RIESGOS JURÍDICO PENALES QUE SE DERIVAN DE LA PRÁCTICA DEL COMERCIO ELECTRÓNICO EN COLOMBIA

VALENTINA GARZÓN OSPINA
SARITA QUINTERO GIRALDO

Director
MIGUEL DÍEZ RUGELES

Trabajo de grado presentado como requisito parcial para optar al título de abogado

Pregrado en Derecho
Escuela de Derecho y Ciencias Políticas
Universidad Pontificia Bolivariana
Medellín
(2021)

Declaración de originalidad

Fecha:

Nombre del estudiante:

Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en esta o en cualquiera otra universidad.

Declaro, asimismo, que he respetado los derechos de autor y he hecho uso correcto de las normas de citación de fuentes, con base en lo dispuesto en las normas de publicación previstas en los reglamentos de la universidad.

_____

Firma del estudiante

RIESGOS JURÍDICO PENALES QUE SE DERIVAN DE LA PRÁCTICA DEL COMERCIO ELECTRÓNICO EN COLOMBIA

CRIMINAL LEGAL RISKS DERIVED FROM THE E-COMMERCE PRACTICE IN COLOMBIA

Resumen:

En la actualidad las relaciones comerciales se han visto modificadas en su práctica como consecuencia de la llegada de la globalización, ocasionando la creación del *e-commerce* y con ello la necesidad normativa de su regulación. Esto implica una realidad social que el derecho penal debe considerar, sobre todo por el surgimiento de los ciberdelitos que atentan contra varios de los bienes jurídicos que esta materia busca proteger, por lo cual el legislador penal adiciona un capítulo de delitos informáticos en el Código Penal colombiano.

Se cuestiona si esta regulación es suficiente para enfrentar la delincuencia cibernética, o si por el contrario surge la necesidad de crear nuevos tipos penales, y cuáles estrategias son útiles para superar la ausencia de presencia física de quienes se ven inmersos en la relación comercial y la complejidad de los sistemas tecnológicos.

Resultado de un arduo estudio de la legislación penal y análisis de la situación actual del país se concluye que, a través de la correcta implementación de herramientas tecnológicas y capacitaciones sobre los sistemas digitales a los funcionarios judiciales, se consigue aminorar la problemática sin necesidad de cambios significativos en la legislación penal.

Abstract:

Currently, the commercial relations has been modify in their practice because of the globalization arrival, causing the creation of e-commerce. This entail a social reality than penal law must consider as a consequence of cybercrime, which atents against several legal assetts that pretends to protect the law; therefore,

the legislator adds a full chapter on "codigo penal colombiano" of informatic crimes and cybercrimes.

it is questionable if these regulations are enough to front those crimes, conversely, emerge the need to create new criminal offenses, and strategies which are usefull to surpass the lack of physical presence from whom get involve on commercial relations and the complexity of technological systems.

In result of a hard work and penal legislation studies after analising the present situation of the country, the correct implementation of technological tools and traininngs on digital systems for judicial officials, the problem may be minnor without significant changes needed in the penal legislation.

Palabras clave: *e-commerce, ciberdelitos, delitos masa, ciberespacio, delitos informáticos, sitios web, ciberdelincuente, consumidor.*

Keywords: *e-commerce, cybercrimes, mass crimes, cyberspace, websites, cyber delinquent, consumer.*

Introducción.

La sociedad actual es el resultado del crecimiento acelerado del internet y de la implementación de herramientas tecnológicas en múltiples actividades cotidianas. La evidencia de ello es el exponencial aumento de las prácticas mercantiles a través del ciberespacio, tanto que hace 20 años era impensable para los sujetos adquirir productos con tan solo unos cuantos *clicks*. Esta nueva modalidad en la que se desenvuelve el comercio sin duda genera impactos positivos en la rapidez de las transacciones y en el amplio acceso a bienes y servicios sin fronteras.

La llegada de las redes no sólo materializó cambios significativos en la aplicación del derecho mercantil en Colombia, sino que también alcanzó otras parcelas del

derecho, entre estas la del derecho penal. Como es sabido, el derecho tiene la tarea de adaptarse constantemente a los cambios e interacciones sociales, así que aquellas actuaciones que realicen los sujetos por intermedio de instrumentos electrónicos que lesionan o ponen en riesgo bienes jurídicamente tutelados por el derecho penal crean la necesidad de estudio y regulación por parte del legislador penal.

Si bien las regulaciones penales en la mayoría de ordenamientos jurídicos se han esmerado por albergar todas las conductas que pueden afectar el correcto ejercicio del *e-commerce*, lo cierto es que en Colombia parece ganar la pelea la criminalidad cibernética por razón de la capacidad de adaptación del sujeto activo para encontrar nuevas modalidades velozmente y esquivar la norma sancionadora sin ser detectado. Por adición, se dificulta no sólo la identificación de la comisión de estas conductas, sino también la actividad probatoria en el marco del proceso penal, situación que hace ineficaz, en la mayoría de casos, la imposición de las sanciones que se indican en la ley penal. A ello hay que sumarle que es posible que se presenten conductas atípicas, cuya regulación resulta urgente porque lesionan alguno de los bienes jurídicos tutelados.

Debido a lo anterior, es imprescindible considerar al autor mexicano Julio Téllez Valdez, quien divide los delitos informáticos en dos conceptos: aquellas actividades que generan daños socialmente relevantes pero que no han sido tipificadas por el legislador penal, y por otro lado el *delito típico* entendiendo por éste todas las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (1996).

El análisis de la problemática que se expone hace necesario un trabajo de cooperación entre el derecho penal y la materia mercantil como parte del derecho privado, para lograr un mayor entendimiento del escenario en el cual se cometen tales conductas reprochables. También será necesario acudir someramente a algunos conceptos económicos e informáticos ajenos a la disciplina jurídica cuyo entendimiento es imprescindible para el presente estudio.

La doctrina del "nuevo derecho penal" habla del concepto de los *cibercrímenes* como los delitos de la actualidad y del futuro, como consecuencia de la era de la tecnología y el internet que trajo la globalización, y que, según Posada (2018), ha convertido a los seres humanos en víctimas híper vulnerables de este nuevo sistema, debido a la incomprensión y desconocimiento de los riesgos que se derivan de las nuevas tecnologías. Adicionalmente, en el derecho penal se han generado cambios significativos en los medios de prueba y las metodologías procesales que en Colombia aún carecen de pronunciamiento suficiente por la Corte Suprema de Justicia. En este sentido, este trabajo investigativo deja a un lado los delitos tradicionales que ya han sido ampliamente estudiados, con la intención de profundizar en la cibercriminalidad.

En cuanto al comercio electrónico puede encontrarse la teoría de "total libertad" expuesta por Barlow (1996), quien sostiene la necesidad de libertad en el margen de las interacciones a través del ciberespacio. En contrapartida, y advirtiendo que esta es la corriente apoyada en este trabajo, hay quienes consideran trascendental la regulación legal del comercio electrónico debido a gran cantidad de controversias en el plano jurídico que se presentan por esta práctica, y que aumentan con el pasar del tiempo.

En desarrollo de la problemática y para efectos metodológicos se considera conveniente desarrollarla siguiente estructura. Se cuenta con tres capítulos, el primero de ellos titulado *"Capítulo I: aspectos generales del comercio electrónico"*, en el cual se hallan tres subcapítulos: el primero llamado *historia del comercio electrónico*, el segundo *definición y conceptos relevantes*, y el tercero sobre *la aplicación y regulación del comercio electrónico en Colombia.*

El segundo capítulo denominado *"Capítulo II: de los delitos informáticos en el marco del comercio electrónico"* se encarga de exponer la relación del comercio electrónico y el derecho penal, haciendo hincapié en las características del *e-commerce,* las cuales crean riesgos jurídico penales y facilitan la comisión de

conductas reprochables, siguiendo con el señalamiento de los fundamentos penales para tipificar las conductas realizadas por estos medios, y finalmente la regulación penal que existe en el país sobre este tema. Está estructurado en dos subcapítulos, uno sobre *los cibercrímenes: regulación nacional y características típicas*, y el segundo llamado *defraudaciones informáticas en el e-commerce.*
Por su parte, el tercer y último "*Capítulo III: la aplicación y regulación del comercio electrónico en Colombia",* se dedica a evaluar si existen vacíos legales respecto a los riesgos jurídico-penales que el *e-commerce* facilita, y proponer una solución viable para mejorar la protección a los bienes jurídicos que se vulneran o corren el riesgo de afectarse en el escenario de las prácticas mercantiles cibernéticas, para disminuir la vulnerabilidad de los usuarios.

Capítulo I: aspectos generales del comercio electrónico

I. Historia del comercio electrónico.

Debe indicarse que la historia del comercio electrónico guarda bastantes similitudes con la historia de la Internet, que surgió como proyecto de la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA). En el 2005 el autor Seoane habla de cuatro generaciones. *La primera* tiene lugar en el año de 1993, cuando posterior a la llegada de la red las grandes empresas se interesaron en crear un sitio web institucional al estilo de blog, donde únicamente era posible hallar información de la compañía. Progresivamente estos sitios fueron convirtiéndose en catálogos virtuales.

Durante *la segunda generación* estas compañías encontraron la posibilidad de usar sus páginas web como centros comerciales virtuales con infraestructura de tienda virtual, llegando incluso a rentar espacios en estos portales para otras tiendas interesadas en promocionar sus productos. En este punto ya se utilizaban como medios de pago las transferencias de dinero que se realizaban con tarjetas electrónicas mediante una tarjeta bancaria en la red.

Será en *la tercera generación* donde se va a pretender automatizar todo el envío de datos acerca de los productos comprados y el proceso de selección de estos. Aparecen los primeros protocolos de pago seguro a través de las tarjetas electrónicas, y la publicidad a través de la red, también llamada *"marketing en la red".*

Posteriormente, durante *la cuarta generación*, las interacciones en la web se vuelven dinámicas a partir de datos suministrados por un sistema de base de datos, se procuran informáticos especializados en la programación de sitios web y se estructuran sistemas de seguridad para los sitios web (Castañeda, D.H.T., & Zavala, J. G., 2012).

Es adecuado reiterar que la inclusión del *e-commerce* en los negocios se dio con la entrada de la internet y es gracias a su crecimiento exponencial a nivel global que la evolución de esta modalidad de comercio ha sido permanente, hasta lograr ser lo que hoy en día representa: un medio esencial a través del cual se realizan ventas, tanto de bienes como servicios; ventas que generan importantes utilidades, pues estas herramientas tecnológicas se han convertido en las preferidas por muchas empresas tradicionales para acaparar la atención de la clientela, porque no requieren de una enorme infraestructura física para oficinas o tiendas ni de grandes inversiones y, además, posibilitan la rapidez de los negocios.

II. Definición y conceptos relevantes.

El *e-commerce* es un modelo de contrato basado en el intercambio de bienes y servicios con el elemento diferenciador de lograr, mediante la implementación de herramientas tecnológicas, un contacto permanente entre los compradores y vendedores. Asimismo, esta forma de comercio cuenta con la característica distintiva de ofrecer a cada uno de los usuarios de manera continuada un servicio especial todos los días, sobreponiéndose a las limitantes geográficas y del tiempo, lo cual permite expandir el alcance de cada negocio y diferenciarse del comercio tradicional (Ferrari, Z. V., 2017)

En la academia se habla de distintas modalidades de comercio electrónico, entre las cuales se encuentran:

En primer lugar, ***el negocio al consumidor o también conocida como Business to consumer -B2C-,*** en la cual los productos se comercializan de forma directa a través de internet y la oferta se hace en una tienda virtual o algún otro medio en la red, con un sistema que permite distintos medios de pago, lo que simplifica la realización de pedidos y las transacciones. Esta modalidad permite que las empresas amplíen su clientela brindando un portal secundario de comercialización.

En segundo lugar, ***de negocio a negocio o Business to business, B2B,*** alternativa que posibilita el intercambio entre las empresas que actúan como comprador y vendedor. Esto se logra mediante una plataforma con un diseño específico para este tipo de intercambios en el cual se reciben órdenes de compra, autorizaciones y pagos.

En tercer y último lugar, la modalidad ***de negocio a gobierno o Business to government, B2G,*** apoyada en el intercambio que existe entre las empresas y los gobiernos a través de una herramienta que permite la administración de información y disposición de servicios a nivel externo e interno. Cabe anotar que el análisis objetivo de este escrito se concentrará en las modalidades de comercio electrónico ***B2B y B2C.***

En el *e-commerce* hay ciertas características que se tornan primordiales para poder ofertar bienes y servicios y lograr fraccionar el mercado (Laudon, 2009). *La ubicuidad* consiste en que el internet se encuentra en todas partes, es posible encontrarlo en cualquier lugar y en cualquier momento, lo cual erradica la necesidad de un lugar físico. Surge lo que se conoce como *Marketplace* que permite realizar compras por medio de dispositivos móviles. La segunda característica es el *alcance global,* que se refiere a la totalidad de usuarios con

acceso a internet que un negocio de comercio electrónico puede tener, conformando un mercado potencial para las empresas, lo cual genera a su vez mayor efectividad en las transacciones.

Asimismo, los *Estándares Universales* aminoran considerablemente los costos de entrada al mercado con la implementación de plataformas y métodos estándar. Esto de forma consecuente reduce el esfuerzo de búsqueda por parte de los usuarios.

La cuarta característica del comercio electrónico es *La Riqueza del servicio web*, permitiendo a los comerciantes la utilización de herramientas, tales como mensajes de texto, audios, videos, etc., en el proceso de compra, facilitando la oferta de bienes y servicios con unas características más complejas sin necesidad de una presentación de forma directa.

Continuando con las características, otra de estas es *La Interactividad* que se da entre el usuario y el comerciante, creando un gran compromiso con los consumidores en interés de la satisfacción de sus necesidades. Otra singularidad del *e-commerce* es la *Densidad de la Información* que se encuentra disponible para todos los participantes de este mercado en igualdad de condiciones, trayendo consigo una operación de mayor calidad a un menor costo, y en último lugar la *Personalización/ Adecuación* que permite enviar diferentes mensajes de marketing personalizados en atención a los intereses o necesidades de cada usuario en particular, atendiendo a las preferencias o su comportamiento anterior en la red.

Dicho esto, es claro que a través del uso de procesos comerciales se da una transformación a la hora de aplicar nuevas tecnologías de las comunicaciones y la información. El comercio electrónico es, entonces, una variación inteligente a los negocios tradicionales. En su esencia, el comercio electrónico lleva el contrato de compraventa a otro nivel, pues permite descubrir lo que busca el consumidor, sus necesidades, sus gustos, y no solo respecto al consumidor pues

en ese descubrimiento se encuentran inmersos los comerciantes y las empresas. Adicionalmente, el comercio electrónico permite abaratar costos en los desplazamientos y de operaciones, permite una mejora en los tiempos de entrega y es clave entender el comercio electrónico como una manera de mejorar las actividades tradicionales de una empresa usando las diferentes tecnologías.

Por último, se torna clave entender que el comercio electrónico se encuentra dividido en diferentes categorías (Cuellar, D. & Roa, E. F, 2019), las cuales facilitan el entendimiento sobre cuándo y dónde surge el punto de quiebre en el que el comercio se vuelve vulnerable a ciertas conductas que se explicarán más adelante.

Los sitios transaccionales se utilizan para realizar cualquier tipo de pago, moviendo una gran cantidad de dinero, por tanto, se hace necesario un gran énfasis en seguridad y tecnología para soportar este tipo de sitios. En los *sitios de servicios o retail* se da la posibilidad de obtener productos o contratar servicios necesarios para el día a día, simplificando así muchas labores y facilitando la vida de los usuarios. (Chaffey, 2002). Luego están los *sitios de construcción de relaciones,* donde ve reflejada la facilidad de conocer nuevas personas y socializar a través del ciberespacio, aquí encuadran plataformas como Instagram, Facebook, Tinder, etc, plataformas que día a día reciben millones de visitas. Finalmente, el *advertising* o bien conocido como publicidad, normalmente se encuentra en los portales de búsqueda y redes sociales, esto debido a la cantidad de visitas que reciben a diario. (Chaffey, 2002)

III. La aplicación y regulación del comercio electrónico en Colombia

La regulación del comercio electrónico ha sido frecuentemente cuestionada por la existencia de tres tendencias: la primera sobre la abstención absoluta de intromisión legislativa en el ciberespacio, la segunda sobre la autorregulación a partir del marco propiciado por todos los sujetos involucrados, y la tercera sobre la regulación legislativa (Rincón, C. E., 2004).

El 17 de diciembre de 1996 en el marco del derecho mercantil internacional se promulga la Ley Modelo de Comercio Electrónico (1996) aprobada por la CNUDMI, cuya pretensión es facilitar el uso de los medios de comunicación modernos en el desarrollo de todas las actividades y se encuentra conformada por dos grandes secciones (Orrego, G. S. 2015). La primera ofrece una comprensión general del *e-commerce*, y la segunda sección lo aborda de forma específica. Empero, la ley deja varios aspectos sin regulación para ser tratados en el futuro de acuerdo con las circunstancias propias de tiempo, modo, lugar o cambios tecnológicos (Ferrari, Z. V., 2017).

En Colombia la iniciativa legislativa sobre los asuntos del comercio electrónico surgió bajo la ley modelo de la CNUDMI, que sirvió de guía para lo que más adelante tomó el cuerpo legislativo de la Ley 527 de 1999. Sin embargo, no fue la primera ley en mencionar la utilización de tecnologías informáticas y electrónicas, pues hay antecedentes legislativos que ya hacían una que otra consideración sobre la temática desarrollada.

El primero de estos es el Decreto 663 de 1993, por el cual se actualizó el Estatuto Orgánico del Sistema Financiero y contempló la posibilidad de usar sistemas e intercambios electrónicos. En el año 1995 se expide la Ley 222 que contempla la posibilidad de incorporar avances tecnológicos en las reuniones de accionistas sin exigir la presencia física de los socios (Artículo 19). También la Ley 223 de 1995, el decreto 1094 de 1996, el concepto de la DIAN No.40333 de 2000 y el decreto 2242 del 24 de noviembre del 2015 se encargan de la incorporación y regulación de la factura electrónica.

El objetivo de la ley 527 de 1999 es otorgar de valor probatorio a toda la información digital, por lo que actualmente el tratamiento y los efectos jurídicos que se les da a este tipo de datos es exactamente el mismo que se le da a la información que se encuentra en documentos físicos y otros soportes escritos. El ámbito de aplicación es el siguiente:

> **ARTÍCULO. 1º - Ámbito de aplicación.** La presente ley será aplicable a todo tipo de información en forma de mensajes de datos, salvo en los siguientes casos a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales: b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo". (Ley 527, 1999).

De la lectura es dable inferir que la aplicación de esta ley es de carácter general ya que puede ajustarse a todo tipo de información. Las dos principales sentencias de la Corte Constitucional en lo relacionado al ámbito de aplicación de la Ley 527 de 1999 son la sentencia C-831 de 2001 y la sentencia C-662 de 2000, decisiones que denotan que los mensajes de datos tienen plena aplicación, desde un punto de vista jurídico, en todos los asuntos, salvo en las obligaciones contraídas por el Estado colombiano producto de tratados internacionales, convenios o respecto de las advertencias legales necesarias para la defensa de los derechos de los consumidores cuando la información pueda ser verificada para ser consultada posteriormente.

La Corte hace énfasis en cuanto a la recopilación de información, de manera independiente a la forma en que se presente, debe ser interpretada tal cual está sin ningún tipo de restricción, permitiendo garantizar los derechos de los consumidores (sentencia C-831, 2001). La ley de comercio electrónico va más allá de lo presupuestado por la CNUDMI, aunque las dos primeras partes de la norma incluyen de manera estricta los principios de la Ley Modelo.

El último antecedente de este recuento es la Ley 1480 de 2011, también conocida como Estatuto del Consumidor, producto del auge que tuvo el derecho del consumo. Esta Ley tiene unos pilares fundamentales en pro de garantizar los beneficios de los consumidores nacionales y extranjeros que realicen cualquier tipo de operación y es por esto por lo que dentro de sus artículos se contempla el acceso a la información adecuada. El Estatuto dota de la posibilidad a cada uno de los consumidores de proteger y exigir sus derechos en caso de que se

presenten asimetrías en la información respecto productores, expendedores y otros miembros involucrados en la cadena productiva.

Capítulo II "de los delitos informáticos en el marco del comercio electrónico".

I. Los cibercrímenes: regulación nacional y características típicas.

Los delitos informáticos o cibercrímenes, nombre atribuido por la doctrina penal técnica, son propios del *nuevo derecho penal* bajo la modalidad de actuaciones delictivas de *cuello blanco.* Los primeros estudios académicos sobre estos delitos tuvieron su origen en los años setenta en Europa y a inicios del siglo XXI en Colombia (Posada, 2018). La primera figura delictiva agregada al ordenamiento jurídico penal colombiano fue el delito de *Acceso abusivo a sistema informático protegido con medida de seguridad* artículo 195, declarado inexequible por la Corte Constitucional (sentencia C-913. 2010), con posterioridad a la Convención sobre la Ciberdelincuencia de Budapest en el año 2001, estatuto internacional que declara la necesidad de fijar una política penal común con el fin de legislar en los Estados convenidos la criminalidad informática.

El 5 de enero del 2009 a través de la Ley 1273 se modifica al Código Penal (2000), adicionando un nuevo bien jurídico tutelado que recibe el nombre "de la protección de la información y de los datos", en el Título VII bis a partir del artículo 269A al 269J, legislación que evidencia las limitaciones de los delitos tradicionales para hacerle frente a las conductas delictivas que se realizan en el ciberespacio, que atentan contra la intimidad, el almacenamiento de datos y el patrimonio.

Algunos doctrinantes aseveran que los delitos informáticos no constituyen una categoría delictiva autónoma, sino que se trata de los mismos delitos tradicionales agravados porque su ejecución se lleva a cabo mediante sistemas

tecnológicos, y en el mismo orden no crean un bien jurídico tutelable diferente a los que ya se encuentran previstos por el legislador penal.

Este entendimiento, sin embargo, parece equívoco al considerar las particulares características de estos delitos, a saber: i) la necesidad de proteger la seguridad de la información, datos o sistemas informáticos, y subsidiariamente otros bienes jurídicos tutelados, y ii) que estos delitos se traducen en actuaciones realizadas en un lugar deslocalizado virtual, en una realidad simulada que solo existe en la red de sistemas.

Los *ciberdelitos* presentan una mayor complejidad por diversos factores, entre estos el espacio en que son ejecutados, el cual no es un lugar físico sino virtual (Miró, L. F., 2012), y, adicionalmente, la rapidez en el intercambio y almacenamiento de datos, generan cambios en el desarrollo de la teoría de la conducta punible y sus consecuencias. Al respecto, Buompadre (2013) resalta que en los delitos informáticos predominan las estructuras típicas de simple actividad ligadas a delitos de peligro abstracto y que ocasionan la temprana intervención del derecho penal, así como mayor imprecisión en la descripción de los comportamientos típicos.

Otro distintivo de estos delitos está en cabeza de los actores y las víctimas. Si bien es cierto que los delitos tratados no consagran expresamente en su tipificación calidades especiales del sujeto activo, la realidad práctica demuestra que este debe contar con mínimas capacidades informáticas o técnicas para acceder a la red y traspasar la seguridad de los datos en la nube. En contrapartida, el sujeto pasivo de estos comportamientos digitales usualmente es vulnerable por su falta de conocimiento e ingenio para el uso seguro y preventivo de las herramientas del internet.

Esta categoría autónoma delictiva está dividida en varios bloques o grupos de cibercriminalidad en atención a los intereses cuya protección se regula. Se tratan

del intrusismo, espionaje, sabotaje, defraudaciones informáticas, y otras conductas punibles tradicionales cuyo medio es la red.

El intrusismo es la violación de funciones informáticas o la comisión de conductas delictivas informáticas, como el acceder sin autorización previa a una red Wi-Fi o ingresar abusivamente a correos electrónicos. En este subgrupo de *cibercrímenes* se concretiza el riesgo en los bienes jurídicos de intimidad, seguridad de datos, información y sistemas informáticos, y el legislador penal nacional tipifica el intrusismo en el artículo 269A del Código Penal (2000) con el nombre de "acceso abusivo a un sistema informático". Por su parte, *el espionaje informático* se refleja en un conjunto de actividades ilícitas encaminadas a violentar la intimidad de personas naturales o jurídicas. Se interceptan, captan o desarrollan información, datos, imágenes, sonidos, vídeos, mensajes, etc., en red o la nube, de naturaleza pública o privada. (Posada, 2018. Pág 167 y 168) En la ley penal para hacerle frente a este problema se tipifica el artículo 269F titulado "*Violación de datos personales"*.

El sabotaje informático regula aquellas conductas ilegales que tienen por fin interferir, obstaculizar, suprimir, dañar o alterar el servicio de sistemas informáticos o redes de comunicación públicas o privadas de datos; bases de datos o documentos electrónicos de valor para el orden social, estatal o económico; y funciones de tratamiento y transmisión siempre que sean necesarias para el funcionamiento de infraestructuras informáticas. El artículo 269D de nuestro Código Penal (2000) tipifica el sabotaje bajo el nombre de *"Daño informático"*.

En último lugar están *las defraudaciones informáticas*, que por cierto son las más cometidas en el ciberespacio y cuyos efectos son más evidentes por lesionar y poner en riesgo el patrimonio. Son conductas delictivas que acarrean resultados perjudiciales a través de la manipulación de sistemas informáticos, con la especial finalidad de lucro o ánimo fraudulento para obtener un incremento

patrimonial ilícito de activos que a su vez trae detrimento injustificado en el patrimonio de un tercero, víctima de la conducta.

II. Defraudaciones informáticas en el e-commerce.

Según el Centro Cibernético Policial en el Balance del Cibercrimen año 2020 las principales modalidades de delitos informáticos reportados al CAI Virtual de la Policía Nacional son, en orden de incidencia, la estafa y/o compra de bienes y productos con 2.391 casos, el *phising -envío de correos electrónicos aparentemente confiables que pretenden engañar al tercero receptor para obtener de este información personal, que posteriormente será utilizada para realizar actuaciones ilegales-* con 1.753 casos conocidos por la autoridad competente. El mismo balance señala que del 25 de marzo al 08 de noviembre del 2020 se denunciaron 10.208 casos de hurto por medios informáticos y semejantes, 3.499 casos de suplantación de sitios web de retail o servicios, y 2.064 casos por transferencia de datos no consentida. En Colombia hasta finales del año pasado las ciudades con cifras más altas en la denuncia de estos delitos eran Bogotá con 37%, Medellín en segundo lugar con 10%, Cali en tercer lugar con 7%, Barranquilla 5%, Bucaramanga 4% y Cartagena con 2.5%.

Estas cifras son un claro ejemplo de la alta incidencia *ciberdelictiva* en el país, que de hecho tuvo un incremento en comparación con el año 2019. Los comportamientos ilícitos informáticos denunciados ponen en riesgo o lesionan subsidiariamente el bien jurídico patrimonio. La honorable Corte Constitucional se ha referido al patrimonio como un atributo indispensable, “el hombre no podría cumplir su cometido de ser social, ya que lo necesita para realizarse como tal y ha de contar con él para atender por lo menos las exigencias económicas de supervivencia suya y de su núcleo familiar” (Sentencia T-553. 1993).

Recuérdese que *el patrimonium* es una ficción legal, una universalidad de contenido económico que ostenta una persona natural o jurídica, compuesta por bienes materiales o inmateriales, derechos y obligaciones. (Morales, F. S &

Daza, C. S. 2016). Las relaciones obligacionales mercantiles, con independencia de si son ejecutadas tradicionalmente o por medios informáticos tienen como requisito, de cara al comerciante o quien realiza actos de comercio, la obtención de utilidades, de allí el principio general del derecho mercantil de onerosidad. Las utilidades se pueden representar en diversas figuras como en partes de interés o dividendos en materia societaria, o en activos, bienes y créditos respecto al negociante. (Castro de Cifuentes, M. 2009).

Aquellas personas, sean naturales o jurídicas, que ofrezcan bienes o servicios, o los adquieran, bajo diferentes modelos de contratación, de forma reiterada con ánimo de lucro alguno, en el ciberespacio o sistemas de telecomunicación digital, pretenden al final un beneficio para sus patrimonios, ya sea en el incremento de los activos o la protección de estos evitando su decrecimiento. Por esta razón, el patrimonio de las compañías o los empresarios que confían en las plataformas digitales para la realización de sus actividades, como los consumidores que adquieren los bienes o servicios ofrecidos por estos medios en aras a la satisfacción de sus necesidades o intereses, además de la seguridad de su información, debe ser protegido no exclusivamente por la *Superintendencia de Industria y Comercio* en ejercicio de sus funciones jurisdiccionales, sino que también debe ser objeto de prevención en el ordenamiento penal nacional. Como se ha previsto, un alto número de comportamientos ilícitos inescrupulosos que ponen en efectivo riesgo el bien jurídico patrimonio son cometidos por delincuentes que aprovechan los conocimientos técnicos y especializados en sistemas informáticos de reducido manejo por las personas en general, creando riesgos jurídico penales en el *e-commerce* en detrimento de la seguridad y estabilidad económica de sus usuarios.

Retomando con el grupo de *cibercrímenes* sobre *defraudaciones informáticas*, en aquellas está presente la manipulación de los sistemas informáticos, ya sea falseando o modificando con un software los programas de funcionamiento de estos, o también haciendo un *uso indebido* directo o indirecto del almacenamiento, procesamiento o transferencia de datos, o información

escritural económica o financiera. Es necesario que acontezca una manipulación, introducción, falsificación, alteración o borrado de datos registrados en los sistemas informáticos. y posteriormente hacer uso ilegal de estos con propósito de lucro y fraude.

Una técnica que ejemplifica las defraudaciones es *la técnica de salami* (Posada, 2018. pág 174), donde se infecta un sistema con programas que permiten separar de las transferencias consentidas de activos, reducidas cantidades de dinero en beneficio ilegítimo de los agresores. Estas prácticas han de ocasionar recelo en los usuarios de plataformas bancarias o de ventas de bienes o servicios, quienes conocedores o víctimas de estos ilícitos van a pensarlo más de una vez antes de preferir la virtualidad para la celebración y ejecución de dichas actividades, resultando un panorama desalentador para las compañías, tanto pequeñas como grandes, y los negociantes que utilizan el mundo digital como una extensión de sus negocios considerablemente más cercana a los destinatarios.

En Colombia hay controversia sobre las diferencias existentes entre los delitos económicos comunes, en concreto el hurto y la estafa, y los *ciberdelitos* de naturaleza patrimonial, como la transferencia no consentida de activos y el hurto por medios informáticos o semejantes. *La ingeniería social* se convierte en un concepto trascendental en el entendimiento de la discusión, consistente en engañar a las víctimas para ganar su confianza e infringir procedimientos normales de seguridad, causando que sean ellos mismos quienes les abran camino a los ciberdelincuentes (Romero, D. 2019), disponiendo de sus activos o información sensible como contraseñas de cuentas bancarias, correos electrónicos, direcciones físicas, ubicación, etc.

Es el caso de las estafas por mensajes de correo electrónico, donde los ciberdelincuentes se hacen pasar por entidades bancarias para que la víctima, bajo engaño, consigne sus datos. Asimismo, la oferta fraudulenta de supuestos descuentos en el precio de productos de alguna reconocida empresa, imitando

sus sitios web o enviando mensajes de datos, para que las víctimas confiadamente envíen su dinero creyendo que están adquiriendo un bien que no existe realmente, en beneficio ilícito del estafador cibernético.

Capítulo III. ¿Basta con la regulación actual sobre los delitos informáticos?

Como se ha señalado, los delitos informáticos que trae el legislador penal en el año 2009 están a partir del título VII bis denominado “de la protección de la información y los datos”, compuesto por diez tipos penales que van del artículo 269A al 269J. Una vez más se reitera que el esfuerzo del legislador penal en tratar de regular este tipo de conductas específicas que surgen con el internet y el uso de medios electrónicos no es en vano ni desacertado, ya que algunos de estos tipos penales son útiles para castigar ciertas conductas *ciberdelictivas* que no estaban prohibidas en los delitos tradicionales, como sucede con el daño informático 269D, el acceso abusivo a sistema informático 269A, el uso de software malicioso 269E y la suplantación de sitios web para capturar datos personales 269G. Para la tipificación de estos comportamientos fue necesario entender e introducir conceptos informáticos que hasta el momento eran ajenos a los tipos penales ya existentes, lo cual imposibilitaba la función de los jueces por el límite al poder punitivo que establece el principio de tipicidad (artículo 10, Ley 599. 2000).

Los delitos anteriormente indicados, se considera, cumplen con la finalidad del legislador a la hora de proponerlos, y gozan de completa utilidad en la tarea del ente acusador, porque tipifican satisfactoriamente esta clase de conductas específicas que deben ser previstas y prohibidas por la ley penal para la protección del bien jurídico de seguridad de la información y datos. Empero, no se tiene la misma consideración en cuanto al tipo penal 269I de “Hurto por medios informáticos”, pues este delito conlleva obligatoriamente a observar la conducta descrita en el artículo 239 y siguientes sobre el hurto tradicional y sus agravantes.

> **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. 2000)

Aunque este tipo penal se puede clasificar como una modalidad especial y autónoma del delito de hurto calificado tradicional, no es un *cibercrímen* o delito informático. Este delito procura completar las descripciones típicas contenidas en el artículo 239 y siguientes, y por esto se remite expresamente a estos. El delito común de hurto consiste en sancionar a *"aquel que se apodere de una cosa mueble ajena, con el propósito de obtener beneficio para sí o para otro".*

Claramente el propósito ilícito de obtener beneficio propio o para un tercero será necesario en el *ciberdelito* con independencia de su realización a través de sistemas informáticos. El problema está en el verbo rector, el cual consiste en "apoderarse", y el objeto sobre el cual recae la acción que es "cosa mueble ajena". Apoderarse de algo implica necesariamente la tenencia material del bien, el cual deberá necesariamente ser mueble *(tangibles o divisas)*, cuya propiedad sea de otra persona ajena al sujeto activo de la conducta. Las cosas intangibles no están consagradas en este delito, y la intangibilidad es la característica principal de todo lo que se encuentra en el ciberespacio. Esto no quiere decir que el legislador penal no haya contemplado la protección de bienes intangibles, pues los regula en el tipo penal de transferencia no consentida de activos *(datos con valor escritural o económico)* buscando variar la estafa tradicional por la figura de estafa electrónica (Corte Suprema de Justicia, 2015).

En la conducta de hurto por medios informáticos el legislador no consagró una nueva acción que sea objeto de mayor juicio de desvalor, sino que se limitó a la acción ya tipificada en el hurto simple, con la asignación de la pena del hurto calificado. No consagró un nuevo verbo rector en este artículo, y en este punto está la dificultad, pues al analizarlo desde el punto de vista del elemento subjetivo

distinto del dolo y el provecho patrimonial ilícito hay conductas que pueden ser hurto pero que los jueces no pueden juzgar por no encuadrarse en este tipo penal. Quizá el error que comete el legislador fue crear este tipo penal con la intención de endurecer las penas del hurto, aunque su finalidad debió ser aminorar los riesgos inherentes a los *cibercrímenes* por desenvolverse en el espacio virtual, tales como el anonimato de quien realiza el comportamiento, su masificación, riesgos técnicos y de prevención.

La consecuencia de que el delito de hurto por medios informáticos no sea un *ciberdelito* sino una extensión del hurto tradicional calificado tiene que ver con el bien jurídico que tutela directamente. Pareciera contradictoria la ley penal al proteger el bien de la seguridad de la información y los datos, cuando en el caso concreto del hurto de artículo 269I el bien jurídico tutelado principalmente es el patrimonio económico, y de forma subsidiaria el de la información y datos. Al respecto la Corte Suprema hace claridad que este es un delito pluriofensivo que protege directamente la información y los datos y de forma indirecta el patrimonio económico (2015), superando la contrariedad.

El comercio electrónico se desarrolla con la intención de salvaguardar o aumentar los activos del patrimonio de una compañía a través de relaciones mercantiles llevadas a cabo en el ciberespacio, motivo por el cual a las empresas que utilicen la red para ejecutar sus actividades, y a su clientela, les afecta negativamente las inconsistencias de la regulación penal sobre los *ciberdelitos* que producen detrimento en sus patrimonios, que se reflejan en los conflictos prácticos que enfrentan en proceso los fiscales de la Nación en su tarea.

Lo anterior sobre el proceso penal amerita mayor ampliación, pues constituye otro obstáculo para la tutela de los bienes jurídicos que requieren protección. El ente acusador que representa los intereses estatales y busca la penalización de los delincuentes, debe procurar hacer su trabajo con las carencias en asuntos probatorios a las que se debe enfrentar. Para la Fiscalía es muy complejo

identificar e individualizar al presunto ciberdelincuente, debido al riesgo de anonimato y a las circunstancias espacio-temporales derivadas de *la ubicuidad* del comercio electrónico, pues hay que tener presente que existen múltiples herramientas que cada vez facilitan más la actividad cibercriminal, como el uso de sistemas, programas o aplicativos que encubren la identidad del sujeto activo o la verdadera dirección IP del dispositivo utilizado para la comisión de estas conductas. La recolección de pruebas que logren individualizar al presunto delincuente, para realizar la debida acusación ante el juez y determinar el momento y circunstancias específicas en que se comete la conducta, exige de un trabajo conjunto de expertos en seguridad en sistemas y profesionales en derecho, lo cual aumenta considerablemente los costos y cargas en cabeza del Estado.

Desde el punto de vista económico, costo-beneficio y facilidad probatoria para la fiscalía, una propuesta desafortunada sería que la carga de la prueba en el proceso se traslade a la defensa, generando que no sea la fiscalía quien tenga que probar que el incremento al patrimonio del sujeto activo fue ilícito, sino que será la defensa quien tenga que probar que ese incremento patrimonial producto de una actividad comercial a través de sistemas informáticos tuvo origen lícito. Empero, no resulta proporcional sacrificar la presunción de inocencia, consignada en el artículo 29 de la Constitución Política (1991), característica esencial de nuestro Estado personalista y el principio penal *In Dubio pro-reo,* en defensa del comercio electrónico. Sobre esta presunción la Corte Constitucional ha enfatizado lo siguiente:

> La actividad probatoria que despliegue el organismo investigador debe entonces encaminarse a destruir la presunción de inocencia de que goza el acusado, a producir una prueba que respete las exigencias legales para su producción, de manera suficiente y racional, en el sentido de acomodarse a la experiencia y la sana crítica. Así pues, no le incumbe al acusado desplegar ninguna actividad a fin de demostrar su inocencia, lo que conduciría a exigirle la demostración de un hecho negativo, pues por el contrario es el acusador el que debe demostrar su culpabilidad (Corte Constitucional. 2012).

Una solución más factible y respetuosa de la constitución, será entonces, invertir en las diferentes herramientas investigativas, en capacitaciones y a su vez fortalecer la cooperación internacional respecto a este tipo de delitos que no reconocen frontera alguna, con esta propuesta se lograría mayor efectividad del proceso penal por conductas denunciadas y reducción en la impunidad de las mismas, recuperando la seguridad que los usuarios y comerciantes del *ciberespacio* deberían sentir al ejecutar estas interacciones mercantiles, sintiendo el respaldo estatal debido en la prevención de daños y protección de bienes jurídicos por la amenaza de ciertas conductas ilícitas.

En el mismo sentido, es necesario analizar la agravante punitiva número 17 contenida en el artículo 58 de la parte general del Código Penal Colombiano, adicionada por la ley 1273 de 2009, que aplica a todos los delitos tradicionales, salvo que haya sido previsto de otra manera. Serán agravadas aquellas conductas típicas que sean realizadas por medios electrónicos o telemáticos, lo cual amplía las posibilidades de castigar conductas ilícitas bajo modalidades llamativas que parecen no encajar en principio con ningún tipo penal, pero que de cumplir con todos los requisitos descritos por el legislador en algún delito, y adicionalmente ser realizados a través de medios informáticos, podrán ser imputados bajo algún delito tradicional.

Esto es importante porque los delitos comunes también podrían adaptarse a las conductas susceptibles de atentar contra la seguridad del comercio electrónico y el patrimonio económico, sin necesidad de acogerse exclusivamente a los delitos informáticos que trae el legislador, los cuales, como ya se ha desarrollado, no necesariamente consideran todas las conductas ilícitas posibles de comisión bajo el marco de las relaciones mercantiles virtuales. Es el caso del delito de estafa, ya que no hay un *ciberdelito* que contemple este comportamiento, aunque en caso de cometerse una estafa mediante sistemas informáticos entonces podrá imputarse el delito tradicional de estafa con la agravante del numeral 17 del artículo 58.

Supóngase, para ejemplificar, que una persona crea un perfil de empresa en la red social Instagram, sube imágenes de productos que baja de Google, ofreciéndolos para su venta a un determinado precio. Estos productos realmente no existen, pues esta persona no los tiene ni mucho menos busca vender. Su objetivo es hacerle creer a sus seguidores que en efecto vende los productos para que realicen una compra supuestamente segura. Un usuario que recientemente ve el perfil que está amparado bajo la modalidad de empresa por la red social, decide seguirla, y comprar unos cuantos productos. El usuario envía a través de transferencia bancaria el dinero que la supuesta vendedora le indica por precio, y una vez la persona recibe el dinero bloquea al usuario y elimina la cuenta.

Este caso es de gran ocurrencia hoy en día en las diferentes plataformas digitales, pues se ha convertido en una modalidad para estafar a los usuarios, a quienes solo les queda confiar en la inocencia y buena fe de quienes se hacen llamar empresas que ofrecen bienes y servicios, ya que la mayoría de denuncias no prosperan más allá de un simple acto de comunicación a la autoridad competente por las razones que arriba se describen, obstáculo que se podría superar realizando un proceso de recepción de las denuncias más eficiente, mediante la identificación de todas las víctimas y procesamiento de estos ilícitos como *delitos masa*, los cuales se componen de un elemento subjetivo consistente en un único propósito del sujeto activo, que usualmente pretende un lucro global; un perjuicio sufrido por las diferentes víctimas del fraude, sin tomarlos como independientes; y el sujeto pasivo integrado por una colectividad sobre las cuales se dirige indeterminadamente la actuación fraudulenta del sujeto activo (Sainz, 1971).

Conclusiones

Lo planteado con antelación sobre los *ciberdelitos* del título VII bis y los delitos tradicionales bajo la agravante de realización por medios electrónicos o telemáticos, pone de presente que es innecesario crear nuevos tipos penales para enfrentar las complicaciones de aplicación de las conductas ilícitas que se pueden desarrollar en el marco del *e-commerce*, pues sería una solución imprecisa si lo que se quiere es lograr efectividad en la penalización de comportamientos que ejecuten los ciberdelincuentes en el comercio, porque continuaría la dificultad interpretativa y ambigüedad en la imputación del delito presuntamente cometido. Lo único que causaría es continuar con la *hiperproducción legislativa* que caracteriza al país.

Se podría pensar la necesidad de crear nuevos tipos penales respecto a ciertas conductas como el *phishing,* pero es pertinente evaluar la situación desde dos perspectivas. En primer lugar, la posibilidad de crear un nuevo tipo penal como delito de peligro anticipando las barreras de protección del bien jurídico, o desde una segunda perspectiva, conservando la línea actual de nuestro legislador, entendiendo que al tratarse de conductas preparatorias no constitutivas de delito es injustificado tipificarlas por no representar un peligro efectivo para el bien jurídico en cuestión, sin negar la posibilidad de sancionarlas desde otras parcelas del derecho.

No se niega que el derecho debe actualizarse constantemente, y en penal se deberán crear nuevos tipos penales de acuerdo con las exigencias sociales y en el momento en que las nuevas conductas ilícitas no logren adaptarse a ningún delito, ya sea informático o tradicional, producto de la carencia legal el legislador a futuro tendrá que modificar la legislación.

Lo anterior no implica que al día de hoy la solución a las problemáticas prácticas e interpretativas de los ilícitos que son cometidos en el comercio electrónico sea la producción de nuevos tipos penales, lo que se cree conveniente es una reestructuración en la redacción de los delitos informáticos, acompañada de una guía interpretativa creada de la mano de los expertos en ingeniería informática

que definan lo que debe entenderse por ciertos conceptos técnicos propios de los sistemas informáticos, inteligible para cualquier persona del común de la forma más sencilla posible, y una inversión estatal en términos económicos para disponer de los instrumentos técnicos y llevar a cabo las capacitaciones del personal judicial, con el propósito de facilitar la tarea de los jueces y las partes del proceso. En ese sentido y no menos importante, considerar el tratamiento de las miles de denuncias recibidas ante las autoridades en relación con los *ciberdelitos* como *delitos masa*, que exigen de la Fiscalía una mayor atención e inmediatez.

Referencias

Libros:

- Castro de Cifuentes, M. (2009). *"Derecho Comercial: Actos de comercio, empresas, comerciantes y empresarios".* Uniandes y Temis, Bogotá D.C, Colombia.
- Laudon, C. K,. (2009). E-commerce: negocios, tecnología y sociedad. Cuarta edición. México: Pearson Educación.
- Miró, L. F. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio.* Marcial Pons, Ediciones Jurídicas y Sociales. Madrid, España.
- Posada, M. R (2018). *Los cibercrímenes: un nuevo paradigma de criminalidad.* (1a. ed). Bogotá D.C: Universidad de los Andes y Grupo Editorial Ibáñez.
- Seoane, E. (2005). *La nueva era del comercio electrónico: Historia del comercio electrónico.* (page.13). Vigo, España.
- Téllez, V. J. (1996). Derecho Informático. 2ª. ed. México. Mc Graw Hill Pp.103-104

Publicaciones periódicas:

- Barlow, P. J. (1996). Declaración de independencia del ciberespacio. Davos, Suiza.
- Castañeda, D. H. T., & Zavala, J. G. (2012). Comercio electrónico. *Contribuciones a la Economía*, *7*.
- Centro Cibernético P. (2020). Balance Cibercrímen. Cai Virtual Policía Nacional. Sitio Web: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf
- Orrego, G. S (2015). El comercio electrónico y los mecanismos online para la resolución de disputas. Universidad EAFIT, Medellín. (Pág. 91 y 92.)
- Rincón, C. E. (julio-diciembre, 2004). Últimos retos para el derecho privado: las nuevas tecnologías de la información. 6(2), pp. 430-500.
- Sainz, C. J. (1971). *El delito masa.* Recuperado de file:///Users/mac/Downloads/Dialnet-ElDelitoMasa-2785140%20(3).pdf

Trabajos de grado:

- Buompadre, J. (2013). *Violencia de género, feminicidio y derecho penal: los nuevos delitos de género*. Alveroni. Córdoba, Argentina.
- Cuellar, D. & Roa, E. F. (2019). Evolución del comercio electrónico en Colombia en la última década. Universidad de La Salle. Bogotá D.C.

- Morales, F. S & Daza, C. S. (2016). “El concepto de patrimonio y su aplicación en España”. Universidad Católica de Colombia. Bogotá, D.C., Colombia.
- Romero, R. D. (2019). “El arte de la Ingeniería Social”. Universidad Piloto de Colombia. Bogotá D.C, Colombia.
- Ferrari, Z. V. (2017). El comercio electrónico en Colombia: barreras y retos de la actualidad (pág 19). Bogotá D.C.

Documentos legales:

Normas jurídicas:

- Constitución Política de Colombia [Const]. Art 29. 7 de julio de 1991 (Colombia)
- Ley Modelo sobre Comercio Electrónico, (1996), Comisión de las Naciones Unidas para el Derecho Mercantil.
- Colombia. El presidente de la República. Estatuto Orgánico del Sistema Financiero, Decreto 663 (1993).
- Colombia. Congreso de la República. “Por la cual se modifica el libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones”. Ley 222 (1995).
- Colombia. Congreso de la República. Sobre uso de mensajes de datos, del comercio electrónico y de las firmas digitales, Ley 527 (1999).
- Colombia. Congreso de la República. “Por la cual se expide el Código Penal”. Ley 599 (2000)

- Colombia. Congreso de la República. “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”. Ley 1273 (2009).
- Colombia. Congreso de la República. “Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones”. Ley 1480 (2011).

Sentencias:

- Corte Constitucional de Colombia (1993). Bogotá D.C. Sentencia T-553. Magistrado ponente Hernando Herrera Vergara.
- Corte Constitucional de Colombia (2000). Bogotá D.C. Sentencia C-662. Magistrado Ponente Fabio Morón Díaz.
- Corte Constitucional de Colombia (2001). Bogotá D.C. Sentencia C-831. Magistrado Ponente Álvaro Tafur Galvis.
- Corte Constitucional (2012). Bogotá D.C. Sentencia C-289. Magistrado ponente Humberto Antonio Sierra Porto.
- Corte Suprema de Justicia. (2015). Bogotá D.C. Sentencia SP 1245. Magistrado Ponente Eyder Patiño Cabrera.