ANÁLISIS JURIDICO DEL LA LEY 1273 DEL 2009 Y EL SURGIMIENTO Y EXPANSIÓN DEL DELITO DE HURTO Y SEMEJANTES POR MEDIOS INFORMÁTICOS.

YENIFER YIRLESA BECHARA PALACIOS
ALAN YECID MOSQUERA PALACIOS
EDWAR ESTIVIN LEDEZMA LEDEZMA

UNIVERSIDAD COOPERATIVA DE COLOMBIA

FACULTAD DE DERECHO

PROGRAMA DE DERECHO

QUIBDÓ

2020

ANÁLISIS JURIDICO DEL LA LEY 1273 DEL 2009 Y EL SURGIMIENTO Y EXPANSIÓN DEL DELITO DE HURTO Y SEMEJANTES POR MEDIOS INFORMÁTICOS.

YENIFFER YIRLESA BECHARA PALACIOS
ALAN YECID MOSQUERA PALACIOS
EDWAR ESTIVIN LEDEZMA LEDEZMA

TRABAJO PRESENTADO PARA OBTENER EL TITULO DE ABOGADO

UNIVERSIDAD COOPERATIVA DE COLOMBIA

FACULTAD DE DERECHO

PROGRAMA DE DERECHO

QUIBDÓ

2020

DEDICATORIA:

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi Padre, Isaías Mosquera Salazar, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras diferencias de opiniones.

Por: Alan Yecid Mosquera Palacios.

El presente trabajo investigativo lo dedicamos principalmente a Dios, por ser el inspirador y darnos fuerza para continuar en este proceso de obtener uno de los anhelos más deseados a lo largo de toda nuestra carrera universitaria y a lo largo de nuestras vidas. A todas las personas especiales que nos acompañaron en esta etapa, aportando a nuestra formación tanto profesional y como ser humano.

Por: Yenifer Yirleza Bechara Palacios

Como primero le dedico a Dios que es quien hizo esto posible, a mis padres Jenny Ledezma Armijo que es a la que todo se le debo y Jesús Ramiro Ledezma Chavera (Q.E.P.D.) que desde cielo siempre ha estado acompañándome en mis proyectos.

A mis Hijos Eyner, Emanuel y Edward que son los que me motivan siempre hacer cosas que les sirvan de ejemplo, a mi esposa Sayr Vanessa Ruiz, que ha estado estos últimos 16 años en mis luchas, y a todos los familiares, compañeros y profesores que hicieron esto posible.

Por: Edwar Estivin Ledezma Ledezma

AGRADECIMIENTOS

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presente.

De igual manera mis agradecimientos a la Universidad Cooperativa de Colombia, a toda la Facultad de Derecho, a mis profesores en especial a la Dra. Freya Mery Mosquera, Dr. Marcos Tobías Cuesta y Dr. Robert Asprilla quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada uno de ustedes por su paciencia, dedicación, apoyo incondicional y amistad. Finalmente quiero expresar mi más grande y sincero agradecimiento al Dr. Yousser Ortiz Cuesta, principal colaborador durante todo este proceso, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de este trabajo.

Por: Alan Yecid Mosquera Palacios.

Quiero expresar un sincero agradecimiento, en primer lugar a Dios por brindarnos salud, fortaleza y capacidad; también hago extenso este reconocimiento a todo el personal académico y administrativo de la universidad cooperativa de Colombia sede Quibdó quienes nos han dado las pautas para nuestra formación profesional; y de manera muy especial a nuestros docentes Yousser Ortiz cuesta y Freya Mery Mosquera como asesores del proyecto de investigación quienes nos ha guiado con su paciencia, y su rectitud que gracias a sus consejos y correcciones hoy puedo culminar este trabajo.

Por: Yenifer Yirleza Bechara Palacios

Agradecer a **Dios** porque es el quien guía los pasos de mi vida, a mi madre **Jenny Ledezma** y mi Padre **Jesús Ramiro** (Q.E.P.D.), A nuestra alma mater la Universidad Cooperativa de Colombia, Al Dr **Freya Mery Mosquera** y a mi apreciado Dr. **Yosser Ortiz Cuesta**, que con sus valiosos aportes sacamos este proyecto adelante, además de todos los docentes que aportaron a un crecimiento intelectual a sí mismo a mis compañeros de estudio que también fueron muy valiosos en todo este proceso.

Por: Edwar Estivin Ledezma Ledezma

Tabla de contenido

ANÁLISIS JURIDICO DEL LA LEY 1273 DEL 2009 Y EL SURGIMIENTO Y EXPANSIÓN DEL DELITO DE HURTO Y SEMEJANTES POR MEDIOS INFORMÁTICOS.

Resumen

En la actualidad el mundo de las tecnologías y comunicaciones ha logrado pasar todas las fronteras, es por ello que el actual interés sobre la tecnología y los constantes cambios y avances en materia tecnológica y en especial su relación con las personas nos lleva como estudiantes y futuros profesionales del Derecho a ampliar nuestro conocimiento y su relación con el mismo. Por ello la importancia del tema del derecho informático especialmente el delito es importante pues en muchos países incluido Colombia, tipos de delitos informáticos conocidos incluyen ataques contra sistemas y datos informáticos, usurpación de la identidad, distribución de imágenes de agresiones sexuales contra menores, estafas, subastas realizadas a través de Internet, intrusión en servicios financieros en línea, difusión de virus, botnets (redes de ordenadores infectados controlados por usuarios remotos) y distintos daños por correo electrónico, como el phishing (adquisición fraudulenta de información personal confidencial) para acceder a la información de los servidores sin control., entre otros, los cuales pretenden causar daño a la información como activo vital para las empresas al igual que pérdidas financieras invaluables.

En este trabajo de grado se trata de describir los avances jurídicos en materia de delitos informáticos y su regulación en Colombia, especialmente lo referente a la ley 1273 de 2009 en los artículos 269I y 269J sobre el hurto por estos medios, que reformaron el código penal colombiano (Ley 599 de 2000).

Palabras Claves: Hurto, delitos informáticos, tecnología, derecho penal, código penal colombiano.

Abstrac

At present, the world of technologies and communications has managed to cross all borders, which is why the current interest in technology and the constant changes and advances in technology and especially its relationship with people leads us as students and futures Legal professionals to expand our knowledge and its relationship with it. Therefore, the importance of the issue of computer law, especially crime, is important because in many countries including Colombia, types of known computer crimes include attacks on computer systems and data, identity theft, distribution of images of sexual assaults against minors, scams, auctions made through the Internet, intrusion into online financial services, virus dissemination, botnets (networks of infected computers controlled by remote users) and various damages by email, such as phishing (fraudulent acquisition of confidential personal information) to access the information of the servers without control., among others, which are intended to cause damage to the information as a vital asset for companies as well as invaluable financial losses.

This grade work is about describing the legal advances in computer crime and its regulation in Colombia, especially regarding law 1273 of 2009 in articles 269I and 269J on theft by these means, which reformed the penal code Colombian (Law 599 of 2000).

Key words: Theft, computer crimes, technology, criminal law, Colombian criminal code.

INTRODUCCION

En seis décadas se ha desarrollado el sistema informático que se han convertido en uso de la vida de los individuos. Este proceso de evolución se ha ido perfeccionando pues cada día hay avances en materia informática de indiscutible utilidad que agilizan no solo la sociedad, la economía y la industria en la actualidad.

Hay que empezar con establecer el concepto de informática, se tomará la definición del término contenida en el Diccionario de la Real Academia, que a la letra dice: "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores o computadores".

Con el internet es cada día mayor la frecuencia y mayor impacto en los dispositivos de acumulación y procesamiento de información –llámense servidores, estaciones de trabajo o simplemente PC– son transgredidos en sus elementos más sensibles, dejando en riesgo los múltiples, significativos datos de distinto valor personal, financiero, crediticio, trascendental en empresas y en productos entre otros temas, lo que deja vulnerable el patrimonio real de personas y organizaciones y/u empresas pero lo más importante en muchos casos es la dignidad, la honra y su vida de las personas individuales.

La constitución política de Colombia en su artículo 15 establece “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución”.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley”.

Es irrefutable que en Colombia se ha avanzado en el uso de las nuevas Tecnologías digitales de la Información y la Comunicación – NTIC-, ya su acceso es fácil por los avances en la masificación del Internet en los últimos gobiernos, además que con la globalización en todas las áreas de nuestro desarrollo tanto económico y social.

Si miramos más allá la sociedad moderna actualmente depende de sistemas computarizados, que regulan por ejemplo el tráfico terrestre y aéreo, la operatividad de ciertos

servicios públicos domiciliarios, el fluir de las personas en su vida de relación con presunciones de crear ambientes de seguridad personal, y por supuesto, las operaciones bancarias, las comunicaciones personales, el entretenimiento y es una realidad hace más de un cuarto de siglo. (Möhrensch-lager, 1992, pp 99), ya son pocas actividades que se hacen cara a cara y todo se nos pide reglar en formatos que obtenemos vía Internet.

Pues en el mundo actual las tecnologías van avanzando en un abrir y cerrar de ojos, las personas en segundos tienen acceso a información de toda índole por medio de buscadores de internet los cuales con ingresar una palabra se da respuesta a las inquietudes que nacen en la mente humana, es algo natural, pero puede generar algunas irregularidades en esta clase de medios en donde todas las personas sin limitación alguna tienen acceso, quienes no solo utilizan estos servicios de forma correcta sino que se encaminan a lo ilegal y dañar a las personas.

Hay que indicar que el carácter social del Estado social de Derecho en Colombia profiere un trabajo eficiente de las autoridades y una responsabilidad inmutable en la promoción y difusión de la justicia social. Es por lo tanto que el Estado Social de Derecho deja de ser una abstracción para la nación y se plasma en la prevalencia y cumplimiento inmediato de los derechos fundamentales en este trabajo hablamos de las Entidades Estatales del poder Judicial. Es así como la justicia social hace referencia a la salvaguardia de los principios de solidaridad y dignidad humana. (Corte Constitucional, Sentencia T-505 de 1992).

El Estado Social de Derecho es el pilar de los Derechos Fundamentales; bienes jurídicos a proteger. Estos representan un orden de valores justos, principios que se materializan en los derechos fundamentales; la Corte Constitucional colombiana en su sentencia T-227 de 2003 expresó: "los derechos fundamentales son aquellos que (i) se relacionan funcionalmente con la realización de la dignidad humana, (ii) pueden traducirse o concentrarse en derechos subjetivos y (iii) encuentran consensos dogmáticos, jurisprudenciales o de derecho internacional, legal y reglamentario sobre su fundamentalidad"

El Estado Social de Derecho arroga los principios determinados dentro del ordenamiento jurídico colombiano y al igual debe avalar su goce a los ciudadanos, pero hay que precisar que por más que el Estado colombiano quiera responder al cumplimiento de dichos mandatos, existen fenómenos sociales que están fuera de lo que teóricamente cobija; estos sucesos apreciables afectan a la comunidad. Precisamente es consecuencia de los cambios, de la forma de ver y pensar de la actual sociedad, la cual se va transfigurando con el avance tecnológico y las facilidades para comunicarse.

Precisamente dentro de las finalidades se encuentra la de respetar y velar por los derechos ciudadanos por eso el Estado debe realizar el mayor esfuerzo para garantizar los mismos frente a las nuevas tecnologías. Por lo tanto, es la creación de espacios jurídicos transnacionales que, en primicia es garantizar y herramientas jurídicas que hacen más fácil la asechanza de nuevas conductas delictuales, que se muestran en el siglo XXI.

Debido a la situación que se presenta con este tipo de delitos se crea el “Convenio de Ciberdelincuencia” del Consejo de Europa que se firma en noviembre de 2001 en Budapest y trae una clasificación de los delitos informáticos, organizados en los siguientes grupos:

Un primer grupo aquellos que hacen referencia a los Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos
- Interceptación ilícita de datos informáticos
- Interferencia en el funcionamiento de un sistema informático
- Abuso de dispositivos que faciliten la comisión de delitos
- Algunos ejemplos de este grupo son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

Un segundo grupo se encuentra en los delitos como son:

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

En el tercer grupo nos encontramos con aquellos delitos cuyo contenido es el punto importante y se pueden clasificar de la siguiente manera:

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
- Delitos relacionados con infracciones de la propiedad intelectual y derecho afines (Consejo de Europa, 2008)

Precisamente el Consejo de Europa en el 2008 adiciona otros delitos tratando de criminalizar los actos de racismos y xenofobia cometido por medios informáticos y por ello expide el "Protocolo Adicional al Convenio de Ciberdelincuencia", las medidas que toma son:

- Difusión de material xenófobo o racista
- Insultos o amenazas con motivación racista o xenófoba
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Por lo tanto, estos cambios en la información y de la informática, como se ha analizado anteriormente, justifica que el derecho penal se ocupe de ciertas conductas que se observan lesivas de intereses que, infaliblemente, acceden y viabilizan las posibilidades de participación de las personas en su vida de relación. Este advenimiento de la llamada sociedad de riesgo ha

deslucido consigo el derecho penal por la cantidad de delitos que se han generado, al punto que este tema se ha convertido en algo paradigmático el delito imprudente.

El Derecho como una ciencia que estudia los cambios sociales y en especial los que afectan el orden y la justicia, debe manejar los distintos conceptos, técnicas y especialidades, que se den desde la esfera sociológica, puesto que la tecnología más allá de fierros "equipos", programas, o tecnologías, residen mandados por una nueva conducta y nuevas necesidades, donde asimismo surge un nuevo significado del capitalismo y de los negocios, a los cuales el desarrollo de las redes de datos, ha inventado nuevas técnicas conexas con el ataque informático, y al traer un ejemplo de la consecuencia generada por este hecho, en España, el legislador concibiendo este fenómeno de avance acelerado, por lo cual ha verificado transformación respecto a la ley de protección de la información, como un esfuerzo para no ceder ante las nuevas tecnologías. (De la mata, 2010).

Precisamente los hallazgos del Tanque de Análisis y creatividad de las TIC (TicTac), la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional ha establecido que los incidentes cibernéticos en el país tuvieron un incremento del 54 % con respecto al 2018, según registros de las autoridades. Además, de los 28.827 casos reportados, 15.948 fueron denunciados como infracciones a la ley 1273 de 2009, que tipifica los delitos informáticos en Colombia. Solo este año se han realizado 274 capturas por la infracción de esta normativa. El informe también encontró que de 2017 a hoy se reportaron 52.901 denuncias, de las cuales lideran los hurtos que se realizan a través de medios informáticos (31.058), seguido por el robo de identidad (8.037),

donde Bogotá fue la ciudad que más incidentes reportó (5.308), luego Cali (1.190) y Medellín (1.186). (Diario El tiempo, 2019).

El principal interés de los Cibercriminales en Colombia se basa en la motivación económica y la posterior monetización de las ganancias generadas en cada Ciberataque.

El delito informático más denunciado en Colombia es el Hurto por medios informáticos con un total de 31.058 casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca.

Es por ello que en Colombia fue creada la ley 1273 de 2009 denominada "De la protección de la información y de los datos" el 5 de enero de 2009 por el congreso de la república, por la cual se modifica el código penal y se crea un nuevo mecanismo legal, cuyo objetivo es sancionar todo comportamiento ilícito frente a la comisión de los delitos informáticos en el país. Este gran progreso asimismo ha comenzado una especie de mal presagio para la pervivencia del hombre, de allí que la preocupación apunte en la dirección de cómo advertir los riesgos y en punto a lo que nos incumbe, la investigación es de qué manera y hasta dónde puede (y acaso debe) el derecho penal participar en esa tarea preventiva.

En la ley 1273 del 2009 tenemos los siguientes artículos:

Artículo 269I. -Hurto por medios informáticos y semejantes-. El que, superando medidas de seguridad informáticas, realice la conducta 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.

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.

Como se puede apreciar la ley 1273 de 2009 es un gran aporte contra los delitos informáticos en Colombia por ello este trabajo de grado intenta describir los comportamientos que se pueden reconocer como delitos informáticos en dichas redes y como se está ajustando la normatividad en nuestro país en este crecimiento constante de las tecnologías de información y comunicación, como lograr prevenir, proteger y establecer un adecuado manejo. Pues es claro el debido al desconocimiento de la legislación por los ciudadanos que hacen de los usos informáticos y que depositan su confianza en el uso de internet, pero adicionalmente la falta de compromiso de la rama judicial en este tema.

CAPITULO I - ANTECEDENTES HISTÓRICOS, NORMATIVOS Y JURISPRUDENCIAL DE LA LEY 1273 DEL 2009

Actualmente los medios de comunicación esgrimidos entre las personas se han transfigurado con el universo de las redes sociales, dado que este sistema propició la metamorfosis de relaciones interpersonales y grupales pues la manifestación de ideas, de los pensamientos, de las opiniones y demás expresiones pasaron a un plano digitalizado y no personal. En este mundo cibernético la intimidad se convierte en dominio popular; esto dispone una cadena de efectos secundarios generados en muchas ocasiones por la extralimitación de la libertad de expresión que dichos espacios dejan a disposición de la opinión de todo aquel que se encuentra vinculado a ella.

La problemática de esta situación surge cuando de la mano de las redes sociales surge una problemática más compleja como son los ciberdelitos, cuando se roba además de la información personal con fines extorsivos, se utiliza los datos financieros, sociales y demás que cada día cambian y que muchas veces no cobija en el actual ordenamiento jurídico, y por este motivo, se encuentra en total indefensión ante cualquier controversia que se presente por el uso de estas nuevas tecnologías.

Para tener un bosquejo general del tema se presenta una investigación histórica sobre la normatividad y la jurisprudencia especialmente referente a la ley 1273 de 2009.

1. INSTRUMENTOS INTERNACIONALES

1.1. CONVENIO DE BUDAPEST 2011

Es tan grave los delitos por medios informáticos para la sociedad que la comunidad internacional determino con base en esa preocupación el Convenio de Budapest de 2001 o convenio sobre la Ciberciminalidad, que entro en vigencia en el año 2004 en los estados parte Albania, Croacia, Estonia, Hungría, Lituania, Rumania, para posteriormente adherirse Alemania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Bulgaria, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Finlandia, Francia, Islandia, Italia, Letonia, Macedonia-Antigua República de Yugoslavia, Noruega, Países Bajos, Portugal, República de Moldavia, Serbia y Ucrania. Este instrumento internacional nació en el seno del Consejo de Europa siendo el primero en tratar de combatir la cibercriminalidad, pues se estableció como un deber de los estados firmantes antes anotados.

1.2. DECISION MARCO 222 DEL 2005

El 23 de febrero el Consejo de Europa suscribió la Decisión Marco sobre los ataques a los sistemas de información, que consagra en su artículo 2:

1. Cada Estado Miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

2. Cada Estado Miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad. (Consejo de Europa, 2005, p. 3)

Este convenio establece unas directrices a los Estados, en su Capítulo I – Terminología Articulo 1 Definiciones generales, las cuales se consagran en los siguientes términos:

A los efectos del presente Convenio:

> Por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. Por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función (…). (Consejo de Europa, 2001, p. 4)

Las anteriores nociones hacen parte entonces, de la tipificación del delito de acceso abusivo a sistemas informáticos consagrada en el capítulo II –Medidas que deberán adoptarse a nivel nacional- Sección 1- Derecho Penal sustantivo- Título I – Delitos contra la Confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos, en su artículo 2 denominado "acceso ilícito" que establece:

> Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las partes podrán exigir que el delito se cometa infringiendo

> medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con sistema informático conectado a otro sistema informático. (Consejo de Europa, 2001, p. 4).

Ahora ellos dejan a libertad de los Estados definir en sus ordenamientos jurídicos si estos elementos de circunstanciales son necesarios para configurar el tipo de delito.

1.3. ANTECEDENTES NORMATIVOS LEY 1273 DEL 2009

Colombia no es uno de los países desarrollado es un país en desarrollo que no tiene la tecnología y la industrialización de muchos otros países, pero le ha tocado evolucionar en términos jurídicos en materia tecnológica debido a los nuevos desarrollos tecnológicos que avanzan cada día.

Por ello el estado en su afán de ajustar la normatividad a los nuevos cambios y practicas llevo a que en la ley 599 se estableciera la primera sanción para quienes ataquen los medios informáticos; así en el libro II, del título III Delitos contra la Libertad individual y otras Garantías, Capítulo VII De la violación a la intimidad, reserva e interceptación de telecomunicaciones, artículo 195, se tipifica el delito de "Acceso Abusivo a un Sistema Informático": "Artículo 195. Acceso Abusivo a un Sistema Informático. El que abusivamente se introduzca a un sistema informático, protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene Derecho a excluirlo, incurrirá e multa" (Congreso de Colombia, Ley 599 de 2000, p. 181) (Código Penal Colombiano, derogado por el art. 4. de la Ley 1273 de 2009).

Este artículo no duro sino 9 años, su utilización fue nula, pues la trascendencia de la conducta incluyendo el legislador no daba para la privación de la libertad, en si a la hora de proteger el sistema informático, solo se pensó en una simple multa en primer lugar, pues no había el interés real sobre el riesgo que merecía, ni sobre el impacto que generaría posteriormente la comisión de esta conducta. Además del desinterés de la justicia, pues no se generaron actividades investigativas y sanciones efectivas convirtiendo la norma en obsoleta por desuso.

1.3.1. Proyecto de ley

Debido a la creciente criminalidad en materia informática y a la necesidad de que Colombia alcanzara un nivel normativo similar al de otros países que, de tiempo atrás, venían sancionando infracciones relacionadas con el abuso de los sistemas informáticos y los datos personales —Convenio sobre la ciberdelincuencia de Budapest (2001), adoptado por el Consejo de Europa—, en el Congreso de la República surgió una primera iniciativa —Proyecto de Ley 42 de 2007 Cámara (26)(sic) (27) — destinada a modificar y adicionar algunos tipos penales regulados en el capítulo VII del Código Penal relativos a la "Violación a la intimidad, reserva e interceptación de comunicaciones" (28) y a endurecer las penas del hurto calificado, el daño en bien ajeno, la violación de reserva industrial o comercial y el espionaje, cuando quiera que se ejecuten utilizando medios informáticos o se vulneren las seguridades informáticas de las víctimas.

La exposición de motivos fue expresa en señalar que, de los tres modelos legislativos posibles, a saber, i) ley especial —no integrada al Código Penal—, ii) capítulo especial —incorporado al estatuto sustantivo— y iii) modificación de los tipos penales existentes, se optó por el tercero a fin de garantizar la protección de otros bienes jurídicos distintos al de la información que también podían resultar lesionados con actividades relacionadas con la cibercriminalidad.

Así lo concibió el legislador:

> Cuando se ha optado por una legislación o un capítulo especial que compendie los llamados delitos informáticos se ha partido de la base de la elevación a bien jurídico tutelado el derecho a la información, referida al dato informático (información almacenada, procesada y transmitida a través de sistemas informáticos), o si se quiere, el bien jurídico a salvaguardar es la seguridad informática, teniendo en cuenta que a través de su ataque se pueden vulnerar otros bienes como la intimidad, la propiedad, la libre competencia y hasta la misma seguridad del Estado. Es por eso que algunos doctrinantes catalogan a ese derecho a la información o a la seguridad informática como bien jurídico intermedio que se hace digno de tutela penal, por su propio valor y por el peligro potencial que encierra su quebrantamiento para los demás bienes jurídicos.
>
> Desde ese punto de vista han denominado al delito informático como una acción delictiva en la cual la computadora o los sistemas de procesamiento de datos han estado involucrados como material o como objeto de la misma; y se ha desarrollado el tema alrededor de la triple dimensión de los datos informáticos: confidencialidad, integridad y disponibilidad. Su respeto trae consigo un sentimiento de seguridad y tranquilidad a todos los asociados. De ahí que su transgresión deviene de la afectación de un derecho colectivo o supraindividual que por lo mismo debe ser digno de protección. Por eso es un bien intermedio para la afectación de derechos individuales.
>
> (…). Nuestra reciente tradición jurídica viene decantándose por la otra modalidad de legislación para este tipo de comportamientos consistente en la modificación de los tipos existentes para adecuarlos a la realidad, manteniendo tales conductas dentro de los capítulos correspondientes sin alterar los bienes jurídicos protegidos, y en esa dirección apunta el presente proyecto pues, como veremos, en gran parte de la iniciativa lo que se busca es agravar conductas actualmente tipificadas, o ampliarles el verbo rector, y solo en algunos casos se pretende tipificar comportamientos no contemplados en la ley penal.
>
> La principal razón para optar por este camino es que son varias las conductas que si bien utilizan medios informáticos para la comisión de los delitos, bien puede asegurarse que no corresponderían a lo que se ha denominado delitos informáticos, sino que son delitos tradicionales remozados con nuevas formas de comisión, pero que ameritan un pronunciamiento expreso de la ley penal para aumentar su castigo dado la alarma social

> que genera la ruptura de la confianza que se deposita en una actividad cotidiana y necesaria de la vida moderna en la que el derecho a la información ha cobrado vida propia (29) (resaltados no originales).

Posteriormente, surgió una segunda iniciativa legislativa —Proyecto de Ley 123 de 2007 Cámara (30) —, con fundamento en un proyecto elaborado por un juez de la República Alexander Díaz García y la asesoría de su equipo de trabajo, integrado por los doctores Fernando Velásquez Velásquez, Jarvey Rincón y Gabriel Roldán Restrepo a través de la investigación realizada presentaron el proyecto de ley acerca de los delitos informáticos (Congreso de Colombia, Ley 1273 de 2009).

El proyecto intentaba transformar el Código Penal para adicionar el "título VII BIS" el cual asimismo erigir el bien jurídico "de la protección de la información" con el propósito de que fuera tutelado por el derecho penal, también normaliza todas las conductas que tienen como fin la afectación de la información (Díaz, 2010).

La idea inicialmente era la creación de nuevos tipos penales que alcanzaran contextos de "nuevos riesgos" que no tuvo acogida para quienes poseían en sus manos la contingencia de iniciar el proyecto, por dos razones principalmente: 1) que no se consideraba necesario la modificación del código penal para integrar nuevas tipificaciones que incluyeran dichos riesgos (excluyendo de plano todos los adelantos originarios de la convención de Budapest); y 2) Que era una modificación procedimental no tanto sustancial, era una discernimiento errado del

proyecto pues con la creación de nuevos tipos penales se hablaba de derecho penal de fondo y no de forma (Díaz, 2010).

Es así que, luego de la audiencia pública, en la que se enfatizó sobre la necesidad de proteger el patrimonio y los sistemas informáticos, se acumularon las dos propuestas legislativas en el Proyecto de Ley 42 Cámara, 123 Cámara y Senado, dando lugar a la proposición de crear un título VII bis al Código Penal, destinado, esencialmente, a la salvaguarda de la información y los datos, tomando como base, para el efecto, las conductas reguladas en el Convenio sobre la Ciberdelincuencia de Budapest y algunas que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, las cuales fueron ubicadas en el capítulo I y un segundo grupo de punibles definidos bajo el rótulo de "otras infracciones", concretamente, el hurto por medios informáticos y semejantes, la transferencia no consentida de activos, la falsedad informática, el espionaje informático, la violación de reserva industrial o comercial valiéndose de medios informáticos (cap. II). Separaron, pues, en dos conjuntos de normas, los atentados contra la confianza en el tráfico informático y los también lesivos de este bien y otros intereses jurídicos.

En esta oportunidad, explican los informes de ponencia para primer y segundo debate en Cámara que, se escogió el sistema legislativo consistente en confeccionar un título adicional para ser incluido en el texto del estatuto punitivo porque si bien, era más técnica la expedición de una ley especial, ella podría perderse "dentro de todo el entramado del ordenamiento jurídico, sin merecer la atención requerida por parte de estudiosos y administradores de justicia, quienes,

pretextando dificultades técnicas, falta de preparación, etc., prefieren dejar en el olvido este tipo de normatividades que terminan por no ser aplicadas o, si lo son, de una manera deficiente" y, asimismo, el modelo adoptado en el proyecto original —042— debido a que contraía "la dificultad de permitir la dispersión de esta problemática a lo largo del articulado lo que le quita fuerza y coherencia a la materia, (…) amén de que (sic) dificulta en extremo la precisión del bien jurídico que se debe proteger en estos casos, esto es, la protección de la información y de los datos" .

Una afirmación como la recién transcrita podría sugerir un único valor jurídico a ser protegido: la información y los datos, pero son las mismas ponencias las que precisan frente a los punibles de hurto por medios informáticos y semejantes y transferencia no consentida de activos, que el primero procura "completar las descripciones típicas contenidas en los artículos 239 y siguientes del Código Penal, a las cuales se remite expresamente" y el segundo busca variar la estafa clásica por la figura de la estafa electrónica.

Repárese, en este punto, que, en relación con los otros delitos ubicados inicialmente en el capítulo II, los ponentes admitieron que además del interés por proteger la información y los datos también, pretendían salvaguardar bienes como la información privilegiada industrial, comercial, política o militar relacionada con la seguridad del Estado, en el caso del espionaje informático, y el orden económico y social, en tratándose de la violación de reserva industrial o comercial.

Después de toda esta oposición al fin el proyecto logró ser gestionado por la Cámara de Representantes asumiendo como ponente al Dr. Carlos Arturo Piedrahita Cárdenas de la Comisión Primera de dicha célula legislativa. Tras superar todos los debates, incluso mediante la definición del articulado por una Comisión de Conciliación, finalmente se logró su sanción presidencial el 5 de enero de 2009 para derivar en la expedición de la denominada Ley de delitos informáticos 1273 de 2009 (Díaz, 2010).

El proyecto, así concebido fue aprobado en Cámara, pero en Senado su trámite sufrió algunas dificultades, al punto que la ponencia para primer debate en esa sede fue negativa y reclamó su archivo definitivo por considerarla innecesaria, de cara a la regulación penal existente para la fecha.

El ponente, luego de referirse a la tendencia colombiana a la hiperproducción de leyes y al casuismo; al derecho penal como ultima ratio y a la consecuente imposibilidad de dispensar una pronta y cumplida justicia; y a la importancia de acudir a los conceptos de "esencias y fenómenos" para distinguir entre el tipo penal con sus denominadores comunes o genéricos y sus modalidades, concluyó que no se deben "crear tipos con "nuevas" denominaciones o descripciones" pues "preexisten tipos que genéricamente recogen la esencia del comportamiento a reprimir".

Particularmente, en cuanto se refiere al injusto de hurto por medios informáticos y semejantes, descrito en el artículo 269I, la ponencia señaló que se asimila al reato de hurto

agravado y agregó que "[s]i se observan los actuales artículos 239 y 240 de la (sic) C.P., dicha relación se establece sin ninguna modificación, pues el numeral cuarto del artículo 240 agrava el hurto con ganzúa, llave falsa superando seguridades electrónicas u otras semejantes. En consecuencia, no es correcto recalcar la relación ya existente".

Sometido este informe a la aprobación de la Comisión Primera del Senado, se llegó al acuerdo de no archivar el proyecto, siempre que se hicieran algunos ajustes a los tipos penales, teniendo en cuenta, la creciente necesidad de regular las defraudaciones patrimoniales a los ahorradores de los sistemas financieros, "a quienes les copian por medios electrónicos —por ejemplo, las bandas magnéticas de las tarjetas de crédito a quienes les ingresan a las cuentas corrientes— y con claves descifradas transfieren fondos de una cuenta a otra y eso no es nuevo" .

El proyecto, con sus modificaciones —las que, en esencia, consistieron en eliminar del articulado los reatos de falsedad informática, espionaje informático y violación de reserva industrial o comercial — fue aprobado por la plenaria del Senado, por lo que se designó una comisión de conciliación que, finalmente, conservó como únicos delitos del capítulo II, los de hurto por medios informáticos y semejantes y transferencia no consentida de activos.

En este punto, es bueno precisar que ante las preocupaciones del senador Germán Navas Talero por la confusión que podría suscitarse en la definición del bien jurídico protegido en aquellos casos en que además de la información y los datos se atentara contra el patrimonio económico y la solución propuesta de agregar a los tipos básicos la modalidad informática y la

inquietud del también senador Omar de Jesús Flórez Vélez acerca de "[s]i en el proyecto o la norma que se pretende aprobar, quedan debidamente protegidos, tutelados, los derechos de los ciudadanos, usuarios del sistema financiero, personas naturales y/o jurídicas, que sean objeto o víctimas de transacciones financieras, a través de la tecnología, a través de la utilización indebida, por parte de organizaciones criminales en la Internet" (45) , uno de los ponentes —Carlos Arturo Piedrahita Cárdenas— aclaró que aunque el bien jurídico protegido es el de la protección a la información y los datos, la nueva ley de la República procuraba amparar al sistema financiero y a sus usuarios de las defraudaciones patrimoniales.

1.3.2. Exposición de motivos

En este parágrafo anotamos la exposición de motivos de dicha ley que no viene siendo más la razón porque nuestros legisladores impulsaron la creación de la misma por eso se cita en la investigación.

(…) "Precisiones Judiciales:

(…) Se pone en consideración del Honorable Congreso de la República de Colombia, este proyecto de ley sobre los delitos informáticos, que pretende regular y sancionar una serie de conductas, que sorprendentemente, no son tenidas en cuenta por nuestra Legislación Penal.

Se trata de un decálogo de tipos penales, muchos de ellos con nuevos verbos rectores, que sólo se conjugan en las circunstancias informáticas origen del presente estudio.

Antes de entrar a considerar más en detalle los delitos informáticos, se torna obligado exponer el tema sobre la legitimidad del documento electrónico, el dato y, por

consiguiente, la información en Colombia, que es a la postre el bien jurídico tutelado susceptible de ser vulnerado, cualquiera que sea el propósito ilegal pretendido por el sujeto activo de la conducta. Lo anterior, permite establecer claras fronteras entre un verdadero delito informático y un hecho punible que ha usado medios electrónicos para su consumación. La mayoría de los expositores se refieren al tema de los delitos informáticos, sin detenerse a reflexionar que, para poder hablar de un delito informático, son necesarios dos presupuestos básicos: uno, que la conducta constitutiva del mismo esté tipificada por la Ley; y dos, que medie una sentencia condenatoria en la cual el funcionario judicial, haya declarado probada la existencia concreta de una conducta típica, antijurídica y culpable del delito informático, lo que permite colegir sin profundas elucubraciones que la conducta informática socialmente reprochable es atípica en Colombia.

Así las cosas, es necesario precisar y explicar, en qué consiste el bien jurídico tutelado de la información (almacenada, tratada y transmitida a través de sistemas informáticos), en toda su amplitud, titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad e intimidad, sin perjuicio de que, con su vulneración, subsidiariamente y en tratándose de intereses colectivos, afecte otros bienes jurídicos como la propiedad generalmente.

Así mismo, se debe mostrar cómo el decálogo de conductas aquí propuesto, está constituido por tipos autónomos y no subordinados por circunstancias genéricas o específicas de agravación punitiva de otros tipos, como ha sido la costumbre legislativa en el mundo.

Igualmente, se debe tener en cuenta que algunas de las expresiones utilizadas aparecen en idioma inglés, porque muchas de esas conductas están en esa lengua o porque su texto original en ese idioma ha sido modificado caprichosamente por los llamados ―hackers‖, lo que obliga a utilizar locuciones castellanas, que de forma más o menos aproximada, permitan tipificar las susodichas conductas.

(…) Los Bienes Jurídicamente Tutelados

A lo largo de la evolución del Derecho Penal, se han distinguido diversos conceptos de bien-jurídico. En efecto, la noción acuñada por Birnbauma mediados del siglo XIX, se refiere a los bienes que son efectivamente protegidos por el Derecho; esta concepción, sin embargo, es demasiado abstracta y por ello no cumple con la función delimitadora del Ius puniendi, que persigue un derecho penal de inspiración democrática. Según Von Liszt, y bajo una concepción material del bien jurídico, su origen reside en el interés de la vida existente, antes del Derecho y surgido de las relaciones sociales. El interés social no se convierte en bien jurídico hasta que no es protegido por el Derecho. A su turno, el concepto político criminal del bien jurídico trata de distinguir el bien jurídico de los valores morales, o sea, busca plasmar la escisión entre Moral y Derecho, que, si bien a veces pueden coincidir en determinados aspectos, no deben ser confundidas en ningún caso. Esta concepción del bien jurídico es obviamente fruto de un Estado Social y Democrático de Derecho, y dada su vertiente social, requiere una ulterior concreción de la esfera de actuación del Derecho penal a la hora de tutelar intereses difusos. El origen

de la noción de bien jurídico está, por tanto, en la pretensión de elaborar un concepto del delito previo al que forma el legislador, que condicione sus decisiones, de la mano de una concepción liberal del Estado, para la cual éste es un instrumento que el individuo crea para preservar los bienes que la colectividad en su conjunto quiera proteger.

En otras palabras: el bien jurídico es la elevación a la categoría del bien tutelado o protegido por el derecho, mediante una sanción para cualquier conducta que lesione o amenace con lesionar este bien protegido; de ello se infiere que el bien jurídico obtiene este carácter con la vigencia de una norma que lo contenga en su ámbito de protección, más si esta norma no existiera o caduca, éste no deja de existir, pero si de tener el carácter de jurídico. Esta característica proteccionista, que brinda la normatividad para con los bienes jurídicos, se hace notar con mayor incidencia en el ámbito del Derecho penal, ya que en esta rama del orden jurídico más que en ninguna otra la norma se orienta directamente a la supresión de cualquier acto contrario a mantener la protección del bien jurídico. Por ejemplo, el delito de espionaje informático busca sancionar los actos que difunden en forma irregular la información privilegiada industrial o comercial a través de medios electrónicos.

En la actualidad, la conceptualización del bien jurídico no ha variado en su aspecto sustancial de valoración de bien a una categoría superior, la de bien tutelado por la ley, en cuanto a ciertos criterios como el origen o como el área del derecho que deba contenerlos. El Derecho Penal, pues, tiene su razón de ser en un Estado Social, porque es el sistema que garantiza la protección de la sociedad a través de la tutela de sus bienes jurídicos, en su calidad de intereses muy importantes para el sistema social y, por ello, protegibles por el Derecho Penal. Sin embargo, no debe olvidarse que existen bienes jurídicos, que no son amparados por el Derecho Penal, por ser intereses sólo morales, por lo cual, no todos los bienes jurídicos son bienes jurídico-penales.

(…). Los Bienes Jurídicos Penales

Un Estado Social y democrático de Derecho, debe amparar sólo las condiciones de la vida social, en la medida en que éstas, perturben las posibilidades de participación de los individuos en el sistema social. Por tanto, los bienes jurídicos serán jurídico-penales sólo si revisten una importancia fundamental, o sea cuando las condiciones sociales a proteger sirvan de base a la posibilidad de participación de los individuos en la sociedad. En un Estado democrático, cabe destacar la importancia de la participación de los individuos de vivir en sociedad, confiando en el respeto de la propia esfera de libertad individual por parte de los demás. Otra característica esencial de los bienes jurídico-penales, es la necesidad de protección de los mismos, o sea, que a través de otros medios de defensa que requirieran menos intervención y, por tanto, fueran menos lesivos, no se logre amparar satisfactoriamente el bien. El bien jurídico nace, de una necesidad de protección de ciertos y cambiantes bienes inmanentes a las personas como tales, esta protección es catalizada por el legislador al recogerlas en el texto constitucional, de la cual existirían bienes cuya protección será cumplida por otras ramas del derecho, es decir, que no todos los bienes jurídicos contenidos en la Constitución, tienen una protección penal, pues también existen bienes jurídicos de tutela civil, laboral, administrativa etc. Aquellos bienes jurídicos cuya tutela sólo y únicamente puede ser la tutela penal, son los

> denominados bienes jurídicos penales; al determinar cuáles son los bienes jurídicos que merecen tutela penal, siempre se tendrá en cuenta el principio de tener al Derecho penal como última ratio o última opción para la protección de un bien jurídico, ya que, éste afecta otros bienes jurídicos, con el fi n de proteger otros de mayor valor social.
>
> De otro lado, es claro, que no aparece otro factor que se revele como más apto para cumplir con la función limitadora de la acción punitiva, pues —como hemos observado—, sólo se deben proteger los bienes jurídicos de mayor importancia para la convivencia social y cuya protección por otras ramas del derecho, hagan insuficiente la prevención que cualquier transgresión los afecte‖. (Rincón Ríos J., Naranjo Duque V. 2011)
>
> Esta exposición de motivos, considera como un pilar fundamental el haber logrado la antinomia existente entre el principio de intervención mínima y la creciente necesidad de encajar dicha problemática como una conducta nociva y peligrosa dando una acogida a estas nuevas formas delincuenciales y lograrlas encajarlas en el código penal (Ley 599 de 2000).

Es claro que el proyecto de ley en su relativa exposición de motivos, arguyó que dicha necesidad se procedió de los contratiempos que surgieron como resultado del mal uso de las TICs y de sus principales herramientas (como lo son los computadores y el internet), ya que se generaron efectos lesivos tanto a personas naturales como jurídicas.

Necesariamente estos líos el proyecto reflexionó legítima la protección de tales intereses sociales a través de la creación de un nuevo bien jurídico, pues recordó que al ser elevados a "bien tutelado" por el Derecho, su vulneración acarrearía sanciones severas, las cuales ayudarían a disminuir su lesión. En consecuencia, se dijo que se necesitaba de una norma que le otorgara ese carácter jurídico al mero interés social.

Además, se argumentó que, si bien el Derecho protegía infinidad de bienes jurídicos desde cualquiera de sus ramas, es el Derecho penal el que se debía ocupar de los más significativos para la convivencia en sociedad y cuya protección mediante otras herramientas o ramas del Derecho son ineficaces para prevenir su lesión, por esto ameritan una protección desde la última ratio como ocurrió con la información.

Es de concluir que el método que se venía dando por el legislador resultaba escaso para salvaguardarla pues no avalaba su amparo integral y dejaba vacíos que proveían su vulneración.

Entonces que la información es tan importante en este caso, por lo tanto, el bien jurídico tan relevante, su amparo no puede darse de manera indirecta por otros tipos penales, o como agravante, sino que necesita de la creación de tipos penales autónomos, donde el fin principal sea este bien y así su tutela resulte más eficaz.

En palabras de Pardini (2002):

> Retomando la noción del nuevo ámbito en el cual se mueve el hombre, posibilitado aquel por la aparición de Internet, es fácil advertir que esta nueva dimensión trae aparejada una nueva categoría de derechos a proteger. Entendiendo que existen nuevos bienes jurídicos a tutelar, se deduce que estos presentan nueva o especial vulnerabilidad. Así mismo, estos bienes, y los tradicionales, pueden ser objeto de nuevos ataques, en virtud de lo cual aparece una categoría distinta de ejecutores. (p. 64)

De ahí germina la necesidad de tipificar los delitos informáticos, pues su fin supremo es velar por la protección de la información (cuando esta es el fin de una conducta), a diferencia de lo que se denomina por la doctrina como criminalidad informática, donde si bien se utilizan herramientas generadas por las TICs, se usan con la intención de desarrollar otro tipo de conductas que vulneran bienes jurídicos distintos a la información, como podría ser la afectación del patrimonio a través "de estafas o extorsiones comunes, realizadas utilizando la internet" (Posada, 2013a, p. 6).

Se concluye entonces que no cabe duda de que existe la necesidad de tipificar penalmente el acceso ilegítimo a sistemas informáticos, pues en el intento de aplicar disposiciones similares mediante el uso de la analogía se presentó un grave problema, pues, "en todos los países resultaba muy difícil aplicar los tradicionales tipos penales al acceso no autorizado de

información", lo cual, como ya se dijo, genera impunidad de la conducta antijurídica. (Castro, 2008, p.630)

Finalmente, como ya se mencionó, con este proyecto de ley se crearon nuevos tipos penales que consisten en las conductas que constituyen delitos informáticos, "con ello el legislador penal colombiano confirmó su deseo de garantizar la seguridad de las funciones informáticas propiamente dichas, en contra de ataques cibercriminales, como figuras autónomas frente a los tipos penales tradicionales" (Posada, 2013b, p.4) (Subrayado fuera del texto).

CAPITULO II - INCIDENCIA DEL BIEN JURÍDICO EN ESTOS TIPOS PENALES ARTÍCULOS 269I Y 269H

Debemos analizar esta ley partiendo desde el bien jurídico tutelado que es "de la protección de la información y de los datos", elementos entendidos en lo que tiene que ver con sujeto activo, sujeto pasivo, los verbos rectores, comprendidos a lo largo del articulado de la ley objeto de estudio de este trabajo de grado; también el objeto material, las circunstancias de modo, tiempo y lugar, dosificación penal, analizando los tipos de resultado, con sus respectivas circunstancias de agravación punitiva.

La ley 1273 del 2009, tiene como objeto proteger el bien jurídico concerniente a la información y a los datos como anteriormente ya se ha mencionado; y que a lo largo de su articulado se pueden evidenciar los sujetos involucrados en la comisión de un delito, teniendo y determinando al sujeto pasivo y al sujeto activo; en dicha ley como indeterminado singular, es decir; la persona que participo en el hecho objeto de delito; que haciendo un recorrido por cada artículo de la ley 1273 de 2009 se evidencia que es indeterminado como se puede evidenciar en los artículos:

- **Artículo 269A. Complementa el tema relacionado con el -acceso abusivo a un sistema informático-,** que se manifiesta cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer

beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de la información.

- **Artículo 269B**. **Contempla como delito la -obstaculización ilegítima del sistema informático o red de telecomunicación**-, y se origina cuando el hacker informático bloquea en forma ilegal un sistema o impide su ingreso por un tiempo, hasta cuando obtiene un beneficio por lo general económico. Aquí también se enmarca el acceso a cuentas de correo electrónico sin el debido consentimiento de sus propietarios y el manejo o bloqueo de las claves obtenidas de distinta forma.

- **Artículo 269C**. **Plantea la infracción relacionada con la -interceptación ilícita de datos informáticos**-, también considerada en el Artículo 3 del Título 1 de la Convención de Budapest de 2001. Se presenta cuando una persona, valiéndose de los recursos tecnológicos, obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los transporte.

- **Artículo 269D**. **El delito relacionado con los -daños informáticos**-, y se comete cuando una persona que, sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos.

- **Artículo 269E**. **En los recursos de las TIC, contempla el delito vinculado con el -uso de software malicioso**- técnicamente denominado malware, ya generalizado en internet. Se presenta cuando se producen, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que causen daños en los recursos de las TIC.

- **Artículo 269F**. **El delito sobre -violación de datos personales- (hacking)**, y está orientado a proteger los derechos fundamentales de la persona como dignidad humana y libertad ideológica. Se presenta cuando un individuo sin estar facultado, sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en ficheros, archivos, bases de datos o medios similares con el fin de lograr utilidad personal o para otros.

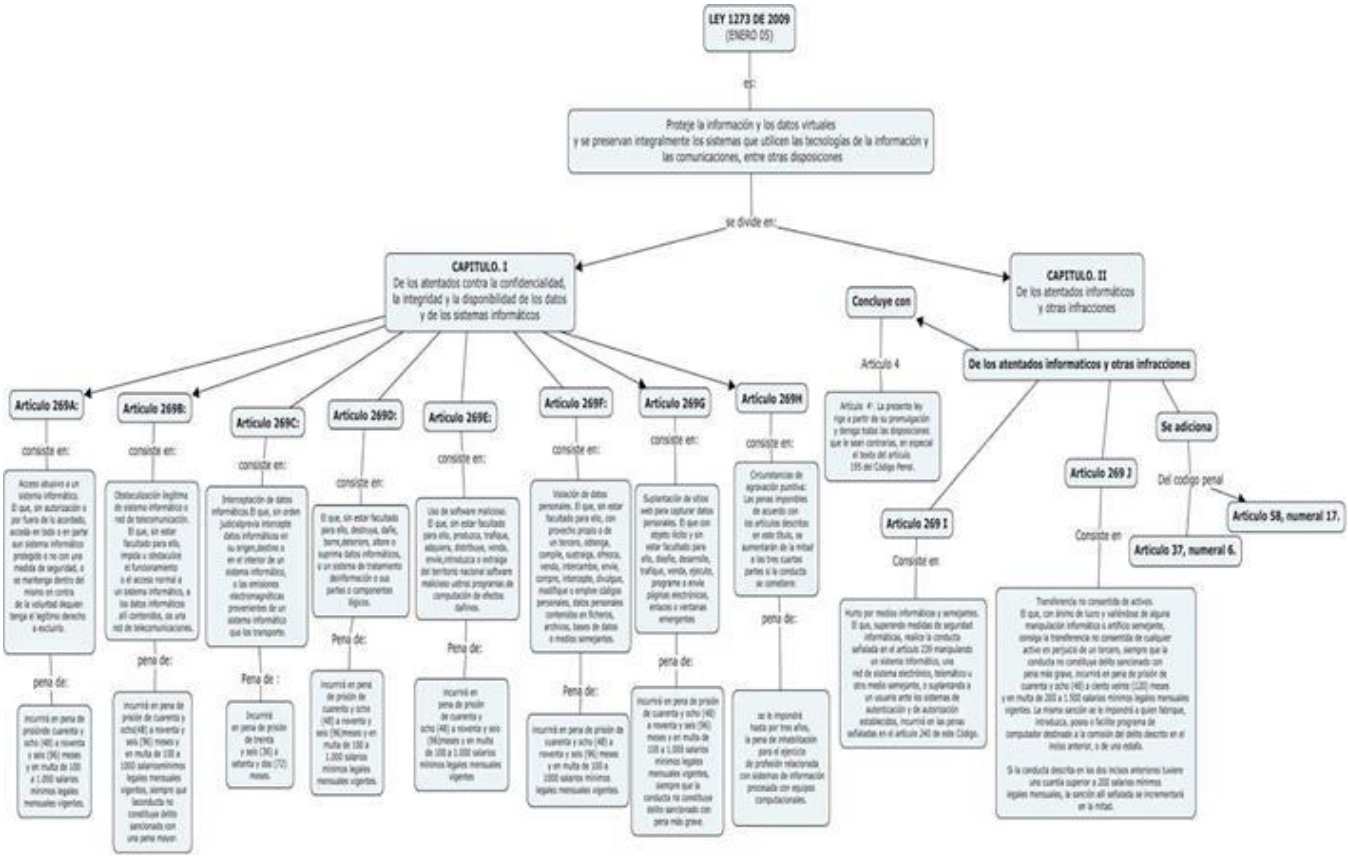
- **Artículo 269G**. **Trata de la -suplantación de sitios web para capturar datos personales**-. Sucede cuando el suplantador (phisher) o delincuente informático crea Hacking es el conjunto de técnicas a través de las cuales se accede a un sistema informático vulnerando Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una página y un dominio similar al de la entidad a la cual desea abordar, lo ubica en un hosting (espacio en un servidor) desde donde envía correos spam9 o engañosos. Al no distinguir la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias que el suplantador almacena en una base de datos y luego ordena la transferencia del dinero de la víctima a cuentas de terceros quienes prestan sus cuentas o servicios (testaferros), que luego reclama o distribuye.

- **Artículo 269H. -Circunstancias de agravación punitiva**-, las penas imponibles de acuerdo con los artículos descritos en esta ley, se aumentarán de la mitad a las tres cuartas partes.

- **Artículo 269I. -Hurto por medios informáticos y semejantes**-. El que, superando medidas de seguridad informáticas, realice la conducta 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.

- **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.



En cada uno de los anteriores artículos mencionados, el legislador inicia con la expresión “el que”, no exige ninguna condición, requisito, o exigencia para determinar al sujeto que cometa la acción.

Sujetos Activos

La definición que el Código Penal trae de autor (art. 29 C. Penal). Es autor quien realiza la conducta punible por sí mismo o utilizando a otro como instrumento. Son coautores los que, mediando acuerdo común, actúan con división del trabajo criminal atendiendo a la importancia del aporte), y que describe en el art. 269I, no exige a quien comete la conducta punible calidad alguna, por lo que autor es "el que" la ejecute, esto es, cualquier persona natural puede cometer la conducta punible. Sin embargo, es necesario indicar que este tipo de delitos rara vez es cometido por un solo individuo, pues casi siempre, la acción es desplegada por varios sujetos que comparten la autoría (coautoría) o participan del hecho punible.

Sujetos Pasivos

El sujeto pasivo de la infracción, no está expresamente determinado en la Ley 1273 de 2009, aunque es posible inferirlo de la conjunción de los tipos base y subordinado, de tal suerte, que lo será el titular del derecho patrimonial birlado o poseedor del dinero sustraído, que, según el caso, podrá serlo el usuario financiero y/o la persona jurídica que lo custodia, dependiendo de cuál sea la barrera informática, telemática o electrónica comprometida para acceder al circulante.

El sujeto pasivo, persona natural o jurídica, son aquellos que padecen el desmedro económico y perjuicio en sus intereses patrimoniales. Sin embargo, el sujeto pasivo de la acción puede ser diferente al perjudicado, pues éste es la persona que fue objeto de un perjuicio directo como consecuencia de la acción penalmente tipificada realizada por el autor, aunque hay oportunidades en que las dos calidades personales coincidan. Esta distinción es importante de

resaltar por dos razones. La primera porque existe la discusión de quién es el sujeto pasivo en este tipo de delitos; es decir, si es el titular de la cuenta bancaria a la que a través de esas maniobras de clonación de su tarjeta y observación de su clave le fue sustraído el dinero, o el banco quien tiene la custodia del dinero que fue sustraído de manera fraudulenta, utilizando una tarjeta clonada y la clave personal del cliente.

Elementos del tipo objetivo y subjetivo

Son elementos del tipo objetivo del hurto cuya modalidad es materia de estudio, los siguientes:

a. El sujeto activo es indeterminado, y es la persona que comete la conducta;

b. El sujeto pasivo lo es el titular de la relación posesoria económica legítima, es decir el poseedor del dinero sustraído;

c. El objeto material lo constituye la cosa mueble: el dinero que se sustrae mediante cualquiera de las modalidades;

d. La conducta en el hurto por medios informáticos y semejantes a través de la utilización de cualquiera de las modalidades previstas consiste en superar las seguridades informáticas mediante la manipulación del sistema informático, la red de sistema electrónico, telemático u otro semejante; y

e. Los elementos normativos de estas modalidades delictivas son los conceptos de mueble y ajena en el tipo básico, y los de seguridades informáticas, sistema informático, red de sistema electrónico y telemático, en el tipo especial, porque se requiere de una especial valoración por parte del intérprete para entender el alcance de estas expresiones.

Los elementos del tipo subjetivo son:

a. El propósito de aprovechamiento, señalado por el tipo básico; y

b. El dolo, que puede ser directo o eventual, dado que el hurto no admite la modalidad culposa.

Como el tema de este trabajo es el hurto por medios informáticos, se centra el análisis en la conducta típica en estas modalidades, tan utilizadas en la actualidad para atentar contra el patrimonio económico ajeno.

La forma especial de hurto analizada ha de llevarse a cabo mediante la realización de dos comportamientos: i) la superación de medidas de seguridad y ii) la manipulación de un sistema informático, una red de sistema electrónico, telemático u otro semejante, o la suplantación de un usuario ante los sistemas de autenticación y de autorización establecidos.

La acción o conducta

El texto del artículo 269I que tipifica el delito de hurto por medios informáticos y semejantes es del siguiente tenor:

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.

El objeto material

La redacción del artículo remite a lo descrita en el canon 239 CP, esto es, se hace referencia a una "cosa mueble", que es aquél bien corporal (como el dinero o incorporal) como la información privilegiada, que va implícita en la acción del apoderamiento descrita en el artículo 269I CP. Ambos bienes muebles (dinero e información), como se sabe tienen valor económico, el primero de ellos, por cuanto es algo tangible y el segundo, dependiendo el tipo de información que haya sido sustraída, así como su utilidad dentro del mercado en el que se ofrece y quién o quienes estén interesados en ella.

Sin embargo, hay que precisar dos momentos relevantes en la ejecución de la conducta para establecer cuándo se produce el apoderamiento del objeto material. El primero se presenta en el momento en que es copiada la información o se desapodera al titular la tarjeta débito o crédito y las claves para ingresar a un sistema a fin de suplantar a un usuario y el segundo, cuando se da el apoderamiento físico de la cosa mueble ajena, que puede ser dinero, retirado previamente de un cajero o transferido a otra cuenta; o en el caso de la información personal o empresarial, al momento de ser recopilada en cualquier medio magnético que sirve para su copiado. En esos instantes señalados es cuando se consuma la conducta punible, pues el tipo de hurto por ser de resultado, exige ese apoderamiento físico del bien, lo que consuma de manera instantánea el ilícito.

Tratamiento penal

El artículo 269I (hurto por medios informáticos y semejantes), de la Ley 1273 de 2009, establece que quien realice un hurto 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 del Código Penal (Ley 599 de 2000).

De acuerdo a lo anterior, se examina lo consagrado en dicho artículo que establece lo siguiente:

Artículo 240. Hurto calificado. La pena será de prisión de seis (6) a catorce (14) años, si el hurto se cometiere:

1. Con violencia sobre las cosas.

2. Colocando a la víctima en condiciones de indefensión o inferioridad o aprovechándose de tales condiciones.

3. Mediante penetración o permanencia arbitraria, engañosa o clandestina en lugar habitado o en sus dependencias inmediatas, aunque allí no se encuentren sus moradores.

4. Con escalonamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes.

La pena será de prisión de ocho (8) a dieciséis (16) años cuando se cometiere con violencia sobre las personas.

Las mismas penas se aplicarán cuando la violencia tenga lugar inmediatamente después del apoderamiento de la cosa y haya sido empleada por el autor o partícipe con el fin de asegurar su producto o la impunidad.

La pena será de siete (7) a quince (15) años de prisión cuando el hurto se cometiere sobre medio motorizado, o sus partes esenciales, o sobre mercancía o combustible que se lleve en ellos. Si la conducta fuere realizada por el encargado de la custodia material de estos bienes, la pena se incrementará de la sexta parte a la mitad.

La pena será de cinco (5) a doce (12) años de prisión cuando el hurto se cometiere sobre elementos destinados a comunicaciones telefónicas, telegráficas, informáticas, telemáticas y satelitales, o a la generación, transmisión o distribución de energía eléctrica y gas domiciliario, o a la prestación de los servicios de acueducto y alcantarillado.

Resumen de los Tipos Penales del trabajo de grado 269I y 269 J

TIPO PENAL: **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.

ELEMENTOS DEL TIPO PENAL

a. SUJETO ACTIVO: Indeterminado singular.

b. SUJETO PASIVO: ―titular del derecho patrimonial.

c. VERBOS RECTORES: Apoderar.

OBJETO JURÍDICO: Derechos patrimonial sobre medios informáticos y semejantes.

e. OBJETO MATERIAL: Cosa mueble ajena.

f. OBJETO REAL: La confidencialidad de la información y los datos.

g. ELEMENTOS NORMATIVOS: desde el punto del sujeto activo realiza la conducta superando medidas de seguridad informáticas.

h. ELEMENTOS SUBJETIVOS: la conducta es realizada con el propósito de obtener un provecho para sí o para otro.

i. CIRCUNSTANCIAS DE MODO: esta conducta tipificada es realizada a través de medios especiales tales como sistemas informáticos u otro medio semejante, además suplantando al usuario.

j. SANCIÓN PENAL: Art 240 texto original Ley 599 de 2000: prisión de 3 a 8 años, Ley 890 de 2004 prisión de 3 a 8 años, Ley 1142 de 2007: prisión de 6 a 14 años.

k. CLASIFICACIÓN DEL TIPO PENAL: este artículo tiene tipos penales de lesión, resultado objetivo, conducta instantánea y mono ofensivo.

EL TIPO PENAL: 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.

ELEMENTOS DEL TIPO PENAL

a. SUJETO ACTIVO: Indeterminado singular

b. SUJETO PASIVO: ―titular de los derechos de autor lesionados.

c. VERBOS RECTORES: Transferir, Fabricar, Introducir, Poseer, Facilitar.

d. OBJETO JURÍDICO: Seguridad informática. Patrimonio económico

e. OBJETO MATERIAL: Cualquier activo

f. OBJETO REAL: la confidencialidad de la información y de los datos.

g. ELEMENTOS SUBJETIVOS: la conducta tipificada con ánimo de lucro y en perjuicio de un tercero.

h. Circunstancias de modo: que la conducta tipificada es realizada a través de manipulación informática o artificio semejante. Además, el tipo penal también será aplicable a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito.

i. SANCIÓN PENAL: ―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‖.

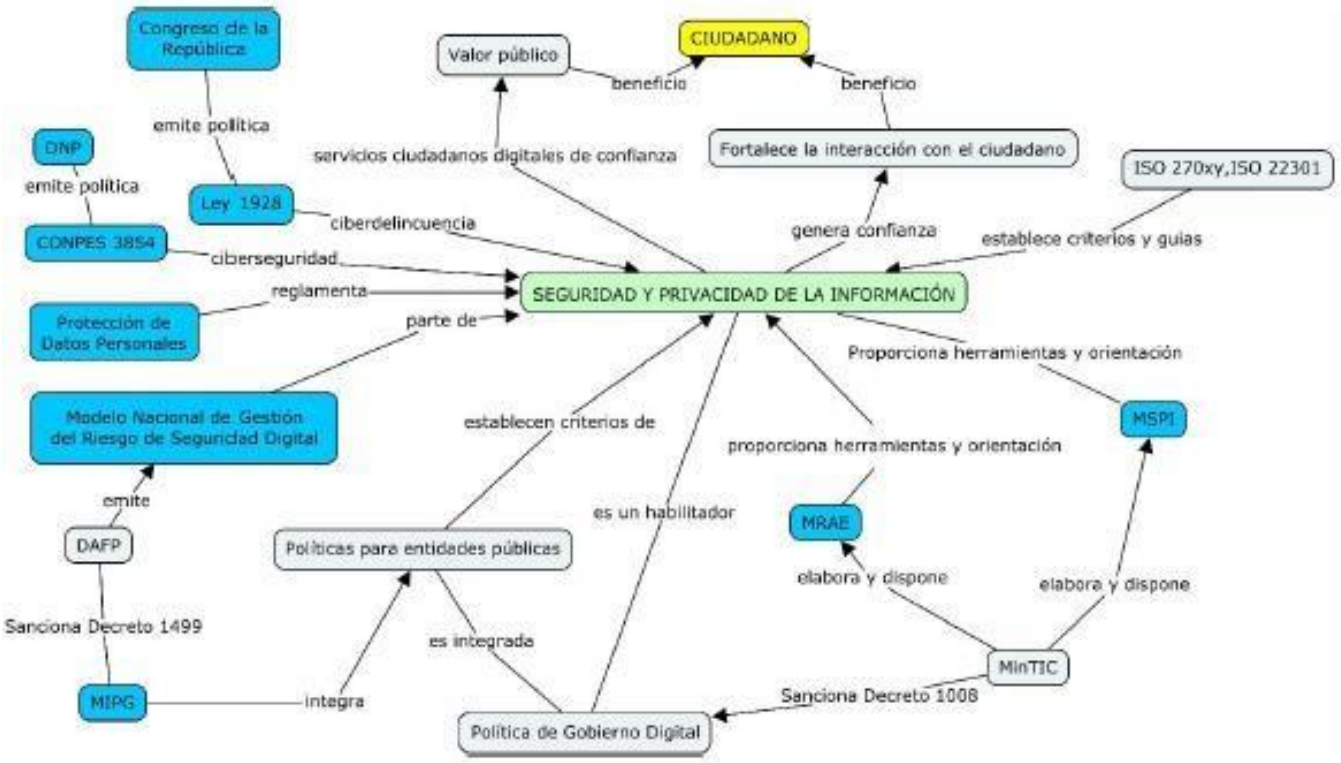
j. CLASIFICACIÓN DEL TIPO PENAL: en el inciso primero tipo penales de lesión, resultado, un solo acto y en el inciso segundo serían los tipos penales de peligro, mea conducta y de varios actos.

La Ley 1273 de 2009, es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea. Precisamente por ello se expide la ley 1928 del 2018 donde se retoma el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest, lo que lleva al Gobierno Nacional a tomar todas las acciones legales necesarias para evitar este tipo de delitos.

El cuadro que se anexa nos muestra la red que se ha establecido en el país en este tema los hallazgos del Tanque de Análisis y creatividad de las TIC (TicTac), la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional ha establecido que los incidentes cibernéticos en el país tuvieron un incremento del 54 % con respecto al 2018, según registros de las autoridades. Además, de los 28.827 casos reportados, 15.948 fueron denunciados como infracciones a la ley 1273 de 2009, que tipifica los delitos informáticos en Colombia. Solo este año se han realizado 274 capturas por la infracción de esta normativa. El informe también encontró que de 2017 a hoy se reportaron 52.901 denuncias, de las cuales lideran los hurtos que se realizan a través de medios informáticos (31.058), seguido por el robo de identidad (8.037), donde Bogotá fue la ciudad que más incidentes reportó (5.308), luego Cali (1.190) y Medellín (1.186). (Diario El tiempo, 2019).

El principal interés de los Cibercriminales en Colombia se basa en la motivación económica y la posterior monetización de las ganancias generadas en cada Ciberataque.

El delito informático más denunciado en Colombia es el Hurto por medios informáticos con un total de 31.058 casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca.



CAPITULO III - CAMBIOS Y PROPUESTAS SOBRE EL DELITO DEL HURTO INFORMATICO

En el año 2017, según cifras de la DIJÍN, no solo acrecentaron este tipo de delitos un 28%, también aparecieron nuevas amenazas para la seguridad cibernética en el país que no solo atacan el bolsillo y la privacidad de los ciudadanos, sino también atenta contra su vida. Las autoridades están buscando la manera de hacerle frente a ese panorama a través, sobre todo, de la articulación de las investigaciones y las operaciones entre la Policía y la Fiscalía. Además, se reportaron 52.901 denuncias de las cuales el mayor número de hurtos se realizan a través de medios informáticos (31.058), seguido por robo de identidad (8.037), donde Bogotá fue la ciudad que más incidentes reportó (5.308), luego Cali (1.190) y Medellín (1.186).

El otro gran objetivo de los cibercriminales son la estafa en el año 2017 fueron 6.372 ciudadanos lograron haber sido estafados por internet, por un valor que sumado supera los 15.000 millones de pesos. La mayoría de víctimas cayeron a través de compras que pagaron y que nunca se materializaron. Alrededor de 2.000 personas denunciaron haber sido asaltadas a través de llamadas telefónicas y mensajes de texto.

En el año de 2019 el 45.5% de las denuncias se hacen por canales virtuales y se reportaron 28.827 incidentes de ciberseguridad empresarial en el país, de los cuales 17.531 casos han sido denunciados ante la fiscalía. Es decir, se ha ejecutado un incremento operativo del 27.5% respecto al año 2018 materializándose 241 capturas y 11 operaciones de impacto por diferentes modalidades de delitos informáticos contempladas en la Ley 1273 del año 2009, al

igual por medio del servicio Cai Virtual 24/7 se han atendido 12.959 incidentes aumentando la capacidad de atención en un 53.7% respecto al 2018."

En el país, los ataques por malware durante lo corrido del año crecieron un 612%, el monto pagado por rescate de información está entre los 32 millones y los 160 millones de pesos. Frente a este escenario, Colombia se encuentra entre los países que recibió el mayor número de ataques por ransomware en Latinoamérica con un total de 252 lo que corresponde al 30% después de Brasil y Argentina.

Ahora estos delitos o comportamientos delictivos son realizados en el ciberespacio por cosas o sistemas dominados por hombres, que cada día son más sofisticados, es decir, ejecutados en una realidad virtual que solo tiene existencia en sistemas y redes de dispositivos informáticos. En sentido material, dichos comportamientos digitales, aunque tienen origen físico en una acción-decisión humana (un Clic que algunos consideran un simple acto preparatorio del delito), producen resultados que no superan el mundo digital, pues se dan mediante el tratamiento, la manipulación y el almacenamiento de datos informáticos basados en el sistema binario que, aunque representan materia y ubicación, realmente son ondas de energía que forman bytes susceptibles de agruparse en archivos y que pueden ser leídos por software y "traducidos" por el sistema en signos comprensibles para los seres humanos. Es allí que se da el problema porque en la mayoría de los casos los resultados del delito no trascienden el mundo físico, aunque pueden impedir a los usuarios la disponibilidad.

Pero hay que tener en cuenta que la acción digital o virtual se explica porque represente la ejecución de instrucciones procesables por los sistemas informáticos. Ahora además la interacción directa o a distancia con el sistema no se da mediante una acción lineal sino claramente interactiva/reactiva que, mediante links asociados a páginas vinculadas a sitios web, accede buscar información (en distintos formatos: video, audio, texto, etcétera) según los intereses del usuario o realizar actividades que se pueden desplegar en distintos espacios de esta realidad, de manera indefinida e incluso automática.

La posibilidad de programar los actos informáticos de ataque permite, inclusive, que los procesos virtuales sean realizados cuando el sujeto activo no se encuentra consciente, esté dormido o imposibilitado para tener una injerencia física o para desarrollar un control real sobre las conductas punibles. Es de concluir entonces que estas acciones han originado nuevas dinámicas criminales que se traducen en la instrumentalización de cadenas de víctimas inconscientes en la realización del delito, mediante el uso de sus sistemas informáticos. Por lo tanto técnicamente hablando estos ataques distribuidos mediante los cuales se utilizan automáticamente redes de computadores infectados (Botnet), sin conocimiento o (con la complicidad) de sus usuarios titulares; lo cual, desde la perspectiva del desvalor de acción objetivo, comporta una forma particular de ejecutar los delitos que facilita su comisión y la producción de sus efectos frente a la comunidad titular de los derechos a la disposición, el acceso y el tratamiento de información confiable e integral.

Por lo tanto, se debe profundizar en el tema debe establecerse políticas y estrategias de seguridad de la información, especialmente para las entidades financieras y las empresas; establecer capacitaciones en el conocimiento y aplicación de normas sobre seguridad y delitos informáticos; además deben establecerse los planes de seguridad y continuidad del negocio; crear gestión de riesgos y vulnerabilidades tanto las empresas como las personas, deben darse procedimientos de seguimiento y control, técnicas y herramientas de auditoría y especialmente hay que invertir en seguridad informática.

Hay que precisar que la normatividad debe estar actualizada por que la conducta humana que es la base de la conducta del cibercrimen cambia constantemente como objeto que se desvalora en las distintas categorías del delito, por lo que sus características deben ser objeto de una precisa caracterización dogmática por parte de la doctrina nacional, que permita combatir y estudiar adecuadamente estas fenomenologías criminales.

4. CONCLUSIONES

Nuestro país ha logrado avances en la materia, el legislador trato con la ley 1273 de 2009 por medio de la cual modifican el código penal colombiano, cuya necesidad era reglamentar todo lo posible sobre los delitos informáticos para salvaguardar el bien jurídico tutelado “de la protección de la información y de los datos”. Está estructurada en dos capítulos, el primero de los cuales tipificó “los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y el segundo “los atentados informáticos y otras infracciones”. En ellos se incorporan, entre otros, los delitos de hurto por medios informáticos y semejantes y la “transferencia no consentida de activos”. En el segundo capítulo encontramos las circunstancias de agravación punitiva, las cuales son aplicables a todos los tipos penales descritos en el Título VII de la Ley 599 de 2000.

En este trabajo se puede concluir que el continuo progreso de las tecnologías de la información, está causando, además de múltiples beneficios para la sociedad, la divulgación de los designados delitos informáticos. La delincuencia informática se afirma en el delito instrumentado por el uso de la tecnología a través de redes telemáticas y la interconexión de los computadores, aunque no son los únicos medios.

Es poco el conocimiento y la cultura informática es un factor crítico en el impacto de los delitos informáticos de la sociedad en general, pues los cambios constantes en este tipo de tecnologías conllevan mayores conocimientos en tecnologías de la información, las cuales asienten tener un marco de referencia admisible para el manejo de dichas situaciones. Además, la

naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que, a nivel general, se poseen pocos conocimientos y experiencias en el manejo de esta área pro parte de los juristas es por ello que los cambios normativos deben ser constante.

Ahora el articulo 269I de la Ley 1273 consagra el delito de hurto por medios informáticos, con el fin de proteger el patrimonio económico de los ciudadanos, instituyendo que quien superando medidas de seguridad informáticas, ejecute la conducta señalada en el artículo 239 (hurto) maniobrando un procedimiento 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.

Hay que precisar que antes de la expedición de la Ley 1273 del 2009, nuestro Código Penal en distintas normas hace referencia a la descripción de conductas punibles ejecutadas utilizando medios informáticos, no explícitamente dentro de un título como tal, sino que estas se hallaban dispersas por varios de ellos; y el procedimiento penal que se concedía al mismo, era el de hurto simple (artículo 239); situación que cambio con la entrada en vigencia de esta nueva ley, pues en ella se consagra el tratamiento penal, como el de un hurto calificado, consagrado en el artículo 240 de la Ley 599 de 2000, y tendrá una pena de prisión de seis (6) a catorce (14) años, si el hurto se cometiere: 1. Con violencia sobre las cosas; 2. Colocando a la víctima en condiciones de indefensión o inferioridad o aprovechándose de tales condiciones; 3. Mediante penetración o permanencia arbitraria, engañosa o clandestina en lugar habitado o en sus dependencias inmediatas, aunque allí no se encuentren sus moradores; 4. Con escalonamiento, o

con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes.

Dentro del análisis se pudo establecer que el Estado colombiano ha realizado las medidas para tratar de disminuir los casos de delitos informáticos una muestra de ello es la ley 1928 del 2018 donde se retoma el "Convenio sobre la Ciberdelincuencia" tratando de aplicar todas las herramientas jurídicas para evitar su avance.

BIBLIOGRAFIA

Acuña Gamba, Eduardo José y Sotelo Vargas, Diego Andrés. (2015). Ley 1273 de 2009: ¿Los Jueces del Cibercrimen? Revista Iter Ad Veritalem. pp. 181-193.

Álvarez Ramos, Benjamín. (2004). Avances en criptología y seguridad de la información. Ediciones Díaz de Santos. España.

Avilés Gómez, Manual de Delitos y Delincuentes. (2010). Editorial Club Universitario.

Álvarez-Marañón, Gonzalo & Pérez-García, Pedro Pablo (2004). Seguridad informática para la empresa y particulares. Madrid: Mc- Graw-Hill.

Barrio Andrés Moisés. (2015). Ciberdelitos Amenazas Criminales del ciberespacio. Editorial Reus

Cárdenas Quintero, Beitmantt Geovanni y Fonseca Ruiz, Hilma Ximena. (2012). Rol del derecho penal y la información forense en la protección de la información en la era digital. Revista Academia y Virtualidad. Universidad Militar Nueva Granada.

Castro – Jaramillo, Ángela María; Guevara – Valencia, Sídney y Jaramillo – Rojas, Carlos Alberto. (2016) Análisis socio jurídico del surgimiento y expansión de las redes sociales en internet y la intimidad en Colombia. Revista Criterio Libre Jurídico.

Camargo Cardona, Leonardo. (2019). Regulación en Colombia de los delitos informáticos. Universidad piloto de Colombia.

Camacho-Losa, Luis (1987). Delito Informático. Madrid: Gráficas Cóndor.

Cedeño Velasco, Eddy Hardany. (sf). El mundo cibernético y los delitos informáticos.

Cristiano Cristiano, Karen Milena y Mayorga Ortiz Mariluz. (2015). Análisis Criminológico del Cibercrimen. Universidad la Gran Colombia.

Choclan-Montalvo, José Antonio (1997). Estafa por computación y criminalidad económica vinculada a la informática. Actualidad Penal. 22-28.

Córdoba, A. (2014). Ciberespacio amenazado. Necesidad de leyes de protección a la privacidad. Bogotá: Universidad de la Salle.

Corte Constitucional. Sentencia C-640 de 18 de agosto de 2010. M. P. Mauricio González Cuervo.

Corte Constitucional. Sentencia SU-157 de 10 de marzo de 1999. M. P. Alejandro Martínez Caballero.

Corte Constitucional. Sentencia T-414 de 16 de junio de 1992. M. P. Ciro Angarita Barón.

Corte Constitucional. Sentencia T-632 de 15 de agosto de 2007. M. P. Humberto Sierra Porto.

Corte Constitucional. Sentencia T-634 de 13 de septiembre de 2013. M. P. María Victoria Calle

Cuervo Álvarez, José. Delitos Informáticos: Protección Penal de la Intimidad. Ávila (1997). Delitos informáticos y entorno jurídico vigente en Colombia. Cuaderno de contabilidad.

Davara-Rodríguez, Miguel Ángel (2007). Código de internet. Madrid: Aranzadi.

Gonzales Guzmán, Diego Alejandro. (2017). 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.

Gómez-Perals, Miguel (1994). Los delitos informáticos en el derecho español. Informática y Derecho: Revista Iberoamericana de Derecho Informático (4), 481-496.

Gómez-Vieites, Álvaro (2006). Enciclopedia de la seguridad informática. Madrid: Alfa omega.

Guevara Medina, Luis Elkin y Arzuaga Herrada Toyber Santiago. (2012) Los delitos del nuevo siglo: los delitos informáticos. Revista Ciencias Humanas. Volumen 9 No. 1.

Fernández de Soto, María Clara. (2001). Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos. Tesis de Grado. Universidad Sergio Arboleda. Escuela de Derecho - Santa Marta.

Montañez Parraga, Andrés Camilo. (2017). Análisis de los delitos informáticos en el actual sistema penal colombiano. Universidad Libre.

Modelos de imputación en el derecho penal informático. Derecho penal y criminología, número 85, paginas 37-54.

Ley 1273 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. 5 de enero de 2009. Diario Oficial, núm. 47223.

Ojeda-Pérez, Jorge Eliecer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-
Martínez, Libardo Alberto, Delitos informáticos y entorno jurídico vigente en Colombia. Cuaderno de contabilidad (2010).

Peña Valencia, Juliana. (sf). Legislación aplicable a las conductas delictivas en Internet. Universidad de San Buenaventura.

Piattini-Velthuis, Mario Gerardo & Peso-Navarro, Emilio del (2001). Auditoría informática. Madrid: Alfaomega.

Posada Maya, Ricardo. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Revista Nuevo Foro Penal Vo. 13. No. 88. pp 72-112.

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

Sánchez Castillo, Zulay Nayiv. (2017). Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. Universidad Nacional Abierta y a distancia. UNAD.

Santos, S. (1998). La Globalización del Derecho. Los nuevos caminos de la regulación y la emancipación. Bogotá: Ilsa. Disponible en: https://es.scribd.com/doc/132426068/Santos-Boaventura-de-Sousa-La-Globalizacion-Del-Derecho.

Santos, S. (2008). Sociología Jurídica Crítica Para un Nuevo Sentido Común en el Derecho. Bogotá: Ilsa. Disponible en: https://es.scribd.com/doc/167600737/Sociologia-juridica-critica-para-un-nuevo-sentido-comun-en-el-derecho-Santos-pdf

Suárez González, Carlos. J. (sf). "Derecho penal y riesgos tecnológicos", en Crítica y justificación del derecho penal en el cambio de siglo

Suarez Sánchez, Alberto. Manual del delito informático en Colombia. Análisis Dogmático de todos los Tipos Penales de los Delitos Informáticos descritos en la Ley 1273 de 2009 (2017). Universidad Externado de Colombia.

Téllez Valdez Julio. Derecho informático (2008). Universidad Nacional Autónoma de México

Torres Stepa Andrea, López Sanabria Indira Fabiola y Sarmiento Avella, María Alejandra. (sf). "IN" Seguridad de la información y delitos informáticos en Colombia

Ramírez Riveros Diego Armando y Castro Serrato Elmer Francisco. (2108) Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia. Universidad Nacional abierta ya distancia “UNAD”

Reyes Cuartas, José Fernando. (sf). El Delito informático en Colombia: Insuficiencias Regulativas.

Riascos Gómez, Libardo Orlando. (2012). Los delitos contra los datos personales y el habeas data en la ley 1273 de 2009. Revista Derecho y realidad. Núm. 20.

Villamizar Cesar, Orjuela Ailin y Adarme Marco. (2015). Análisis forense en un sistema de información en el marco normativo colombiano. Universidad Simón Bolívar. Colombia. pp 36-43