Contextualizacion del cibercrimen en Colombia

Clara Lucía Guzmán A.

Recibido el 10 de junio de 2009. Aprobado el 23 de octubre de 2009

Resumen
Con la nueva ley de Delitos informáticos se inicia una etapa novedosa en el plano de la legislación Colombiana. Para entender sus alcances, se hace necesaria una contextualización que permita al lector tener claridad sobre la intención de la ley, sus postulados y la razón de ser de las penas que contempla. De otra parte, el nuevo Sistema Acusatorio permite al experto en temas de Seguridad Informática e Investigación Forense aportar su conocimiento en pro de la investigación de los delitos y conductas irregulares en estos campos.

***Palabras clave**:*
Cibercrimen, delitos informáticos, acceso abusivo, sistemas informáticos, hackers, estafa informática, software malicioso.

***Abstract**:*
With the new Computer Crime Acts (Cibercrime Law) starts a novel stage in the plane of the Colombian law. To understand this, its necessary to prepare the reader to undersand the law intention, principles and spirit of the penalties. In addition, the new Prosecuter Investigation System, helps the experts in Information Security and Forensic Investigation, increase their knowledge towards the investigation of crimes and misconduct in these areas.

Keywords
Cibercrime, Forensic Investigation, Computer Crime, Informatic Scam, hackers, malware, informatic systems.

I. Introducción.

Si bien es cierto, el Cibercrimen es un fenómeno mundial, se pretende con este documento generar un primer espacio de reflexión respecto al tema en Colombia, y las implicaciones de este tipo de delitos en el ámbito colombiano.

Con el crecimiento de las tecnologías de la información y telecomunicaciones, ha surgido también la necesidad de proteger no solo la información que se crea, almacena, recoge, preserva, etc., sino también los canales tecnológicos por medio de los cuales se accede o transmite la misma.

En la actualidad, han surgido muchos problemas relacionados con el uso de las computadoras, amenazas que afectan negativamente tanto a los

individuos como a las empresas. La proliferación de estos instrumentos que se han constituido en la principal herramienta de funcionamiento en casi todos los niveles de convivencia, así como la creación de la red global, ha provocado que cada vez más personas ingenien formas y medios para lucrarse, hacer daño o causar perjuicios a través del uso de dichas herramientas.

El gran avance de la tecnología de las Telecomunicaciones y la Informática a nivel mundial, ha traído consigo, un inevitable aumento de actos con consecuencias jurídicas. Tal es el caso, de la expansión mundial de la Internet, cuyo efecto globalizador ha ido desencadenando profundas transformaciones a los postulados tradicionales en materia de regulación jurídica, haciendo cada vez más notoria la importancia del Derecho Informático; pero igual importancia adquiere para todo aquel que utilice de alguna manera cualquier tipo de soporte informático.

Es necesario conocer al criminal informático, su psicología, así como los estándares de legislación que existen con el fin de proteger los intereses alrededor de este bien jurídico. Para nadie es un secreto que la información y los datos, así como los dispositivos informáticos y electrónicos, son objeto del ataque inclemente de los hackers del momento. Si bien el hacker es considerado como aquel "enamorado de la tecnología", no siempre su móvil es totalmente sano, y es por eso que desde la década de los años noventa se les ha perseguido incansablemente.

Historias delictivas, llenas de acción en la red, se ven en el cine y la televisión, en apología de la delincuencia informática. ¿O es mas bien advertencia a un sin número de falencias de los medios informáticos y dispositivos asociados?

El daño a la información, la supresión de datos, los ataques fraudulentos a los sistemas de información ponen hoy en peligro el sistema financiero, las bases tributarias e incluso los mismos expedientes judiciales y de investigación, y lo que es peor, la seguridad de los Estados. Hoy no nos encontramos solamente frente a la guerra de los soldados en el campo de batalla, o los virus diseñados desde casas farmacéuticas con fines criminales; hoy la guerra también se halla en la red: se le denomina "warware" y sus alcances se acercan cada día más a la ciencia ficción.

Es obvio: Los Estados deben extender su mirada a la virtualidad. Deben revisar sus controles, pero también cuidando y respetando los derechos fundamentales, permitir el acceso libre a la información.

¿Y cuáles deben ser estos límites?, ¿quién los impone?. De esta forma, surgen para el lector desprevenido, muchas dudas sobre su quehacer personal a través de los computadores, celulares y otros dispositivos, y si se tiene en cuenta que la ignorancia de la ley no sirve de excusa, puede estar cometiendo conductas delictivas, con graves consecuencias que pueden repercutir en sus recursos económicos e incluso, en su condición de libertad.

Siendo el tema de los delitos informáticos tan importante y de amplio espectro la investigación en este sentido permite al académico, al empresario y al público en general, permear su conocimiento y entender cuán importante es hoy la actividad con el uso de las tecnologías y aunque, a la fecha no se ha desarrollado investigación en Cibercrimen, la contribución de este tipo de trabajos, se considera importante para el desarrollo del país en general y para la normativa que rige este importante tema en particular.

Por lo anterior, desde Agosto de 2008, se inició en la Facultad de Ingeniería de la Corporación Univeristaria Minuto de Dios (UNIMINUTO), un trabajo de investigación, cuyo objeto es llenar el vacío temático para el caso especifico de Colombia, y las implicaciones jurídicas de este tipo de delitos a través del Programa de TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA.

Con esta investigación se espera que los usuarios y desarrolladores de las TICs afronten acertadamente las situaciones legales derivadas del uso y desarrollo de la informática y de telecomunicaciones, propias del quehacer cotidiano en dichos campos.

II. Planteamiento del problema

En la actualidad se evidencia una falta de ilustración de los usuarios de los dispositivos informáticos, respecto a la legalidad o ilegalidad de algunas conductas. Casos sencillos, como el copiar música o videos de la red, se han convertido en verdaderas acciones delictivas, que han soportado toda una industria ilegal en el mundo. Las casas editoras y disqueras ya han tomado algunas acciones para contrarrestar este mal que obviamente les hace perder sustancialmente ganancias dados los perjuicios generados por quienes copian sin autorización las obras puestas en la red.

No solamente en este campo se presentan problemas. A través de la red se hacen negocios, se accede a información gubernamental, y en ocasiones a bases de datos que son de carácter privado. Sin embargo, ni siquiera los funcionarios de la Justicia (Jueces,

Fiscales, Investigadores, etc.) tienen claridad sobre las conductas delictivas a través de la red o mediante dispositivos informáticos, y mucho menos la conciencia de la investigación de estas conductas.

Se presenta un problema general que radica en la escasa ilustración sobre el CIBERCRIMEN, su tratamiento tanto al interior del país como transnacional, y por supuesto, la penalización de las conductas.

Por lo tanto surge la pregunta:

¿Cuál debe ser la tipología de los delitos informáticos en el Código Penal Colombiano?

Si bien desde enero de 2009 rige la Ley de Delitos informáticos, el tema está prácticamente virgen. No se han efectuado desarrollos sobre el mismo, y solo los teóricos se acercan al tema sin los conocimientos técnicos necesarios para poder aportar. A pesar de que la Ley es el resultado de tres proyectos radicados en las diferentes Cámaras, no abarca las necesidades actuales, generando incluso vacíos al momento de aplicar la normatividad.

III. Los delitos informáticos en Colombia

La Legislación Penal colombiana está regida actualmente por el CODIGO PENAL; Ley 599 de 1999. En dicha Ley están descritas las conductas que se consideran punibles, es decir, susceptibles de pena y que tienen una sanción, sea de prisión, arresto, multa y otras accesorias.

Un principio básico de la legislación es el PRINCIPIO DE LEGALIDAD, que establece que nadie podrá ser juzgado sino conforme a las leyes preexistentes al acto que se le imputa. Esta norma quiere decir que si la conducta no se encuentra descrita *"exactamente dentro de un tipo penal especifico"*, no podrá ser juzgada por el ordenamiento penal. Es decir, si bien algunas conductas pueden parecer delicuenciales, sólo es delito aquella conducta que se ha precisado como tal. No quiere decir que las demás conductas sean impunes para la Justicia, sino que su ámbito de cobertura solo cubre al particular, quien tiene en su mano la posibilidad de accionar ante el Estado para que se protejan sus derechos a través de acciones civiles con un fin claro de indemnización o resarcimiento de perjuicios. Pero no se consideran de carácter penal, es decir, el infractor no será tratado como DELINCUENTE.

Para mayor precisión es necesario tener en cuenta que para que una conducta sea objeto de la legislación penal, es decir PUNIBLE, debe tener tres elementos fundamentales:

1. TIPICIDAD: Se refiere a la descripción exacta, expresa, clara e inequívoca de la conducta en un texto penal, es decir que la estructura del delito o de la conducta corresponde de modo preciso a una descripción.

2. ANTIJURIDICIDAD: Se requiere que lesione o ponga efectivamente en peligro, sin justa causa, el bien jurídicamente tutelado por la ley penal. Como se verá a lo largo del presente documento, la estructura de nuestro ordenamiento penal está conformada por bloques de bienes tutelados y tutelables, que permiten entender las vulneraciones. Es decir, que la conducta vulnere una protección especial. A manera de ejemplo, el Homicidio vulnera La Vida, que es protegida por el Estado, desde la Constitución y desde el mismo Código penal.

3. CULPABILIDAD: Se refiere a la intención de causar daño (Dolo), Es importante anotar que la mayoría de los delitos contemplados en nuestra legislación son de carácter doloso, es decir, se presentan con la intención de causar daño. Sin embargo, en el caso de algunas conductas que lesionan gravemente a los particulares, aun sin tener la intención dañina, se encuentran el homicidio culposo y las lesiones personales culposas, que se consideran delitos por la gravedad de las mismas. En estos casos, aun sin tener la intención, se causa un daño que debe ser reparado.

Así las cosas, son varios los bienes protegidos por nuestra legislación penal:

- La vida e integridad personal
- Las personas y bienes protegidos por el derecho Internacional Humanitario
- La libertad individual
- La Autonomía personal
- La intimidad, reserva y las comunicaciones
- La libertad de trabajo y asociación
- El sentimiento religioso y el respeto a los difuntos
- La libertad, integridad y formación sexuales
- La integridad moral
- La Familia
- El patrimonio económico
- Los derechos de autor
- La Fe Pública
- El Orden económico social
- Los recursos naturales y el medio ambiente
- La seguridad pública

Como se puede apreciar, en el campo de los delitos informáticos, o conductas que atañen a la generación, uso, conservación y transmisión de la informa-

ción, no se encontraba un capítulo específico que hiciera referencia a la INFORMACIÓN como bien jurídico tutelado y tutelable.

De tal manera que bajo los postulados de la Ley 599 de 2000, sólo podía remitirse a algunos tipos penales, encuadrados en bienes tutelados diferentes a la información, pues no se tenía conciencia de ella por su valor e impacto en las empresas.

Se presentaban discusiones en este sentido:
Si una persona accede al correo personal electrónico de otra, teniendo en cuenta que la ley no permite interceptar las comunicaciones, ¿esta forma de acceso se convierte en una interceptación? O acaso el correo corresponde a parte del territorio de la persona, es decir el domicilio, ¿nos estamos enfrentando a la Violación de habitación ajena?

En este último caso, teniendo en cuenta que la conducta se refiere a quien se introduce arbitraria, engañosa o clandestinamente en habitación ajena o en sus dependencias inmediatas, o que por cualquier medio indebido escucha, observa, graba, fotografía o filma, aspectos de la vida domiciliaria de sus ocupantes, se pregunta hoy si el espacio virtual se convierte en habitación o en lugar de trabajo; siendo así, la red termina convirtiéndose en un lugar, ubicable por cierto, pero que también debe ser objeto de la protección del legislador.

Y de esta manera, siendo parte del domicilio de una persona, siendo su espacio privado, no puede otro de manera ilegítima y sin autorización acceder o mantenerse en él, de manera arbitraria.

De otra parte, el Artículo 192 de la Ley 599 describía la Violación ilícita de comunicaciones como aquella conducta en que ilícitamente se sustrae, oculta, extravía, destruye, intercepta, controla o impide una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido. Y la pena para esta acción era de prisión de uno (1) a tres (3) años.

Quiere decir que a la luz de estos artículos, ¿el acceso al correo en el ejemplo anterior tiene una peña de un año?.

Ahora bien, por ejemplo, cuando se utilizan dispositivos informáticos para completar hurtos, no existía en nuestra legislación una norma que considerara esta situación. El funcionario de justicia debía entonces regirse por el artículo 239, donde la conducta tiene una pena de prisión de 2 a 6 años. Cuando mucho, la calificación establecida en el artículo siguiente permitía aumentar la pena de 3 a 8 años, si el hurto se cometía mediante penetración o permanencia arbitraria, engañosa o clandestina en lugar habitado o en sus dependencias inmediatas, aunque allí no se encuentren sus moradores.

Y derivado de esto, múltiples conductas se aprecian hoy en nuestro entorno, que definitivamente DEBIAN ser reguladas y penalizadas fuertemente.

Un agregado obtenemos en la Ley 1032 de 2006, que si bien regula conductas y situaciones relativas a los sistemas de comunicaciones y asuntos de derechos de autor, debe entenderse como un avance importante en el tratamiento de datos y voz, dándole una importancia que en la Ley 599 de 2000 no tenia el tema. Conductas como la prestación, acceso o uso ilegales de los servicios de telecomunicaciones que consiste en prestar, acceder o usar servicios de telefonía móvil, con ánimo de lucro, mediante copia o reproducción de señales de identificación de equipos terminales de estos servicios, o sus derivaciones, tiene con esta ley una pena de 4 a 10 años, y multa de 500 a 1000 salarios mínimos, con igual pena para quienes comercialicen servicios de telefonía sin autorización.

IV. Proyectos de ley

En septiembre de 2007, se presentaron dos Proyectos de Ley para regular los delitos informáticos (042 y 127), de igual manera en el año 2008 se presentó el proyecto 281 en el mismo sentido. Se deciden acumular los textos y revisarse conjuntamente. Los proyectos iniciales apuntaban entre otras cosas a:

- Crear un nuevo bien jurídico tutelable denominado LA INFORMACIÓN
- Preservar integralmente los sistemas que utilicen tecnologías de la información y comunicaciones
- Desarrollar o tipificar varios delitos de carácter informático.

Este Proyecto se sustentaba en el valor intrínseco de la información, almacenada, tratada y transmitida a través de sistemas informáticos. Una de sus características era la utilización de expresiones en inglés, términos empleados en todo el mundo pero que para nuestra legislación debe restringirse al uso del Español. Es así como se describían conductas como el "White hacking" que no es otra cosa sino el acceso no autorizado a los recursos informáticos, de alta ocurrencia. Otra conducta proyectada como delito es el Spamming, que según el proyecto es un flagelo informático que ha generado problemas económicos a los usuarios del correo electrónico, vulnerando también derechos fundamentales como el de la intimidad virtual y el hábeas data a los usuarios de la Internet y de las telecomunicaciones. También se encuentra el Phishing, en donde a través de una car-

nada con un dominio similar al de la entidad victima, logra acceder a datos personales de los demás usuarios. El delincuente captura los datos y procede a realizar operaciones electrónicas en su beneficio o de terceros.

En suma, y para mayor ilustración del lector, los proyectos contemplaban como delitos:

1. El espionaje informático
2. Acceso ilegitimo a sistemas informáticos
3. Bloqueo ilegitimo a sistemas informáticos
4. Uso de virus (software malicioso)
5. Abuso de uso de medios informáticos
6. Daño informático
7. Estafa informática
8. Suplantación de sitios web
9. Falsedad informática y
10. Violación de datos personales.

Sólo algunos de ellos, nutren nuestra nueva Ley de Delitos informáticos, misma, que será objeto de la investigación, no solo desde el espectro de la ley, sino desde la casuística existente para nutrirlos con los conocimientos de los Tecnólogos de la Universidad.

V. La información y los datos. Nuevos bienes tutelados

La nueva LEY, sancionada el pasado cinco (5) de Enero modifica el CODIGO PENAL adicionando un nuevo bien jurídico tutelado: LA INFORMACIÓN.

El Capítulo pertinente se denomina **"De la Protección de la información y de los datos"**, con dos tipos de descripciones:

Si los bienes jurídicos protegidos son la INFORMACIÓN y los DATOS, es necesario referirnos a ellos, desde los mismos postulados legales.

En cuanto a la Información y para nuestros efectos, debemos remitirnos a la Ley de Archivo, No.594 del año 2000, en donde se refiere a la información como el sustrato de los archivos y documentos en general. A manera de ilustración, se presentan algunas definiciones:

> *Archivo. Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.*

Como se aprecia, se muestra la importancia de los datos e información, pues de allí se desprenden los archivos y fondos documentales.

Y los insumos básicos de los archivos son los documentos, que según la norma son el *"…Registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones".*

Estos documentos tienen un soporte documental, que es sobre el cual se contiene la información, según los materiales empleados. *Además de los archivos en papel existente los archivos audiovisuales, fotográficos, fílmicos, informáticos, orales y sonoros.*

Según esta ley, *las entidades del Estado pueden incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos:*

> *a) Organización archivística de los documentos;*
> *b) Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.*

En el ámbito privado, es necesario remitirse al Código de Comercio, que ilustra sobre la información comercial, contable y empresarial, obligando al empresario a conservarla a través de los medios que permite la misma ley. Y parte de esos medios son precisamente los soportes informáticos o digitales.

De otra parte, respecto a los datos electrónicos, la Ley 527 de 1999, llamada la Ley de Comercio electrónico, ilustra un poco en algunas definiciones:

a) Mensaje de datos. La información generada, enviada, recibida, almacenada comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

e) Intercambio Electrónico de Datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto,
f) Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o pro-

cesar de alguna otra forma mensajes de datos.

Véase entonces que el dato se refiere Respecto a la integridad de los mensajes de datos, dice el artículo 9º: *"…se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.*

En cuanto a la conservación, la misma ley en su artículo 12, establece condiciones de conservación, a saber:

1. Que la información que contengan sea accesible para su posterior consulta.

2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y

3. Que se conserve, de haber alguna, toda información que permita. determinar el origen, el destino del mensaje. la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

Como se aprecia, con la nueva ley la protección va a ser más efectiva, pero también traerá problemas de interpretación que a lo largo de la investigación se apreciarán.

VI. La nueva ley: 1273 de 2009

Dos tipos de conductas contiene la nueva Ley de delitos Informáticos

- Los atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos
- Atentados informáticos y otros

Corresponde al titular (es decir al propietario) de los datos y la información, implementar una serie de seguridades de carácter físico, documental, legal y electrónico con el fin de garantizar la confidencialidad, integridad y disponibilidad de los mismos.

Sin embargo, aun con las seguridades que nuestros expertos Tecnólogos desarrollan o aplican, los sistemas de información son burlados por el delincuente informático. Conductas sencillas propias de jovenzuelos arrojados, ahora son consideradas delitos con penas mayores a los 4 años de cárcel, que NO SON EXCARCELABLES.

Delitos contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos

Actualmente se encuentran tipificados en la ley:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación
- Interceptación de datos informáticos
- Daño informático
- Uso de software malicioso
- Violación de datos personales
- Suplantación de sitios web

Por ser de especial interés, se transcribe cada tipo penal:

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,

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

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 trasporte

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

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

Violación de Datos Personales. El que, sin estar facultado para ello, con provecho propio o de un ter-

cero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

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. 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.

Todas estas conductas tienen como pena desde 48 meses hasta 96 meses de cárcel y multas que pueden oscilar entre los 100 y 1000 salarios mínimos legales mensuales vigentes, excepto la Interceptación que tiene una pena menos gravosa, de 36 a 72 meses

Sin embargo, si hay victimas en la cadena del delito, se agrava de una tercera parte a la mitad y de la mitad a tres cuartas partes si se desarrollan están conductas sobre redes oficiales o financieras, por servidor publico, aprovechando la confianza o relación contractual, revelando el contenido de los datos obtenidos, obteniendo provecho, con fines terroristas o riesgo defensa o seguridad, utilizando a un tercero de buena fe o si el autor es el responsable de la información.

Para este ultimo, surge igualmente la pena accesoria de Inhabilidad para ejercer la profesión u oficio.

Otros atentados informaticos En cuanto a los Atentados informáticos se encuentran dos delitos tipificados.

·Hurto por medios informáticos
·Transferencia no consentida de activos

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.

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.

VII.Referencias

[1] Decreto 410 de 1971, Código de Comercio.Diario Oficial Colombiano No.33.339, Bogotá, Colombia, 16 de junio de 1971
[2] Ley 527 de 1999, Ley de Comercio Electrónico. Diario Oficial Colombiano No. 43.673, Bogotá, Colombia. 21 de agosto de 1999.
[3] Ley 594 de 2000, Ley de Archivo. Diario Oficial Colombiano No. 44.093, Bogotá, Colombia, 20 de julio de 2000.
[4] Ley 599 de 2000, Código Penal. Diario Oficial Colombiano No.44.097, Bogotá, Colombia, 24 de julio del 2000.
[5] Ley 1032 de 2006, Sistemas de Comunicaciones y asuntos de Derechos de Autor, Diario Oficial Colombiano No. 46.307, Bogotá, Colombia, 22 de junio de 2006.
[6] Ley 1273 de 2009. Protección de la Información. Diario Oficial Colombiano No. 47.223, Bogotá, Colombia, 5 de enero de 2009.

Clara Lucía Guzmán Aguilera. *Abogada Universidad Militar Nueva Granada. Especialista en Administración de Empresas Universidad del Rosario, Especialista en Derecho Comercial Universidad Externado de Colombia. Experta el Propiedad Intelectual. Experta en Derecho Informático. Docente en Legislación en Telecomunicaciones y Derecho Informático de la Corporación Universitaria Minuto de Dios (UNIMINUTO).*
cguzman@uniminuto.edu