La protección de información y los datos en el marco de la Ley 1273 de 2009: Un estudio del dato y la información como objeto material en el tipo penal hurto por medios informáticos.

Diego Alejandro González Guzmán

Universidad La Gran Colombia
Facultad de Posgrados
Especialización en Derecho Penal y Criminología
Bogotá
2017

Índice

Índice de tablas

Resumen

Dado el rápido y descontrolado crecimiento del Internet y las Tecnologías de la información y comunicación (TIC´s) en la sociedad actual, es muy recurrente que el derecho se vea rezagado respecto a tal desarrollo tecnológico que genera problemas para la protección de bienes sociales jurídicamente tutelables que cada día se ven lesionados por lo que se denomina en Colombia denominados como "delitos informáticos" desde el nacimiento a la vida jurídica de la Ley 1273 de 2009, Ley pensada para hacer frente a todas estas vulneraciones procedentes de fuentes informáticas. Por intentar ofrecer una rápida solución a esos problemas, el legislador confundió intenciones y teorías doctrinarias expuestas por los ponentes de los proyectos de Ley 042 y 123 de 2007 que dieron vida a la Ley 1273 de 2009 creando confusiones y dudas en lo que hace énfasis la presente investigación, respecto a la redacción de uno de los tipos penales incluidos en la citada Ley, el hurto por medios informáticos, por la forma en que sus elementos de tipicidad objetiva, en especial al objeto material no corresponde al propósito que se le debía dar a la Ley 1273 de 2009.

Palabras clave: Hurto, Ley 1237 de 2009, Informática, Delito; Objeto material, tipo penal, TIC´S, cibercrimen.

Abstract

By the fast and uncontrolled growing of the Internet and the communication and information technologies (TIC´s) in the actual society, is very common that the law go slower than that technology development what causes troubles to protect a legal social values that everyday can be injured for the "informatics crime" called in Colombia since the law 1273 of 2009 get in the legal life. This Law has been thought to fight against all the violations coming from the informatics sources. The legislator for try to offer a quickly solution, he confused intentions and doctrines theories exposed by the proponents Law 1273 of 2009 furthermore the legislator created confusions like that will be exposed in this research, a review of one typology criminal redaction from the Law 1273 of 2009 , in specific respect to the steal by informatics ways by the way that his criminal type objectives, specifically the material object does not match with the purpose that must be given to the law 1273 of 2009.

Keywords: steal, Law 1273 of 2009, computing, crime, material object, criminal type, TIC´s, Cybercrime

1. Acercamiento al Tema de Investigación

1.1.Introducción

El año 2009 fue importante para Colombia en materia de legislación penal porque se consolidó y entró en vigencia la Ley 1273 de 2009 o Ley de delitos informáticos, la cual ha sido una de las obras legislativas más novedosas y que impulsó a Colombia al marco internacional respecto a otros países latinoamericanos en la lucha contra este tipo de delitos, lo cual no quiere decir que se encuentre adaptada a estándares internacionales como el Convenio de Budapest sobre cibercriminalidad del año 2001.

Lo anterior se evidencia en el artículo 269I de la Ley 1273 de 2009 que contiene el tipo penal de hurto por medios informáticos, en donde el sentido de la protección de la información y los datos se ve difuminado en la medida en que éstos se mencionan como medio para facilitar la comisión de otra conducta punible como un hurto calificado y no como los datos y la información como fin a causa de que en Colombia no se considera al dato y la información en sí misma un objeto material de protección por falta de conocimiento, por cuestionarse que estos elementos no se consideran tangibles ya que no pueden ser percibidos de forma física por estar en la inmaterialidad característica de lo virtual en sistemas informáticos o en el denominado ciberespacio.

Para el estudio en concreto, se abordará uno de los tipos penales contenidos en la Ley 1273 de 2009, el hurto por medios informáticos, sus antecedentes, el estudio del objeto material de protección en hurto por medios informáticos sin perjuicio de que se aborde preliminarmente el

conflicto entre el dato y la información como bien jurídico tutelado penalmente o como objeto material de protección.

1.2.Planteamiento del problema

El legislador incluyó en la ley 1273 de 2009 un bien jurídico tutelado para la protección de la información y los datos además de un delito denominado hurto por medios informáticos; por error, el legislador confundió el objeto de protección de la ley y decidió proteger con la tipificación del delito por medios informáticos, otro bien jurídico.

La ley 1273 de 2009 presenta muchos vacíos jurídicos respecto a definiciones y conceptos en materia de información y datos que conducen a erróneas interpretaciones de su contenido; tanto así, que la descripción de la conducta del hurto por delitos informáticos, se subsume de forma taxativa en el artículo 239 dentro del cuerpo normativo de la Ley 599 de 2000 creando inseguridad jurídica al confundir y combinar los objetos de protección.

1.2.1. Pregunta

¿El delito hurto por medios informáticos protege la información y los datos como objeto material en el marco de la Ley 1273 de 2009?

1.2.2. Hipótesis

El legislador cambió el sentido de protección que se venía manifestando en las exposiciones de motivos en pro del control y lucha de los denominados “delitos de alto impacto” tal como se refleja en la ley, puntualmente en el artículo 269I, en donde el sentido de la protección de la información y los datos se ve difuminado en la medida en que se menciona a la información y datos como medio para facilitar la comisión de otra conducta punible como un hurto calificado y no la información y los datos como fin a causa de que en Colombia no se considera al dato y la información en sí misma un objeto material de protección por falta de conocimiento y por cuestionarse que estos elementos no se consideran materia física y que no pueden ser percibidos fácilmente por estar contenidos de manera virtual.

1.3.Objetivos

1.3.1. Objetivo general

Identificar y analizar si el delito hurto por medios informáticos protege la información y los datos como objeto material en el marco de la Ley 1273 de 2009.

1.3.2. Objetivos específicos

- Conocer los argumentos político-criminales expresados en las exposiciones de motivos de los proyectos de Ley No. 042 y 123 de 2007 respecto a la protección de la información y los datos.
- Identificar las características del objeto material en el delito de hurto por medios informáticos en el marco de la Ley 1273 de 2009.
- Explorar en que consiste la información y los datos como objeto material en el delito de hurto por medios informáticos en el marco de la Ley 1273 de 2009.

1.4.Metodología

El método de investigación es tipo cuantitativo en la medida que partió de una idea con un tema determinado y concreto que luego de una revisión de literatura fue delimitado construyéndose a partir del problema principal, problemas derivados y en correlación una hipótesis central e hipótesis derivadas modificadas mediante la fijación de objetivos consiguiendo así una coherencia y congruencia entre variables. Se generaron conclusiones partiendo de un método de recolección de datos, que es un punto crítico en la investigación. Sampieri, Collado & Lucio (2010) afirman: “La revisión de literatura consiste en la detección, consulta y obtención de bibliografía útil para el propósito del estudio, se tiene que extraer y recopilar la información relevante y necesaria. Esta selección será selectiva respecto al tema central de investigación” (p. 53).

La metodología adoptada es aceptada por la comunidad científica, brinda una investigación totalmente objetiva partiendo de postulados y normas de carácter jurídico con la concurrencia de pasos estructurados que ofrecen estándares de validez dentro de un ámbito de realidad objetiva, refiriéndose esto a la posición del investigador que será externa e independiente al objeto de estudio. El objetivo de esta investigación cuantitativa es la construcción y la demostración final de una teoría general para ser posteriormente aplicada y tenida en cuenta de forma particular dentro de la comunidad jurídica.

El alcance de este método cuantitativo es de carácter exploratorio porque es un tema que no ha sido desarrollado a plenitud en Colombia, aún más respecto al problema del objeto especifico de estudio dejando asi, un terreno base con conocimientos en materia de los delitos informáticos, del dato y de la información y el hurto por medios informáticos para el posterior desarrollo de investigaciones de mayor profundidad. “Los estudios exploratorios sirven para preparar el terreno y por lo común anteceden a investigaciones con alcances exploratorios, descriptivos, correlaciónales o explicativos” (Sampieri et al, 2010, p.78).

Se realizó la construcción del marco teórico mediante la extracción y recopilación selectiva de lo revisado y consultado usando un vertebramiento a partir de índices generales de carácter normativo y de literatura dividido respecto a cada variable. Dada la considerable cantidad de temas y conceptos nuevos a manejar se hace más eficiente el manejo de este método de construcción del marco teórico de manera que en la creación del índice de manera muy específica en torno a los temas que ocupan el objeto de la investigación sin extender y confundir el contenido del marco teórico.

1.5.Justificación

En Colombia, el tema de los delitos informáticos sigue siendo un tema novedoso a pesar de que la Ley se expidió hace poco más de 8 años. Existe un déficit en el tratamiento y desarrollo de este tema dejando a la Ley, a los jueces, a la Fiscalía General de la Nación , auxiliares de la justicia y todo aquellos que intervienen en la administración de justicia, rezagados en el tiempo volviéndolos ineficaces.

Esta investigación trae consigo el propósito de abrir un espacio por el cual se han de sustentar estudios más profundos en materia de los delitos informáticos en Colombia. Para lograr lo anterior, se necesita abordar problemáticas suscitadas tanto en el ámbito jurídico como en el ámbito social de la actual era de la información con el uso de las tecnologías de la información y comunicación en Colombia con un contraste a nivel internacional.

Se ayudará a replantear la forma en cómo se deben entender los delitos informáticos en Colombia, de ser posible generar una estructuración nueva y especialísima de las instituciones y áreas del derecho penal desde la teoría del delito, la criminología, derecho penal especial etc., ya que pese a haber antecedentes de la necesidad del tratamiento diferenciado a esta especie de bienes virtuales, se siguen tratando y adecuando a conceptos tradicionales como la propiedad y la privacidad que no son suficientes en un espacio de tan amplio tratamiento como es la informática o ciberespacio.

2. Generalidades de los delitos informáticos

2.1. Concepto de delito informático

Bajo una concepción general, se puede entender los delitos informáticos como aquellas conductas ilícitas tipificadas en las correspondientes leyes penales, en este mismo sentido, Menéndez y Santa Cecilia (2014) identificaron que "para las faltas, infracciones administrativas, ilícitos civiles junto con los delitos informáticos se denomina delincuencia o criminalidad informática" (p.319). Así mismo mencionan Rincón y Naranjo (2012) que dadas las características como la dificultad en su descubrimiento, persecución y prueba, por la vulnerabilidad de los sistemas y el nivel de especialización de los delincuentes se llegan a denominar, bajo la famosa teoría de Edwin Sutherland, delitos de cuello blanco en 1943. (Torres, 2002)

Existe un problema de denominación de los delitos informáticos y posteriores concepciones como la cibernética, tanto así que este problema se identifica puntualmente por:

> La utilización de neologismos en el ámbito científico que proceden de traducciones al castellano de términos en otros idiomas es algo inevitable y en ocasiones arriesgada dado que no se trasplanta una identificación completa de los sentidos mediante la traducción; en Estados Unidos, Inglaterra y Australia y demás países que tratan éste tema, no suelen hablar de *cybercriminality o cyberdelinquency* si no de *cybercryme*. Mientras que en castellano se utiliza indistintamente los términos cibercrimen, ciberdelito, cibercriminalidad o ciberdelincuencia. (Miró, 2012, p.33)

Ahora bien Menéndez y Santa Cecilia (2014) mencionan que la denominación ciberdelitos implica carácter trasnacional, un delito que se inicia en un país y el resultado se produce en otro por la incidencia del término ciberespacio, un espacio sin fronteras ni delimitaciones por ningún país.

El problema en la denominación en este tipo de delitos implica una confusión cuando se usan conceptos no correspondidos, eso lo evidencia Miró (2012) cuando "en países de habla hispana otros conceptos como criminalidad informática, delito informático procedentes de términos ingleses y alemanes *computer crime* y *Computerkriminalität* para referirse al mismo fenómeno al que se hace referencia cuando se habla de cibercriminalidad o cibercrimen" (p.34).

Podría hablarse entonces de la coexistencia de este par de términos, los delitos informáticos y los ciberdelitos; respecto al primero, su existencia dependerá de que sean delitos que se desarrollan utilizando medios como los computadores, además de cualquier tipo de tecnología con hardware y software como smartphones y tabletas electrónicas que cuentan con Sistemas Operativos tipo Android de Google o IOS de Apple entre otros como medios principales por los cuales se pueden desarrollar conductas como por ejemplo el acceder a un sistema para desactivar electrónicamente una cerradura o la desactivación de un sistema circuito cerrado de televisión (CCTV), pues se terminan usando estos medios informáticos y tecnológicos como herramientas para la comisión de delitos. Otra forma en cómo se pueden entender los delitos informáticos es en cuanto a que el delincuente usa aquellos elementos tecnológicos conformados por hardware y software (celulares, computadores, etc.) junto con el uso de redes de tráfico de información o mejor dicho de internet que les permite desarrollar sus actividades

delincuenciales, ahora más amplias en la medida en que internet le proporciona un mayor campo de acción al delincuente.

Por otro lado los ciberdelitos tienen un elemento esencial que los hace diferentes de los delitos informáticos y es el ciberespacio, en donde es posible que se desarrollen y se consuman los delitos sin que necesariamente suceda un cambio en la realidad material, solo un cambio en el ámbito virtual; sirve de ejemplo el tipo penal contenido en la Ley 1273 de 2009, la transferencia no consentida de activos del articulo 269J, que en su descripción literal se menciona solamente "la transferencia de un activo valiéndose de habilidades y artificios en perjuicio de un tercero" que no incluye el dinero tangible, físico o materialmente perceptible por los sentidos sino que solamente hay una transferencia que el legítimo depositario de esos activos no percibe tal transferencia sino hasta el aviso de la entidad bancaria donde la depositó. Del aviso dependen los sistemas de seguridad para brindar una óptima respuesta para evitar ese tipo de conductas, en este ejemplo han de considerarse las dos tipologías, la de delito informático porque hizo uso de un computador dentro de la entidad bancaria o usó internet para acceder desde la página web de la entidad bancaria, superando medidas de seguridad para hacer la transferencia; como también puede ser un ciberdelito cuando es posible que la conducta se inicie en un país X y se desarrolle o se consuma en un país Y, su carácter de transnacionalidad en el espacio virtual que se maneja hace que el ciberespacio sea el mundo en donde se cometan estas ilicitudes.

La relecancia de éste tema parte de que existe un atraso en el desarrollo jurídico de lo que son los delitos informáticos y los inconvenientes en la adopción de nuevas concepciones como los ciberdelitos que provocan dificultades en el ámbito judicial tanto para los operadores judiciales y la comunidad jurídica como para los ciudadanos que a través de los medios masivos

de comunicación conocen las manifestaciones de conductas como los ataques cibernéticos a nivel mundial; véase la utilización por parte de los medios de comunicación la denominación *cyber* y a la vez el de delitos informáticos indistintamente.

2.2. De los delincuentes informáticos a ciberdelincuentes

En relacion a la definición y adopción de conceptos de delitos informáticos o ciberdelitos; se encuentra la grave confusión al referirse a todas aquellas personas con habilidades, capacidades y medios en el manejo de la informática y computación para cometer delitos denominándolos como *hackers*. Miró (2012) mencionaba que el cine y consecuentemente los medios de comunicación han descuidado una serie de características que definen y clasifican a los delincuentes que basan su actividad delincuencial con ayuda de la informática, la información, internet tanto en el ámbito informático (reducido) o cibernético (amplio).

Tabla No 1. Clasificación general de delincuentes informáticos y ciberdelincuentes

Hacker	Es un término amplio y general distribuido por el cine para definir al típico delincuente informático con características de ser una persona aislada socialmente, con un coeficiente intelectual alto, joven y con un gusto y habilidades en informática y computación.

True hackers	Los pioneros aficionados de la informática en los inicios de ésta, alrededor de los años sesenta.
Hardware hackers	De los años setenta. Desarrolladores de hardware o dispositivos que brindaron importantes avances tecnológicos en la materia.
Game hackers	De los ochenta. Aquellos dedicados a la creación de software o programas para entretenimiento específicamente videojuegos
Cracker	Éste es el que representa la ilicitud que empieza en los años noventa, que apoyados ya de casi cuarenta años de evolución de la informática buscan el acceso ilícito a sistemas o redes, en un principio, y después al desarrollo de malware.
Pheakers, pirates, pranksters, malicious hackers, personal problem solvers, career criminals, extreme advocates, cyberpunks, scripkiddies, hacktivists, virus writers, cyber-terrorists, snoopers, spoofers, sniffers, spammers.	El desarrollo de las tecnologías y la era de la información ha ocasionado la evolución de los delincuentes informáticos, cada uno centrado en actividades delincuenciales específicas, mientras que el *spammer* adquiere direcciones de correo electrónico mediante el envío masivo de correos electrónicos infectados, el *spoofer*

	se encarga de suplantar la identidad virtual de otro usuario.
Ciberactivistas	Encaminados no necesariamente a la producción de un daño, o intención maliciosa, si no con la intención de lanzar mensajes ideológicos, de luchas políticas en pro, la mayoría de la libertad en internet.
Ciberterroristas	Pueden partir de tres tipos de categorías, la primera como medio de incitación y propaganda terrorista a través de la web; la segunda en donde se reclutan terroristas, se adiestra en diferentes actividades como la fabricación de explosivos, órdenes a las células terroristas etc. y una tercera de un carácter más puro en relación a la actividad en el ciberespacio representado en ataques DoS, infección con malware destructivo e intrusivo.

Nota: tomado de: Miró, F. (2012). *El cibercrimen*.

No se incluyó en la anterior tabla un tipo de *hacker* al que se hace referencia como *white hat*, traducido al español, “sombrero blanco” que son aquellos que muchas veces son contratados

por empresas para que descubran de vulnerabilidades en sistemas informáticos privados para así reducir el de riesgo de un ataque de su contraparte, un *hacker black hat*, traducido al español como sombrero negro o *cracker*.

Miró (2012) explica las modalidades del cibercrimen atendiendo a criterios criminológicos lo que evidencia una mayor gama de conductas que atentan intereses económicos, sociales y políticos mucho más allá de meras intrusiones a sistemas informáticos y el *phishing*.

Tabla 2. Modalidades de cibercrimen

	Ciberataques puros	Ciberataques replica	Ciberataques de contenido
Cibercrimenes económicos	• *Hacking* • *Malware* intrusivo • *Malware* destructivo • Ataques de *insiders* • Ataques DoS • *Spam* • Ciberocupacion red • *Antisocial networks*	• Ciberfraudes (*phishing, pharming, scam, auction fraud…)* • *Cyberspyware* (uso de *sniffers* y demás *spyware*, ciberespionaje de empresa) • *Identity theft* • *Spoofing* (*DNS spoofing, ARP spoofing, IP spoofing, web spoofing*) • Ciberblanqueo de capitals • Ciberextrosion • Ciberocupacion	• Distribución de pornografía infantil en internet • Ciberpirateria intelectual
Cibercrimenes sociales		• *Spoofing* • *Cyberstalking*	

		• *Cyberbullying* • *Online harassment* (ciberamenazas, coacciones, injurias, etc.) • *Sexting* (y extorsión con imágenes de *sexting*) • *Online grooming*	
Cibercrimenes políticos	• Ataques DoS (*cyberwar)* • Ataques DoS (*cyberhacktivism)* • *Malware* intrusivo	• Cyberespionaje terrorista • Ciberguerra	• *Online hate speech* • Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

Nota: tomado de: Miró, F. (2012). *El cibercrimen*. p.50

Ya lo mencionaba Rincón y Naranjo (2012) al *hacking*, entendido como el acceso legitimo informático y el *cracking* como destrucción o daño de la información en medio informático; es decir que la diferenciación de cada tipo de delincuente es importante dado que criminológicamente requiere un estudio diferenciado para la comprensión del fenómeno delictivo para la elaboración de una política criminal sólida y coherente que pueda atender a este tipo de delincuencia en el contexto colombiano, que en gran parte desconoce de todas estas facetas y evoluciones.

2.3. Evolución del término delincuencia informática a cibercriminalidad

Miró (2012) explicó la evolución de los conceptos desde Alemania así:

> En un principio, los alemanes, pioneros de la Ley de delitos informáticos alrededor de los años setenta, construyeron este concepto no para identificar un grupo autónomo por su metodología, por su contenido de protección o por cuestiones de política criminal si no por sus características, es decir, como medio o como objeto sobre el que recaía el ataque; posturas aceptadas doctrinariamente; lo que implicaba que eran aquellos actos realizados a través de procesos electrónicos o por el desarrollo base de delitos tradicionales que recaían sobre bienes relacionados con la informática, el hardware y el software sin que aún se hiciera un estudio de respecto a los bienes jurídicos afectados en los delitos de contenido económico. Ulrich Sieber, *Computerkriminalität und Strafretch* (como se cita en Miró, 2012, p.34)

Ulrich Sieber (1985), jurista alemán pionero en este país en tratar el tema de la informática y sus implicaciones en el derecho, en específico en el área de los delitos informáticos, distingue entre tres categorías los delitos informáticos, la primera consistente en aquellos de contenido patrimonial, fraude informático, espionaje y sabotaje informático; la segunda de delitos cometidos por medio de sistemas informáticos contra derechos de la personalidad y la tercera referente a la afectación de bienes sociales o supraindividuales. Luego se amplían estas categorías por parte del mismo jurista atribuyendo aquellos delitos que son lesivos de la privacidad; Es así que en la categorización de Sieber se distingue que los “delitos informáticos” protegen aquellos bienes como patrimonio y orden económico, la libertad sexual e

intimidad y otros supraindividuales o difusos. Ulrich Sieber, *Informations technologie und Strafrechreform* (como se cita en Miró, 2012, p.35)

El problema de identificar un bien jurídico común para proteger bienes sociales fue un asunto complicado de delimitar por cuestiones de la evolución de la informática y la tecnología con la adaptación de la sociedad a tales cambios. La solución era entonces crear un ámbito de riesgo en cada momento de la evolución de estas tecnologías lo que implicaba el cambio de los tipos penales preexistentes para adecuarlos o la creación de nuevos tipos penales que abarcaran la naciente realidad tecnológica. (Miró, 2012)

Se retoma entonces, la idea de que a partir de estos cambio tecnológicos descontrolados por su rápida expansión y evolución, Miró (2012) afirma que algunos países han optado por variar el término delitos Informáticos hacia el término, de origen anglosajón *cybercrime*; es necesario resaltar que tal cambio de denominación es la inclusión del prefijo *cyber*, que hace referencia a lo que exponía el novelista William Gibson en su obra *Neuromancer* en 1984, un mundo virtual separado del real, donde las personas interactuaban denominado "*the cyberspace"* o el ciberespacio; así pues que el prefijo *cyber* junto con el término *crime* para identificar a la delincuencia y el crimen hacen que la palabra *cybercrime* haga referencia a toda la delincuencia y los crímenes desarrollados en el ciberespacio.

Torres (2002) menciona desde otra perspectiva en relación a su origen, que "la palabra cibernética, etimológicamente proviene del griego *cibernetics [sic]* que significa arte del timonero".

El cambio de denominación tiene raíces criminologías dado los nuevos comportamientos y preocupaciones legales que se desarrollan es este nuevo espacio. Gracias a la concientización de la existencia de este ciberespacio se ha creado un nicho histórico en los delitos informáticos o ciberdelincuencia que puede dividirse en tres momentos según Wall (2007) explicados así:

> Un primer momento anterior al ciberespacio donde los computadores eran medio de comisión de delitos, un segundo momento en donde gracias a la expansión del internet y las redes de comunicación, los delitos se cometían específicamente a través de internet y un tercer momento en donde estos delitos están determinados por la existencia del internet y de las tecnologías de la información y comunicación. Ya no se concibe la idea de que el computador es mero medio para la comisión de delitos, o que solo mediante el uso del internet es posible comisión de delitos si no que es posible que el mismo internet sea un medio para desarrollar los delitos y posiblemente sea también internet susceptible de afectación, modificación, daño, etc. David Wall *Cybercrime: the transformation of crime in the information age* (Como se cita en Miró, 2012, p.44)

2.4. Confusión con el término delitos electrónicos

"Los delitos electrónicos son una especie del género de delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha no se encuentran legislados pero que poseen como bien jurídico tutelado en forma

específica la integridad de los equipos electrónicos y la intimidad de sus propietarios" (Rincón y Naranjo, 2012, p.53).

Rincón y Naranjo (2012) toman como base las manifestaciones del profesor Campoli respecto a la diferenciación entre delito informático y delito electrónico, en que los primeros ya se encuentran tipificados con su respectivo bien jurídico tutelado y respecto a los segundos que al ser perpetrado a través de medios informáticos entra en la especie de los delitos informáticos.

2.5. Contextualización de los delitos informáticos en Colombia antes de la Ley 1273 de 2009

2.5.1. normatividad anterior.

El decreto 1360 de 1989 fue uno de los primeros antecedentes normativos en Colombia respecto a la protección de la información o datos en materia de propiedad intelectual, en éste decreto se reglamentaba el registro de software o soporte lógico en el Registro Nacional de Derechos de Autor y posteriormente en la Ley 44 de 1993 que modifica y adiciona la Ley 23 de 1982 sobre derechos de autor, en el título IV se sanciona conductas que atentan a los referidos derechos de autor.

En la Ley 599 de 2000 se incluyeron delitos contra la libertad individual en materia de intimidad, reserva e interceptación de comunicaciones en artículos como el Artículo 192 (Violación ilícita de comunicaciones), Artículo 193 (Ofrecimiento, venta o compra de

instrumento apto para interceptar la comunicación privada entre personas), Artículo 194 (Divulgación y empleo de documentos reservados), Artículo 195 (Acceso abusivo a un sistema informático), Artículo 196 (Violación ilícita de comunicaciones o correspondencia de carácter oficial) y el Artículo 197 (Utilización ilícita de equipos transmisores o receptores).

Luego se expidió la Ley 679 de 2001 que estableció un estatuto para la prevención de la explotación, pornografía y turismo sexual de menores de edad, que permite sancionar, de carácter netamente administrativo a los servidores, proveedores, administradores o usuarios que alojen imágenes, textos, etc., relacionados a la materia del estatuto. Para darle alcance penal a la Ley 679 de 2001 se sanciono la Ley 1336 de 2009 en la cual se castiga con penas de prisión y multas por las mismas conductas.

Nace a la vida jurídica la Ley estatutaria 1266 de 2008 que dispone y regula el Habeas Data y el manejo de la información de bases de datos personales en especial, de carácter financiero.

2.5.2. antecedentes jurisprudenciales.

En materia jurisprudencial se ha aclarado situaciones relacionadas al manejo de los datos informáticos, la revisión de equipos, la inspección registro y allanamiento en materia informática en sentencias C-366 de 2007 y C-334 de 2010 de la corte constitucional respecto a la introducción de los archivos digitales o documentos computarizados como susceptibles de registro.

En sentencia T 414 de 1992, el Magistrado Ponente Ciro Angarita Barón invitó a un experto investigador en materia de ingeniería de sistemas y computación Ernesto Lleras para emitir un concepto en la elaboración del fallo de tutela, en donde se evidencian aspectos totalmente novedosos para esa época como lo fueron:

> La propiedad o titularidad del dato desde la teoría de la información; la responsabilidad en el manejo de los bancos de datos; el "poder informático" o capacidad de control sobre la acción de las personas que pueden llegar a tener quienes manejan bancos de datos; el derecho a la información y el derecho a la intimidad; la vigencia del dato y el derecho al olvido. (Corte constitucional de Colombia, Sentencia de Tutela No. 414)

En esta sentencia se menciona que ahora se demandaría la protección ante lo que se denominó el “poder informático” y de esta misma forma una diferenciación de la intimidad en dimensiones como el secreto a la vida privada y la libertad. La corte considera pertinente en esta sentencia tratar el problema jurídico del tratamiento de datos e información bancaria, el tema del dato y su propiedad.

La Corte Constitucional de Colombia (Sentencia de Tutela 414 de 2002) mencionó que:

> El dato es un elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que el dicho dato adquiera sentido. Los modelos se plasman en forma de textos y mensajes que consisten en una serie de signos algunos de los cuales les llamaremos datos, organizados de acuerdo a sistemas de reglas o gramática.
>
> El dato se constituye entonces en el elemento básico de información sobre eventos o cosas. El dato que constituye un elemento de la identidad de la persona, que en conjunto

con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso. Datos de este tipo serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo en las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una "huella digital" porque el individuo es identificable a través de ellos. Por las características propias de los datos, una vez producidos (codificado un evento u objeto por alguien o eventualmente una máquina) pueden diseminarse con relativa facilidad. Esto hace que puedan ser usados, en combinación con otros de procedencias distintas pero adscribibles a la misma persona. Así se va configurando lo que ha dado en llamar un "perfil de datos de una persona". Estos perfiles pueden construirlos quienes tengan bancos de datos bien sea manuales o sistematizados, y el poder de información y control social que estos tengan depende del uso de la tecnología disponible. El problema del "poder informático" existe siempre que se poseen datos sobre las personas bien sea en forma manual o por medios electrónicos. Con el desarrollo de estos últimos, las posibilidades de acción de ese poder en contra de la libertad de las personas se magnifican y harían necesaria una legislación especial.

El "perfil de datos" de la persona se constituye entonces en una especie de "persona virtual" sobre la cual pueden ejercerse muchas acciones que tendrán repercusión sobre la persona real. Desde el envío de propaganda no solicitada, hasta coerción u "ostracismo" social como en el caso que se presenta. Un "buen" manejo de Bancos de Datos permitiría identificar hasta perfiles poblacionales desde distintos puntos de vista, lo cual constituye un evidente

> peligro de control social de aquellos que ostentan "poder informático", no solamente contra la libertad de las personas individuales sino contra la de sectores sociales más amplios.

Así mismo hacía énfasis la Corte Constitucional de Colombia (Sentencia de Tutela 414 de 1992) en la adopción del dato como un objeto especialísimo y su aplicación jurídica, es decir que para el dato no podía aplicarse el derecho clásico de propiedad y que en este ámbito virtual se podrían diferenciar varios sujetos como lo son: “El sujeto del cual se dice algo o le concierne algo; el que aplicando códigos o gramáticas hace que el dato se convierta en información y otro el que hace circular o hace difusión de la información”.

En sentencia de unificación SU 082 de 1995 menciona que el núcleo esencial del habeas data está conformado por el derecho a la autodeterminación informática y la libertad, en especial la económica. “La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales” (Corte constitucional de Colombia, SU 082 de 1995).

La sala de casación de la corte suprema de justicia manifiesta que:

> El delito de hurto por medios informáticos y semejantes protege un bien jurídico intermedio, por cuando salvaguarda “la confidencialidad, integridad y disponibilidad de los sistemas informáticos, de las redes y de los datos” y por igual es una “figura llamada a completar las descripciones típicas contenidas en los artículos 239 y siguientes del Código Penal, a las cuales se remite expresamente”. El hurto por medios informáticos y semejantes por tratarse de una conducta punible que protege un bien jurídico intermedio, puesto que a la par que ampara la información, las redes y los datos, también salvaguarda el patrimonio económico, de manera que es indudable que integre la denominación genérica (*nomen iuris*) de los

> delitos contra el último bien jurídico en cita. Por tanto, no le asiste la razón al demandante cuando aduce que la infracción anotada (hurto por medios informáticos y semejantes) no está dentro de aquellos ilícitos que protegen el patrimonio económico y que de allí se deriva la afectación al principio de congruencia. (Sala de Casación penal, Corte Suprema de Justicia, No.45865)

2.5.3. antecedentes de iniciativas respecto a la protección de información y datos.

Los antecedentes directos los traen de primera mano las exposiciones de motivos de los proyectos de Ley número 042 y 123 de 2007; en el primero de ellos se manifestó que en una sociedad altamente tecnificada y globalizada se encontraba bajo el influjo de la informática que ha transformado el modo de vida de las personas para facilitar la forma de comunicación entre ellas, aunque este avance y esta interconectividad pueda ser usada para ocasionar daños por aquellos que tienen talentos y conocimientos en los sistemas de información (Cotrino, 2007).

Por ser novedosas tales conductas basadas en la información y los medios informáticos, no se encuentran tipificadas, y si lo estuvieran para casos en concreto, presentarían problemas en la aplicación.

En la exposición de motivos del segundo de los proyectos de Ley se insistía una vez más ante el congreso de la república la importancia de sancionar y regular conductas que no se tenían en cuenta en materia penal. Gómez y Piedrahita (2007) hacen la primera diferenciación respecto a lo que es un delito informático y un hecho punible que ha usado medios “electrónicos” para su consumación, también se manifestaba que ya eran conductas socialmente reprochadas. Se

expresa que los tipos penales contenidos en el proyecto de Ley eran solamente autónomos y no subordinados siguiendo la costumbre legislativa en el mundo además tener la observancia de cómo se debe abarcar o tratar la teoría de los delitos informáticos en cuanto a que sean como medio o como fin; entre otros.

Aun luego de haberse expedido la Ley de delitos informáticos, se empezaron a crear instituciones, divisiones y organismos dedicados a manejar asuntos de las tecnologías de la información y la comunicación; Se encuentra que en el 2009 mediante la Ley 1341 se crea el ministerio de las tecnologías de la información y comunicaciones, se propone el Consejo Nacional de Política Económica y social de la Ciberseguridad del Departamento Nacional de planeación, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT, el Comando Conjunto Cibernético de las Fuerzas Militares y el Centro Cibernético Policial. (Rincón y naranjo, 2012)

Es así que desde ese momento, se está comprendiendo el problema de la delincuencia informática y se ha propuesto el desarrollo de formas de protección y control de las tecnologías de la información y de la comunicación.

3. Ley de delitos informáticos en Colombia

Para que pudiera existir la Ley 1273 de 2009, el proyecto de Ley 042 se acumuló con el proyecto de Ley 123 ambas del 2007, ya que individualmente los trámites legislativos correspondientes a cada uno, estos proyectos fueron archivados.

Por parte de una ponencia del senador Parmenio Cuéllar Bastidas ante la Comisión Primera del Senado donde los proyectos de Ley 042 y 123 acumulados se convirtieron en el proyecto de Ley 281 de 2008, haciendose varias apreciaciones entre las que se destacan a manera de critica la hiperproducción de leyes penales sin la creación de otras formas o vías para la solución de problemas de una "sociedad con múltiples problemas y pocas oportunidades", con base en el derecho penal se cuestiona la característica del derecho penal como de *ultima ratio* o derecho penal mínimo; se apoya más en la idea del manejo de la adecuación de tipos penales a las realidades que en la creación de nuevas denominaciones y descripciones porque en la legislación preexisten varios tipos penales que podrían adecuarse a tales conductas en relación al uso de las redes y el internet.

Una de las manifestaciones más importantes para la presente investigación es la mención de que si preexisten tipos penales que recogen la esencia del comportamiento a reprimir, es completamente innecesario crear nuevos tipos con "nuevas" denominaciones y descripciones. (Rincón y Naranjo, 2012)

Un punto importante mencionado por el senador Cuéllar está relacionado con elementos como la preexistencia de tipos penales para reprimir comportamientos similares, señalado por la

comisión primera, fue la definición de la técnica en la creación de la tipicidad, a saber, la relación entre los conceptos de esencias y fenómenos como límites al causismo como enemigo de la cientificidad; el causismo es entendido como el intentar dar soluciones a todos los casos o fenómenos en concreto si no la creación de la regla general alrededor de un fenómeno principal así evitando la explotación legislativa. (Rincón y naranjo, 2012)

Se explica lo anterior con la figura del Hurto, partiendo de la esencia del apoderamiento de algo ajeno; existe el paquete chileno, el hurto violento o la apropiación de dinero por medios informáticos que siendo individuales no se pueden agrupar pero si se recurre a la mencionada esencia para unirlos se encuentra que se corresponden. (Rincón y Naranjo, 2012)

Posteriormente la comisión en un estudio de los proyectos de ley acumulados y al llegar al asunto del hurto por medios informáticos lo que se alude por parte del senador Cuéllar ante la comisión primera es textualmente:

> Trata el artículo de convertir el hurto por medios informáticos en hurto agravado. Si se observan los actuales artículos 239 y 240 del código penal, dicha relación se establece sin ninguna modificación, pues el numeral cuarto del articulo 240 agrava el hurto con ganzúa, llave falsa, superando seguridades electrónicas u otras semejantes. En consecuencia no es correcto recalcar la relación ya existente. (Rincón y naranjo, 2012, p.106 y 107)

Lo que se demuestra lo mencionado anteriormente por la comisión respecto a la preexistencia de conductas y el causalismo. Así pues el senador Cuéllar concluye su ponencia

proponiendo el archivo del proyecto de Ley 281 de 2008 (acumulado de los proyectos 042 y 123 de 2007). (Rincón y Naranjo, 2012, p.109)

Se sabe que se concilió el texto del proyecto de Ley 281 de 2008 corrigiendo lo mencionado por el senador Cuellar ante la comisión primera mediante una comisión accidental de conciliación ante las plenarias del Senado de la República y de la Cámara de Representantes, en donde al final prosperó y se aprobó la Ley 1273 de 2009. (Rincón y Naranjo, 2012)

3.1. Proyecto de Ley 042 de 2007

3.1.1. exposición de motivos.

Germán Varón Cotrino, representante a la cámara y ponente en la exposición del proyecto de Ley 042, empieza a hacer referencia de la situación en la que se encontraba la sociedad para el año 2007, la tecnificación, la globalización y la situación de las relaciones sociales permeadas por la tecnología. En el sentido en que la sociedad se adaptaba al rápido desarrollo tecnológico, también lo hacían los delincuentes que, a palabras de Cotrino "utilizan su privilegiado talento y conocimiento en los sistemas informáticos para sacar provecho en detrimento de sus semejantes". Conductas que por ser tan novedosas que no estaban tipificadas o que si se hacía aplicación de la norma penal existente no terminaban de adecuarse al tipo penal lo que implicaba o resultaba en una atipicidad objetiva.

La presentación de ese proyecto tenía la iniciativa de castigar las novedosas conductas y de agravar unos tipos penales cuando en esos tipos penales, el verbo rector se desarrolle a través de medios informáticos o cuando recaigan sobre éstos, todo lo anterior bajo el argumento de que estas personas que aprovechando todas esas habilidades y condiciones en el área de la informática, necesitan mayor censura porque es la mayoría de la población la que se encuentra en desventaja frente al uso de las TIC; puesto que una cosa es el manejo "normal" basado en la comunicación, relación social y como elemento de ofimática y otra la habilidad que tienen otras personas para hacer intrusiones a sistemas, modificar, eliminar o copiar datos y archivos, transferencia de dinero, desactivación de seguridades, etc., que un ciudadano del común no podría desarrollar, en eso se basa la desventaja.

También se hace mención de tres tendencias internacionales respecto al manejo de los delitos informáticos; la primera tendencia es la legislación especial diferente a la penal; la segunda es la de optar por crear un espacio especial en la legislación penal para la protección de un nuevo bien jurídico a tutelar: la Información y Seguridad Informática y la tercera tendencia ha sido modificar el articulado preexistente sin la necesidad de crear nuevos bienes jurídicos tutelados o de modificar los existentes.

En el anterior aparte de la exposición de motivos se hace evidente, pero necesario el mostrar que efectivamente al final se optó por la creación de un nuevo acápite y un nuevo bien jurídico tutelado, el presente proyecto de Ley se inclinaba a la modificación del articulado preexistente sin que se hiciera el ejercicio de crear un nuevo bien jurídico tutelado bajo la óptica de que hay que adaptar la norma penal a nuevas realidades y que si bien hay conductas

tradicionales que utilizan los medios informáticos como medios, no los hacen delitos informáticos .

Es así que ésta la propuesta parece resolver el asunto de atipicidad relativa. argumenta el señor Cotrino que cuando se opte por la creación de un capítulo especial que contengan a los delitos informáticos "con base en la elevación a bien jurídico tutelado del o el derecho a la información relacionada con el dato informático (información almacenada, procesada y transmitida a través de sistemas informáticos) o el bien jurídico de la seguridad informática en la medida de que así se entiende la necesidad de protección en contra de ataques que pueden lesionar otros bienes jurídicos tutelados como la intimidad y la propiedad", también menciona que la doctrina ha señalado tanto al derecho de la información o la seguridad informática como bienes jurídicos medio que protegen otros bienes jurídicos como dignos de tutela penal; se generan así propuestas para el legislador al momento considerar la creación de un nuevo bien jurídico tutelado y su posterior denominación entre las dos posibles denominaciones tal como lo exponía la exposición de motivos y no como terminó denominándose en la Ley 1273.

Se resalta al delito informático como una acción delictiva en donde los computadores o los sistemas de procesamiento de datos son material y objeto; se parte de una triple dimensión de los datos como lo son la confidencialidad afectados por conductas como espionaje informático o la intrusión en sistemas informáticos; la integridad afectada a su vez por conductas como el sabotaje informático mediante el uso malware o software malicioso y la dimensión de la disponibilidad de los datos afectada mediante el *spam* o los ataques de denegación de servicios (DoS). Así pues que el respeto de estas dimensiones crea seguridad a todos y por otro lado el

irrespeto de estas dimensiones afectaría derechos colectivos o supraindividuales que son dignos de protección.

3.1.2. contenido normativo.

Este proyecto fue una de las primeras propuestas para la elaboración de una Ley que castigara conductas derivadas del uso ilícito de las tecnologías de la información y la comunicación.

Tabla 3. Proyecto de Ley 042 de 2007

Bien jurídico con intención de proteger: la información o la seguridad informática	
Artículo 1°. Definiciones	Sistema Informático. Es todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa de ordenador. Datos Informáticos. Cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función. Dato personal. Todo dato que permita la identificación e individualización de una persona natural y que sea susceptible de tratamiento informático.

	Sistema de autenticación. Cualquier procedimiento que se utilice para identificar de manera unívoca a un usuario de un sistema informático. Sistema de autorización. Cualquier procedimiento que se utilice para verificar que un usuario identificado está autorizado para realizar determinadas acciones.
Artículo 2°. Modificación artículo 193 de la Ley 599 de 2000	Se cambia el verbo rector que era múltiple, de ofrezca, venda o compre, por poseer y comercializar
Artículo 3°. Modificación artículo 195 de la Ley 599 de 2000 quedará así	Se modifica el tipo relativo al Acceso Abusivo a un sistema informático para darle claridad a su descripción, cambiando el ambiguo término abusivamente por el de sin autorización o con finalidad distinta de la autorizada que facilita su aplicación al operador jurídico. Igualmente se endurece la pena buscando efectos persuasivos para la conducta.
Artículo 4°. adición nuevo artículo al Capítulo VII Título III del Libro Segundo de la Ley 599 de 2000	Artículo 195A. Violación a la disponibilidad de datos informáticos. El que sin autorización, por cualquier medio impida el acceso normal a un sistema informático o a los datos informáticos allí contenidos
Artículo 5°. adición nuevo artículo al Capítulo VII Título III del Libro Segundo de la Ley 599 de 2000	Artículo 195B. Circunstancias de agravación punitiva. Las penas previstas en los artículos 195 y 195A se duplicarán si concurriere alguna de las siguientes circunstancias: 1. Cuando se haya instalado un programa de ordenador o instalado un dispositivo que de

	cualquier manera atente contra la confidencialidad o integridad de los datos informáticos almacenados en el sistema informático. 2. Cuando los datos informáticos almacenados en el sistema informático pertenezcan a una entidad que cumpla funciones públicas. 3. Cuando los datos informáticos almacenados en el sistema informático pertenecen al sector financiero4. Cuando la acción se realizare por una persona con una relación contractual con el propietario de los datos. 5. Cuando la persona obtuviere provecho para sí o para un tercero. 6. Cuando se den a conocer a terceros los datos informáticos así obtenidos o se procese, recolecte o circule los datos personales o los datos de autorización o autenticación del sistema informático. En todos los casos el juez podrá imponer como pena accesoria la interdicción de acceder o hacer uso de sistemas informáticos.
Artículo 6°. Modificación numeral 6 del artículo 240 del Código Penal quedará así	Manipulando un sistema informático, redes de sistemas electrónicos, telemáticos u otro medio semejante; superando medidas de seguridad informáticas o suplantando un usuario ante los sistemas de autenticación y autorización establecidos. El juez podrá imponer como pena accesoria a la conducta calificada en este numeral la interdicción de acceder o hacer uso de sistemas informáticos.
Artículo 7°. Adición parágrafo al artículo 265 de la Ley 599 de 2000 quedará así	Parágrafo. Si el daño recae en datos y sistemas informáticos ajenos la pena será de dieciocho (18) a treinta y seis (36) meses.

Artículo 8°. Aumento de penas en el artículo 308 de la Ley 599 de 2000 quedará así	La pena será de cuarenta y ocho (48) a ciento veintiséis (126) meses de prisión y multa de ciento treinta y tres punto treinta y tres (133.33) a cuatro mil quinientos (4.500) salarios mínimos legales mensuales vigentes, si se obtiene provecho propio o de tercero o si el acceso indebido de que trata el inciso anterior se logra valiéndose de medios informáticos y superando las medidas de seguridad informáticas existentes.
Artículo 9°. Aumento de penas en el artículo 463 de la Ley 599 de 2000 quedará así	La pena será aumentada en una tercera parte si la conducta se realiza por medios informáticos con violación de la seguridad informática existente.

Nota: Información tomada de Cotrino, G. (2007). *Proyecto de Ley 042 de 2007*.

Su contenido distribuido en diez artículos comprenden conceptos básicos para la adecuada aplicación de la norma, la modificación y adición de artículos a la Ley 599 de 2000 en el título correspondiente a la violación de la intimidad, reserva y violación de comunicaciones como el cambio de verbos rectores, aclaración de ambigüedades y la adicción de una modalidad de delito informático denominada secuestro de datos, se agregaron causales de agravación y el endurecimiento de las penas en tipos penales como el hurto calificado.

3.2. Proyecto de Ley 123 de 2007

3.2.1. exposición de motivos.

En este proyecto de Ley, el senador Luis Humberto Gómez Gallo y el representante a la cámara Carlos Arturo Piedrahita con aportes de un tratadista, un académico y dos jueces

colombianos, colaboraron para abrir nuevamente el debate de la necesidad de la tipificación de los delitos informáticos. Resaltan nuevamente la importancia de que en la sociedad actual el uso de los computadores y sus amenazas que afectan tanto a individuos como empresas, se construyó así un decálogo de tipos penales con nuevos verbos rectores aplicables solamente a las circunstancias que ofrece el campo de la informática.

Se trata el tema de la legitimidad del documento electrónico, el dato y la información en Colombia, lo que los haría susceptibles de ser el bien jurídico tutelado vulnerado, se menciona también que para hablarse de delito "electrónico" debe haber dos presupuestos básicos, uno es que esté tipificada en la Ley y el segundo que mediante sentencia condenatoria se haya demostrado la existencia de una conducta típica, antijurídica y culpable; presupuestos que aún no tienen aplicación en Colombia lo que se traduce en una atipicidad de una conducta socialmente reprochable.

Precisamente es necesario explicar en qué consiste el bien jurídico tutelado de la información, que ha sido almacenada, tratada y transmitida a través de sistemas informáticos; en su amplitud, titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad e intimidad y la observación de que subsidiariamente pueda proteger otros bienes jurídicos tutelados como la propiedad.

Se hace énfasis en que los tipos penales que se encuentran en el proyecto de Ley 123 son tipos autónomos no subordinados por circunstancias genéricas o específicas de agravación de otros tipos penales, es así como se ha venido manejado en el mundo.

Se hacen precisiones de que el delito informático, la informática, los datos y la información son en principio medios para la comisión de otros delitos; por otro lado su contenido autónomo puede afectar un bien jurídico como la información y una última concepción en donde son como fin en sí mismos en la medida en que el sobre el mismo computador recaiga la ofensa al igual que los datos e información contenida en él. Como medio es simplemente como herramienta para cometer delitos tradicionales y como objeto de prueba en la medida en que pueden contener elementos materiales probatorios de un acto delictivo.

Se hace una descripción detallada de cada uno de los diez nuevos tipos penales como la protección de información privilegiada, el uso de software malicioso, estafa informática entre otros de los cuales no se encuentra el hurto por medios informáticos.

3.2.2. contenido normativo.

El primer artículo de este proyecto trata la adición del título VII bis denominado de la protección al código penal, bajo el artículo primero se agregan al título los siguientes tipos penales y las descripciones de las conductas constitutivas de delito.

Tabla 4. Proyecto de Ley 123 de 2007

Bien jurídico tutelado: la protección de la información	
Artículo 269A. Espionaje informático	El que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida o recicle datos informáticos de valor

	para el tráfico económico de la industria, el comercio, o datos de carácter político y/o militar relacionados con la seguridad del Estado
Artículo 269B. Acceso ilegítimo a sistemas informáticos	El que haga uso de los medios informáticos o de telecomunicaciones y sus soportes de información, programas y sistemas operativos, de aplicaciones de seguridad, poniendo en riesgo la confidencialidad, seguridad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca, conserve o transmita. Parágrafo. Si los hechos descritos en el artículo anterior se cometen utilizando redes o sistemas estatales, gubernamentales, de organizaciones comerciales o educativas, nacionales, internacionales, o de país extranjero, la pena se aumentará
Artículo 269C. Bloqueo ilegítimo a sistemas informáticos	El que sin estar facultado, emplee medios tecnológicos que impidan a persona autorizada acceder a la utilización lícita de los sistemas o redes de telecomunicaciones Parágrafo. Si el bloqueo genera riesgo para la seguridad nacional, la pena se aumentará
Artículo 269D. Uso de virus (software malicioso)	El que produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional virus (software malicioso) u otros programas de computación de efectos dañinos Parágrafo. La pena prevista en este artículo se aumentará si la conducta se realizare en provecho propio o de un tercero por parte de empleado o contratista del propietario del sistema informático o telemático, o por un servidor público.

Artículo 269E. Abuso de uso de medios informático	El que sin autorización o excediendo la que se le hubiere concedido, con el fin de procurar un beneficio indebido para sí o para un tercero, intercepte, interfiera, use o permita que otra use un sistema o red de computadoras o de telecomunicaciones, un soporte lógico, un programa de computación o una base de datos, o cualquier otra aplicación informática o de telecomunicaciones Parágrafo. La pena prevista en este artículo se aumentará si la conducta se realizare con el propósito de enviar correos o mensajes no solicitados o autorizados en forma masiva o individual.
Artículo 269F. Daño informático	El que destruya, altere o inutilice un sistema de tratamiento de información o sus partes o componentes lógicos, o impida, altere, obstaculice o modifique su funcionamiento La pena se aumentará cuando: 1. El propósito o fin perseguido por el agente sea de carácter terrorista. 2. Como consecuencia de la conducta del agente sobreviniere peligro o daño común. 3. El acto dañoso se ejecute sobre bien de propiedad de una entidad estatal. 4. Si la conducta se realizare en provecho propio o de un tercero, por parte de empleado o contratista del propietario del sistema informático o telemático, o por un servidor público.
Artículo 269G. Estafa informática	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 Parágrafo. La pena se aumentará hasta si el monto del activo transferido es superior a 100 salarios mínimos legales mensuales vigentes.
Artículo 269H. Suplantación de sitios web para capturar datos personales (Phishing).	El que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas (web site), enlaces (links) o ventanas emergentes (pop up). En las mismas sanciones incurrirá el que, con el fin de inducir, convencer a los consumidores a divulgar información personal o financiera, modifique el sistema de resolución de nombres de dominio, lo que hace al usuario ingresar a una IP diferente en la creencia de que está accediendo a su banco u otro sitio personal o de confianza La pena señalada en los dos incisos anteriores se agravará si para consumarlo el phisher ha reclutado Phishing mulas en la cadena del delito.
Artículo 269I. Falsedad informática	El que sin autorización para ello y valiéndose de cualquier medio electrónico, borre, altere, suprima, modifique o inutilice los datos registrados en una computadora
Artículo 269J. Violación de datos personales	El que, con provecho para sí o para un tercero y sin autorización, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee datos personales que se encuentren en ficheros, archivos, bases de datos o medios semejantes, públicos o privados Las penas previstas en este artículo se aumentarán si las conductas se realizaren en provecho propio o de un tercero por parte de empleado o

	contratista del propietario del sistema u operador informático o telemático, o por un servidor público. Las mismas sanciones se impondrán al que realice dichas conductas cuando la información vulnerada corresponda a un menor de edad.

Nota: Gómez, L., y Piedrahita, C. *Proyecto de Ley 123 de 2007*.

Lo especifico de las conductas descritas en la tabla, del proyecto de Ley 123 presentan de manera muy especial las formas en que actúa la delincuencia, se extraña la presencia de un apartado en donde explique conceptos y términos técnicos de la informática para la correcta aplicación por parte del operador judicial, este tipo de proyecto bajo observación estaba permeada por la cultura de la alta positivización de conductas, elevando aún más esa mala praxis legislativa.

3.3. Generalidades de la Ley 1273 de 2009

Tabla 5. Ley 1273 de 2009

Bien jurídico tutelado: de la protección de la información y de los datos	
Artículo 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.
Artículo 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.
Artículo 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.
Artículo 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.
Artículo 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.
Artículo 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.
Artículo 269G:	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 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.
Artículo 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.
Artículo 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.

Adiciónese al artículo 58 del Código Penal con un numeral 17	Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.
Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6	De los delitos contenidos en el título VII Bis.
Derogación artículo 195 del código penal	Acceso abusivo a un sistema informático.

Nota: Colombia, Congreso Nacional de la Republica (2009, 5 de enero), "Ley 1273 del 5 de Enero de 2009

Teniendo en cuenta que no hay una exposición de motivos especifica de la Ley 1273 de 2009 se hace alusión a los mismo argumentos de las exposiciones de motivos de los proyectos de Ley 042 y 123 de 2007, combinados en el proyecto de Ley 281 de 2008 para que se aprobara la como Ley.

De lo que se venía planteando, para la cuestión de la denominación y alcance del bien jurídico tutelado a proteger, finalmente se concilió "de la protección de la información y los datos", realmente acorde por lo manifestado en las exposiciones de motivos, pero tipos penales como la violación a la disponibilidad de datos informáticos y las circunstancias de agravación punitiva como la instalación un programa de ordenador o dispositivo que atente contra la confidencialidad o integridad de los datos informáticos almacenados en el sistema informático, que los datos informáticos almacenados en el sistema informático pertenezcan a una entidad que cumpla funciones públicas, que los datos informáticos almacenados en el sistema informático pertenezcan al sector financiero, que la acción se realizare por una persona con una relación contractual con el propietario de los datos, que la persona obtuviere provecho para sí o para un tercero y cuando se den a conocer a terceros los datos informáticos así obtenidos o se procese,

recolecte o circule los datos personales o los datos de autorización o autenticación del sistema informático del proyecto de Ley 042 y conductas como el espionaje informático, el acceso ilegítimo a sistemas informáticos y falsedad informática no están incluidos en la Ley 1273, conductas descritas en los tipos penales que también poseían gran importancia como forma de protección de los datos personales, en sus características de amplitud, titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad e intimidad.

Es de cuestionar la falta de un apartado de definiciones para facilitar la comprensión de elementos específicos y técnicos de la informática para el operador judicial; aunque no se tuvieron en cuenta varios tipos penales contenidos en los proyectos de ley 042 y 123 si se incluyó uno que no se encontraba en ninguno de los dos proyectos de Ley, el hurto por medios informáticos, este es un tipo penal que rompe con todo lo ya mencionado en las exposiciones de motivos en razón a que los tipos penales debían ser autónomos puesto que la idea era la tipificación de nuevas conductas y la construcción de un bien jurídico tutelado exclusivo para estas conductas tal como se pretendía en el proyecto de Ley 123; se tipificaron conductas en donde la informática es solo un medio para la comisión de delitos tradicionales, contrario al interes al que se inclinaba el proyecto de Ley 042 el cual consistía en la modificación de los tipos penales ya existentes y adaptarlos a la realidad del uso de los medios informáticos.

También en el documento del Consejo Nacional de Política Económica y Social (2011) se evidenció que Colombia aun no tenía una estrategia nacional en ciberseguridad y ciberdefensa lo que generaba incremento de la delincuencia cibernética, riesgo indebido a la información, la afectación del normal funcionamiento y continuidad en la prestación de servicios y la

persistencia de impunidad para manejar estos delitos, que fueron los problemas identificados para tal fecha.

Basado en lo anterior, un documento Conpes del año 2016 evidencia que si bien se dieron los lineamientos de política para seguridad y defensa en el documento Conpes del No. 3701 de 2011, se necesita un mayor esfuerzo en elementos como la gobernanza, educación, regulación, cooperación internacional y nacional entre otras dado el aumento del uso de las TIC.

3.4. El hurto por medios informáticos en Colombia

3.4.1. Articulo 269I de la Ley 599 de 2000

> Artículo 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. (Ley 599 de 2000)

Como se manifestó en anteriores apartados, el hurto por medios informáticos es un tipo penal nuevo y no pensado por las iniciativas propuestas en los proyectos de Ley 042 y 123 de 2007 como se pudo evidenciar en el apartado de los proyectos de Ley. Este tipo penal aparece momento en que se hace la acumulación de los ya archivados proyectos de ley 042 y 123 de 2009 ante la cámara de representantes.

Rincón y naranjo (2012) señala que el tipo penal tiene un enfoque respecto al uso de redes atendiendo a criterios de eficiencia y celeridad implementados por las entidades bancarias y financieras lo que las hace un objeto de vulneración. Hace mención de una "transferencia electrónica de fondos" que se caracteriza por la intervención de la entidad bancaria con gestión informatizada, el traslado de créditos de una cuenta de dinero a otra, sin que el dinero sea desplazado físicamente y tampoco importa si es o no a través de medios informáticos.

De esta manera se confundió este tipo penal que era denominado estafa informática en el proyecto de Ley 123 de 2007 y que en la Ley 1273 de 2009 es transferencia no consentida de activos se menciona la transferencia electrónica que en realidad es informática.

El mismo autor manifiesta la dificultad al atribuirle elementos típicos del hurto simple al hurto por medios informáticos respecto a la cosa mueble ajena por la falta de tangibilidad, y que solo puede ser considerado como tal al momento en que el sujeto activo sustraiga el dinero. (Rincón y Naranjo, 2012). Es decir que para el autor, aparte de la reiterada confusión del ámbito de lo electrónico e informático, hace referencia que lo único que puede ser hurtado es el dinero, cuando en realidad los datos pueden contener información bancaria o datos que actualmente pueden ser *bitcoins* como tipo de moneda virtual, ademas hay información que sin ser dinero o sin representar un valor económico pueden tener valores representados en aspectos como la intimidad, la confidencialidad entre otros elemento mencionados en los dos proyectos de Ley.

Díaz (2002) hacía mención que para el año 2002 en su propia clasificación de delitos informáticos se encontraba el delito de hurto calificado tal como se conoce hoy en dia en el actual código penal; describe específicamente que es aplicable ese delito para las transacciones electrónicas de fondos y que es denominado este hurto calificado como fraude informático en

legislaciones como en el Perú., de esta manera el autor clasifica como hurto calificado como lo que hoy se conoce como hurto por medios informáticos

Rincón y Naranjo (2012) señalan que autores como Poullety y Nuñez Ponce han manifestado que la conducta de esta transferencia de dinero no se hace mediante desplazamiento de bien mueble si no mediante la alteración de datos, información o software. Posición que iría más acorde a una Ley de delitos informáticos y no de delitos electrónicos.

Existen serios problemas en la delimitación del objeto material en la medida en que el hurto por medios informáticos tiene dependencia de sus componentes respecto al hurto tradicional y el problema de, que si se habla del campo de lo electrónico, la preexistencia de un agravante en el delito de hurto calificado cuando se violan o superan seguridades electrónicas u otras semejantes, que podrían ser las informáticas o cibernéticas.

El hurto por medios informáticos es un tipo penal que en Latinoamérica, solo existe en Colombia y en Venezuela, aunque en éste último si consta como un tipo penal autónomo (Palomá, 2012); y en países mayoritariamente europeos, no se maneja la figura del hurto en el campo de los ciberdelitos o delitos informáticos, los delitos informáticos respecto a una finalidad económica. Miró (2012) señala que este tipo de delitos a pesar tener una finalidad que es la obtención de un beneficio patrimonial directo o indirecto que afecta el patrimonio de personas naturales o al sistema económico en las transacciones comerciales a través de internet, también pueden afectar otros bienes jurídicos como la intimidad, la seguridad de los sistemas y redes así como se evidenció en la tabla No. 2 de modalidades de cibercrimen. Los cibercrimenes

económicos se pueden dividir en unos que son meros actos instrumentales o mediales como el hacking, el *spam* o el uso de *malware* y otros tipos de cibercrimenes puros desarrollados en el ciberespacio como el *phishing* el *Scam* entre otros.

Es decir, con otros tipos penales de la Ley 1273 de 2009 pueden determinarse como delitos mediales como el caso de los artículos 269A al 269F o puros como el contenido en el 259G que protegen de la afectación al patrimonio económico que era la intención que manifestó el legislador cuando decidió incluir el tipo penal de hurto por medios informáticos.

3.4.2. Elementos del tipo

Tabla 6. Elementos del tipo penal hurto por medios informáticos

Sujeto activo	Indeterminado
Sujeto pasivo	Indeterminado
Verbo rector	Apoderar
Objeto material o bien jurídico tutelado	Cosa mueble ajena
Bien jurídico tutelado	La confidencialidad de la información y los datos
Elemento normativo	El sujeto activo realiza la conducta superando medidas de seguridad informáticas
Elemento subjetivo	La conducta tipificada es realizada con el propósito de obtener un provecho para sí o para otro

Circunstancias de modo	La conducta tipificada es realizada a través de medios espaciales como sistema informático, red de sistema electrónico, telemático, u otro medio semejante o la suplantación de usuario
Clasificación	Tipo de lesión, tipo de resultado, tipo mono ofensivo.

Nota: información tomada de Rincón, J., y Naranjo V. (2012). *Delito Informático Electrónico de las Telecomunicaciones y de los Derechos de Autor*

En la anterior tabla se indica que el bien jurídico tutelado a proteger es la confidencialidad y los datos, un bien jurídico tutelado diferente al creado mediante la Ley 1273 de 2009 que es de la protección de la información y los datos. A parte de ser diferente no hay correspondencia en la protección porque lo que se entendida como una Ley para la protección de datos e información, lo redujo al ámbito de la intimidad de la información y datos.

4. El dato y la información

La corte constitucional bajo sentencia de tutela numero de 1992 expuso que:

> El dato es el elemento básico de la información. Para el profesor Ernesto lleras: "el dato es un elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que dicho dato adquiera sentido

Los datos son propiedad de la persona por cuanto son elementos de su identidad. La Corte Constitucional en sentencia T-414 de 1992 aclara que:

> El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso. Datos de este tipo serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo de las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una "huella digital" porque el individuo es identificable a través de ellos.
>
> Los datos son comunicados a través de mensajes que les otorgan sentido en un determinado contexto. Tales mensajes cumplen con los requisitos precisos de orden convencional y gramatical establecidos según el medio utilizado para su divulgación. El cumplimiento de los objetivos trazados para su difusión permite que tales datos, así

> estructurados, alcancen entidad social. La existencia de múltiples datos de muy distintas personas, sumado a los avances tecnológicos, han permitido la conformación de los "bancos de datos", que son entidades susceptibles de causar daños jurídicos a las personas. "un banco de datos no es otra cosa que un conjunto de informaciones que se refieren a un sector particular del conocimiento, las cuales pueden articularse en varias bases de datos y ser distribuidas a los usuarios de una entidad que se ocupa de su constante actualización y ampliación" Mario Losano, *informática per le scienze social* (Citado por la sentencia T-414 de 1992 de la Corte constitucional)

Velásquez (2012) indica que el sentido de los datos puede tener incidencia en la violación del derecho a la intimidad, especialmente cuando estos datos no están aislados, si no que hacen parte de bancos de datos a partir de los cuales es factible establecer el perfil de las personas propietarias de ellos.

Sobre el poder informático y la necesidad de su regulación la sentencia t-414/92 plantea:

> La posibilidad de acumular datos sobre las personas genera el llamado "poder informático", de cuyo uso pueden desprenderse desde violaciones de sus derechos fundamentales y ataques a la libertad personal hasta el diseño de mecanismos de control social en la medida en que se disponga de bancos de datos de un amplio núcleo poblacional. El más elemental uso de los bancos de datos es el que se deriva del envió de publicidad y correo directo de entidades financieras y comerciales a destinatarios cuya dirección privada éstos no hayan entregado, lo que puede constituir en violación de la intimidad cuando tales datos se emplean sin autorización expresa de la persona. El poder informático es otra forma de poder de dominio social sobre el individuo.

> Por su compleja naturaleza es claro que frente al dato no puede aplicarse en todo su rigor el derecho clásico de propiedad. En verdad, bien miradas las cosas, salta a la vista la existencia de varios sujetos con distintas relaciones. Uno es el sujeto del cual se dice algo o al cual algo le concierne en el universo informativo construido a partir del dato, otro es el sujeto que, aplicando unos códigos o gramáticas como instrumentos auxiliares, hace que el dato se convierta en información. Pueden existir otros cuya labor específica es la circulación y difusión de la información con destino a los clientes habituales de los medios de comunicación, la labor primordial de estos últimos sujetos es, como se ve, hacer que el dato se convierta en esa mercancía denominada a veces noticia.

4.1. Como bien jurídico tutelado u objeto material

4.1.1. objeto material.

Velázquez (2010), explica el objeto material así:

> Como tal a una persona o cosa material o inmaterial sobre la que recae la acción del agente, el sujeto pasivo. Puede ser de un hombre vivo o muerto, consciente o inconsciente, de una persona jurídica o entidad colectiva, de una colectividad de personas, toda cosa animada o inanimada de carácter material o no. Es todo aquello en donde se concreta la trasgresión del bien jurídico tutelado y hacia dónde se dirige el comportamiento del agente (pág.382)

En el décimo congreso de las naciones unidas sobre la prevención del delito y tratamiento al delincuente (2000) se comentó que en la legislación penal de los países se empleaban comúnmente nociones jurídicas tales como las de propiedad, robo y tenencia, pero que esas nociones no eran necesariamente aplicables a los datos informáticos, los cuales, por naturaleza, eran incorpóreos. La facilidad con que los datos podían modificarse también había originado nuevos problemas jurídicos relacionados con su recopilación, conservación y utilización como prueba en los procesos judiciales.

Flores (2012) afirma que la información informática puede contener muchos datos informáticos y de éste último se puede entender que lo conforman miles de *bytes o* bits; Flores (2012) citando a Negroponte explica estos últimos como elementos describiéndolos sin color, tamaño ni peso y que viajan a la velocidad de la luz siendo considerado como el elemento más pequeño en el ADN de la información, consistente en combinaciones binarias compuestas exclusivamente por dos números, el 1 y el 0.

De igual manera explica Flores (2012) que los bits

> Siempre han sido el elemento básico de la computación digital, pero que durante los últimos veinticinco años hemos ampliado enormemente nuestro vocabulario binario hasta poder representar mucho más que solo números. Hemos conseguido digitalizar cada vez más tipos de información, auditiva y visual por ejemplo, reduciéndolos de igual manera a unos y ceros. (P.15)

4.1.2. bien jurídico penalmente tutelado.

Velázquez (2010) menciona que el bien jurídico es una exigencia objetivizada mediante los elementos objetivos en todo tipo penal para su protección; son conceptos abstractos que no pueden ser confundidos con el objeto sobre el que recae la acción del agente.

Miró (2012) explicaba la construcción alemana de los delitos informáticos así:

> La categoría de delitos informáticos como construcción doctrinal penal alemana y española de mediados de los años setenta, ochenta y noventa y principios del nuevo siglo, no se usaba para identificar como un grupo autónomo de infracciones penales, o de un objetivo material de protección o para generar políticas criminales para tutelar bienes sociales. (p.34).

Rincón y Naranjo (2012) exponían que la disciplina jurídica ha tenido que ocuparse de este problema a través de la Ley, del ordenamiento penal para enfrentar conductas que pongan en riesgo la tranquilidad y el continuo devenir de una sociedad globalizada, es decir, la informática no es entendida como un instrumento al servicio del derecho si no por el contrario se convierte en objeto del derecho que es preciso analizar para ofrecer respuestas y garantías sociales con una función del estado de amplio alcance, es decir no limitado a asegurar las condiciones fundamentales de la vida en común si no a promover el desarrollo y mejoramiento de la sociedad. Para Sieber, los bienes jurídicos protegidos por los “delitos informáticos” eran el patrimonio y orden económico, bienes personalísimos como la intimidad o la libertad sexual, y bienes supraindividuales o difusos. (Miró, 2012)

Bajo otra postura, en materia de delitos informáticos y la necesidad de precisar que bienes jurídicos tutelados son los que se encuentran en riesgo y necesitan protección, Rincón y Naranjo (2012) enuncian que los bienes jurídicos tutelados penalmente que ya están regulados como el honor o el patrimonio con tipos penales como las injurias, calumnias, hurtos y estafas, al igual se plantea la pregunta de entonces cual es la correcta aplicación en este ámbito del delito informático, la respuesta no es la falta de tipificación en materia de delitos penales si no en aquellos en donde el delito se desarrolla a través de medios informáticos ya que no se está en presencia de un nuevo delito.

Flores (2012) menciona que es precisamente cual es la distinción entre conducta, como modo de afectar un bien jurídico y bien jurídico como valor esencial del afectado, la que nos pone sobre la pista del tratamiento penal de la nueva delincuencia informática. Asi también se menciona que al menos por el momento de la legislación penal española, no ha hecho nacer nuevos valores o bienes jurídicos que no fueran ya objeto de protección.

Acosta (2003) que el principal bien jurídico a proteger dada la incorporación de tipos penales informáticos no es otra que la información ya que ésta es un fenómeno que no ha sido contemplado den los tipos penales clásicos, además citando a Rovira el cual señala que el principal bien jurídico protegible es la información y secundariamente los datos informáticos en sí mismos, la información con un valor variable y la segunda, los datos o los sistemas y redes informáticos como mecanismos materiales.

Acurio, s.f., indica que dada la emergente sociedad de la información se hace necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección, tambien explica que tal información puede ser considerada de varias formas, como

valor económico, como valor intrínseco de la persona, por su fluidez, además de la equiparación a bienes jurídicos tradicionales como el patrimonio en el caso de los fraudes y manipulaciones de datos, la reserva, la intimidad y la confidencialidad de los datos, la seguridad o fiabilidad del trafico jurídico y probatorio y el derecho de propiedad sobre la información o elementos físicos del sistema informático.

4.2. En la Ley 1273 de 2009

En la Ley 1273 de 2009 no se encuentran argumentos que expliquen las razones por las cuales se decidió insertar el hurto por medios informáticos, la labor investigativa de esta investigación evidencia como España como representante europeo, su desarrolló el hurto y su relación con las tecnologías de la información y comunicación. Flores (2012) menciona que “no hay una referencia expresa a internet o a los instrumentos digitales como medios o instrumentos de comisión en relación con el resto de delitos contra el patrimonio” (p.286)

teniendo en cuenta que actualmente se desarrollan operaciones financieras en soportes digitales, son modalidades clásicas de delitos patrimoniales como fraudes en ofertas y subastas, supuestos accesos gratuitos a internet, el *adult check*, oferta de servicios gratuitos por un periodo reducido, ventas de tipo piramidal, defraudaciones en las contratación de billetes de avión, viajes y arrendamientos. (Flores, 2012)

La Unión Internacional de Telecomunicaciones (2014) expone que en la categoría de delitos informáticos se encuentran el fraude informático, la falsificación informática, el robo de identidad y la utilización indebida de dispositivos.

Dado que la intención de los proyectos de Ley 042 y 123 de como de Ley 1273 de 2009 era impulsar a Colombia a un nivel europeo todo lo relacionado sobre los delitos informáticos se encuentra dos situaciones:

La primera es en cuanto al contenido del Convenio de Budapest (2001) que ningún momento se menciona al hurto por medios informáticos como modalidad de delito informático, solamente se contempla la posibilidad de adecuar tipos penales como la falsificación informática respecto a la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos para la generación de datos no auténticos; y la tipificación del fraude informático respecto al perjuicio patrimonial mediante la introducción, alteración, borrado o supresión de datos o interferencia en el funcionamiento de un sistema informático, es decir que no hay un fundamento para la adopción de la figura del hurto por medios informáticos en Colombia teniendo en cuenta que en la legislación penal colombiana existe el hurto calificado describiendo la misma conducta; y la segunda es respecto a que si la intención de Colombia como un país no miembro del Consejo de Europa de donde proviene la convención de Budapest, ¿porque aún hoy, año 2017 no se ha firmado y ratificado tal convenio a pesar de las múltiples invitaciones del Consejo de Europa para la firma y ratificación de tal convenio?

Conclusiones

Se reconocen de los argumentos en las exposiciones de motivos de los proyectos de Ley 042 y 123 de 2007 que el ideal manifestado del primero de los proyectos de Ley fue dar una oportuna solución a la atipicidad y lograr el aumento de penas en diferentes tipos penales ya existentes; en el segundo de los proyectos de Ley, muestra que es necesario optar por la construcción de un nuevo bien jurídico tutelado ya que dada la especialidad de las conductas desarrolladas a través de la informática que no permiten que se subsuma en delitos tradicionales, hace ademas necesaria la creación de nuevos tipos penales, así que el ideal de esta última propuesta fue la creación de un bien jurídico tutelado denominado “la protección de la información” en aspectos como titularidad, disponibilidad, seguridad, transmisión, confidencialidad e inclusive hasta la intimidad y propiedad.

Se puede recalca que en ninguna de las propuestas iniciales de proyecto de Ley está presente el tipo penal de hurto por medios informáticos.

Las características del delito de hurto por medios informáticos, y en especíal en su objeto material hace referencia a lo ya desarrollado por el hurto simple y en cuanto a las características del hurto calificado; el objeto mueble ajeno con la característica de que éste tenga una equivalencia económica;

múltiples autores están de acuerdo respecto a que el objeto material, el bien mueble ajeno, hace relación al dinero cuyo caso, el tipo penal de la transferencia no consentida de activos articulo 269J tampoco estaría siendo eficaz, así pues que el objetivo del valor socialmente

relevante reflejado en el bien jurídico tutelado de la protección de la información y los datos se inclina en este caso a solo a la protección exclusiva de bienes jurídicos tutelados como el patrimonio económico.

Dentro de la ley 1273 de 2009 no se pueden hacer exploraciones para indagar en que consiste la protección de la información y los datos como bien jurídico tutelado penalmente y mucho menos la idea de concebir a la información y los datos informáticos como un objeto de protección ya que la referenciada Ley, fue modificada desde las presentaciones de los proyectos de Ley en los que perdió en buena parte aspectos importantes que podrían ayudar a interpretar, por ejemplo los motivos que llevaron a que el legislador ad un tipo penal como el hurto por medios informáticos.

Como conclusión general, el delito por medios informáticos no protege ni la información ni los datos como objeto material porque nunca se pensó ni se desarrolló con ese propósito a pesar de la importancia que tiene la información y los datos como objetos virtuales valiosos que contengan o no implícitamente una estimación económica en la actual era del ciberespacio.

Glosario

***Adult Check*:** modalidad de estafa realizada a través de páginas generalmente pornográficas en las que se solicita el numero de una tarjeta de crédito para comprobar que el internauta es mayor de dieciocho años y con posterioridad se facturan, normalmente desde países remotos, cargos por servicios no solicitados

***Antisocial networks*:** comportamiento consistente en la manipulación de redes sociales o de grupos de ellas con finalidad de utilizarlas posteriormente para el fraude o para cualquier otro tipo de ciberdelito.

Auction Fraud: fraude cometido en las subastas, consistente en la tergiversación de un producto o su no entrega conforme a lo pactado en los sistemas de subasta *online* tipo Ebay.

***Black hat hacking* (*hacking* negro):** *hacking* realizado con ánimo destructivo o ilícito.

***Bot*:** tipo de virus que permite el acceso remoto del sistema informático a través de la Red.

***Botnet*:** Conjunto de redes de ordenadores comprometidos (*bots*) y controlados por el mensajero.

Ciberacoso: o acoso en el ciberespacio, estaría conformado por el uso de las TIC para atentar de forma continuada, con amenazas, insultos, actos de persecución, etc., contra la dignidad de una persona.

Ciberataque replica: aquellos ciberataques en los que el ciberespacio es el nuevo medio desde el que realizar delitos que tienen correspondencia en el espacio físico.

Ciberataques de contenido: todos aquellos ciberataques en los que el centro de la infracción lo constituye el contenido que se comunica o se trasmite a través de las redes telemáticas, particularmente de Internet.

Ciberataques puros: todos aquellos ataques en el ciberespacio que no tienen correspondencia en el espacio físico al consistir en un concreto uso de las TIC, previamente no existente fuera de Internet.

Ciberblanqueo de capitales: cuando se utiliza el ciberespacio y sus diferentes servicios para el lavado de dinero y activos procedentes de actividades ilegales, generalmente de mafias organizadas.

Cibercrimen económico: todo cibercrimen o ciberataque realizado con el propósito final de obtener un lucro económico con el consiguiente perjuicio de uno o varios usuarios. Son cibercrímenes económicos tanto aquellos ciberataques en los que la conducta termina en un fraude, como otros que no son más que un acto preparatorio de los ciberataques defraudatorios finales.

Cibercrimen político: dícese de la utilización, por sujetos individuales, instituciones, grupos e incluso Estados, de Internet como forma de difusión de un determinado mensaje político o como forma de ataque a un Estado o a concretas instituciones no gubernamentales.

Cibercrimen social: grupo de delitos en Internet que tienen que ver con las relaciones sociales entre las personas y que no son más que la transposición al ciberespacio de los crímenes tradicionales derivados entre personas.

Cibercrimen: cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan.

Ciberespacio: término que indica el lugar de intercomunicación social transnacional, universal, popularizado y en permanente evolución derivado del uso de las TIC.

Ciberextorsión: consiste en la solicitud de importantes cantidades económicas a cambio de cesar en la realización de algún tipo de ciberataque o incluso de empezar a ejecutarlo.

Ciberfraudes: fraude en el que las redes telemáticas se convierten en el instrumento mediante el cual se logra un beneficio patrimonial derivado de un perjuicio patrimonial a una víctima.

Ciberguerra: actos de guerra entre Estados o contra Estados que tienen lugar en el ciberespacio.

Ciberhacktivismo: conjunto de ataque llevados a cabo por *hackers* informáticos pero no con una finalidad maliciosa de defraudar a las víctimas, de robarles información para traficar con ella o de causar daños para perjudicarles económicamente, sino con la intención de lanzar un mensaje ideológico, de lucha política y defensa de ideas generalmente relacionadas con la libertad en Internet, aunque teniendo cabida cualesquiera otras convicciones ideológicas.

Ciberpirateria intelectual: forma de explotación ilícita de obras protegidas por derechos de propiedad intelectual utilizando Internet.

Ciberterrorismo: conjunto de actividades realizadas en el ciberespacio por una organización terrorista para difundir sus mensajes, obtener financiación, facilitar la acción de sus bases o directamente ara realizar ciberataques terroristas contra objetivos concretos.

***Cracker*:** *hackers* que utilizan el acceso informático para robar información relevante, defraudar o causar algún tipo de daño.

***Cyberbullying*:** ciberacoso escolar o a menores, esto es, variante del ciberacoso en la que un menor atormenta, amenaza, hostiga, humilla o molesta de alguna otra manera a otro, haciendo uso de internet, teléfono móvil, videoconsola o alguna otra tecnología telemática de comunicación.

Cybergrooming: ciberacoso sexual a menores.

Cyberhate speech: difusión de mensajes de odio racial en el ciberespacio.

***Cyberstalking*:** ciberacoso continuado a una persona, consistente en el seguimiento, hostigamiento y persecución de la víctima por medio del uso de internet. También se define, en sentido amplio a la utilización de internet para realizar uno o más actos de amenazas, insultos, uso indebido de la imagen, solicitud sexual o cualquier otra forma de hostigamiento a una persona.

Dato: elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que el dicho dato adquiera sentido.

***Denial of Service* (DoS):** denegación de servicio. Ciberataque consistente en saturar el servidor del sistema logrando que el mismo se centre en la petición que realiza el atacante sin que pueda atender a ninguna más.

***Domain Name Server* (DNS):** servidor de nombres de dominio

eBay: es el mayor centro de compra y venta en Internet: un lugar en el que se reúnen compradores y vendedores para intercambiar cualquier mercancía. El vendedor opta por aceptar solo pujas por el artículo u ofrecer la opción de precio fijo que permite a los compradores adquirir el artículo de inmediato.

***Game hackers*:** *hackers* que en los años ochenta desarrollaron aplicaciones de *software* para juegos.

***Hacker*:** experto informático (y apasionado por Internet y nuevas tecnologías) que busca superar barreras por el mero hecho de su existencia sin entrar en el campo de lo delictivo, en ocasiones incluso usando sus conocimientos para la mejora de la seguridad de las redes y los sistemas (también denominados samuráis). También se utiliza el término para referirse al sujeto que accede de forma ilícita al sistema informático ajeno.

***Hackers* clandestinos:** concepto casi idéntico al de *cracker* que englobaría los *hackers* que se dedican tanto a la intromisión informática, a la realización de ataques DoS, a la creación de webs para el fraude, al diseño de virus, a la infección de *bots*, al envió de *spam*, y todo ello con finalidad económica (generalmente) o bien política, y que actúan de forma individualizada o formando parte de un grupo que tanto puede ser una banda organizada tradicional que opera ahora en el ciberespacio, como una ciberbanda de *hackers* que unen sus esfuerzos para un fin criminal común.

***Hacking*:** cualquier conducta por la cual un sujeto accede a un sistema o equipo informático sin autorización del titular del mismo, de una forma tal que tiene capacidad potencial de utilizarlo o de acceder a cualquier tipo de información que esté en el sistema.

***Hacktivismo*:** difusión de mensajes de protesta en internet generalmente dirigidos contra organismos o Estados en relación con la voluntad de mantener libre de normas el ciberespacio.

***Hardware hackers*:** en los setenta desarrollaron algunos de los equipos y tecnologías más importantes.

***Hardware*:** conjunto de los componentes que integran la parte material de una computadora.

***Hosting*:** servicio que consiste en proveer un espacio para alojar una página web.

***Identity theft*:** robo o fraude de identidad en que se suplanta la personalidad de un usuario con ánimo defraudatorio.

***Insiders*:** cibercriminal que pertenece o trabaja para la institución o empresa víctima de la infracción.

Internet: red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

***Malware*:** *software* malicioso destinado a dañar, controlar o modificar un sistema informático.

***Online grooming*:** acercamiento sexual a menores con el propósito de realizar posteriormente un contacto o abuso sexual.

***Pharming*:** táctica fraudulenta que consiste en cambiar los contenidos del DNS ya sea a través de la configuración del protocolo TCP/IP o del archivo Imhost para que el usuario, cuando teclea una dirección web de su entidad bancaria en su navegador entre, en realidad, a una web falsa muy parecida o igual a la original en la que acaba desvelando sus datos bancarios.

***Phishing* tradicional:** tipo de *phishing* en el que se utiliza la imagen corporativa de una entidad bancaria o de una institución, para solicitar a la víctima por medio de correo electrónico que envíe a una dirección de correo que simula ser de tal entidad los datos bancarios requeridos.

***Phishing*:** mecanismo criminal que emplea tanto ingeniería social como subterfugios técnicos para robar los datos de identidad personales de los consumidores y de sus tarjetas de crédito o cuentas bancarias.

***Phreakers*:** *hackers* que manipulan las líneas telefónicas, para conseguir, entre otras cosas, el uso gratuito de las telecomunicaciones.

Protocolo IP: protocolo para el envío y recepción de datos a través de una red de paquetes conmutados.

Protocolo TCP/IP: protocolo de control de transmisión, protocolo de internet, protocolo básico de comunicación.

***Scam*:** concepto que podría englobar casi todos los fraudes en el ciberespacio, si bien se suele utilizar como referencia de los más burdos de ellos, aquellos en los que el engaño es poco elaborado y en los que el error de la víctima puede ir más allá de lo común.

***Scriptkiddies*:** jóvenes que, no siendo *hackers* expertos capaces de acceder a sistemas mediante programaciones propias, realizan sus ataques informáticos, generalmente eligiendo las victimas al azar, aprovechando programas básicos y causando daños en muchos casos, mas fruto de su impericia o de la daño del *malware* utilizado, que de sus habilidades.

***Sexting*:** tipo de *online grooming*. Consiste en la realización por parte de menores, de fotografías propias de desnudos completes o partes desnudas y su envío, generalmente por medio de

teléfono móvil, a otros, junto con textos obscenos y con la finalidad de conocer personas o de enviar mensajes de amor o de odio.

***Sniffer*:** programas de captura de tramas de información que no están destinadas a él o persona que rastrea y captura información por la red por medio de los denominados "*packet sniffers*".

***Software*:** conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

***Spam*:** correo electrónico no solicitado que suele enviarse a un gran número de direcciones electrónicas bien a través de una dirección electrónica de las ofrecidas por los servicio de correo gratuitos estilo Hotmail, o bien desde un sistema informático infectado, convertido en *botnet* y utilizado por el *spammer* que adquiere las direcciones de correo *hackeando* sistemas informáticos o utilizando *spyware* u otros sistemas de búsqueda de direcciones electrónicas a través de la red.

***Spammer*:** *hacker* encargado de realizar envíos masivos de correo electrónico no deseado.

***Spoofer*:** persona que suplanta la identidad de otro usuario en la red.

***Spoofing*:** suplantación de identidad.

***Spyware*:** virus que captura información de los sistemas informáticos o software que se instala en un sistema y que recopila determinada información de éste que después envía a otro sistema.

TIC: Tecnologías de la Información y la Comunicación.

***True hackers*:** aficionados pioneros de la informática en los primeros días de la aparición de esta tecnología en los años sesenta.

***White hat hacking* (*hacking* blanco):** tipo de *hacking* consistente simplemente en acceder al Sistema o a sus datos e información, pero sin ningún propósito de sabotaje o utilización posterior de la información.

Referencias

Acosta, A. (2003). *Hacking, Cracking y Otras Conductas Ilícitas Cometidas a Través de Internet.* (Tesis Derecho). Universidad de Chile. Facultad de Derecho, Santiago.

Acurio, S. *Delitos Informáticos: Generalidades***.**

Austria, Organización de Naciones Unidas (2000) Décimo Congreso De Las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, 10 a 17 de abril de 2000, Viena

Colombia (2013), *Código Penal*, Bogotá, Temis.

Colombia, Congreso Nacional de la Republica (2009, 5 de enero), "Ley 1273 del 5 de Enero de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. *Diario Oficial,* núm. 47.223, de 5 de enero de 2009, Bogotá.

Colombia, Corte Constitucional (1992, junio), "Sentencia de Tutela No. 414", M. P. Angarita Barón, C., Bogotá

Colombia, Corte Constitucional (1995, marzo) "Sentencia SU - 082", M. P. Arango Mejía, J., Bogotá

Colombia, Sala de Casación Penal, Corte Suprema de Justicia (2015, febrero), "Sentencia de Casación No SP1245-2015", M. P. Patiño Cabrera, E., Bogotá.

Consejo de Europa. (2001). *Convenio Sobre la Ciberdelincuencia*. Budapest, Hungría.

Consejo Nacional de Política Económica y social. (2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa.* Documento Conpes No. 3701, Bogotá, Colombia.

Consejo Nacional de Política Económica y social. (2016). *Política Nacional de Seguridad Digital.* Documento Conpes No. 3854, Bogotá, Colombia.

Cotrino, G. (2007). *Proyecto de Ley 042 de 2007*. Gaceta del congreso 355, Colombia: Cámara de Representantes.

Díaz, A. (2002). *Derecho Informático.* Bogotá, Colombia: Leyer

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

Gómez, L., y Piedrahita, C. *Proyecto de Ley 123 de 2007.* Gaceta del congreso 450, Colombia: Cámara de Representantes.

Losano, M. (1985). *Informática per le scienze social*. Giulio Einaudi editore s.p.a, Italia.

Menéndez, J., y Santa Cecilia, E. (2014). *Derecho e Informática: ética y legislación.* España: Bosch Editor

Miró, F. (2012). *El cibercrimen*. Madrid, España: Marcial Pons.

Palomá, L. (2012). *Delitos Informáticos (en el ciberespacio)*. Bogotá, Colombia: Ediciones Jurídicas.

Rincón, J., y Naranjo V. (2012). *Delito Informático Electrónico de las Telecomunicaciones y de los Derechos de Autor*. Bogotá D.C, Colombia: Ibañez.

Sieber, U, (1980). *Computerkriminalität und Strafretch.* Koln/Berlín/Bonn/Munchen: Carl Heymanns.

Sieber, U. (1985). *Informations technologie und Strafrechreform.* Koln/Berlin/Bonn/Munchen: Carl Heymanns.

Torres, H. (2002). *Derecho Informático*. Bogotá, Colombia: Gustavo Ibáñez.

Unión Internacional de Comunicaciones. (2014). *Comprensión del Ciberdelito: Fenómenos, Dificultades Y Respuesta Jurídica.* Oficina de Desarrollo de las Telecomunicaciones, Ginebra, Suiza.

Velásquez, F. (2010). *Manual de Derecho Penal Parte General.* Bogotá, Colombia: Ediciones Jurídicas Andrés Morales.

Velásquez, J. (2012). *Derecho a la Comunicación General y especial.* Medellín, Colombia: Universidad Pontificia Bolivariana

Wall, D. (2007). *Cybercrime: the transformation of crime in the information age.* Cambridge, Polity Press.