de que cualquier persona pueda encontrar en estas bondades, un mecanismo idóneo para cometer conductas ilícitas y por ende, el derecho penal como mecanismo de control social en el Estado social de Derecho no puede ser ajeno a esta realidad y menos ante el hecho de que dadas las características particulares de este tipo de conductas es necesario crear nuevos tipos penales y así mismo, revalidar las estructuras de algunos tipos ya existentes los cuales se quedan cortos ante estas nuevas formas de criminalidad informática.

Es necesario entender que siempre que el hombre logra una invención que reporte algún beneficio o utilidad, habrá que detenerse un momento para contemplar los riesgos o las consecuencias adversas que dicha invención puede acarrear, pues ante toda novedad no explorada ha de surgir necesariamente un margen de inseguridad ante el desconocimiento natural que de dicha invención se tiene. En este sentido, el profesor, *Mata Y Martin* (2003) señala:

> *"Hoy nos puede sorprender, pero podemos ver algunos ejemplos de estos sobresaltos a los que se ha visto sometida la sociedad. (...) Otro ámbito en el que se generan temores y precauciones será el de los Automóviles. Con estos nuevos medios de transporte la sensación de inseguridad se reproduce. Así el Código Penal español de 1928 establece como agravante genérica aplicable, en principio, a cualquier delito) la realización del hecho punible o la huida mediante un vehículo a motor, lo que delata la preocupación del legislador por este nuevo medio técnico a disposición de los criminales".* (P. 937)

En definitiva, las TIC, al estar inmersas en casi la totalidad de aspectos relevantes para la vida en sociedad, sin duda entran a ocupar un papel determinante, de vital trascendencia para las personas y en esta medida, se convierten en elementos generadores de riesgos que en tiempos anteriores ni se dimensionaban y que sin duda, dadas sus características, deben ser tenidas en cuenta por el derecho penal.

III. LA TECNOLOGÍA COMO NUEVO FACTOR GENERADOR DE CRIMINALIDAD.

Históricamente, la dogmática jurídico-penal y la criminología, han reconocido a la criminalidad como una consecuencia de diferentes factores, los cuales han

sido desde siempre las razones que han llevado a las personas inmersas en una colectividad social a la comisión de los diferentes delitos.

En primer lugar y a modo de ejemplo, se ha indicado que la pobreza es uno de los factores preponderantes que generan criminalidad[10], en tanto se tiene que quienes han sido marginados de derechos prestacionales como son el trabajo o la vivienda, que garanticen su dignificación, se han abocado hacia las conductas delictivas como un mecanismo necesario para obtener la reivindicación social y así superar la desigualdad, o cuando menos, satisfacer una necesidad básica insatisfecha.

Otro de los factores que ha sido históricamente reconocido como generador de criminalidad ha sido la violencia que se ha expresado de diferentes maneras a lo largo del tiempo. Las formas de agresión física, moral o psicológica han deteriorado la calidad de vida de los sujetos y propician sentimientos de frustración, odio y venganza. Esta violencia se traduce en atentados contra la integridad familiar, personal, social entre otras. Así mismo, esta violencia, genera un patrón de conducta el cual genera un ahondamiento de la criminalidad que hoy día es innegable y más tratándose de una sociedad como la colombiana, tal como lo indica León (2009).

[10] En este sentido, ver *"Conflictividades sociales, conductas delictivas",* de Guadalupe León, (2009).

Pues bien, así como en su momento se establecieron dichos factores, se han sugerido otros tantos y en la actualidad habría que evaluar la viabilidad de considerar a los sistemas informáticos como un elemento que genere criminalidad y que en virtud del mismo se determine una política criminal clara para poder contrarrestar sus efectos criminógenos.

Consideramos entonces, que no solo es viable, sino también necesario y pertinente entender el ciberespacio[11] como un nuevo ámbito de oportunidad delictiva. ¿Por qué?, pues en primer lugar, el ciberespacio es eso, un espacio, un "lugar" distinto, un nuevo contexto de interacción en el que las personas que acceden a él se encuentran y se relacionan entre sí, sin embargo, este espacio existe y es jurídicamente relevante en la medida en que dure el proceso de contacto o la interacción entre los individuos, es en ese momento en el que cobra vigencia y relevancia para el derecho.

A lo anterior, hay que agregarle que en el ciberespacio es evidente la desaparición de todo tipo de leyes naturales o de principios básicos de la materialidad habitual del ser humano como son por ejemplo el tiempo y el espacio físico. En esta realidad, el espacio físico no es limitante alguno para la interacción personal, pues a modo de ejemplo, dos personas ubicadas a miles de kilómetros pueden perfectamente estar interactuando en simultaneidad y la

[11] El Ciberespacio, ha de entenderse como un *"Ámbito artificial creado por medios informáticos"*. (RAE. 2012)

distancia física, no es óbice alguno para ello. En ese mismo sentido, el tiempo[12], entendido como magnitud física, también se ve desplazado en este tipo de interacciones, lo cual en últimas conlleva a que quienes se encuentren inmersos en esta realidad cibernética, tengan inmensas facilidades para cometer delitos al interior de la misma y es que no es lo mismo celebrar un contrato con una persona a la cual he visto, a la que conozco, de la cual se su dirección, quienes son sus familiares, con la que posiblemente he firmado un documento, a celebrar un contrato por intermedio de un computador con una persona que se encuentra a miles de kilómetros, con una persona que creo conocer pero que a ciencia cierta puede no ser quien se identifique ante mí y ello por supuesto genera una suerte de ventajas para la realización de conductas punibles.

De lo anterior, se desprende la necesaria transnacionalidad del ciberespacio, en donde las barreras limítrofes que establecen los Estados en ejercicio de su soberanía y a través de distintos tratados internacionales, no tienen vigencia alguna, pues en el ciberespacio estas limitaciones espaciales no encuentran razón de ser, pues no hay forma de hacerlas valer al interior de esta realidad virtual. Sea esta la oportunidad perfecta para recordar como en nuestra realidad material, la seguridad de los bienes jurídicos de las personas está en cabeza de los Estados los cuales tienen el deber de garantizar la protección de aquellos

[12] Según la RAE (2016), el tiempo es aquella *"Magnitud física que permite ordenar la secuencia de los sucesos, estableciendo un pasado, un presente y un futuro, y cuya unidad en el sistema internacional es el segundo"*

intereses necesarios para la vida en sociedad, pero en el ciberespacio, el Estado no tiene jurisdicción alguna en principio, es decir, debido a que la realidad virtual existe en la medida en que sea utilizada por X o Y, serán quienes la utilicen los encargados de la protección en su interior. Es así como debe adquirirse toda suerte de herramientas (antivirus, Firewalls, mecanismos de encriptación y enmascaramiento de datos o mecanismos de autenticación de contraseñas, usuarios, cuentas o personas y certificados de confianza de páginas o aplicativos web) para encontrar seguridad dentro de los sistemas informáticos.

Así mismo, es evidente la popularidad y la universalización del Internet[13] en nuestro tiempo. El hecho de que sea la red telemática más grande de todas y que sea utilizada por gran parte de la población mundial, es un factor que aumenta la probabilidad de riesgo para las personas.

Otro aspecto importante, que genera la necesidad de considerar a las redes informáticas como un elemento que genere criminalidad, es el anonimato que le brindan a las personas que actúan dentro de la misma, las cuales encuentran respaldo en este sentido para la comisión de conductas punibles; la dificultad para ubicar o individualizar a quien actúa inmerso en una red informática o telemática, representa una gran limitación para las entidades encargadas de la investigación criminal.[14]

---

[13] Según la RAE (2012), la Internet es la *"Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación"*.

[14] Al respecto, menciona Vásquez Azuara (2.013), la dificultad que tuvo el Gobierno Mexicano y los entes de investigación respecto del caso del Sacerdote Rafael Muñiz López, acusado por las

Los problemas que tienen las autoridades judiciales para poder llevar a cabo una actividad investigativa y de judicialización de quienes cometen estas conductas es un elemento más que genera preocupación a la hora de combatir estas conductas, los elementos precarios de investigación se tornan obsoletos para cumplir sus finalidades. Es decir, el delincuente informático tiene en esta imposibilidad institucional, un factor determinante y ampliamente atractivo que lo motiva a la comisión del crimen.

De todo lo anterior, resulta evidente que el delito informático trae en sí una serie de connotaciones y elementos que generan la necesidad de romper el paradigma tradicional delimitado por las relaciones sociales personalísimas, en un ámbito territorial y temporal tangible, para contemplar la nueva realidad que propone el ciberespacio y la cual desafía a las estructuras dogmáticas tradicionales del derecho penal, así como también le hacen frente (con una importante posibilidad de vencerla) a la fuerza de investigación de las entidades judiciales y en esta medida, es necesario considerar a las TIC como un nuevo y verdadero factor

---

autoridades de Xalapa, Veracruz por pederasta y apodado por los medios de comunicación como el "cibercurapederasta". Específicamente menciona: *"Trajeron personas del FBI que rastrearon la dirección IP, lo ubicaron, le decomisaron la laptop y él ya la había borrado (refiriéndose al contenido pornográfico), pero claro, los del FBI recuperaron la información. (...) y Así fue como lograron fijar la responsabilidad del padre de San Benito, pero lo importante es que tuvieron que traer gente de afuera, porque aquí no hay quien maneje la materia".* Vásquez C. 2.013-mayo-28. CONFERENCIA DELITOS CIBERNÉTICOS.
(Archivo de video). Recuperado de https://www.youtube.com/watch?v=cg7vYTE6Z6k

generador de criminalidad dadas las situaciones especialísimas indicadas con anterioridad.

IV. CONCEPTO DE DELITO INFORMÁTICO, BIEN JURÍDICO Y TEORÍAS AL RESPECTO.

Sobre el concepto de delito informático, hay que indicar que en primer lugar, nuestra legislación nacional colombiana no ha determinado ni en el código penal, ni en alguna otra ley, un concepto específico sobre este tipo de delitos. Ante esta situación, se ha suscitado una discusión respecto de ¿qué se ha de entender por delito informático? ¿Qué bien jurídico protegen, si es que protegen alguno? y ¿qué elementos deben comprender dichas conductas? En ese orden de ideas, habría que verificar si la jurisprudencia se ha pronunciado al respecto y en ese sentido, se llegará a la conclusión de que ni la Corte Constitucional, ni la Corte Suprema de Justicia en su Sala de Casación Penal, han entrado a estudiar este tipo de conductas al punto de brindar un concepto claro y unánime sobre las mismas. Sobre esta cuestión particular, la Jurisprudencia de la Sala de Casación Penal de la Corte Suprema de Justicia, solo ha entrado a analizar en sentencia de radicado número 42.724 del 11 de Febrero de 2015, en la cual, la Sala decide respecto de un conflicto de competencias, algunos elementos del hurto por medios informáticos. Los hechos correspondientes del caso indican que:

"(...) por medio de una transacción bancaria realizada el 28 de mayo de 2009, originada desde la ciudad de Barranquilla, de manera ilícita y

superando barreras electrónicas, se trasfirió a varios destinos bancarios (nueve cuentas) la suma de ciento nueve millones de pesos ($ 109.000.000.oo) que estaban en una cuenta de Bancolombia, de la Oficina ubicada en el Centro Comercial Campanario de la ciudad de Popayán, de propiedad del mismo Centro Comercial.

En este caso, la Fiscalía Séptima Seccional Adscrita ante la URI de Barranquilla competente en primera medida, imputo cargos a un total de 5 personas por el delito de hurto calificado (por haberse cometido superando seguridades electrónicas, según lo indicado en el art. 240,4) con circunstancia de mayor punibilidad (atendiendo a la coparticipación criminal).

Fue así como el proceso llegó al despacho del Juzgado Octavo Penal del Circuito con Funciones de Conocimiento de Barranquilla, para que allí se adelantara la etapa de juzgamiento.

La Fiscalía 46 presentó ante el Juzgado de conocimiento un escrito en el que promovía el incidente de definición de competencia, fundamentada en los siguientes argumentos: a) como el delito se consumó en la ciudad de Popayán, es la autoridad judicial de tal distrito judicial la llamada a juzgarlo; y, b) de acuerdo con el artículo 1º de la Ley 1273 de 2009 el delito corresponde a la denominación de "hurto por medios informáticos y semejantes", es un juez penal municipal el que tiene la competencia funcional para su conocimiento, por disposición expresa de la misma ley,

que adicionó un numeral al artículo 37 de la Ley 906 de 2004, en tal sentido.

Ya en la audiencia de formulación de acusación, adelantada el 31 de mayo de 2010, el Juzgado de Barranquilla resolvió enviar el proceso al Tribunal Superior de Popayán para que fuera dicha autoridad la que determinara cuál era el juez competente para conocer de los hechos contenidos en el escrito de acusación, Corporación que a su vez reenvió el proceso a la Sala Penal con el mismo objetivo." (P.4)

Ahora bien, en punto específico al desarrollo tecnológico y particularmente al hurto por medios informáticos, la Corte destacó el espíritu protector de bienes jurídicos de ‘este tipo penal en el siguiente sentido:

*"**El desarrollo tecnológico facilitó el vertiginoso avance de las comunicaciones, creando un escenario casi universal, -o global, si se quiere- en el que se puede desplegar un creciente número de actividades, pero también brindando nuevos espacios para el delito, por tal razón el ejercicio de los derechos en los sistemas informáticos, como la propiedad, la intimidad, la información deben ser resguardados y protegidos**.*

Esa nueva dimensión de la relación entre el tiempo y el espacio que se ha sido determinada a partir de las tecnologías de la información y las comunicaciones, fue regulada por nuestro legislador a través de la Ley 1273 de 2009, la cual fue promulgada en el Diario Oficial 47.223 de 5 de enero de 2009, que creó en el Código Penal el Título II Bis, dedicado a la

> *"Protección de la información y de los datos", con dos capítulos, en el primero de los cuales tipificó "los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"; y en el segundo, "los atentados informáticos y otras infracciones", en el que se incorporaron, entre otros, los delitos de "hurto por medios informáticos y semejantes" y "Transferencia no consentida de activos".*

Continúa la Corte indicando:

> *"Pues bien, dicha normatividad, vigente para la fecha -28 de mayo de 2009- en que de manera ilegal se transfirió una gruesa suma de dinero de propiedad del Centro Comercial Campanario de su cuenta bancaria a nueve cuentas de particulares; adicionó el artículo 37 del Código de Procedimiento Penal, asignando a los jueces penales municipales la competencia para el conocimiento de los delitos contenidos en el Título VII Bis del Código Penal."(Subrayado fuera del texto)(P.7)*

Es así, como con esta decisión se denota el sentido pluriofensivo que pueden tener este tipo de conductas, específicamente el hurto por medios informáticos, el cual (en el sentir de la sala), protege no solo a los sistemas informáticos, sino que además de ello, también el patrimonio económico de las personas, cuestión que es evidentemente destacada por la sala en el fallo en comento.

De este modo, podemos indicar sin temor a equívocos, que ni la ley colombiana, ni la jurisprudencia nacional han brindado un concepto suficiente de lo que debe entenderse cuando se habla de un delito informático, sino que únicamente, la definición de estas conductas ha sido estudiada y desarrollada por parte de la doctrina jurídico-penal especializada, estudio el cual ha generado una serie de debates respecto de la denominación jurídica que ha de dársele a este tipo de delitos y sobre el contenido de estos mismos.

Pues bien, sobre el particular, existen dos teorías preponderantes o de mayor acogimiento por parte de la doctrina. Una de ellas, la cual entiende a los delitos informáticos en una concepción amplia o genérica y otra teoría que abarca los mismos en un sentido específico o restrictivo.

A continuación, se analizaran brevemente las diferentes posturas que se han planteado.

A. CONCEPCIÓN AMPLIA DEL DELITO INFORMÁTICO.

Esta postura, considera que se está en presencia de un delito informático tanto con las conductas o delitos "comunes" o "tradicionales" (hurto, injuria, calumnia, pornografía infantil, etc.) que se realizan a través de medios

informáticos; así como con las conductas que atentan contra los sistemas de información y la información misma allí contenida[15].

Según esta corriente, los tipos penales que se incluyen en esta clasificación no deben tener rasgos comunes, ni presentar problemas dogmáticos iguales, tampoco han de proteger el mismo bien jurídico, sino que basta con que sean realizados con la utilización de algún medio tecnológicos.

Apoyando esta teoría, Miró (2.012) indica lo siguiente:

> *"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." (p.35)*

[15] Algunos que adoptan este concepto son por ejemplo: Téllez, (2004) quien los define dependiendo de si están establecidos en la legislación penal o no, como las *"actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (Concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (Concepto Típico)." (P. 163).*
Así mismo, León (2001), citando a Guerrero Matéus y otro, los define como *"Toda conducta cometida en el campo de la actividad informática contra bienes, sean estos tangibles o no, relacionados al tratamiento automatizado de datos, o infracciones en que el ordenador es un instrumento para cometer o consumar el hecho"* (Pág. 166).

Ahora bien, esta teoría genera algunos inconvenientes, los cuales generan amplias dificultades para su adopción, pues el hecho de que sea una clasificación ampliamente genérica que no delimita elementos o criterios comunes a estos delitos, así como el que tampoco involucre un bien jurídico general a todas ellas que a la postre permita su incorporación sistemática a un código penal, ni un estudio conjunto de las mismas, hará que en ultimas no se genere la sistematicidad necesaria para lograr un tratamiento especial con miras a una política criminal estatal coherente. Así mismo, la simple vinculación del medio informático en la comisión del delito, no podría entenderse como suficiente para creer que se está ante un fenómeno criminal autónomo que merezca un estudio particular y con ello una política criminal diferencial en atención al medio especial (las TIC) con el que se cometen.

B. CONCEPCIÓN ESPECÍFICA O RESTRICTIVA DEL DELITO INFORMÁTICO.

Para esta teoría, en nuestro sentir, un poco más sopesada y delimitadora, el delito informático ha de entenderse como aquel ataque en contra de un sistema informático o telemático, o en contra de la información que éste mismo contiene. Bajo esta concepción, no basta con que el delito que se comete tenga vinculación de alguna forma con un elemento tecnológico; es necesario que se dé un ataque estricta y necesariamente en contra de la

información o los datos contenidos en el sistema o que el ataque se dé directamente contra el sistema informático o la red telemática.[16]

Es decir, según esta corriente, no puede entenderse como delito informático cualquier delito común en el que exista alguna influencia de un elemento tecnológico o que éste se utilice como medio para la comisión, puesto que no es más que una herramienta utilizada para la comisión de una conducta delictiva común desarrollada anteriormente por parte del legislador penal.[17]

Ahora bien, debemos tomar postura al respecto, y en ese sentido, debemos indicar que nos encontramos de acuerdo con esta última denominación sobre el delito informático, es decir, compartimos el sentir de aquel sector de la doctrina que acoge la concepción restrictiva del delito informático, lo anterior por cuanto **(i).** en primer lugar, teleológicamente, de la denominación de esta clasificación "Delitos informáticos", se desprende que el objeto de protección del bien jurídico es la "informática"[18], y no otros bienes jurídicos que ya son protegidos por otros tipos penales, es decir y a modo de ilustración, en los delitos contra la administración pública, se protegen las diversas manifestaciones de este bien jurídico, pero en últimas,

[16] Palazzi (2000), adopta esta tendencia, cuando indica que *"(…) estamos frente a un delito informático en el caso de daño a datos o programas informáticos, pero no cuando lo atacado es una simple máquina, y como consecuencia de ello se daña la información que está contenida"* (Pág. 36).
[17] Además de Palazzi, adoptan esta postura: Herrera y Núñez (1999), Araujo (1994).
[18] Por informática, ha de entenderse el área de la tecnología encargada del "tratamiento automático y racional de la información y los datos por medio de las computadoras" (RAE, 2012)

es la administración pública lo que se protege; en ese mismo sentido, con los delitos informáticos ha de protegerse la informática, entendida como se indicó anteriormente. **(ii).** los delitos informáticos entendidos en la acepción estricta, si tienen en común un mismo bien jurídico objeto de protección, cual es, el sistema informático y los datos almacenados en el mismo, lo cual se materializa o se concreta específicamente en tres aspectos específicos como son, su integridad[19], confidencialidad[20] y disponibilidad[21]; lo que a la postre, deriva en la posibilidad que tienen de estudiarse en forma conjunta, debido a las características similares que comparten y al bien jurídico que protegen que es el mismo para todos.

En este sentido, Rueda Martin (2.013) apoyándose en Bustos Ramírez, indica:

> *"Los bienes jurídicos no tienen una entidad material o física sino que, por el contrario, son valores ideales que se atribuyen por la comunidad social a determinados objetos, cosas, situaciones o*

[19] La integridad del sistema informático, hace referencia a que tanto el sistema como la información misma allí contenida, se mantengan incólume, sin modificación alguna, todo esto de acuerdo a la voluntad y el deseo de quien es su titular.
En este sentido, Rueda Martin (2.009) lo describe en los siguientes términos: *"La integridad de un sistema informático alude a su utilización con las pertinentes modificaciones del contenido de la información almacenada en el sistema por parte de la/s persona/s autorizada/s" (P. 187)*

[20] En cuanto a la confidencialidad del sistema, esta implica que tanto el sistema, su funcionamiento y estructura, como la información que el mismo contiene, sean de conocimiento exclusivo de su titular y no de dominio público por parte de terceros.
Rueda Martin (2.009) simplifica la situación indicando que *"La confidencialidad de dicho sistema se basa en que su utilización corresponde exclusivamente a la/s persona/s autorizada/s" (P. 187)*

[21] La disponibilidad implica que tanto el sistema, como la información que el mismo contiene, puedan ser utilizados por su titular en la forma y el tiempo que este desee. En este sentido, Rueda Martin (2.009) afirma que la confidencialidad se refiere "al control sobre la utilización de un determinado sistema por parte de la/s persona/s autorizada/s." (P. 187)

> *relaciones en virtud de su aptitud e idoneidad instrumental para la satisfacción de necesidades individuales y colectivas. Estas necesidades y los intereses que satisfacen ya sean individuales o colectivos son además plurales, variados y, a menudo, también contrapuestos. Sin embargo, el bien jurídico debe ser una entidad libre de conflictos y antagonismos, pues en cuanto instrumento social y políticamente sancionado y dispuesto para la satisfacción de necesidades e intereses plurales, el bien jurídico, como afirma Bustos Ramírez, surge como una síntesis normativa (fijada por el ordenamiento jurídico) de una relación social determinada y dinámica"* (Pág.179)

En este orden de ideas, debemos indicar que en cuanto al contenido del bien jurídico, éste es en nuestra legislación el de *"la información y de los datos"*, esto a la luz de la ley 1273 del 5 de enero de 2.009, que adiciona al Código Penal (Ley 599 del 2.000), el Titulo VII Bis, denominado "*De la protección de la información y de los datos"*, es decir, a través de estas conductas descritas en el código a partir de la ley 1273 (las cuales desarrollaremos más adelante), se busca proteger el bien jurídico naciente de la información y de los datos, pues es con estas conductas que se puede llegar a afectar el bien jurídico en mención.

Todo lo anterior, resultan ser razones más que suficientes para indicar la pertinencia y utilidad de esta propuesta terminológica.

Ahora bien, en la Ley 1273 del 2009 en comento, se agregaron un total de nueve tipos penales que buscan proteger el bien jurídico de la información y de los datos en principio, y decimos en principio, por cuanto, este Título incorpora por ejemplo, el delito de "*Hurto por medio informático*" (Art 269I) el cual, en efecto protege este bien jurídico, pero que además de ello, se presenta como un delito pluriofensivo, el cual protege inmediatamente el bien jurídico del patrimonio económico de la persona y de forma mediata el de la información y los datos[22]. Lo anterior para evidenciar que al parecer el legislador nacional no adopto la tesis restrictiva del delito informático, sino que decidió incorporar un concepto de delito informático en sentido amplio, lo cual resulta desde nuestro punto de vista un esfuerzo innecesario y una falta de técnica legislativa, un total despropósito, pues tratándose del hurto por medios informáticos, hubiese bastado determinarlo como un agravante del delito de hurto y no como un delito "informático" en una categoría autónoma e independiente que en ultimas lo único que genera son problemas de inseguridad jurídica.

En este punto, debemos manifestar que si bien hay aproximaciones de distinta naturaleza sobre lo que puede entenderse por delito informático y lo que este abarca, lo cierto es que es un concepto que está en desarrollo, sobre el cual no hay una definición expresa y sobre el que se seguirá discutiendo.

[22] Al respecto, ver Sentencia 42724 del 11 de Febrero de 2015, de la Sala de Casación Penal de la Corte Suprema de Justicia, M.P. Eyder Patiño Cabrera.

Razón ésta que no obsta para que los legisladores penales intenten proteger a las personas, su información y sus datos, mediante la creación de conductas que limiten los usos que se dan a esta nueva fuente de riesgos, cual es, las tecnologías de la información y de la comunicación, pues es claro que hay que buscar una forma para proteger a las personas ante estas nuevas formas de ataque inmateriales, pues como indica León (2001) *"El manejo de un bien inmaterial como la información, acarrea como consecuencia que el actuar delictivo contra él, se elabore también inmaterialmente".*

Ahora bien, esta tarea de enormes proporciones y de vital importancia, no ha de entenderse en cabeza exclusivamente de los legisladores nacionales de cada país que considere necesaria su regulación, no, la comunidad internacional tiene también un deber importante al respecto. La facilidad con que estas conductas generan efectos sin importar las fronteras limítrofes o territoriales, destaca la necesidad de lograr una cooperación internacional en cabeza de los Estados nacionales por emprender una lucha eficaz contra esta criminalidad emergente.

Consientes de esa necesidad, la comunidad europea se ha puesto en la tarea y ha decidido combatir conjuntamente todas las formas de criminalidad[23]

[23] Cierto es que las naciones europeas se han destacado por su cohesión y su éxito en la lucha mancomunada contra toda forma de delincuencia. Esto no solo se ha denotado en la delincuencia informática, sino que han tenido especial interés en articular esfuerzos con por ejemplo, los actos de terrorismo, lo cual los vuelve un referente necesario en cuanto a cooperación internacional, pues

que agobian a estas naciones y la criminalidad informática no ha sido ajena a esa iniciativa. Es así como el Consejo de Europa suscribió el 23 de noviembre del 2.001 el "*Convenio sobre la Ciberdelincuencia" en la ciudad de Budapest, Hungría.*

En este instrumento, todos los miembros de dicho organismo, se comprometen a desarrollar esfuerzos desde la legislación, las formas de investigación y por supuesto, la cooperación internacional para efectos de la persecución criminal de los delitos informáticos, pues en su preámbulo se comprende la necesidad de regular conjuntamente la actividad cibernética y así evitar eventuales ataques contra el bien jurídico de la información y de los datos en cuanto a su confidencialidad, integridad o disponibilidad. Indica el mencionado preámbulo:

> *"Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente convenio,*
>
> *Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;*

---

como indica Ambos (2.007), *"En el ámbito europeo, los esfuerzos por articular instrumentos jurídicos para la lucha contra el terrorismo se remontan a mucho antes del 11 de septiembre de 2.001. En el ámbito del Consejo de Europa se mejoró considerablemente la persecución de actos terroristas gracias al Convenio Europeo para la represión del terrorismo, de 27 de enero de 1.997, especialmente porque los actos terroristas dejaron de considerarse como delitos políticos o conexos a éstos, con lo que se removieron todos los obstáculos que la extradición planteaba respecto a aquellos delitos."* (P. 30).

Reconociendo el interés de intensificar la cooperación con los otros Estado Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular frente a la adopción de una legislación adecuada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas*;*

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información;

Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal;

Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos

> ***informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internación y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;*** *(…)"* (Subrayado fuera del texto). (P. 1)

Sin duda, este instrumento se erige como uno de los principales ejemplos a seguir por parte de las legislaciones foráneas alrededor del mundo. Pues bien, sin duda, los lineamientos establecidos en esta convención son la base para la construcción legislativa para la protección al bien jurídico de la información y de los datos de la mayoría de legislaciones suramericanas; Colombia por supuesto fue permeada por esta iniciativa al momento de regular dicha materia, pero pese a ello, es cierto que los esfuerzos por lograr una unificación y una unidad de acción en contra de la criminalidad informática en nuestro continente, están lejos de ser una realidad semejante a como ya lo es en las naciones europeas.

V. CARACTERISTICAS PRINCIPALES DEL DELITO INFORMÁTICO.

De lo expuesto anteriormente, y dadas las dificultades para optar por un concepto determinado, se intentará entonces generar una aproximación a la categoría que se estudia a partir de unos aspectos criminológicos que pueden contribuir a una comprensión detallada de la misma.

a. Según León (2012), son conductas eminentemente dolosas, es decir, quien incurre en la comisión de las mismas, lo hace con el objetivo claro de afectar el bien jurídico protegido por ellas. En este sentido, no admiten modalidad culposa en su comisión. A modo de ilustración y para dar un ejemplo, el "*hacker*[24]" que

[24] Tradicionalmente, se ha considerado que el "*hacker*", es aquella persona malévola, con intensiones dañinas, que tiene como finalidad acceder a los sistemas informáticos para cometer todo tipo de conductas desviadas o lesivas. Tal es el alcance generalizado de esa concepción que se tiene de los "*hackers*" o piratas informáticos que incluso la RAE (2.016) lo define como aquel que *"accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta."*
Ahora bien, uno de los expertos en sistemas y tecnologías más importantes del mundo, el español Chema Alonso (2.015) indica como es necesario que la sociedad entienda lo que verdaderamente es un "*hacker*". En primer lugar afirma que "hacker" no es igual a "Cracker"(este último se refiere a la figura negativa), luego, hay que distinguirlo del "hacker" en su acepción positiva y lo define como *"una persona que se delita en tener un conocimiento íntimo y profundo en el funcionamiento de las tecnologías (...) para nosotros un "hacker" es esto, es un investigador, una persona que lleva la tecnología más allá del límite inicial para el que fue construida y evidentemente mucho tiene que ver con los ingenieros, que estamos aquí para construir cosas, para hacer cosas. Para nosotros un "hacker" siempre es una persona que hace algo con la tecnología".*
Tomado de Maligno A. 2.015-abril-30. Semana de la Informática 2015: Ingenieros y Hackers. (Archivo de video). Recuperado de https://www.youtube.com/watch?v=m6WPZmx7WoI
Además de ello, este hacker español afirma (2.012) que la labor que realizan los "*hackers*" es fundamental para el desarrollo de las grandes compañías y las empresas tecnológicas, pues los ingenieros informáticos que trabajan al servicio de estas, tienen la tarea de analizar los sistemas informáticos, escudriñar en los mismos para encontrar fallos de seguridad y de esa manera lograr reconfigurarlos para mejorar sus condiciones de seguridad y finalmente blindar al sistema informático contra eventuales ataques perpetrados por "*crackers*". En sus palabras *"(...) encontrar fallos, vulnerabilidades se ha vuelto un auténtico negocio en el mundo de la seguridad informática*

emprende un ataque informático, jamás tiene en mente, nunca decide atender o acatar deber objetivo de cuidado alguno, no, al contrario, para poder realizar esta conducta debe decidir los medios adecuados (conocimiento y voluntad) para la irrupción en el sistema informático, pero además de ello, ejecutar las actos idóneos e inequívocamente dirigidos a la realización de la misma, es decir, el despliegue de esta serie de actividades denotan la presencia de un plan criminal y su posterior ejecución y que en esa medida no es connatural al delito de acceso abusivo a sistemas informáticos, ni a ningún delito de esta categoría, que se presenten en modalidad culposa.

b. Quien las comete, es una persona que ostenta un conocimiento específico sobre sistemas y tecnología; no cualquiera logra llevar a cabo este tipo de conductas y quien lo hace, se basa en unas habilidades previamente adquiridas. Ahora bien, este conocimiento en la actualidad no es para nada de difícil acceso, de hecho, hoy día es posible encontrar en Internet manuales que enseñan a las personas a cometer este tipo de conductas, como por ejemplo el *"Mujahideen Secrets 2"* o el *"Manual de obtención de información de objetivos de Google",* que son

---

(...) encontrar un fallo de seguridad tiene una implicación de mucho trabajo, de mucho tiempo y luego puede ser utilizado para muchas cosas". Así mismo, expone como el trabajo de los "hackers" es de tan amplia importancia y tan bien valorado por la industria de la tecnología, que inclusive existen unos premios que se entregan a los mismos, *"(...) tenemos premios, hay premios a los mejores "hackers", son los "PWNIE AWARDS" (...) se dan al que ha descubierto el mejor fallo de seguridad al lado del servidor, el mejor fallo de seguridad al lado del cliente, a la peor respuesta de seguridad de un fabricante de software o cualquier tema relacionado con la seguridad informática".*
Alonso C. 2.012-abril-20. The App Fest 2012 - Hacking, ciberguerra y otras palabrotas - Chema Alonso.
(Archivo de video). Recuperado de https://www.youtube.com/watch?v=QccQjXhgub0

utilizados por "*Al Qaeda*" para la comisión de este tipo de delitos y que se encuentran al alcance de cualquiera; basta hacer un par de "*clicks*" en el buscador *"Google"* y se tendrá acceso a ello[25].

c. Sin lugar a duda estas conductas revisten un grado de dificultad importante respecto de su investigación, pues las autoridades encargadas de ello, requieren no solo de los conocimientos especializados, sino de las herramientas y la infraestructura idónea que les permita llevar a cabo una actividad investigativa exitosa.

d. Son delitos que tienen vocación hacia la internacionalidad, en la medida en que pueden afectar a personas que se encuentren a cientos de miles de kilómetros, en diferentes países.

En este sentido, León (2001) afirma que:

> *"De ordinario son delitos que se cometen a nivel nacional o local, pero en virtud de la existencia de los sistemas informáticos de utilización integral, para la elaboración y ejecución de programas de alcance internacional, se convierten en delitos informáticos internacionales, para los cuales respecto a su penalización e investigación se deberá recurrir a la celebración de*

[25] Alonso C. 2.012-abril-20. The App Fest 2012 - Hacking, ciberguerra y otras palabrotas - Chema Alonso.
(Archivo de video). Recuperado de https://www.youtube.com/watch?v=QccQjXhgub0

tratados internacionales entre los Estados o se deberá aplicar los conceptos de la ley penal en el tiempo y en el espacio" (P. 170).

VI. DELITOS INFORMÁTICOS EN LA LEGISLACIÓN COLOMBIANA.

Finalmente, es necesario entrar a mirar lo que es y lo que podríamos entender en Colombia como un delito informático a la luz de la legislación existente al respecto.

Pues bien, en Colombia esta categoría de delitos se crea en el año 2.009, a través de la ley 1273 del 2.009[26] a partir de la cual se crea el bien jurídico *"De la información y de los datos"* y se busca proteger mediante la punición de nueve conductas[27] distintas que según el legislador colombiano atentan contra este bien jurídico ya desarrollado con anterioridad.

Parece ser entonces, que en contradicción de los planteamientos desarrollados en este análisis, el legislador colombiano ha decidido adoptar un concepto de delito informático en un sentido amplio, esto resulta ser así, por cuanto, como ya se esbozó con antelación, encontramos en uno de los tipos penales, el 269I, denominado *"Hurto por medios informáticos"* y es a partir de la delimitación de este bien jurídico que se infiere dicha postura. ¿Por qué ello es así? Recordemos que según la

[26] Para mayor detalle, revisar el Diario oficial del Congreso de la Republica No. 47.223, del 5 de enero del 2.009.

[27] Los tipos penales creados son: (i) Artículo 269A: Acceso abusivo a un sistema informático; (ii) Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación; (iii) Artículo 269C: Interceptación de datos informáticos; (iv) Artículo 269D: Daño Informático; (v) Artículo 269E: Uso de software malicioso; (vi) Artículo 269F: Violación de datos personales; (vii) Artículo 269G: Suplantación de sitios web para capturar datos personales; (viii) Artículo 269I: Hurto por medios informáticos y semejantes; (ix) Artículo 269J: Transferencia no consentida de activos.

teoría amplia del delito informático, que reiteramos no es en nuestra opinión sistemáticamente admisible, estamos ante un delito informático en dos eventos: **(i)** cuando se realice un ataque a un sistema informático o a la información contenida en el mismo y **(ii)** cuando se cometa cualquier delito de aquellos denominados "comunes" con la utilización de un medio o dispositivo informático. Esto último es precisamente la descripción de lo que ocurre con el hurto por medios informáticos, es decir, nos encontramos ante un evento en el que hay un tipo penal básico (Hurto contenido en el artículo 239) el cual se realiza con la "novedad" del medio, es decir, con un medio informático como herramienta para la comisión del mismo.

Evidente es entonces la contradicción que existe entre la legislación existente, los fundamentos de la misma y la posición de este autor, por cuanto entendemos inadecuada la posición tomada por el legislador por cuento, en primer lugar, el entender la concepción amplia del delito informático genera problemas en cuanto a seguridad jurídica. En punto al hurto por medio informático, ¿Por qué no sancionarse con el tipo penal básico contenido en el artículo 239 de la ley 599 del 2.00 si la sanción contemplada en el 269I remite a la impuesta en el 240 prevista para el tipo básico de hurto?

Además de lo anterior, consideramos que es un norma que genera mayor *"inflación normativa*", ¿Acaso no hubiese bastado con la creación de una causal de agravación o de calificación para sancionar este tipo de conductas? ¿Era necesario crear un tipo penal autónomo e independiente para ello? Parece ser que no.

Detengámonos a pensar un momento lo siguiente. ¿Es el medio para cometer un delito un criterio suficiente que fundamente la necesidad de crear una categoría autónoma de delitos? Es decir, ¿debemos agrupar en una categoría especifica de delitos todos los que se cometan mediante de un mismo medio? Si la respuesta a ello es si, podríamos entonces pensar en crear una categoría de delitos por ejemplo automovilísticos, en donde agrupemos todos los delitos que puedan cometerse con la utilización de un medio como son los automóviles y entonces tendríamos en una misma categoría los homicidios ocasionados con vehículos, las lesiones ocasionadas con vehículos, los daños en bienes ajenos cuando se ocasionen con estas máquinas y ello, desde luego resulta inapropiado e inequiparable. Así podríamos entonces, seguir creando categorías delictivas agrupadas en forma indebida, porque no pensar en delitos "armamentísticos", para agrupar todas las conductas que cometa con la utilización de armas y así, podríamos aglutinar tipos penales ya existentes en categorías "especializadas" según la utilización de un medio determinado que generaría una clasificación anti sistemática de tipos penales, por cuanto protegeríamos con una misma categoría, bienes jurídicos que (i). Ya están siendo protegidos por otro tipo penal y (ii). No tienen características en común que permitan su estudio sistemáticamente.

Pero bueno, pese a lo expuesto anteriormente, lo cierto es que en Colombia es esa y no otra la realidad respecto de los delitos informáticos y es precisamente esa realidad y la necesidad imperiosa de modificarla motivación suficiente para el análisis que en este estudio se ha planteado.

Para efectos de lograr una aproximación general respecto de los tipos penales creados en el ordenamiento jurídico y con finalidades expositivas, en el presente acápite, desarrollaremos de forma esquemática el contenido de las conductas creadas en la ley 1273 del 2.009, por cuanto un estudio detallado en donde se pormenoricen de forma específica cada uno de sus problemas y las discusiones existentes sobre cada uno de ellos, ameritaría un trabajo cuya finalidad resultaría totalmente distinta a la del presente, razón por la cual se hará el siguiente análisis, que consta de una mención al tipo penal; su ubicación en nuestra legislación nacional; la conducta que debe desplegarse por el sujeto agente y con la cual se configura objetivamente el tipo penal; los verbos rectores de las mismas; los ingredientes normativos que son constantes en estos tipos penales; así como la pena a imponer por su realización. En punto al tipo subjetivo, no se ahondara en este tema, por cuanto en todos estos delitos se requiere un tipo subjetivo doloso en su comisión, dado que sería imposible pensar en una utilización de estos medios o un ataque a los mismos y que ello pueda estructurarse bajo modalidad culposa. Es de esta manera como se tiene lo siguiente:

1. ACCESO ABUSIVO A 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."

ARTÍCULO CÓDIGO PENAL	Artículo 269A
CONDUCTA	• *Acceder en todo o en parte a un sistema informático protegido o no con una medida de seguridad.* • *Mantenerse dentro de un sistema informático protegido o no con una medida de seguridad en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.*
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	• Acceder • Mantenerse
INGREDIENTES NORMATIVOS	• Sistema informático • Medida de seguridad
PENA A IMPONER	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

2. 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."

ARTÍCULO CÓDIGO PENAL	Artículo 269B
CONDUCTA	• *Impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.*
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	• Impedir • Obstaculizar
INGREDIENTES NORMATIVOS	• Sistema informático • Red de telecomunicaciones
PENA A	*Pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a*

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

3. 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."

ARTÍCULO CÓDIGO PENAL	Artículo 269 C
CONDUCTA	*Interceptar 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.*
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	Interceptar
INGREDIENTES NORMATIVOS	• Datos informáticos • Sistema informáticos • Emisión electromagnética
PENA A IMPONER	*Pena de prisión de treinta y seis (36) a setenta y dos (72) meses de prisión.*

4. 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."

ARTÍCULO CÓDIGO PENAL	Articulo 269 D
CONDUCTA	• Destruir, • Dañar, • Borrar, • Deteriorar, • Alterar • Suprimir 1. Datos informáticos, o 2. Un sistema de tratamiento de información o 3. Sus partes o componentes lógicos
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	• Destruir, • Dañar,

	• Borrar, • Deteriorar, • Alterar • Suprimir
INGREDIENTES NORMATIVOS	1. Datos informáticos, o 2. Un sistema de tratamiento de información o 3. Sus partes o componentes lógicos
PENA A IMPONER	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.

5. <u>USO DE SOFTWARE MALICIOSO.</u>

"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."

ARTÍCULO CÓDIGO PENAL	Artículo 269 E
CONDUCTA	• Producir, • Traficar, • Adquirir, • Distribuir, • Vender, • Enviar, • Introducir, • Extraer del Territorio nacional → 1. Software Malicioso 2. Otros programas de computación dañinos
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	• Producir, • Traficar, • Adquirir, • Distribuir, • Vender, • Enviar, • Introducir, • Extraer
INGREDIENTES NORMATIVOS	• Software Malicioso • Otros programas de computación
PENA A IMPONER	*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.*

6. 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."

ARTÍCULO CÓDIGO PENAL	Artículo 269 F
CONDUCTA	• Obtener • Compilar • Sustraer • Ofrecer • Vender • Intercambiar • Enviar • Comprar • Interceptar • Divulgar • Modificar • Emplear 1. Códigos personales 2. Datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	• Obtener • Compilar • Sustraer • Ofrecer • Vender • Intercambiar • Enviar • Comprar • Interceptar • Divulgar • Modificar • Emplear
INGREDIENTES NORMATIVOS	• Códigos personales • Datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
PENA A IMPONER	*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.*

7. SUPLANTACIÓN DE SITIOS 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."

ARTÍCULO CÓDIGO PENAL	Artículo 269 G
CONDUCTA	• Diseñar • Desarrollar • Traficar • Vender • Ejecutar • Programar • Enviar → 1. Páginas electrónicas 2. Enlaces 3. Ventanas emergentes • Modificar → Sistema de resolución de nombre 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.*
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	• Diseñar • Desarrollar • Traficar • Vender • Ejecutar • Programar • Enviar • Modificar
INGREDIENTES NORMATIVOS	• Páginas electrónicas • Enlaces • Ventanas emergentes • Dominio • Dirección IP
PENA A IMPONER	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.

	La pena señalada se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito

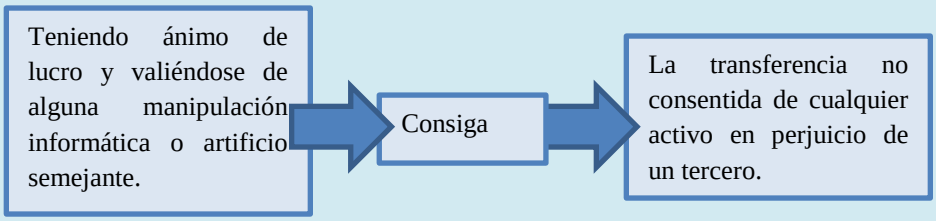
8. <u>HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.</u>

"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."

ARTÍCULO CÓDIGO PENAL	Artículo 269 I
CONDUCTA	Apoderarse de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro. • Manipulando un sistema informático, una red de sistema electrónico, telemática u otro medio semejante. • Suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	• Apoderarse
INGREDIENTES NORMATIVOS	• Medidas de seguridad informáticas • *Sistema informático,* • *Red de sistema electrónico,* • *telemático*
PENA A IMPONER	De prisión de seis (6) a catorce (14) años.

9. 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."

ARTÍCULO CÓDIGO PENAL	Artículo 269 J
CONDUCTA	
SUJETO ACTIVO	*"El que"* • Sujeto activo indeterminado
SUJETO PASIVO	Sujeto pasivo indeterminado
VERBO RECTOR	Conseguir
INGREDIENTES NORMATIVOS	• Manipulación informática
PENA A IMPONER	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.

VII. CONCLUSIONES FINALES.

Para terminar, concluiremos en este sentido:

a. Dadas las circunstancias particulares en las que se encuentran las sociedades modernas, en donde toda estructura social se encuentra involucrada con las nuevas tecnologías, su utilización se ha popularizado, casi toda la población tiene acceso a estos mecanismos, lo que genera indudablemente la primer conclusión sobre este tema, cual es, la preponderante necesidad de que el derecho penal llegue a contrarrestar las eventuales conductas delictivas que se puedan generar con estas nuevas formas tecnológicas.

b. Existen nuevos riesgos que se pueden tornar en conductas lesivas contra un nuevo bien jurídico existente que debe ser objeto de protección penal, este nuevo bien jurídico es el denominado *"la información y de los datos".*

c. Todas las personas pueden llegar a ser víctimas de este tipo de delitos, así como otras tantas pueden llegar a ser verdaderos victimarios de los mismos.

d. Siguiendo la conclusión anterior, es claro que con los delitos informáticos, un número inimaginable de personas pueden verse afectadas en sus bienes jurídicos y de no controlarse, de no enviar el correspondiente mensaje de prevención general, surgirán un número exorbitante de eventuales delincuentes informáticos.

e. Es necesario repensar las instituciones básicas del derecho penal para que estas se ajusten a las nuevas modalidades delictivas que sin duda nos llevan a replantear la forma en que pensamos al derecho penal.[28]

f. El legislador nacional consideró la teoría de los delitos informáticos en sentido amplio para la creación de la ley 1273 del 2.009, pero es necesario que desde esas esferas se vuelva a analizar el tema para desarrollar una legislación coherente y capaz de proteger el bien jurídico en mención.

g. Es necesario que los Estados generen una cooperación internacional que permita unir esfuerzos y hacer frente a estas conductas de manera eficiente, pues por su naturaleza, estas conductas pueden generar verdaderas dificultades por parte de las autoridades en términos de investigación y judicialización de las mismas.

---

[28] Miró (2.012) contextualiza la discusión que existe al respecto, señalando tres de las distintas posiciones que al respecto pueden tomarse: *"Las TIC, en general, e Internet como red global en particular, han supuesto la creación de un lugar de comunicación social transnacional, universal y en permanente evolución tecnológica que se ha venido en denominar ciberespacio, y respecto al cual nos interesa plantearnos si el mismo puede definirse como un nuevo ámbito de oportunidad delictiva, un contexto de riesgo criminal distinto al espacio nacional físico tradicional o idéntico a éste en sus caracteres esenciales; o por el contrario**, **constituye un tipo de delincuencia esencialmente nueva y respecto de la cual no son válidas las teorías criminológicas aplicables al delito llevado a cabo en el espacio físico-nacional.** En este sentido, se puede hacer referencia, en primer lugar, y desde una visión más extrema, a que la ciberdelincuencia es un tipo de delincuencia nueva para la cual no son válidas las teorías tradicionales creadas para explicar el espacio físico. En el polo opuesto se puede estar afirmando que el ciberdelito es idéntico estructuralmente al delito cometido en el espacio físico, cambiando únicamente el aspecto del mismo, pero en ningún caso sus caracteres configuradores. Y también cabe una posición intermedia, conforme a la cual la cibercríminalidad comparte con la delincuencia todos los elementos definitorios del concepto de «crimen», pero dándose los mismos de una forma tal en el nuevo ámbito que es el ciberespacio, que puede influir significativamente en la explicación del delito y, por tanto, en su prevención198. La anterior discusión se presenta debido a que los caracteres del ciberespacio en los que se ven modificados los parámetros espacio-temporales, pueden incidir en una modificación de los condicionantes del delito. Esto ya tendría una gran relevancia, pues el descubrimiento de tales modificaciones será esencial para la comprensión, primero, del alcance real de esta criminalidad, y de las razones de su aparición y desarrollo, y para su prevención, después, por medio de la modificación de las reglas de la prevención, posición que parece ser la más acertada"(P. 143)*

h. Para contestar al planteamiento inicial que motivó esta investigación, a la pregunta de si **¿Mediante el derecho penal debe protegerse o no a los sistemas informáticos?,** es necesario responder con total contundencia y basado en la seguridad que nos brindan todos los argumentos recogidos en el camino realizado con el presente estudio, que no solo puede protegerse a los sistemas informáticos, sino que además de ello **ES ABSOLUTAMENTE NECESARIO Y SE ENCUENTRA TOTALMENTE JUSTIFICADA ESTA PROTECCIÓN** de cara al nuevo bien jurídico tutelado y el papel fundamental, de vital importancia que este representa para todas las personas inmersas en esta nueva *"sociedad del conocimiento"*.

i. Es necesario entonces que el legislador nacional tenga en cuenta este estudio y las argumentaciones que en el mismo se dilucidan para que con base en ellos se replantee de manera más eficiente la protección penal de los sistemas informáticos, que si bien la normatividad vigente (ley 1273 del 2.009) es un paso importante en ese camino, así mismo encuentra bastas dificultades en cuanto a su estructuración, fundamentación dogmática y por supuesto, ello generará los respectivos problemas en su aplicación y puesta en ejecución por parte de los entes jurisdiccionales.

j. Finalmente y como se mencionó en la introducción de este trabajo, la seguridad informática, los sistemas informáticos y la información contenida en ellos, son responsabilidad de todos y cada uno de nosotros y es necesario ocuparnos de los mismos antes que sea demasiado tarde. Lo cierto es que no estamos lejos de experimentar las consecuencias adversas e inimaginables

que de su mala utilización o de su inadecuada protección puedan darse a nuestros bienes jurídicos y que de esta manera, con ello se logre poner en jaque la sociedad que conocemos y en la cual todos nos desarrollamos.

REFERENCIAS.

BIBLIOGRÁFICAS.

1. Amador, J. (2.016). Derecho Penal, vigilancia y control social. Bogotá: Grupo Editorial Ibañez.
2. Ambos, K. (2.007). El Derecho Penal frente a amenazas extremas. Madrid: Editorial Dykinson.
3. Anarte, B. (2.001). *INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS EN EL SISTEMA PENAL. APROXIMACIÓN AL DERECHO PENAL EN LA SOCIEDAD DE LA INFORMACIÓN*. Huelva: Universidad de Huelva.
4. Araujo, J. (1994). *Computer Crimes and Other Crimes against Information Technology in Brazil*. En Sieber, U. (ed) (1994). *Information Technology crime.* Köln; Berlin; Bonn; Munchen: Heymman.

5. Cabero, J. (1.998). *Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones educativas*. Granada: Grupo Editorial Universitario.
6. Herrera, R; Nuñez, A. (1999). *Derecho informático.* Santiago de Chile: Ediciones Jurídicas La Ley.
7. León, G. (2009). *Conflictividades sociales, conductas delictivas y la respuesta del sistema penal oral acusatorio en Colombia.* Bogotá: Milla Ltda.
8. León, W. (2001). *De la comunicación a la informática jurídica penal bancaria.* Bogotá: Ediciones Doctrina y Ley LTDA.
9. Mata y Martin, R. (2003). *Criminalidad informática: una introducción al cibercrimen.* Revista Actualidad Jurídica. Número 37.
10. Miró, F. (2012). *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.
11. Negroponte, N. (1.995) *El mundo digital*. Barcelona. Ediciones B. S.A.
12. Rueda, M. (2.013). *LOS ATAQUES CONTRA LOS SISTEMAS INFORMÁTICOS: CONDUCTAS DE HACKING. CUESTIONES POLÍTICO-CRIMINALES.*
13. Téllez, J (2004). *Derecho Informático*. México: Mc Graw Hill.
14. Vásquez, A (2.012). Combate a la delincuencia Cibernética. Xalapa, Veracruz: Editorial Universidad de Xalapa.

ENCICLOPEDICAS

1. Enciclopedia de la Real Academia de la Lengua Española. 2.016. Tomado de: http://www.rae.es/

LEGALES

1. Ley 599 del 2.000
2. Ley 1273 del 2.009
3. Diario Oficial del Congreso de la República. Edición 47.223 del Lunes 5 de enero del 2.009

NORMATIVAS

1. Convenio sobre la Ciberdelincuencia de Budapest. (23-Noviembre-2.001).

JURISPRUDENCIALES.

1. Corte Suprema de Justicia, Sala de Casación Penal. Sentencia 42724 del 11 de febrero de 2015. M.P. Eyder Patiño Cabrera.

SIMPOSIOS Y CONFERENCIAS

1. Vásquez C. 2.013-mayo-28. *CONFERENCIA DELITOS CIBERNÉTICOS*. (Archivo de video).

   Recuperado de https://www.youtube.com/watch?v=cg7vYTE6Z6k

2. Alonso C. 2.015-abril-30. *Semana de la Informática 2015: Ingenieros y Hackers.* (Archivo de video).

   Recuperado de https://www.youtube.com/watch?v=m6WPZmx7WoI

3. Alonso C. 2.012-abril-20. *The App Fest 2012 - Hacking, ciberguerra y otras palabrotas - Chema Alonso.* (Archivo de video).

   Recuperado de https://www.youtube.com/watch?v=QccQjXhgub0

VIDEOS EN LÍNEA.

1. Jose2News (2.012-octubre-12). SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN (Archivo de video).

   Recuperado de https://www.youtube.com/watch?v=m7bnF7XkqnU