DE LOS DELITOS DESCRITOS EN LOS ARTÍCULOS 269I Y 269J DE LA LEY 599 DEL 2000 Y SU APLICABILIDAD EN EL TERRITORIO COLOMBIANO.

FERNANDO LEÓN RESTREPO SÁNCHEZ
DIANA PATRICIA RÍOS USUGA

DOCTOR, NELSON ANTONIO LOPERA ARANGO
DOCENTE EN EJERCICIO Y MAGISTER EN DERECHO PENAL

Línea de Investigación:
Derecho Penal

Facultad de Derecho
Universidad Autónoma Latinoamericana

Agradecimientos.

En este viaje del conocimiento que emprendemos por casualidades de la vida, nos encontramos seres humanos maravillosos, personas que nos motivan a ser mejores, porque creen en nuestra capacidad, gracias, Diana Patricia Ríos porque juntos lo lograremos, quiero agradecer infinitamente y de manera muy especial a quien me motivo a llevar a cabo esta maravillosa carrera del Derecho, estando siempre dispuesto como docente, como persona y como amigo, en el trasegar de este objetivo. quien es parte fundamental como el asesor de este trabajo de grado. A él toda mi admiración, y respeto.

Muchas gracias por su conocimiento y Disposición, Doctor. NELSON ANTONIO LOPERA ARANGO, Dios los Bendiga.

> *Uno recuerda con aprecio a sus maestros brillantes, pero con gratitud a aquellos que tocaron nuestros sentimientos. (Gustav Jung, 1875-1961).*

RESUMEN

El presente trabajo se desarrolla conforme a los parámetros de una investigación de tipo cualitativo a través del análisis de textos académicos, leyes, periodísticos, artículos prensa, jurisprudencia y doctrina, relacionados con el tema propuesto. Y que, aportan bases teóricas para asumir una postura critico analítica del estado del arte que sobre el tema propuesto se tiene actualmente.

En cuanto a la estructura de la investigación, esta se presenta en tres partes distribuidos de la siguiente manera:

En la primera parte se desarrolla la conceptualización e identificación del tratamiento legal y jurisprudencial aplicable a los delitos en mención.

En la segunda parte, se identifican las distintas modalidades de Hurtos y Transferencia no Consentidas que se han cometido utilizando para ello medios informáticos dentro del territorio nacional.

En la tercera parte, abordaremos las diferentes estrategias dirigidas a minimizar las posibilidades de ser víctimas de estos dos delitos (Hurto por Medios Informáticos y Transferencia no Consentida de Activos) dentro del territorio nacional. Y para finalizar, propondremos unas conclusiones que en el desarrollo del presente trabajo se pudieran obtener.

Palabras clave: Código penal Art. 269I y 269J, hurto, medios electrónicos, suplantación, tecnología

ABSTRACT

The present work is developed according to the parameters of a qualitative research through the analysis of academic texts, laws, journalistic, press articles, jurisprudence and doctrine, related to the proposed topic. And that, they provide theoretical bases to assume a critical analytical position of the state of the art that we currently have on the proposed topic.

Regarding the structure of the research, it is presented in three parts distributed as follows:
In the first part, the conceptualization and identification of the legal and jurisprudential treatment applicable to the crimes in question is developed.

In the second part, the different modalities of Theft and Non-Consensual Transfer that have been committed using computer means within the national territory are identified.

In the third part, we will address the different strategies aimed at minimizing the chances of being victims of these two crimes (Theft by Computer Means and Non-Consensual Transfer of Assets) within the national territory. And finally, we will propose some conclusions that could be obtained in the development of this work.

Keywords: Criminal Code Art. 269I and 269J, theft, electronic media, impersonation, technology

Introducción 1
Capítulo 1 Delitos informáticos 6
1.1 Referente Histórico en Colombia de los Delitos Informáticos 6
1.2 Análisis Normativo 9
1.3 Análisis Jurisprudencial 11
1.4 Análisis Del Tipo Penal De Hurto Por Medios Informáticos 18
1.4.1 ART. 269 I.-Adicionado.L.1273/2009, ART.1. Hurto por Medios Informáticos y Semejantes 18
1.4.2 ART. 269J. Adicionado. l. 1273/2009, ART.1. Transferencia no consentida de activos 29
1.4.3 Bien jurídico protegido en los delitos de Hurto Por Medios Informáticos y Transferencias no consentida de activos……35
1.4.4 Análisis entre el delito de Hurto por Medios Informáticos y Transferencia No Consentida de Activos. Art. 269I y 269J……..……42

Capítulo 2 Descripcion del modus operandi en comision de las conductas que atentan contra el nuevo bien juridico tutelado 45
2.1 Utilización de tarjeta falsa en cajero automático 45
2.2 Obtención de la Tarjeta Digital 45
2.3 Duplicación de Tarjeta 46
2.4 El Phishing. 46
2.5 Software Espía – Spyware. 47
2.6 Ransomware. 48

Capítulo 3. Estrategias orientadas a evitar ser víctima del delito de Hurto A Través De Medios Informáticos Y Transferencia No Consentida De Activos 49
3.1 ¿Qué hacer para evitar que nos clonen nuestras tarjetas sean estas débito y crédito? 50
3.2 ¿Cómo evitar que nos cambien nuestras tarjetas? 51
3.3 ¿Cómo evitar ser víctima del Phishing? 52
3.4 ¿Cómo evitar se víctima del Software espía?. 53
3.5 Enfoque cuantitativo de la comisión de los delitos descritos en los Arts. 269i Y 269j dentro del territorio nacional 53
3.6 Los ataques cibernéticos están en auge, la comisión de este tipo de conducta se incrementó en un 30% durante el primer semestre de este año según la Fiscalía 56
3.7 Los delitos informáticos vistos como otra pandemia más al lado del coronavirus 58

Conclusiones 62
Referencias 64

Introducción.

La evolución informática que se viene dando desde la década del 2000, trajo una serie de utilidades incalculables en las comunicaciones a nivel global pero, así como se evidencian ventajas, también estos avances tecnológicos traen consigo desventajas y esto se debe a que hay personas que se provechan de estas tecnologías ya no para realizar actividades licitas, sino por el contrario para través de ellas ejecutar actos que van en contra de la Ley, siendo los de mayor ocurrencia el hurto por medios informáticos y la Transferencia no consentida de activos descritos en los artículos 269I y 260J de la Ley 599 (2000).

Este accionar delictivo tiene relación directa con las operaciones realizadas por personas que utilizan tarjetas bancarias para hacer sus diferentes transacciones, pero recaen especialmente sobre aquellas que las realizan a través de medios electrónicos como computadoras, tabletas, equipos celulares o cualquier otro dispositivo, ya que son estos los medios más utilizados por la delincuencia para llevar a cabo trasferencias u operaciones bancarias sin la respetiva autorización.

Se pretende con esta investigación analizar cuál ha sido la aplicabilidad en el territorio colombiano del bien jurídico identificado con el Titulo VII bis, especialmente lo relacionado con los tipos penales establecidos en los Arts. 269I y 269J adicionados al Código Penal por la Ley 1273 (2009) en concordancia con los tipos penales 239 y 240 Numeral 4 de esta misma codificación.

Pregunta de Investigación.

Para el estudio del tema propuesto, partiremos del siguiente interrogante ¿a qué se debe el bajo índice de capturas por estos delitos no obstante las múltiples denuncias?, la respuesta a este interrogante podría estar precisamente en que la fiscalía y las autoridades encargadas de combatir este flageló no cuentan con el suficiente número de

investigadores especializados en esta área, las autoridades colombianas todavía no cuenta con la tecnología suficiente para hacer frente a este método, es decir los problemas que se presentan en el sistema penal acusatorio desde el mismo momento en que se creó respecto a la poca efectividad de las investigaciones judiciales adelantadas cuando se comete un acto delictivo se trasladan a estos nuevos dos delitos creados por el legislador, con un agravante, que en estos dos delitos que se traen a colación en esta investigación los descritos en los artículos 269I y 269j, se torna mucho más compleja la investigación por el modus operandi en que se cometen y por los equipos tecnológicos que se utilizan para su consumación que obligan a que en estos casos sean verdaderos peritos en el conocimiento y manejo de los mismos los que dirijan la investigación, los cuales o son escasos o no se cuenta con ellos en nuestro territorio. Esto ha impedido combatir este flageló de manera adecuada y capturar o judicializar a las personas dedicadas a este accionar delictivo.

Colombia debe invertir en equipos idóneos y suficientes para afrontar en debida forma este nuevo accionar delictivo, debe preocuparse en capacitar a la policía judicial que se va a encargar de la investigación de este tipo de delitos, darles los equipos y las herramientas necesarias para hacer frente a estas nuevas formas de delincuencia, crear un verdadero grupo en la fiscalía general de la nación que lidere este tipo de investigaciones, mientras no se tomen este tipo de medidas y no se concientice a la ciudadanía sobre el buen uso y manejo de las nuevas tecnologías y la necesidad de denunciar de manera inmediata este tipo de actos, seguiremos siendo víctimas de los delincuentes informáticos y seguirá en auge la comisión de los delitos de dichos delitos que hacemos referencia y que se quiere visibilizar en esta investigación en todo el territorio nacional.

Es importante señalar que los avances constantes en las tecnologías de la información y de los datos, no se va a detener, por el contrario todos los días surgen nuevos medios y métodos de comunicación, en una carrera desenfrenada, lo que hoy es de avanzada, para mañana se considera obsoleto, todo eso hace que cada día estemos más

expuestos, seamos más vulnerables a esta ejecución delictiva a través de estos medios tecnológicos, por eso es necesario que se tomen medidas urgentes por parte de las autoridades, tendientes a minimizar las consecuencias generadas por este accionar delictivo y evitar con esto que los ciudadanos sean víctimas de estos dos delitos informáticos que se traen a colación y que cuando lo sean, la respuesta por parte del estado sea efectiva, en captura y judicialización.

Justificación.

Se justifica realizar esta investigación, porque con ella se busca analizar cuál ha sido la aplicabilidad que han tenido los artículos 269I y 269J de la Ley 599 (2000), en el territorio nacional.

Es de vital importancia ahondar en este tema, debido a que se ha convertido en un problema actual, que está afectando a la comunidad en general, que impacta a toda la sociedad, sin distinción alguna, sea esta de estrato bajo o alto, sea esta persona natural o jurídica, que debido al mal uso de todas estas tecnologías facilitan a los delincuentes llevar a cabo el tipo de conductas delictivas a las que se refiere este trabajo.

Herramientas tecnológicas como (celulares, computadores, Tablet) se han convertido en verdaderas armas o elementos de mucha utilidad para la delincuencia común u organizada que se mueven en este tipo de delitos, esto hace que sea de vital importancia la identificación de las distintas modalidades de hurtos o transferencias no consentidas cometidas a través de medios tecnológicos con aplicaciones informáticas en el territorio nacional.

A nivel legal, constitucional y jurisprudencial, es relevante ahondar respecto a los artículos motivo de esta investigación con la finalidad de establecer el tratamiento en materia penal aplicable a los mismo dentro del territorio nacional.

El estudio del impacto de los delitos objeto de esta investigación, son un tema que está afectando a gran parte de la sociedad y que día a día incrementa y se crean nuevas formas de vulneración, se torna relevante, porque la normatividad penal debe ajustarse a las nuevas necesidades de la sociedad, de igual forma, los delincuentes dedicados a este tipo de conductas, constantemente están creando o innovando su modus operandi a través de estos medios informáticos que les permite acceder a la red, lo cual hace necesario que el Estado adopte o implemente mecanismos idóneos que permitan enfrentar estos delitos y este es el fin primordial de la presente investigación, pues a través de ella se pretende hacer aportes, sugiriendo la implementación de estrategias dirigidas a minimizar el riesgo de ser víctima de estos delitos dentro del territorio colombiano.

Esta investigación va dirigida a cualquier persona sea esta natural o jurídica, pública o privada interesada en conocer de estos dos tipos penales adicionados a nuestra normatividad penal, generando conciencia a los ciudadanos respecto de los riesgos a los que se pueden exponer y que sepan identificar las diferentes modalidades y modus operandi en la comisión de estas dos conductas delictivas, sus tácticas y técnicas de operación, buscando con esta implementar medidas de seguridad que permitan a los ciudadanos establecer mecanismos de protección y de defensa frente a estos dos comportamientos delictivos.

Objetivo General.

- Examinar la aplicación del Art. 269I y 269J dentro del territorio nacional.

Objetivos Específicos.

- Conocer las distintas modalidades de Hurtos y Transferencia no Consentidas que se han cometido utilizando para ello medios informáticos dentro del territorio nacional.

- Establecer e identificar cuáles son los tratamientos penales aplicables a los delitos en mención.
- Plantear diferentes estrategias dirigidas a minimizar las posibilidades de ser víctimas de estos dos delitos (Hurto por Medios Informáticos y Transferencia no Consentida de Activos) dentro del territorio nacional.

Estructura de la Investigación.

El presente trabajo se desarrolla conforme a los parámetros de una investigación de tipo cualitativo a través del análisis de textos académicos, leyes, periodísticos, artículos prensa, jurisprudencia y doctrina, relacionados con el tema propuesto; DE LOS DELITOS DESCRITOS EN LOS ARTÍCULOS 269I Y 269J DE LA LEY 599 DEL 2000 Y SU APLICABILIDAD EN EL TERRITORIO COLOMBIANO. Y que, aportan bases teóricas para asumir una postura critico analítica del estado del arte que sobre el tema propuesto se tiene actualmente.

En cuanto a la estructura de la investigación, esta se presenta en tres partes distribuidos de la siguiente manera:

- En la primera parte se desarrolla la conceptualización e identificación del tratamiento legal y jurisprudencial aplicable a los delitos en mención.
- En la segunda parte, se identifican las distintas modalidades de Hurtos y Transferencia no Consentidas que se han cometido utilizando para ello medios informáticos dentro del territorio nacional.
- En la tercera parte, abordaremos las diferentes estrategias dirigidas a minimizar las posibilidades de ser víctimas de estos dos delitos (Hurto por Medios Informáticos y Transferencia no Consentida de Activos) dentro del territorio nacional. Y para finalizar, propondremos unas conclusiones que en el desarrollo del presente trabajo se pudieran obtener.

CAPÍTULO 1.
DELITOS INFORMÁTICOS.

Cuando fue creado el bien jurídico identificado con el título VII Bis de la protección de la Información y de los Datos, por medio de la Ley 1273 (2009), no fue coincidencia que fuera ubicado por el legislador al lado del título VII de los delitos que protegen el patrimonio económico, de la Ley 599 (2000), pues se observa en lo que tiene que ver con los delitos propuestos en esta investigación (Art. 269I Hurto por medios informáticos y el Art. 269J Transferencia no consentida de activos, que existe una relación directa entre estos dos delitos y las diferentes modalidades de hurto, descritas en el Art. 239 y ss.

1.1. Referente Histórico en Colombia de los Delitos Informáticos.

La primera iniciativa relacionada con los delitos informáticos se presentó en el 2007 a través del proyecto de ley Nro. 042 de ese mismo año en la Cámara de Representantes, el ponente de esta iniciativa fue el Dr. German Varón Cotrino. Básicamente lo que se pretendía en dicho proyecto era la modificación de algunos delitos que protegían la libertad individual y la intimidad, también se pretendía regular con este Proyecto de Ley todo lo relacionado con los equipos que sirvieran para la interceptación de comunicaciones, el acceso a sistemas informáticos, la violación a la disponibilidad de datos y también buscaba endurecer las penas en aquellos delitos donde se utilizaran estos medios informáticos. Este Proyecto de Ley no salió avante y se archivó, pues a pesar del interés mostrado en hacer todas estas modificaciones y adiciones al Código Penal no se pudo conseguir el suficiente apoyo para su aprobación. (Sentencia Sp-1245, 20015), (Gaceta del Congreso, 2007, pp. 39-40). (Gaceta del Congreso No. 355, 2007, p.p 39-40).

Más adelante en el mismo año 2007, se presenta el Proyecto de Ley Nro. 123, en la Cámara de Representantes, este proyecto tuvo como ponentes a los representantes a la cámara Carlos Arturo Piedrahita y Luis Humberto Gómez Gallo, este proyecto fue creado por el Dr. Alexander Díaz García quien para la época fungía como Juez promiscuo de

municipio de Rovira. Con este nuevo proyecto básicamente se buscaba crear un nuevo bien jurídico con el cual se pretendía proteger la información.

En la discusión de este nuevo proyecto participaron dentro de muchos, el mismo German Cotrino quien fue el ponente de la primera iniciativa, senadores, representantes a la cámara, hicieron presencia también representantes de los Ministerios del Interior y de Justicia, de Relaciones exteriores, por parte de la academia estuvo presente la Universidad del Rosario y como expertos en la materia estuvo en representación de la policía nacional el jefe de la unidad de delitos informáticos de la Dijín.

Después de esas discusiones se estableció la necesidad de crear un nuevo bien jurídico que se iba a incorporar al lado del título VII del patrimonio económico, este nuevo bien jurídico se iba a identificar con el título VII bis, con el cual se pretendía proteger específicamente lo relacionado con la información y los datos, a esta conclusión se llegó después de haber analizado algunas conductas incluidas en el Convenio de Budapest (2001), convenio este con él se busca combatir la ciberdelincuencia, principalmente las conductas que atentaban contra la confidencialidad y la disponibilidad de datos entre otros.

Este nuevo bien jurídico iba a estar desarrollado por dos capítulos, en el primero estarían las conductas relacionadas con el acceso abusivo a un sistema informático, la obstaculización ilegitima de un sistema informático o red de comunicación, interceptación ilícita de datos informáticos o de emisiones electromagnéticas, daño informático, uso de software malicioso (malware), violación de datos personales (hacking), suplantación de sitios web para capturar datos personales (phishing)) y un segundo capítulo donde se ubicarían los siguientes tipos penales (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. (Gaceta del Congreso No. 528, 2007).

Después de múltiples dificultades, oposiciones, discusiones y controversias, se pudo salvar el proyecto que estuvo a punto de hundirse en el Senado de la República, pues se sostenía que ya estas conductas delictivas estaban reguladas en el Código Penal lo que resultaría redundante, esto en relación principalmente con delito que se identificaba con el nombre jurídico de Hurto por medios informáticos relacionado en el Art. 269I. (Gaceta del Congreso, 2008, p. 2).

Luego de superar los múltiples obstáculos, se determinó realizar cambios en varios de los nuevos tipos penales con los que se busca proteger las nuevas modalidades delictivas llevadas a cabo a través de medios informáticos que estaban afectando también el patrimonio económico, esto con el fin de ampliar el margen de acción por parte de las autoridades para combatir este nuevo flagelo delictivo, pues se estaban utilizando estos nuevos avances tecnológicos para atreves de ellos defraudar el patrimonio económico no solo de las personas naturales sino también las jurídicas. Este segundo proyecto pudo pasar debido a que se eliminaron los artículos que regulaban lo relacionado a la falsedad informática, espionaje informático y violación de reserva industrial o comercial, con esto se pudo salvar este nuevo proyecto que en últimos dio origen a la Ley 1273 (2009), Ley por medio de la cual se creó y se incorporó al código penal el nuevo bien jurídico denominado de la información y de los datos. (Gaceta del Congreso, 2009, p. 7).

Teniendo en cuenta que en las acciones más reprochadas por la comunidad se involucra la utilización de medios de procesamiento de datos para timar el patrimonio de las personas naturales y jurídicas, además de controlar comportamientos característicos de la cibercriminalidad, el Estado Colombiano aprovechó esta oportunidad para enfatizar en la represión del apoderamiento ilícito, a través de mecanismos informáticos, de los dineros confiados al mercado financiero, al igual que la Transferencia no consentida de activos.

1.2 Análisis Normativo.

Para realizar este trabajo tuvimos en cuenta la Constitución Política de Colombia:

> Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. (Constitución Política de Colombia, 1991. Art 15)

La intimidad entendida como la manifestación necesaria para la vida moral del ser humano, ya que todas las personas tienen por necesidad algo que se reservan para sí, sin intimidad el ser humano sería un simple animal sensitivo pues la racionalidad exige, de suyo, una esfera privada, tal exigencia obedece a que en la esencia humana hay algo de absoluta o limitada reserva según el caso.

La intimidad consiste en el dominio exclusivo y reservado que la persona tiene de su fuero interno, compatible solo con aquellos que la autonomía de su voluntad designe y en algunos casos con quienes naturalmente están ligados a ella por vínculos de familia en una medida no absoluta sino razonable. Dentro del marco de protección de este derecho fundamental, se encuentran la información y los datos que se manejan en el diario vivir y que circulan por las redes sociales y medios electrónicos y al ser esta información de fácil acceso y manipulación, se requiere una protección especial para evitar que personas inescrupulosas a través de los medios tecnológicos las utilicen con fines fraudulentos y delictivos.

Artículo 269I: Hurto por medios informáticos y semejantes: este hace referencia a lo descrito en el artículo 239 del código penal, siendo realizado o violando medidas de seguridad en temas relacionados con programas o software de informática y será sancionado de acuerdo con las penas descritas en el artículo 240 de este código. (Ley 1273, 2009, Art. 269I).

Art. 269J: Transferencia no consentida de activos: este delito nos lleva a entender cuando nuestros datos personales o medios que utilizamos para efectuar movimientos bancarios, transferencias o pagos, son realizados por personas ajenas e inescrupulosas que con el fin de obtener un beneficio propio o para un tercero y sin un consentimiento para estos trámites del titular del derecho, se aprovechen de estos medios digitales para incurrir en delitos con el conocimiento de datos o maneras de manejo de datos a través de las redes o equipos de tecnología informática. (Ley 1273, 2009, Art. 269J).

> Artículo 239. Hurto. El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro. (Ley 599, 2000. Art. 239).

Nos detalla que todo aquel bien material que sea despojado o alejado de la esfera de dominio de su propietario estará considerado como el delito que contempla este artículo y la sanción jurídica para este tipo de comportamiento dependerá de algunas circunstancias que califican o agravan la conducta descrita en los artículos 240, 241, 267 y 268 entre otros.

En el Artículo 240 del Código Penal, el Legislador trae a colación una serie de circunstancias que hacen más gravosa la conducta, circunstancias como la violencia sobre las cosas o las personas, el poner a la víctima en una condición de indefensión o aprovechándose de dicha condición, el llevar a cabo la conducta en el domicilio de la víctima, o cuando se utilizan instrumentos que le permitan llevar a cabo el hurto como llaves falsas o violando mecanismos de seguridad electrónicas, o cuando se comete sobre medios motorizados entre otros. (Ley 599, 2000. Art. 240).

El Articulo 105. trae a colación conductas con las cuales se puede acceder de manera fraudulenta a terminales móviles de servicios de comunicación con el propósito de alterar bases de datos, conductas estas castigadas por el legislador con penas que van desde los 6 a los 8 años de cárcel. (Ley 1453, 2011. Art. 105).

1.3 Análisis Jurisprudencial de los artículos en mención (Arts. 239,240, 241, 269I y 269J.

El inciso segundo del Artículo 239, había sido derogado por el Articulo 30 de la Ley 1153 (2007), Ley de pequeñas causas. No obstante, la Corte Constitucional al declarar la inexequibilidad de dicha Ley mediante la Sentencia C- 879 (2008), dicho inciso recupero su vigencia.

- El objeto material, en el delito de hurto, debe ser de origen licito.

> …cuando un tercero a cometido delitos sobre los bienes que hacen parte del patrimonio económico de una persona, se mantiene vigente la presunción constitucional de buena fe acerca de su origen. La cual solamente se derrumba como consecuencia del agotamiento del respecto proceso dentro del cual se establezca su procedencia, salvo cuando su origen ilícito se determina en la investigación que se adelanta por la presunta conducta delictiva del tercero, aspecto este que adquiere relevancia dentro de la dogmática penal y que no ha sido ajeno para la doctrina. (…)
>
> Tal aspecto tiene incidencia en la estructuración del injusto penal, porque a pesar de tratarse de una conducta que complace los elementos del tipo penal de hurto, la procedencia ilícita del objeto material no permite afirmar que haya habido lesión o siquiera puesta en peligro del bien jurídico de patrimonio económico, pues la posesión material de los bienes sobre los cuales aquella se concrete no genera derechos para quien los obtuvo ilícitamente, toda vez que no sufre detrimento patrimonial alguno" (C.S.J Cas. Penal. Sent. Mayo 22/2013. Rad. 40830. M.P. Gustavo Enrique Malo Fernández.)

- **Momento consumativo del hurto.**

en nuestra ley penal, en el artículo 349, se exige para la tipificación del delito de hurto, que el sujeto activo que es de naturaleza común, "se apodere de cosa

mueble ajena, con el propósito de obtener un provecho para sí o para otro… "esto es, que no exige ni posibilita hacerlo para su consumación el "poder de disponer libremente del bien a que se refiere el doctrinante en cita sino el "propósito de obtener" provecho para sí o para otro que es precisamente lo que ha llevado a la jurisprudencia de esta corporación a sostener que "el delito de hurto se consuma en el momento en que la cosa se extrae de la esfera patrimonial o de la custodia de quien antes la tenía", como se expuso en el fallo del 29 de octubre de 1986, y que ha continuado reiterándose, entre otras decisiones, en el Auto de 20 de abril de 1992 con ponencia del magistrado doctor Jorge Enrique Valencia Martínez y en la decisión del 2 de agosto de 1993, cuando siendo ponente el magistrado doctor Dídimo Páez Velandia, se explicó, que "El momento consumativo del hurto es el de la asunción del poder sobre el bien por el delincuente cuando la víctima pierde la factibilidad de protección o de dominio sobre el mismo a causa de ese inconsulto apoderamiento, y la pierde, cuando, imposibilitada por la acción de aquél, o impotente para perseguir el bien porque v. gr, correr detrás de un vehículo en marcha es tarea que solo podrá hacerse en los primeros instantes del hecho, se limita a mirar el alejamiento de su bien" (CSJ, Cas. Penal, Sent. 10644, mayo 6/99. M, P. Carlos Augusto Gálvez Argote).

- **El bien puede salir de la custodia momentáneamente.**

La guardia policial dispuesta, entonces, así como en general los mecanismos de seguridad de que comúnmente se valen las personas para la protección de sus bienes, por sí mismos no excluyen la posibilidad de la consumación del delito y eso significa que en todos aquellos casos donde se contaba con algún sistema de vigilancia que haya obstaculizado el escape de los asaltantes y permitido su Captura, no necesariamente cabe la conclusión de que la conducta no superó la tentativa. Simplemente porque lo que define si se

> completó la ejecución del delito es la comprobación de si el bien salió de la esfera de custodia de su dueño, poseedor o tenedor, aunque haya sido brevemente, y no que el autor del hecho haya asumido el poder de control y disposición material sobre la cosa, que perfectamente puede no haberlo obtenido y, sin embargo, encontrarse consumada la ilicitud, como cuando huye con el bien y es perseguido por quien lo tenía o por las autoridades". (CSJ, Cas. Penal, Sent. sep. 20/2005, Rad. 21558. M.P. Yesid Ramírez Bastidas).

Las conductas señaladas en los numerales 1°,3° y 4° cuando la cuantía del hurto no superara los diez salarios mínimos legales mensuales vigentes habían sido convertidas en contravenciones mediante el artículo 30 de la ley 1153 del 2007, sin embargo dicho compendio normativo fue declarado inexequible en su totalidad por la corte constitucional, mediante sentencia C-879 del 10 de septiembre del 2008, M.P. Manuel José Cepeda Espinoza, como consecuencia, el contenido original de los numerales antes citados recobra la vigencia que tenía antes de la expedición de la ley 1153 del 2007.

- **Hurto Agravado Por Violación De Morada Ajena Y Delito De Violación De Habitación Ajena.**

> (...) no deben confundirse el llamado delito complejo en que el legislador ha recogido en una norma los varios ordenes de agravio al derecho ajeno, como sucede con el hurto agravado por penetración a habitación de otro, solucionando así el problema, con el acto posterior copenado en que existe lesión de un solo orden. Y, desde luego, si se atiende la noción doctrinal, no dejaría de ser anómalo el concepto de un acto posterior copenado con un contenido injusto mayor que el acto previo, único deducible jurídico penalmente.

Es claro que la preferencia del tipo más rico descriptivamente se da en el delito complejo, como lo ejemplifica el hurto agravado por violación de morada ajena, pero es característica Sobre todo del principio de especialidad, porque los elementos adicionales de las formas agravadas o atenuadas marcan la diferencia especifica Con el tipo básico y conducen a su desplazamiento". (C.S.J. Cas. Penal, Sent. ago. 2289. M.P. Gustavo Gómez Velásquez).

- **Concurso aparente entre los delitos de hurto y secuestro.**

Además de lo expuesto, se impone precisar que respecto del criterio de consunción como solución al concurso aparente de delitos, y más especialmente en cuanto se refiere al denominado hecho típico acompañante, de lo que se trata es que el juicio de desvalor de uno de los comportamientos en aparente concurso, consume el juicio de desvalor del otro delito, dado que la entidad de este último no trasciende ni cobra autonomía en punto de lesión del bien jurídico tutelado, en la medida que su punición ya ha sido establecida por el legislador al tipificar el otro comportamiento. En evento contrario, como ocurre en el caso de la especie, que ambos comportamientos violan de manera ostensible y autónoma diversos bienes jurídicos (patrimonio económico y libertad personal), no hay duda de que la valoración de la finalidad perseguida por el acusado resulta inane, pues sin dificultad se advierte la configuración de un concurso material de delitos, de lo anotado puede concluirse que los argumentos del censor orientados a demostrar que se traté de un concurso aparente de delitos de hurto calificado y secuestro simple y que por ende se violó el principio non bis in ídem no prosperan, al no acreditar que la norma seleccionada y aplicada del secuestro correspondió a un defectuoso proceso de adecuación típica. o que la retención de J… por parte del procesado, con posterioridad a la comisión del delito de hurto calificado, correspondía a un elemento estructural de este comportamiento

(especialidad), o bien que la adecuación de la conducta a tal tipo penal excluía el precepto que tipifica el atentado a la libertad personal (alternatividad), ora que uno de los delitos era subsidiario del otro (subsidiariedad), o que el juicio de desvalor de una de las conductas delictivas consumía el de la otra (consunción)". (CSJ, Cas. Penal, sent. Ene, 26/02005, Rad. 21474. M.P. Marina Pulido de Barón).

- **El Articulo 269I es un tipo penal subordinado al de hurto. Aplicación del artículo 269I a este delito.**

(…). Ahora una lectura apresurada del precepto estudiado podría sugerir, equivocadamente, por supuesto, que la conducta reprochada penalmente es la de superar las seguridades informáticas, caso en el cual el bien jurídico de la protección de la información y los datos estaría en clara correspondencia con la concepción de un único interés superior a tutelar; no obstante, es el legislador el que se ocupó de identificar que el comportamiento objeto de reproche es el señalado en el artículo 239, es decir el de hurto realizado, eso sí, ejecutando la acción complementaria, consistente en superar (violentar) las seguridades informáticas a través de cualquiera de las dos formas modales de realización de la conducta reseñada, como derivaciones del tipo básico. (…).

Agréguese, que dicha remisión al artículo 269I abarca no solo el verbo rector de la conducta de hurto simple, el objeto material –la cosa mueble- y el elemento normativo relativo a la ajenidad del mismo, sino, también el ingrediente especial subjetivo necesario para su comisión, como lo es, el animus lucrando o la finalidad o propósito doloso de obtener un provecho o utilidad –propio o en favor de un tercero de carácter patrimonial. (…).

Siendo ello así, natural es concluir, como lo hiciera la demandante y el representante del ente acusador, que él tipo penal de hurto por medios

> informáticos y semejantes no solo está circunscrito al ámbito de punibles contra la información y los datos, sino, esencialmente a la esfera de los lesivos del patrimonio económico, pues es el valor ético jurídico que al final resultaría atacado con la sustracción de dineros a través de mecanismos ilícitos de manipulación de los sistemas informáticos, electrónicos, telemáticos o similares, o suplantación de las personas ante los sistemas de autenticación y de autorización. (…).
>
> Ahora, lo recién argumentado, no pretende sostener la idea categórica de que el tipo penal de hurto por medios informáticos es necesariamente análogo al de hurto calificado, pues, como resulta obvio, éste no está dentro de la esfera de protección de la información y los datos o la intimidad, como si lo está el punible que nos ocupa; pero lo que, si se encuentra sujeto al criterio analógico, en cuanto resulta ser benigno al procesado, es la posibilidad de otorgar a un supuesto de hecho similar (protección del bien del patrimonio económico), la misma consecuencia jurídica que le imprime el articulo 269 ejusdem a los delitos rubricados bajo los capítulos comprendidos en el título VII.
>
> Esta postura es compatible y fiel al interés del legislador por entregar una ventaja punitiva a aquel que repare en términos económicos el daño causado por delitos que agredan el patrimonio de las personas". (CSU, Cas. Penal, Sent. feb. 11/2015, Rad. 42724, M.P, Eyder Patiño Cabrera).

Se trae también a colación una sentencia de la C.S.J Sala de Casación Penal, del año 2022, donde fueron condenados varios empleados del banco Davivienda por los delitos de concierto para delinquir en concurso con el delito de Acceso abusivo a un sistema informático Art. 269I de C.P. adicionado por la Ley 1273 del 2009, respecto a este último delito, consideramos importante resaltar el análisis que hizo la Corte Suprema

del mismo en sede de casación, porque guarda una relación directa con los tipos penales objeto de esta investigación, toda vez que en muchas oportunidades dentro del modus operandi de los ciberdelincuentes para poder materializar el Hurto por medios informáticos y la trasferencia no consentida de activos, previamente necesitan acceder a sistemas informáticos con el objeto de obtener información respeto de las personas o entidades que se pueden convertir en sus posibles víctimas.

Considero la Corte de importancia resaltar que el tipo penal de acceso abusivo a un sistema informático -art. 269 A del C.P.-, ha sido reconocida por la doctrina como "hacking directo o mero intrusismo informático", es decir, "conductas de meros accesos y/o permanencias perpetradas con el único fin de vulnerar un password o una puerta lógica que permite acceder a sistemas informáticos o redes de comunicación electrónica".

> Sostuvo la Corte que este tipo penal está conformado i) por un sujeto activo que no es calificado por no necesitar de una condición especial para quien accede a un sistema informático "sin autorización", o que teniéndola, decide conscientemente mantenerse conectado; ii) por un sujeto pasivo, que es la persona natural o jurídica titular del sistema informático; iii) por lesionar varios bienes jurídicos tutelados, entre ellos, la información, los datos y la intimidad, ha sido reconocido como un tipo penal pluriofensivo; iv) solo admite el dolo en el actuar del ciberdelincuente; v) es un delito de mera conducta, por cuanto, la sola intromisión en una red informática, en las condiciones establecidas en el tipo penal, afecta el bien jurídico tutelado; vi) contempla dos verbos rectores, acceder o mantener; vii) como ingrediente normativo, exige que el sujeto activo de la acción a) acceda en el sistema informático sin autorización, o, b) aun cuando, teniendo el permiso del titular legítimo del derecho, se mantiene dentro del mismo, excediendo las facultades otorgadas. Respecto de la primera forma de actuar del ciberdelincuente, no

> reviste mayor complejidad, por cuanto, resulta suficiente la introducción ilegítima sin la voluntad del titular de la cuenta. Para la Corte el problema surge con la segunda manera de actuar, en tanto, el ingrediente normativo que la contiene está enfocado a establecer cuáles serían los límites de esa autorización que desbordaría el tipo penal estudiado" (C.S.J, Cas. Penal, Sent. Mar. 11/2022, Rad. 50621, M.P, Diego Eugenio Corredor Beltrán).

1.4 Análisis Del Tipo Penal De Hurto Por Medios Informáticos.

Con la Ley 1273 de 2009, se creó una forma especial de hurto que se realiza o ejecuta superando medidas de seguridad informáticas y la manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante.

1.4.1 ART. 269 I.-Adicionado.L.1273/2009, ART.1. Hurto por Medios Informáticos y Semejantes, dispone:

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.

Este tipo de delito constituye una forma especial de hurto que remite a la estructura del tipo básico establecido en el Art. 239 del hurto del C.P. El profesor Juan Oberto Sotomayor en su curso de derecho penal I de 2012 aborda el estudio de este tipo panal de la siguiente manera:

El tipo penal analizado es de carácter subordinado y ello se establece por cuanto se presenta una subordinación o dependencia de la conducta básica del hurto, conclusión a la que se llega al leer la norma estudiada: "…El que, superando medidas de seguridad

informáticas, realice la conducta señalada en el artículo 239…", surge entonces la subordinación de las determinadas circunstancias adicionales, esto es las "simples derivaciones del tipo básico"1. así mismo es un tipo de lesión si tomamos como referencia el principio de lesividad consagrado en el artículo 11 del Código Penal, que señala que una conducta es punible si se lesiona o pone en peligro el bien jurídicamente tutelado, tomando ello como base, es necesario que con la realización de esa figura se consume un daño al bien jurídicamente tutelado, por lo que debe existir afectación patrimonial, es decir, el apoderamiento del dinero o la información de la persona natural o jurídica, lo cual le ocasiona un perjuicio con valor económico ya sea material o inmaterial. Es además un delito de resultado material porque al ocasionarse ese perjuicio al patrimonio se presenta una modificación en el mundo exterior separable espaciotemporalmente de la acción, modificación que no es otra que esa alteración a través del ingreso ilícito al sistema informático con las consecuencias de la vulneración al bien jurídicamente tutelado del patrimonio económico. Es de conducta instantánea pues la acción típica se agota en el momento en que la víctima es despojada de su dinero a través de los retiros o transferencias fraudulentas utilizando medios informáticos. Es de tipo compuesto dado que en su descripción se presentan una pluralidad de complementos descriptivos, a través de cada uno de los cuales se configura el tipo penal. Esa pluralidad de acciones está enmarcada en el hecho de que, a través de la superación de medidas de seguridad informáticas, se cometa la conducta descrita en el artículo 239, ya sea manipulando el sistema informático, manipulado una red de sistemas electrónicos, o telemáticos, o suplantando a un usuario ante los sistemas de autenticación y de autorización del medio digital, buscando obtener el provecho económico que se busca.

Vemos que son acciones diferentes y que la realización de una sola de ellas a plenitud conlleva la comisión de la conducta punible. Es de medio determinado por

---

1 curso de derecho penal I de 2012, pág. 5. Juan Oberto Sotomayor

cuanto se exige para su realización la afectación patrimonial a través de un medio informático, electrónico o telemático, de ahí entonces su especificidad. Y esto puede darse, primero utilizando la internet como canal de comunicación entre los medios electrónicos o informáticos que se pretenden vulnerar para cometer la conducta punible, y segundo por lo específico del objeto material que se pretende desapoderar a la víctima, que es el dinero de sus cuentas bancarias, o la información privada existente en los medios de almacenamiento digitales.

En cuanto a la tipicidad, esta debe ser abordada desde el artículo 10 del CP, donde se establece: "La ley penal definirá de manera inequívoca, expresa y clara las características básicas estructurales del tipo".

- **Los sujetos activo y pasivo.**

Sujetos activos: La definición que la Ley 599 del 2000 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). 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.

Si se ejecutan hurtos por medios informáticos y semejantes, bajo la manera de clonación de tarjetas, los autores suelen ser varios, uno de ellos es el que instala o utiliza el dispositivo clonador y copia la información de la tarjeta original en una banda magnética que es instalada en otro plástico, hasta allí llega su aporte. Otro sujeto se traslada al banco, ingresa la tarjeta clonada al cajero y digita la clave para extraer de la correspondiente cuenta bancaria el tope máximo de dinero entregado por el dispositivo.

O, como sucede en otros casos, retiran el tope máximo y trasladan el saldo de dinero a cuentas de terceras personas que se prestan para recibirlo y retirarlo de manera inmediata a través de cajeros o taquilla directamente en el banco y un tercer sujeto que recibe el dinero a través de transferencia directa y retira el dinero en oficina bancaria.

Para el presente caso es el autor directo, aquél que se traslada al cajero y con la tarjeta clonada retira el dinero existente en la cuenta del titular, o lo transfiere a la cuenta de un tercero con quien existe un acuerdo previo para su recepción. Ahora bien, quien participa de la clonación de la tarjeta, debe responder a título de cómplice, por cuanto, para ser coautor del delito, debe tener un dominio funcional del hecho, esto es, un dominio subjetivo (dolo de ejecutar la acción) y negativo en el sentido en que su aporte debe ser esencial en la fase ejecutiva, lo cual no se aprecia en este caso, pues su participación sólo va hasta el instante en que instala el dispositivo clonador, lo retira y copia con la información allí recopilada una nueva banda de la tarjeta débito o crédito, por tanto, su aporte es necesario aunque no toma parte durante la ejecución, lo que hace que caiga en el fenómeno de la complicidad. Caso contrario ocurrirá, si quien copia y clona la tarjeta participa activamente en compañía de quien va al banco a realizar los retiros y/o transferencias a otras cuentas receptoras, allí participaría activamente del verbo rector, por lo que sería un coautor.

Por último, es especial el caso de ese tercero que recibe en su cuenta bancaria el dinero proveniente de una transferencia bajo esta modalidad, dado que allí se debe analizar en cada caso y de manera particular si conocía la ejecución y desarrollo el plan común, pues de conocerlo, su aporte es esencial, porque sin él no podría realizarse la transferencia de dinero que exista en la cuenta del titular afectado con el delito y con ello no se consumaría el delito, por tanto, y para no generalizar, pues se estaría incurriendo en un error al tomar una única posición, es que ese deja planteada la posibilidad de que responda a título de coautor, por ser conocedor del plan íntegro y común y además hacer un aporte esencial al desarrollo del delito o también puede responder bajo la figura de la

complicidad necesaria, pues como se indica puede o no tener ese dominio o participación funcional en la fase ejecutiva, dado que si el autor no tiene una cuenta bancaria a donde transferir el dinero, sólo lograría apoderarse de lo entregado en la transacción realizada a través del cajero electrónico.

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 burlado 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.

En este caso es necesario indicar que quien fue poco diligente con el cuidado de su tarjeta y su clave, en los dos casos ejemplificados de clonación y “cambiazo” de la tarjeta, fue el titular de la cuenta bancaria, y que, a través de las maniobras utilizadas por los delincuentes, observaron su código para ingresar al sistema y de allí sustrajeron su dinero. El software del banco, ante la utilización de esos dos elementos (banda magnética

de la tarjeta y clave) permite que un usuario cualquiera que los posea ingrese al sistema y realice las transacciones hasta el tope asignado.

En los casos estudiados, el sujeto pasivo (víctima), será la persona natural de este tipo de conductas de hurto por medios informáticos y semejantes, por lo que es ella quien, ante la poca previsión y cuidado de su documento personal, bajo engaño entregó los medios para que se realizara la conducta descrita en el artículo 269I CP.

En caso contrario, si se clona una tarjeta en un punto denominado de compromiso, – lugar donde se establece por indagaciones que fue vulnerada la seguridad del cajero y se instaló un dispositivo para clonar no una sino varias tarjetas débito o crédito, y con la información allí capturada se sustraen los dineros de diferentes cuentas bancarias; si se vulneró la seguridad del cajero electrónico, no debe ser sujeto pasivo la víctima del hurto el titular de la cuenta bancaria, sino la persona jurídica encargada de la custodia del dinero de sus clientes y la seguridad de sus cajeros, por ello en ciertas oportunidades las entidades reconocen el dinero a los afectados, una vez se ha desarrollado su investigación interna y se ha logrado detectar el denominado “punto de compromiso”.

- **Elementos del tipo objetivo y subjetivo.**

Son elementos del tipo objetivo:

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.

Son elementos del tipo subjetivo:

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.

El hurto por medios informáticos ha de llevarse a cabo mediante la realización de dos comportamientos: 1) la superación de medidas de seguridad y 2) 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 superación de medidas de seguridad:**

Las medidas de seguridad privadas establecidas por los bancos y demás entidades financieras para proteger los dineros depositados en los cajeros automáticos consisten en la cerradura de acceso al lugar donde se encuentren los aparatos y el bloqueo del sistema al que se tiene acceso mediante la introducción de la tarjeta magnética y la pulsación de la clave secreta.

Estas medidas de seguridad informática de los cajeros automáticos son burladas por la delincuencia mediante la introducción de la tarjeta magnética y la pulsación de la clave secreta.

Para consumar esta conducta típica no es suficiente penetrar al habitáculo donde está el cajero, pues si no introduce la tarjeta ni pulsa la clave secreta respectiva el agente no logra el ingreso al sistema informático y menos la superación de las medidas de

seguridad informática. La utilización de la tarjeta falsa sólo le facilitará al sujeto acceder al teclado del cajero, pero no entrar al sistema; por tanto, tal uso no implica la superación total de las defensas privadas instaladas por el titular del bien jurídico.

Quiere decir lo anterior que la introducción de la tarjeta magnética en el cajero y la posterior pulsación de la clave secreta son en últimas los medios eficaces que utiliza el delincuente para superar la defensa particular, dado que la introducción al lugar donde está el aparato no constituye aún el peligro para el bien jurídico; tan es así que en algunos sitios públicos existen cajeros a los que se accede sin necesidad de abrir alguna cerradura.

La barrera de protección que se supera en los casos mencionados no es el habitáculo en el que se encuentra el cajero sino el cajero mismo, en concreto, el dispositivo automático que entrega el dinero; de modo que para la tipicidad de la conducta no interesa el lugar donde se encuentre el cajero, pues bien puede estar en el interior de un receptáculo o en un espacio de fácil acceso para el público.

Si la tarjeta magnética se utiliza para obtener la entrada al lugar donde se encuentra instalado el cajero automático, y además se emplea para acceder al sistema y obtener el apoderamiento del dinero luego de la pulsación de la respectiva clave secreta, la conducta del delincuente no queda reducida a la de entrar al habitáculo que resguarda al cajero e iniciar el acceso al sistema de protección impuesto por la entidad bancaria mediante la inserción de la tarjeta en el cajero, dado que logra entrar de manera definitiva al sistema informático a través de la pulsación de la clave secreta y “el cajero automático, al constatar la pulsación del número personal correspondiente al titular de la tarjeta, es cuando admite la operación y no antes”. (Mata y Martín, en Poder Judicial, núm. 49, 1998(I), p. 354).

Quien penetra al recinto donde se encuentra instalado el cajero automático y no inserta en él la tarjeta ni pulsa el número personal respectivo, no puede superar la totalidad de las defensas privadas instaladas por el titular de la relación posesoria ni

apoderarse de suma de dinero alguna, pues, se repite, las seguridades colocadas por los bancos y las demás entidades financieras para proteger los dineros depositados en los cajeros automáticos consisten en la cerradura de la puerta de acceso al lugar donde se encuentren los aparatos, y el bloqueo del sistema al que sólo se tiene acceso mediante la introducción de la tarjeta magnética y la pulsación de la clave secreta. Si la utilización de la tarjeta magnética va acompañada de la pulsación del número secreto, no hay duda de que se superan las medidas de seguridad informática impuestas por la institución bancaria o financiera.

- **La Manipulación del sistema informático:**

Por manipulación informática ha de entenderse la "modificación no autorizada de datos o contenidos en un sistema informático, en cualquier fase de su incorporación o procesamiento". (Suárez Sánchez, 2009, p. 254).

La manipulación del sistema informático que da lugar a la realización del delito de hurto por medios informáticos y semejantes consiste en el incorrecto uso de un sistema informático, siempre y cuando sea idónea para producir el perjuicio patrimonial no consentido por el titular del bien jurídico.

El uso incorrecto del sistema informático en esta modalidad delictiva, se refiere a la no concordancia que se da entre la utilización del cajero automático y la voluntad de quienes pueden realizar los actos de disposición de los dineros depositados en el mismo (el banco o la entidad crediticia y el titular de la respectiva cuenta), que se concreta cuando el sujeto que ha logrado entrar al sistema, mediante la introducción de la tarjeta y la pulsación de la clave secreta, realiza además las acciones relacionadas con el tratamiento de los datos registrados de acuerdo a las instrucciones del programa informático, es decir, mediante la selección de la operación a realizar, que en este caso es la de retiro de dinero, el señalamiento de la cuantía deseada, la orden de que la entregue y la recepción y el apoderamiento del dinero.

- **La acción o conducta**

La descripción normativa, en su tipo objetivo positivo y en la consecuencia jurídica, no consagra la conducta reprochada, el objeto material, ni la sanción correspondiente, sino que, en cuanto se refiere al comportamiento antijurídico y al referido objeto sobre el que recae la acción prohibida, efectúa un reenvío normativo al tipo base de hurto (artículo 239 del C.P) y a la disposición que lo califica (Art. 240 ejusdem) para determinar la sanción imponible.

De acuerdo al verbo rector consagrado en el art. 269I CP, implica que para ser catalogada la conducta como delito hay que acudir a la prohibición señalada en el artículo 239 de la ley 599 del 2000, cuya acción prohibida es "apoderarse". No hay duda pues, que lo prohibido por esta regla penal es el apoderamiento ilícito de algo, de ese bien mueble que puede estar representado, en el dinero, retirado de las cuentas de los clientes bancarios y en la información privilegiada de empresas, entidades o instituciones públicas o privadas, bien intangible, que en muchas ocasiones tiene un alto valor económico para quien se apodera de él y representa ese elemento normativo del propósito de obtener ese provecho para quien ejecuta a través de medios electrónicos la acción prohibida.

El Art. 269I, es subordinado del tipo básico del hurto artículo 239 y fue diseñado su contenido para evitar ese apoderamiento, no sólo de dinero, sino de información privilegiada de personas, empresas o instituciones públicas o privadas, que como bien intangible posee un gran valor en el mercado, según la jurisprudencia y la doctrina sobre el hurto, estamos en presencia de una conducta de resultado material, que se exige esa alteración del bien jurídico protegido al titular del derecho patrimonial conculcado, pero bajo unas características especiales que es ejecutar la conducta para obtener el apoderamiento del bien, utilizando medios informáticos, por lo que se señala allí esa superación de medidas de seguridad informáticas (caso clonación y cambio de tarjeta), y manipulando el sistema informático o la red de datos o suplantando al usuario, lo que se

obtiene una vez se ejecute la clonación y con banda magnética y clave ilegítimamente obtenidas obtener el apoderamiento del bien, paso final con el que termina la acción.

- **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.

- **Dispositivo amplificador del tipo.**

La Tentativa.

Este delito es de resultado porque debe causarse el perjuicio patrimonial, que se concreta cuando el sujeto activo logra el apoderamiento del dinero depositado en el

cajero automático. Por tanto, nada impide la apreciación de este delito en el grado de tentativa si el autor de la manipulación de la tarjeta falsificada u obtenida ilícitamente ejecuta una acción idónea para apoderarse de una suma de dinero de la cuenta de otro, y no logra disponer del metálico por motivo ajeno a su voluntad, como cuando es descubierto en el instante en que se dispone a retirar el numerario luego de haber introducido la tarjeta, pulsado el número secreto y solicitado la suma respectiva Si a pesar de haber intentado obtener el dinero, la operación no se lleva a cabo por circunstancias como la no disponibilidad de saldo en la cuenta o la utilización de una clave personal errada, por ejemplo, se está ante una tentativa imposible impune, dado que la acción no tiene la capacidad de producir el resultado prohibido.

1.4.2 Análisis del tipo penal de Transferencia No Consentida De Activos.

- **Elementos típicos del Art. 269J CP.**

  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 48 a 120 meses y multa de 200 a 1500 smlmv. 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.

- **Clasificación de la conducta del Art. 269J CP.**

Este es un tipo penal básico, ya que se aplica sin depender de ningún otro tipo penal, su contenido describe de manera independiente el comportamiento que se prohíbe, el cual corresponde a la transferencia no consentida de activos.

Es un tipo penal de lesión, pues al tenor del Art. 11 del CP, exige el daño al bien

jurídicamente tutelado, es de resultado porque exige que se debe concretar la transferencia de activos de la cuenta de la víctima a la del victimario, sin su consentimiento, es de conducta instantánea por cuanto la acción se agota en el momento en que se da el resultado utilizando medios informáticos. Es compuesto y de medio determinado por el número plural de acciones con las que se puede cometer el delito, transferencia no consentida a través de una manipulación informática o un artificio semejante y la utilización para ello un medio informático, de ahí entonces su especificidad.

- **Sujetos activo y pasivo.**

Sujeto activo: Simple, ya que no exige a quien comete la conducta punible calidad especial alguna, por lo que autor es "el que" la ejecute. Esto es, que cualquier persona natural puede ser responsable de ella. Es necesario indicar que, para realizar el tipo penal, el autor, o autores, deben tener amplios conocimientos en informática pues su ejecución y consumación así lo exigen, dado que sólo se llega a la ejecución del delito utilizando la internet y los medios informáticos.

Es importante resaltar que esta conducta punible por lo general no es ejecutada por un solo individuo, sino por un grupo de personas concertadas previamente para ejecutarla, así ha sido establecido por la policía judicial dedicada a combatir este tipo de criminalidad, en cada caso concreto se mirara teniendo en cuenta el grado de participación de cada uno de las personas que intervienen en la comisión de la conducta en que calidad se hará la imputación, si de autor, coautor o participe sea este determinador o cómplice.

Sujeto pasivo: La entidad bancaria, esto debido a que ella es la responsable de la custodia, no sólo del dinero, sino del sistema, y los movimientos bancarios desde las cuentas de los clientes. No obstante lo anterior, debe analizarse cada caso en concreto a fin de determinar cuál es el grado de responsabilidad que recae sobre el titular de la

cuenta bancaria a quien engañaron a través de maniobras electrónicas para despojarlo de su información privilegiada, hasta dónde llega su responsabilidad en estos hechos, y hasta qué punto descuidar la seguridad informática personal, no aplicar los protocolos de anti virus actualizados, de cuidado con la apertura de correos electrónicos y buen manejo de la internet por parte del titular de la cuenta puede ocasionar que la responsabilidad le sea trasladada y pierda el dinero transferido.

La acción: Descomponiendo el tipo, tenemos que el Art. 269 J posee un verbo rector principal que es transferir, y cuatro secundarios en el inciso final, que tienen relación ya no a la transferencia de activos, sino al hecho de fabricar, introducir, poseer o facilitar programas destinados a lograr a través de ataques o técnicas de intromisión la consecución de información que posibilite la transferencia de activos o la comisión de delitos de estafa. El inciso final de la norma se dirige a atacar aquellos grupos de piratas informáticos o hackers dedicados a la elaboración de software malicioso, conocido como virus, gusanos, troyanos, bombas lógicas, spam, etc., que permiten ingresar a los computadores de terceras personas a quienes desapoderan de su información bancaria y claves.

Transferir, según el diccionario de la Real Academia de la Lengua Española es "…cambiar dinero de una cuenta a otra mediante una transferencia bancaria…" o "pasar a una persona o cosa de un lugar a otro" y esto precisamente es lo que ocurre en las transferencias electrónicas no consentidas: se pasa de una cuenta a otra un activo, o suma de dinero señalada al sistema informático mediante órdenes electrónicas.

En el inciso final, se tiene que fabricar no es más que hacer o construir una cosa a partir de una combinación de componentes. Es aquella acción de construir, hacer o crear, mediante lenguajes de programación, software – en este caso malicioso -que permita acceder a través de complejas órdenes lógicas a los ordenadores y la internet a fin de que aquellos ejecuten unas tareas específicas para las cuales fueron diseñados.

Ese software malicioso no es más que la construcción a través de lenguajes de programación de los conocidos como malware, que es un software dañino para el sistema, phishing, que es la creación de páginas falsas, back doors, que son programas que permiten explotar esas vulnerabilidades en los sistemas de computación para obtener datos o hacer algún daño al mismo, etc.

Introducir, puede ser asumido como introducir al país aquellos programas maliciosos, creados por los hackers, destinados a realizar esa invasión o infiltración no detectable en los computadores de las víctimas, o introducir dichos programas directamente a la red, para que a través de aquella se llegue a los ordenadores más vulnerables, por falta de protección en los sistemas de seguridad o antivirus.

Poseer y facilitar, son dos verbos correlacionados entre sí dentro de este tipo penal, pues ellos se dirigen a que quien posea el software malicioso y lo facilite a los ejecutores de la acción de infiltración de los ordenadores, incurrirá en dicha conducta típica.

Es importante señalar que las acciones descritas anteriormente, en nuestro país, son difíciles de demostrar en los estrados judiciales por la falta de preparación de los funcionarios judiciales en la recolección de elementos materiales de prueba digitales, que permitan establecer quién o quiénes son las personas dedicadas a la creación de programas maliciosos e igualmente a la internacionalización de las acciones delictivas, la información que es guardada en la "nube" y a que las programas ejecutados para realizar la comisión de aquellos hechos que llevan al apoderamiento de la información personal se desarrollan casi que exclusivamente en el exterior, siendo principalmente los países asiáticos, Israel y Brasil los principales proveedores de software malicioso.

El objeto material: Para entender este apartado, es necesario entender el concepto de Objeto Material u objeto de acción, pues varios autores asimilan ambos términos al objeto jurídico que se refiere es al bien jurídico tutelado con la norma penal. Santiago Mir Puig, sostiene: "…Debe distinguirse entre objeto material (u objeto de la acción) y el

Objeto Jurídico. El primero se halla constituido por la persona o cosa sobre la que ha de recaer físicamente la acción, por lo que también se conoce como "objeto de la acción". Puede coincidir con el sujeto pasivo (por ejemplo, en el homicidio o en las lesiones), pero no es preciso (ejemplo: en el delito de hurto es la cosa hurtada, mientras que el sujeto pasivo es la persona a quien se hurta) 2 …".

Fernando Velásquez, en relación a este tema, lo titula como objeto de la acción, y lo define como "… la persona o cosa material o inmaterial sobre la cual recae la acción del agente, esto es, puede tratarse de un hombre vivo o muerto, de una persona jurídica o ente colectivo, de una colectividad de personas, del ente estatal mismo, de toda cosa animada o inanimada de carácter material o no. Sin embargo, pareciera más preciso entender por tal todo aquello sobre lo cual se concreta la transgresión del bien jurídico tutelado y hacia el cual se dirige el comportamiento del agente…" 3

Como lo describe la norma el objeto material del delito es un activo. Y un activo es el conjunto de bienes tangibles o intangibles que posee una persona, esos activos generan un beneficio económico a futuro a su dueño, quien puede disfrutar abiertamente de ellos. En las transferencias no consentidas de activos, es el dinero el principal activo que buscan los delincuentes.

- **Elementos subjetivos, descriptivos y normativos del tipo.**

A) El elemento subjetivo para este tipo penal tiene que ver con el dolo, la acción de transferir deber ser dolosa, esto es, el autor debe dirigir su acción a transferir ilícitamente un activo desde un lugar a otro, utilizando para ello medios informáticos.

---

2 lección - Estructura del Tipo Penal – pág. 199, Santiago Mir Puig
3 Manual de Derecho Penal, parte General, pág. 276, Fernando Velásquez

B) El "ánimo de lucro", por su parte, es aquella intención del sujeto activo de aumentar su patrimonio o el de un tercero a costa del de su víctima, esto es lo que ocurre cuando se da esa transferencia no consentida de activos; se despoja a la víctima de su dinero, el cual pasa a engrosar el patrimonio del victimario o de un tercero, quienes en definitiva son los que se lucran del ilícito descrito en el Art. 269 J.

C) El sujeto activo debe valerse de una "manipulación informática" Y de un "artificio semejante" que sería ese engaño o habilidad que se tiene para imitar una cosa, en este caso, concretamente lo que se imita son páginas falsas de aquellas entidades públicas, privadas u organizaciones que generan confianza y respaldo en las personas y que los lleva a que sin ningún tipo de previsión abran cualquier correo electrónico a través de los cuales se instalan los programas espías en sus ordenadores.

La Tentativa: Por ser este tipo penal de resultado y conducta instantánea se presenta el fenómeno de la tentativa, sin embargo, deben existir los actos ejecutivos dirigidos a manipular el sistema informático a través del cual se pretende ejecutar esa transferencia no consentidas de activo, esto es, debe haber un ingreso al mismo de manera fraudulenta por parte del delincuente cibernético. Dicho momento fáctico es difícil de determinar, por cuanto, esas intrusiones de los ejecutores a las cuentas sin saldo disponible, o a los computadores sin información de utilidad para su beneficio, son poco probables de ser descubiertos por el titular de la cuenta o de la información personal, empresarial o secreta, dado que éstos no se percatarán de ello hasta no sufrir una afectación o patrimonial o una pérdida de su información y de sus datos, y podrían caer en casos de delitos tentados imposibles, por in idoneidad de la conducta o inexistencia del objeto material, que son punibles en Colombia.

1.4.3 Bien jurídico protegido en los delitos de Hurto Por Medios Informáticos y Transferencias no consentida de activos.

El derecho penal como herramienta de control social, está en un constante movimiento, es decir es una herramienta dinámica, pues debe ir a la par de las constantes transformaciones que se están dando dentro de la sociedad y es precisamente eso lo que ocurrió con los grandes avances tecnológicos por medio de los cuales se maneja la información y los datos dentro de la sociedad, creando esto la necesidad de expandir el derecho penal para mantener el control social en relación con el manejo de todas estas herramientas tecnológicas que pueden afectar la relación de los ciudadanos, debido a esto surgió la necesidad de crear normas como la Ley 1273 del 2009, por medio de la cual se crean nuevos tipos penales como son los artículos 269i y 269j, que protegen un nuevo bien jurídico; normas que se constituyen en expectativas de comportamiento de los ciudadanos y que al ser infringidas son estabilizadas con la imposición de una pena.

En el caso de los delitos informáticos, el derecho penal existente no alcanzaba a controlar actos reales como los que se cometen utilizando los medios informáticos, por lo que el legislador se vio en la necesidad de elaborar o crear ese nuevo bien jurídico de protección que repercute en el bienestar de la sociedad o de grupos económicos que están siendo vulnerados con dichas conductas. Fue así como se creó, el bien jurídico tutelado en los artículos 269I y 269J que son objeto de estudio, bien jurídico que es definido como “de la protección de la información y de los datos”, el cual fue ubicado y adicionado como título bis, a la parte del código que protege el patrimonio económico, es decir como un apéndice de este.

Encontramos entonces que los delitos de Hurto por Medios Informativos y de Transferencia no Consentida de Activos Art. 269I y 269J, no obstante estar ubicados dentro del bien jurídico de la protección de la información y de los datos, lo que pretenden tutelar realmente es el bien jurídico patrimonio económico, pero lo hacen de

unas de unas específicas y novedosas formas de lesión que implican el empleo de medios informáticos. Formas estas que por ser novedosas no encontraban regulación en la legislación penal.

El objetivo de este trabajo es precisamente analizar esas nuevas formas de atentar contra el patrimonio económico de las empresas y de los ciudadanos, utilizando herramientas tecnológicas que en principio fueron creadas para generar bienestar a la ciudadanía, pero que también están siendo utilizadas por personas inescrupulosas para atentar contra este bien jurídico de tan alta envergadura.

Respecto al bien jurídico tutelado en los delitos tratados en esta investigación, la C.S.J en sentencia de casación Nro. 42.724 del 11 de febrero del 2015. M.P. EYDER PATIÑO CABRERA. Sostuvo lo siguiente. "Sobre la manera de definir los bienes jurídicos tutelados, la doctrina ha reconocido que, generalmente, el interés jurídico tutelado aparece instituido en los títulos y capítulos que agrupan los delitos, pero, en veces, es el intérprete quien debe identificarlo.

> acudiendo a un procedimiento de conjugación de las expresiones literales de los rubros de los títulos y los capítulos, que forman la Parte especial, con el "sentido" de la acción descripta en un determinado tipo (…). Y no pocas veces la forma de la acción indicará que, pese a la localización del bien jurídico enunciado por este solo indirectamente se corresponde con el protegido según el tipo: por ejemplo, [en Argentina] el delito de violación (…) está inserto entre los "delitos contra la honestidad", pero de su contenido se deduce, sin esfuerzos, que lo que en realidad protege es la "libertad sexual".
>
> A veces ocurre que el tipo comprende más de un bien jurídico (p. ej. En el "secuestro" de una persona para pedir rescate (…) entran en juego los bienes jurídicos de la propiedad y de la libertad); en esos casos la tipicidad de la conducta que se examina (…) dependerá del bien jurídico preponderantemente

afectado por la conducta del agente, lo cual será materia de interpretación en cada caso particular.4

Es así como, por ejemplo, el legislador colombiano advirtió que algunas formas delincuenciales en el ámbito de la informática, que trascendían, en muchas ocasiones, las fronteras nacionales, no estaban siendo objeto del reproche punitivo requerido, pues o no estaban reguladas o permanecían subsumidas en el ámbito de protección de otras garantías, verbi gratia, la intimidad, razón por la que se dio a la tarea de "crear"5 –le hace reconocer-, la vigencia de un nuevo bien jurídico que, de manera sistemática y específica, recogiera todos aquellos comportamientos dispersos a lo largo y ancho del Estatuto Sustantivo.

De este modo, mediante la Ley 1273 de 2009 "creó" el título VII bis "De la protección de la información y de los datos" y, en él, varios tipos autónomos que tendrían por objeto evitar la lesión de este interés jurídico, como el acceso abusivo a un sistema informático, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales, por mencionar algunos; no obstante, al final del trámite legislativo menospreció las consecuencias -no inadvertidas inicialmente por cierto-, de regular dentro de este título conductas subordinadas a otros tipos básicos, como lo es el caso del reato de hurto por medios informáticos y semejantes.

Ciertamente, aunque el legislador fue consciente de la dificultad que comportaba la ubicación del bien jurídico protegido respecto de aquellas acciones antijurídicas reguladas dentro del mentado título, que de manera directa afectaban el patrimonio económico, prefirió atar, de manera antitécnica, como lo aseveró el representante de la Fiscalía, la modalidad de la acción típica prohibida –que es el hurto por medios

---

4 CREUS, Carlos. Derecho penal. Parte general. 5ª edición. Editorial Astrea. Universidad del Rosario. Buenos Aires, Bogotá. 2012. P. 194-195.
5 Así lo expresó literalmente el legislador del 2009.

informáticos- al bien jurídico amparado en el referido título VII bis, que adicionar o modificar las circunstancias modales calificantes del artículo 240 del Código Penal, como hubiera sido lo ideal.

De lo hasta aquí dicho, es posible decantar, con meridiana claridad, que pese a la ubicación sistemática del punible de hurto por medios informáticos y semejantes en el título VII bis del Código Penal, rubricado bajo la denominación de la información y los datos, este bien jurídico resulta ser, para el caso concreto -como lo concibió la exposición de motivos del Proyecto de Ley 042 Cámara-, de naturaleza meramente intermedia, pues el interés superior protegido de manera directa es el patrimonio económico, entendido como ese conjunto de derechos y obligaciones, susceptible de ser valorado en términos económicos, más concretamente, en dinero. -Subrayas y negrillas propias-.

En verdad, nadie podría dudar que el mentado ilícito tiene la virtualidad de lesionar tanto la seguridad y la confianza de las personas naturales y jurídicas en los sistemas informáticos, telemáticos, electrónicos o semejantes, con sus componentes de *software* y *hardware*, implementados por las entidades encargadas de custodiar el capital de sus usuarios, como los intereses individuales de contenido económico del titular de la cosa ajena, cuestión que ubica al tipo penal examinado en el contexto de los delitos típicamente pluriofensivos por afectar más de un interés jurídico, el descrito expresamente en la legislación penal codificada –en este caso, el título VII bis- y el que surge de manera remota, pero directa, de la realización de la acción injusta.

Sin embargo, es lo cierto que la afrenta contra el primero de los bienes reseñados –de carácter colectivo-: la información y los datos, es solamente mediata (intermedia), porque solo se vincula con el mecanismo ilícito –de naturaleza informática- de sustracción del dinero que no con el comportamiento prohibido, mientras que el ataque contra el segundo (de orden individual): el patrimonio económico, es inmediato, pues se relaciona con la conducta reprobada misma, o sea, con el desapoderamiento de la cosa

ajena en tanto mandato de prohibición final que tutela la relación de dominio o tendencia de una persona con la cosa.

A esta conclusión es fácil llegar si se examina la naturaleza subordinada y compuesta –que no autónoma- del injusto de hurto por medios informáticos respecto del tipo básico de hurto, que lo sitúa en similar lugar descriptivo que el hurto calificado -pues a su pena se remite-, y cuando se indaga el espíritu del legislador que, como se vio, a pesar del propósito general de regular actividades ilícitas estrictamente relacionadas con la afectación de los sistemas informáticos y los datos, utilizó esta oportunidad para precisar algunas de las modalidades de hurto desarrolladas para transgredir las defensas de protección informáticas.

Sobre el carácter intermedio del bien jurídico protegido en la conducta de hurto por medios informáticos y semejantes, la doctrina ha elaborado las siguientes reflexiones:

> Se trata, entonces, de los denominados bienes jurídicos intermedios, como lo entendía Tiedemann, quien señalaba como ejemplo de tales intereses el tutelado en el delito de estafa informática, que estaría constituido por el correcto procesamiento de los datos electrónicos, que es tenido como un instrumento imprescindible de la vida económica moderna, y el patrimonio económico.*6*
>
> La aceptación de este bien jurídico intermedio*7* tiene una gran incidencia en la delimitación e interpretación del injusto típico del delito de hurto por medios informáticos y semejantes. Esto porque si los delitos protectores de un bien jurídico intermedio se caracterizan frente a los simples delitos pluriofensivos de

---

6 Lecciones de derecho, 1993, p. 34 ss.
7 Luzón Peña, Curso I, 1996, 314, afirma que junto a los tipos sólo de peligro, a veces se configuran "delitos de lesión y peligro", que implican lesión de un bien jurídico y peligro para otro, como el incendio, por ejemplo.

peligro por el hecho de que para su consumación se exige la efectiva lesión de uno de los dos valores que lo conformen, el colectivo o el individual,*8* para poder calificar a aquel delito de hurto como protector de un bien jurídico intermedio hay que aceptar que la conducta típica se dirige a lesionar de manera inmediata un bien jurídico individual, al mismo tiempo que provoca dicha lesión la mediata puesta en peligro de otro valor de índole diversa a la del primero, de carácter colectivo.*9*

En el delito de hurto por medios informáticos y semejantes el bien jurídico intermedio está configurado, de un lado, por el interés en la protección del patrimonio económico, que sería el referente individual, cuya lesión permite, de otro lado, apreciar la puesta en peligro del interés general en la seguridad del tráfico de la información y los datos. Esto debido a que la lesión del patrimonio económico como bien jurídico individual está regulada de manera expresa como una exigencia típica del delito de hurto en el Código Penal colombiano; lo cual conduce a la conclusión de que el patrimonio económico sería el referente individual del bien jurídico intermedio.

Al tenerse al delito de hurto por medios informáticos y semejantes como un delito protector de valores supraindividuales, su estructura ha de consistir en que la conducta se encamina a causar la inmediata lesión de un bien jurídico de naturaleza individual (el patrimonio), y ocasiona, además la mediata y abstracta puesta en peligro de otro bien jurídico de naturaleza colectiva (el correcto funcionamiento de los sistemas de información y datos).*10*,11

---

8 Mata y Martín. Bienes jurídicos intermedios, 1997, p. 58.
9 Galán Muñoz, El fraude, 2005, p. 198.
10 Martínez-Buján Pérez, Penal General, 2007, p. 191 y ss., afirma que no obstante que en los delitos socioeconómicos el bien jurídico mediato será siempre supraindividual, el objeto jurídico mediato puede ser individual o supraindividual, del mismo modo que pueden darse delitos en los cuales si bien en primera línea se afectará a un bien jurídico de naturaleza patrimonial individual (ej. Propiedad industrial, secretos

Siendo ello así, natural es concluir, como lo hiciera la demandante y el representante del ente acusador, que el tipo penal de hurto por medios informáticos y semejantes no solo está circunscrito al ámbito de punibles contra la información y los datos, sino, esencialmente a la esfera de los lesivos del patrimonio económico, pues es el valor ético jurídico que al final resultaría atacado con la sustracción de dineros a través de mecanismos ilícitos de manipulación de los sistemas informáticos, electrónicos, telemáticos o similares, o suplantación de las personas ante los sistemas de autenticación y de autorización"

Es claro entonces según lo sostenido por la Corte Suprema de Justicia en la sentencia en mención que los delitos de Hurto Por Medios Informáticos Art. 269I y el delito de Transferencia no consentida de activos Art. 269J, son delitos que no obstante estar dentro de los delitos de la protección de la información y de los datos, realmente con ellos lo que prende el legislador es proteger el bien jurídico del patrimonio económico.

En el igual sentido se pronunció el Tribunal Superior de Medellín Sala Penal, en sentencia de segunda instancia del 27 de abril de 2017, de radicado Nro. Nro. 2014-22638. M.P. César Augusto Rengifo Cuello.

---

industriales, delito societario de administración fraudulenta), pueden proyectarse inmediatamente sobre un interés de índole supraindividual.

11 Suarez Sánchez, Alberto. El hurto por medios informáticos y semejantes a través de la utilización de tarjeta magnética falsa o ajena en cajero automático. En: Estudios de derecho penal I. Universidad de Bogotá Jorge Tadeo Lozano. Bogotá, 2010, p. 236-237.

1.4.4 Análisis entre el delito de Hurto por Medios Informáticos y Transferencia No Consentida de Activos. Art. 269I y 269J.

Art. 269I Hurto por medios informáticos y semejantes: Tipo penal en blanco, subordinado el supuesto de hecho se debe complementar con el Art. 239, solo que acto de apoderamiento debe hacerse 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. Para la consecuencia Jurídica nos remite al Art. 240. La pena será de 6 a 14. Nral. 4. Con escalonamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o con violando o superando seguridades electrónicas u otras semejantes.

De lesión: debe existir afectación patrimonial, es de resultado material, de ejecución instantánea, compuesto, es de medio determinado exige para su realización la afectación patrimonial a través de un medio informático, electrónico o telemático.
S.A: singular, simple.
S.P: persona natural o jurídica, son aquellos que padecen el desmedro económico y perjuicio en sus intereses patrimoniales.

Elementos del tipo objetivo: 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: **d.** La conducta. Consiste en superar las seguridades informáticas mediante la manipulación del sistema informático, la red de sistema electrónico, telemático u otro semejante; y **e**. Elementos normativos: los conceptos de mueble y ajena en el tipo básico, y los de seguridades informáticas, sistema informático, red de sistema electrónico y telemático.

Elementos del tipo subjetivo: El propósito de aprovechamiento. y El dolo, que puede ser directo o eventual.

La acción o conducta: No consagra la conducta reprochada, el objeto material, ni la sanción correspondiente, efectúa un reenvío normativo al tipo base de hurto (artículo 239 del C.P) y a la disposición que lo califica (Art. 240 ejusdem) para determinar la sanción imponible.

Nota: El Art. 269I, fue diseñado su contenido para evitar el apoderamiento, no sólo de dinero, sino de información privilegiada de personas, empresas o instituciones públicas o privadas, que como bien intangible posee un gran valor en el mercado.

El objeto material: Remite al 239 CP, "cosa mueble", que es aquél bien corporal (como el dinero o incorporal) Ambos bienes muebles (dinero e información), tienen valor económico.

Dispositivo amplificador del tipo: Admite La Tentativa. Por ser un delito de resultado.

Art. 269 J CP. Transferencia no consentida de activos:

Este es un tipo penal básico: Ya que se aplica sin depender de ningún otro tipo penal.

Se diferencia del Art. 269I porque este depende de los Art. 239 y 240 como se explicó en precedencia.

De lesión: Exige el daño al bien jurídicamente tutelado.

De resultado: Porque exige que se debe concretar la transferencia de activos de la cuenta de la víctima a la del victimario, sin su consentimiento.

De conducta instantánea: La acción se agota en el momento en que se da el resultado utilizando medios informáticos.

Compuesto y de medio determinado: por el número plural de acciones con las que se puede cometer el delito, transferencia no consentida a través de una manipulación informática o un artificio semejante y la utilización para ello un medio informático.

S.A: Simple, singular.

S.P: La entidad bancaria. No obstante, lo anterior, debe analizarse cada caso en concreto a fin de determinar cuál es el grado de responsabilidad que recae sobre el titular de la cuenta bancaria.

La acción: El Art. 269 J posee un verbo rector principal que es transferir, y cuatro secundarios en el inciso final, fabricar, introducir, poseer o facilitar.

El objeto material: Es un activo. Conjunto de bienes tangibles o intangibles que posee una persona. El dinero el principal activo que buscan los delincuentes.

Elementos subjetivos y normativos del tipo:

A) El dolo. El "ánimo de lucro".

B) "Manipulación informática" Y de un "artificio semejante".

La Tentativa: Por ser este tipo penal de resultado y conducta instantánea.

CAPÍTULO 2.
DESCRIPCIÓN DEL MODUS OPERANDI EN COMISIÓN DE LAS CONDUCTAS QUE ATENTAN CONTRA EL NUEVO BIEN JURÍDICO TUTELADO.

2.1 Utilización de tarjeta falsa en cajero automático.

Como es sabido muchos dispositivos electrónicos utilizan una tarjeta electrónica que hace similitud a una cedula de ciudadanía, debido a que contiene información valiosa y personal que identifica a cada propietario para ser utilizada en múltiples puntos a nivel nacional e internacional para acceder a las redes informáticas y poder disponer de los beneficios y modalidades de pago, consignaciones, transferencias que estas nos ofrecen dándonos a entender que es más seguro su utilidad que llevar en nuestras manos dinero en efectivo exponiéndonos a un riesgo mayor ante los delincuentes, pero también existe para los dueños de lo ajeno la inventiva de cómo estas tarjetas que son elaboradas de un material plástico con un dispositivo electrónico interno o banda magnética, que lleva toda nuestra información, con otros dispositivos como programas informáticos y lectores de tarjetas que pueden realizar copias idénticas para poder entrar a las terminales sin ninguna otra restricción como datafonos, cajeros electrónicos o redes bancarias por medio de páginas web y realizar todo tipo de actividades ilícitas, todo esto debido a que cuando se le extravía o se le hurta a su propietario y este no la reporta, queda vulnerable a manos de los delincuentes que como lo mencionamos anteriormente hallan la forma de descifrar todos los datos que ella almacena.

2.2 Obtención de la Tarjeta Digital.

La tarjeta llega a manos del delincuente de múltiples maneras, una es por el mismo descuido del propietario, quien la extravía o la deja expuesta para que personas inescrupulosas tengan acceso a ella y lo más grave es que muchas veces la clave de la cuenta está inscrita en el mismo plástico, lo que facilita que se acceda a la cuenta y le extraigan dinero de la misma, otra forma es cuando el usuario se deja engañar por

personas expertas que se ubican en las afueras de las entidades bancarias o en los cajeros electrónicos, quienes previamente colocan dispositivos en los cajeros para que bloqueen la tarjeta, el usuario al ver esta situación permite que estas personas lo asesoren para recuperar la tarjeta cuando en realidad le están haciendo el cambiazo y ya la clave queda gravada en el dispositivo que había sido incorporado con anterioridad en el cajero.

2.3 Duplicación de Tarjeta.

Existen diversas formas de clonarla tarjetas, una manera es cuando el encargado de administrar uno de estos puntos de servicio le dice al usuario que pase la tarjeta por la ranura lectora y que luego digite su clave, luego de unos momentos le dice que hay una falla que vuelva a pasarla y que digite nuevamente su clave, para reiterarle que sigue bloqueada, que por favor se la facilite para verificar en su sistema, pasando la tarjeta a través de una cámara conectada a un software de lectura de datos de este sistema, luego le dice que por favor le dé su número de ingreso para cotejar que si sea la correcta y el usuario ingenuamente se la da, devolviendo su tarjeta pero sin imaginar que han quedado con todos sus datos, después de esto se procede a elaborar la tarjeta plástica que realizan con una impresora de carnets que comercializa en el mercado, para luego proceder a retirar, transferir. Etc. con absoluta tranquilidad consumándose con ello el delito de hurto con poca probabilidad de captura.

2.4 El Phishing.

> El phishing se refiere al envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía etc.) pero que en realidad pretenden manipular al receptor para robar información confidencial. Por eso siempre es recomendable acceder a las páginas web escribiendo la dirección directamente en el navegador. (Panda Security. 2021)

Como sabemos la internet está compuesta por infinidad de navegadores como de páginas web cada una con características propias, pero diferentes de acuerdo a su función o actividad realizadora, hay personas que teniendo poco conocimiento sobre el manejo y riesgo de estas páginas, su mínimo cuidado en la utilización los llevan a caer en manos de quienes los estafaran o hurtaran, ya que es ahí donde se aprovechan los perpetradores para crear paginas similares con plataformas idénticas a aquellas que son las páginas o web legales prestadoras de los servicios a los cuales se ingresan para estas actividades como por ejemplo páginas web de las entidades bancarias, supermercados, puntos de pago etc. no percatándonos de esto o estableciendo una verificación del ingreso si es una página segura y confiable o no, antes de empezar a utilizarla, ingresando todos los datos personales proporcionando sin amenaza y sin violencia.

Para sacar beneficio haciendo de las suyas por medio de los retiros o transferencia hechas con este tipo de método, siendo así como los creadores de estos sitios las diseñan para redireccionar sin que se puedan diferenciar de lugar confiable, las prestadoras de servicio y demás entidades de seguridad nos advierten de utilizar equipos de nuestra propiedad, no utilizar equipos al servicio público, como salas de internet o computadoras que no sean de nuestra propiedad, para no dejar guardadas claves y datos de seguridad en ellas y poder ser más fácil hallar el lugar de donde se efectuó el hecho delictivo debido a que las direcciones utilizadas en los navegadores son utilizadas desde una plataforma VPN, la cual modifica constantemente las direcciones IP, dando como ejemplo: de que se haya utilizado una computadora en Medellín y al instante arrojara que fue desde Bogotá, esto hace para los entes investigadores dificultosa la triangulación y ubicación del sujeto activo. .

2.5 Software Espía – Spyware.

> Estos programas generalmente roban dicha información con fines publicitarios o para comerciar con ella. El spyware es una herramienta

> creada por hackers que se vende en el mercado negro para que otros delincuentes puedan utilizarla para cometer fraudes y otros delitos cibernéticos.
>
> La información que persigue el spyware es muy variada: identificadores de cuentas de correo electrónico, direcciones IP y DNS del ordenador, hábitos de navegación de los usuarios de Internet, etc. (Panda Security. 2021).

Esta modalidad es basada en hacer caer al usuario por algún método como correo electrónico, promociones de ventas, ofertas llamativas que hacen que algún curioso haga el click, y al ingresar a ellas se instala un programa llamado espía o espejo, cuya función es permitir a quien crea este tipo de software tener información de las actividades tanto de páginas como de transacciones, compras que se hayan realizado por medio de su navegar en la internet, dándose cuenta de cada uno de los por menores que consulto, enviando sin su conocimiento al perpetrador un registro completo de cada actividad realizada, teniendo la certeza de que algún usuario mostrara, o copiara información personal que le servirá para su actuar delictivo en las redes realizando una suplantación, Pues por medio de estas incursiones, entramos a correos electrónicos, ingresando nuestra clave, al igual que alguna plataforma para realizar una transacción bancaria.

2.6 Ransomware.

> El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito. (Malwarebytes. 2021).

Este tipo delictivo funciona cuando un usuario descarga o ejecuta al archivo cifrado o no conocido de una fuente confiable el cual instantáneamente activa un archivo ejecutable, el cual codifica la mayoría de sus archivos personales, no permitiéndole abrirlos o utilizarlos de la manera habitual, apareciendo un archivo en cada carpeta con un mensaje que nosotros lo tomamos como extorsivo ya que hace referencia diciendo que no se preocupe, que sus archivos están protegidos y codificados con un software de nivel 1, que si desea recuperarlos debe dirigirse a un correo electrónico que aparece en el informe y una secuencia de números los cuales son la identificación para ellos.

Te expresan de antemano que hay un costo básico para el inicio, que si tienes interés te comuniques para enviarte la prueba con alguno de tus archivos, para luego decir que la recuperación de tus archivos de acuerdo con tu necesidad e importancia tiene un costo mucho más elevado o que puedes pagarlo por cuotas y a medida que pagues te enviaran la información.

CAPÍTULO 3.
ESTRATEGIAS ORIENTADAS A EVITAR SER VÍCTIMA DEL DELITO DE HURTO A TRAVÉS DE MEDIOS INFORMÁTICOS Y TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

Para nadie es un secreto que en Colombia la forma de prevenir, controlar y reprimir todas estas nuevas modalidades delictivas es a través de normas penales, creyendo que la mera letra inscrita en un código penal será suficiente para evitar que los delincuentes sigan delinquiendo, cuando la realidad es otra, pues los altos grados de impunidad existentes en Colombia, antes de disuadir al delincuente para que no siga delinquiendo por el contrario son una invitación a delinquir, pues de cada 100 cien delitos que se cometen en nuestro país, más del 90 por ciento quedan en la impunidad, ahora bien respecto a este nuevo bien jurídico creado por la Ley 1273 (2009), la situación es mucho más gravosa, pues el modus operandi de los delincuentes es más sofisticado, pues las

herramientas utilizadas para la consumación de los delitos objeto de esta investigación son precisamente medios tecnológicos que requieren de unos conocimientos y experiencia especializados, lo que quiere decir que este tipo de conductas solo puede ser investigada por personal altamente capacitado en el manejo de todas esas herramientas tecnológicas y se debe contar con equipos de última generación que permitan detectar de forma oportuna el accionar delincuencial y el problema está precisamente en que nuestros entes investigativos tanto de la fiscalía como de la policía no cuentan con personal suficiente que esté capacitado en el manejo de esas nuevas tecnologías y tampoco se cuentan con los equipos idóneos que permitan combatir este nuevo flagelo.

Antes este oscuro panorama no queda otra que tomar medidas preventivas de manera personal para evitar ser víctima de estos delincuentes cibernéticos, pues si esperamos a que sean las autoridades las que nos protejan de los mismos no vamos a evitar caer en manos de ellos.

3.1 ¿Qué hacer para evitar que nos clonen nuestras tarjetas sean estas débito y crédito?

Antes de contestar este interrogante, es preciso recordar que la clonación de tarjetas se presenta cuando se copia sin autorización la banda magnética de la tarjeta y se obtiene el código o clave a través de una herramienta tecnológica externa.

- **Sugerencias:**

Se recomienda a los usuarios; hacer cambios constantes de las claves, hacer las trasferencias en lugares seguros, la tarjeta es de uso personal, jamás se debe prestar incluso a familiares o amigos porque estos de buena fe la pueden descuidar y ahí es donde pueden aprovechar los delincuentes para clonar la tarjeta y con ella hacer retiros o transferencias, cuando se vaya a usar la tarjeta jamás permitir que personas extrañas se encuentren cerca o se le acerquen ofreciendo ayuda o asesoría para su manejo, si se presenta algún problema con la tarjeta se debe informar de manera inmediata al banco,

bloquearla pero jamás se debe permitir que personas extrañas tengan acceso a la tarjeta con el pretexto de solucionar el problema, por ningún motivo se debe escribir la clave en la misma tarjeta, pues en caso de pérdida esta puede ser usada por los delincuentes lo mejor es memorizarla o en caso de que no sea capaz de memorizarla anotarla en un lugar donde no sea observada por personas extrañas, cuando cambie de clave evite poner datos muy básicos que permitan que los delincuentes los adivinen, evite poner como clave la fecha de su nacimiento, los años de sus hijos en fin datos que fácilmente puedan ser descifrados por los delincuentes.

3.2 ¿Cómo evitar que nos cambien nuestras tarjetas?

Debemos tener en cuenta que los delincuentes no descansan siempre están al asecho, ellos son personas muy habilidosas, expertas en lo que hacen, siempre están pendientes de nuestros errores para aprovecharse de ellos y es precisamente como se presente al cambiazo de las tarjetas, los lugares donde más se presenta esta modalidad es precisamente donde más se utilizan las tarjetas para hacer retiros, es decir en los cajeros electrónicos, los delincuentes ponen algún dispositivo en los cajeros para que estos retengan o la tarjeta o el dinero que se va a retirar cuando usted hace la transacción, usted como usuaria se desespera al ver que no puede retirar el dinero y es ahí donde aprovechan los bandidos para acercarse y ofrecer su ayuda, le piden su tarjeta o como saben cómo sacarla en caso de que esta esté bloqueada tiene acceso a la misma y ahí es donde aprovechaban para entregarnos una tarjeta diferente, y como previamente instalaron una cámara o un dispositivo que les permitió tener acceso a su clave, aprovechan una vez usted cree que solucionó el problema para vaciarle sus cuentas sea haciendo retiros o haciendo transferencia.

- **Sugerencias.**

Las recomendaciones frente a este accionar delincuencial básicamente son las mismas que las relacionados en el acápite anterior, no obstante se itera que lo más

importante para evitar ser víctima de esta modalidad delincuencial es tener mucho cuidado con el manejo de la tarjeta, recordar que esta es personal, que nadie distinto a usted debe tener acceso a ella o a la clave con ella se maneja, estar muy alertas cuando se vaya hacer retiros o trasferencias en los cajeros, si es posible hacer uso de las tarjetas solo en los cajeros que se encuentran al interior de las entidades bancarias, pero en caso de no ser posible, buscar lugares seguros como centros comerciales o molles y cuando se vaya hacer uso de estos cajeros observar previamente que no hayan personas sospechosas alrededor, en fin ser supremamente cautos y cuidadosos para evitar caer en manos de la delincuencia, recuerde que lo que usted no haga por usted mismo, difícilmente otro lo hará incluso las autoridades que como ya se dijo poco hacen para evitar que estos hechos ocurran.

3.3 ¿Cómo evitar ser víctima del Phishing?

Recordemos que esta modalidad delictiva cosiste en que se nos envía un correo electrónico de una supuesta entidad bancaria, en ese correo se nos indica hacer click en un enlace con el fin de actualizar nuestros datos, cuando realmente son hackers que lo que están buscando es tener acceso a nuestros datos con la amenaza de cancelarnos las cuentas, cuando se obtienen los datos ya los delincuentes tienen vía libre para acceder a nuestras cuentas y desocuparlas sin que nosotros nos percatemos.

- **Sugerencias.**

Teniendo en cuenta el modus operandi utilizado por los delincuentes en este tipo de modalidad, la recomendación más importante debe ser la de desconfiar de correos que nos llegan de las entidades bancarias con las que manejamos cuentas y especialmente cuando se trata de actualizar datos, antes de entrar a estas páginas, confirmar con el banco si ese correo fue enviado por ellos, la actitud que se debe tener por parte de los usuarios es de desconfianza frente a todo lo que tenga que ver con entidades bancarias, estar a la defensiva, pensar siempre que se trata de un fraude y esto nos permitirá antes de ingresar

a estas páginas verificar la autenticidad de las mismas, recuerden que los delincuentes están siempre pendientes de algún descuido nuestro para aprovecharse del mismo y hacer de las suyas, nuestra seguridad bancaria depende de nosotros mismos.

3.4 ¿Cómo evitar se víctima del Software espía?

Como su misma palabra lo indica, esta modalidad delictiva consiste en la instalación de programas en un sistema sin autorización, cuando se instala este programa en nuestro computador, el delincuente va a tener acceso no solo a toda la información sino que se va a enterar de todos los movimientos que yo haga con mi computador, todo esto se hace desde otro computador donde está instalado el bandido, por eso se llama espía, porque actúa como tal, le informa al delincuente todos mis movimientos y le da todos mis datos contenidos en mi computador.

Para evitar ser víctima de esta modalidad, lo más importante es revisar constantemente nuestro computador, si es posible instalar antivirus actualizados, utilizar fuentes confiables de software, evitar bajar programas que no están registrados, evitar que su equipo sea manipulado por terceras personas, no meterse a redes públicas o de acceso público, hacer caso omiso a promociones relacionadas con programas de computación no acceder a mensajes de correos que usted no identifica. Verificar el estado de los antivirus cuando utilice su computador u otro equipo con el que pretenda trabajar.

3.5 Enfoque cuantitativo de la comisión de los delitos descritos en los Arts. 269i Y 269j dentro del territorio nacional.

Para poder hacer un análisis estadístico de la comisión de los delitos objeto de estudio dentro del territorio nacional, acudimos a la información que manejan las autoridades encargadas de combatir este flagelo para ver cómo ha sido el comportamiento delincuencial en estos asuntos y cuál ha sido la eficacia de las medidas tomadas por estas instituciones para combatir este tipo de delincuencia.

De acuerdo con la información obtenida de las plataformas que manejan la fiscalía y la policía nacional SIJIN - DIJIN, uno de los delitos de mayor ocurrencia es la suplantación en sitios web y el robo de datos.

Con la llegada del COVID nos volvimos ms virtuales, pues debido a nuestro encierro todo se manejaba por la internet, la educación se volvió virtual, ya se empezó hablar de teletrabajo, el acceso a comercio para satisfacer nuestras necesidades básicas se hacía por internet, en fin la internet se volvió una herramienta de primera necesidad para poder desarrollar la gran mayoría de actividades sociales, toda esta dependía del internet según la fiscalía hizo que se dispararan las cifras de los delitos cibernéticos, pues tan solo en el primer trimestre del 2020, este tipo de delitos se incrementaron en un 37% en comparación con el año anterior.

En ese mismo lapso, se registraron 7.082 denuncias, lo cual representó un incremento de 27%, según datos de la Cámara Colombiana de Informática y Telecomunicaciones. A pesar de la reactivación económica y el fin de la cuarentena generalizada, para noviembre de 2020 hubo un aumento de 83% de los delitos cometidos por medios informáticos, pues se pasó de 21.107 en 2019 a 36.834 delitos.

Delitos como la estafa por medios informáticos, los robos de información de entidades bancarias y la suplantación personal en redes sociales son el pan de cada día de las entidades bancarias. Es que si se hace un análisis serio del motivo del porqué del incremento de los delitos cibernéticos la respuesta es apenas obvia, a mayor uso de estas herramientas tecnológicas relacionadas con el internet, mayor es la exposición al actuar de las personas dedicados a esta modalidad delictiva. Otro problema adicional que debe afrontar la victima de estos delitos, es que debe acudir a la Superintendencia Financiera, para que esta determine la responsabilidad de la entidad bancaria y la de la persona que realizó la actividad fraudulenta.

Aunado a lo anterior, también se presentó un incremento en la suplantación de entidades oficiales, dentro de las cuales se destacan la Dian y el Ministerio de Educación todo esto a través de correos maliciosos que hurtan información. Frente a este tipo de conductas es importante tener en cuenta que ninguna de estas entidades suele comunicarse de manera directa con los usuarios.

Lo que se recomienda frente a este tipo de conductas es denunciar de manera oportuna a la fiscalía o a la policía de manera virtual para que estas a su vez procedan a dar con el paradero de estos delincuentes. Respecto a esta sugerencia es importante precisar que, debido al gran número de conductas delictivas de esta índole, se presentan congestiones en estas páginas web que dificultan interponer las denuncias y fuera de eso cuando se accede a las mismas su manejo se convierte tortuoso debido al mal uso por parte de la ciudadanía de estas redes.

Según información suministrada por la Dijín, los delitos informáticos que se denuncia son de gran variedad: Suplantación en sitios web 4.776 casos durante 2020, con una variación de 435% si se compara con los 892 casos del año inmediatamente anterior, extracción de datos y registros personales también tuvo una gran incidencia en las denuncias hechas durante el año pasado, pues se presentaron 2.663 casos, un incremento importante si se consideran los 563 casos de 2019. Con una variación de 359%, la suplantación de identidad por correo electrónico fue otra modalidad con un alto número de casos, presentando 1.527 durante 2020 y tan solo 333 en 2019.

En cuanto a las modalidades de hurto o fraude electrónico que tuvieron un descenso destacan: los cajeros automáticos tuvieron una variación de -21% con 2.315 casos durante 2020. El acceso remoto no autorizado también sufrió una caída de 37% con 1.287 casos. Y, por último, los ataques por medio de datafonos presentaron una disminución de 39% con 196 casos en 2020, mientras que en 2019 hubo 323. (ver figura 1)

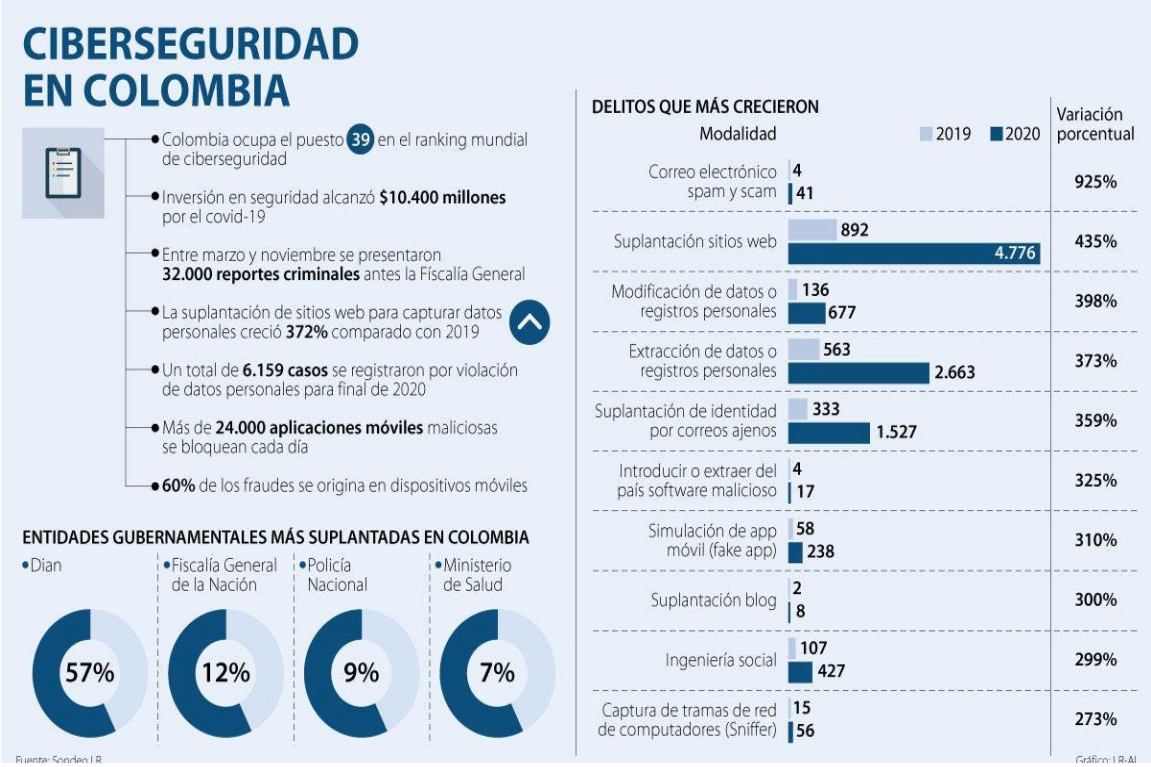

figura 1 Asuntos legales. (2020).

3.6 Los ataques cibernéticos están en auge, la comisión de este tipo de conducta se incrementó en un 30% durante el primer semestre de este año según la Fiscalía.

El reporte arrojó que Bogotá tiene la mayor afectación con 8.355 casos. Le sigue la capital de Antioquia, Medellín, con 1.664 casos La fiscalía general de la Nación afirmó que las cifras de ataques cibernéticos en Colombia aumentaron 30%, con corte a junio de este año. En los primeros seis meses de 2021 se registró un total de 23.000 incidentes criminales, lo cual es una variación significativamente alta si se tienen en cuenta los 18.290 casos en 2020. Por ciudades, el reporte arrojó que Bogotá tiene la mayor afectación con 8.355 casos. Le sigue la capital de Antioquia, Medellín, con 1.664 casos; por último, se encuentra Cali, que, según el reporte de la Fiscalía, ha presentado 1.569 incidentes. (ver figura 2)

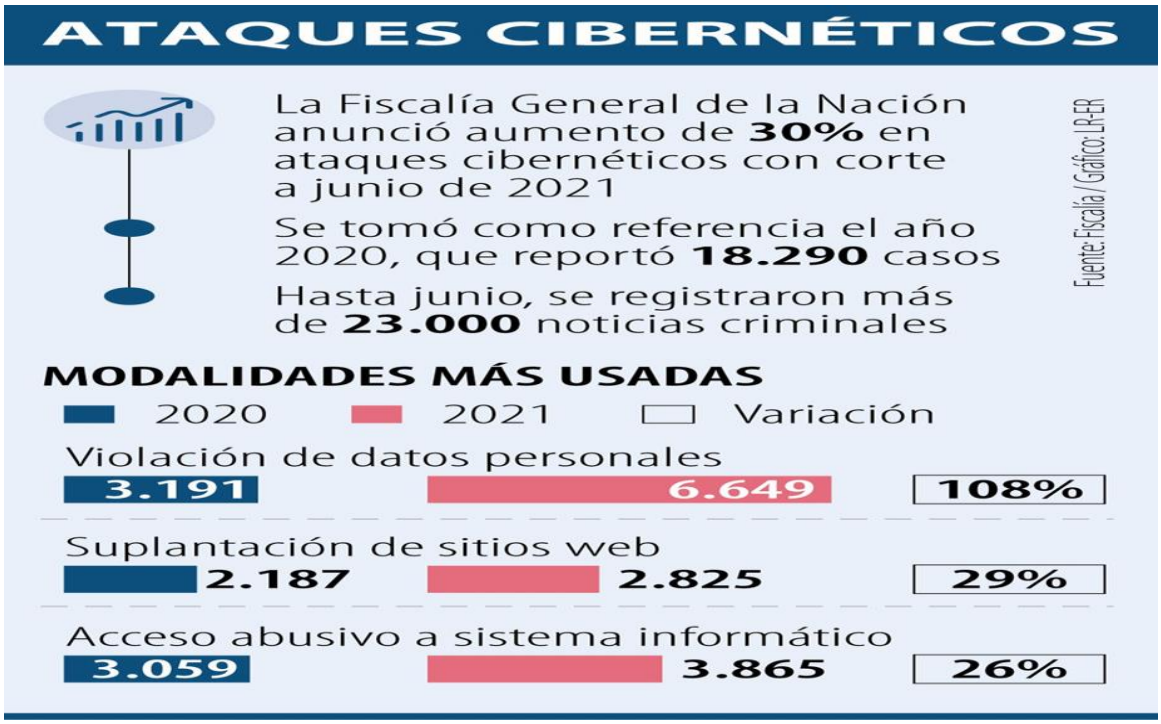

figura 2 Asuntos legales. (2020).

Según esta información se puede concluir que las modalidades más usadas por los ciberdelincuentes durante el primer semestre son las siguientes: Violación de datos personales se ubica en primer lugar, se incrementó de 108% en 2021 con 6.649 denuncias, frente a 3.191 registradas el año pasado.

En segundo lugar, está la suplantación de sitios web, que reportó una variación de 29% en 2021 con 2.825 denuncias en el año. El año pasado se presentaron 2.187. Esta estadística ratifica lo que se viene sosteniendo por parte de autoridades y expertos en la materia, en el entendido de que el incremento en la comisión de este tipo de conductas más que por el coronavirus se debe a la nueva cultura social en relación con el uso más frecuente de redes y del internet en la interacción ciudadana.

3.7 Los Delitos Informáticos Vistos como Otra Pandemia más al Lado del Coronavirus.

Cuando se hace un análisis del impacto que han tenido los delitos informáticos en todo el territorio nacional, las estadísticas muestran que el número de casos se incrementó en un 59%, frente a esta nueva realidad, los expertos hablan ya es recomendaciones dirigidas a evitar ser víctimas de los ciberdelincuentes, esto en gran medida por la incapacidad del Estado para frenar este nuevo modus operandi delincuencial.

Las cifras manejadas por la policía coinciden con las de la fiscalía pues las cifras más recientes del Centro Cibernético de la Policía Nacional respecto a los delitos informáticos establecen un incremento del 59% en el primer semestre, en comparación con el año anterior y la explicación de este incremento lo encuentran en que las personas están dando un mayor uso al internet y a las redes sociales, impulsado especialmente por el confinamiento debido al COVID -19.

Quiere decir lo anterior que entre enero y junio del 2021 se interpusieron 17.211 denuncias, 6.340 más que en el primer semestre del año 2019 cuando no había confinamiento. También se presentaron 2.103 casos de suplantación de sitios web, un delito que creció en 364%.

Teniendo en cuenta la situación de nuestro país en relación con los ciberdelitos, una reciente investigación de TransUnion, donde se tuvo en cuenta nuestro país, determino que el ‘phishing’ es el principal esquema de fraude digital en todo el mundo. En esa investigación, el 27% de los consumidores manifestaron haber sido víctimas de este tipo de estafa con temas relacionados con la pandemia.

El 21% de los encuestados manifestaron haber sido víctima de estafas de terceros originados mediante enlaces desde sitios web legítimos de comercio en línea, mientras

que un 19% indicó que fue estafado a través de supuestos fondos de recaudación para caridad.

Siguiendo con esta información estadística del manejo de los delitos informáticos en el territorio nacional se pudo establecer que en el 2020 se interpusieron más de 40.700 denuncias relacionadas con ese tipo de delitos, esto es más de 111 cada día y cerca de 5 por hora. Lo triste del asunto es que frente a este arsenal de denuncias las autoridades de policía solo capturaron 1.130 personas vinculadas con la ciberdelincuencia, 349 fueron por hurto por medios electrónicos.

Este oscuro panorama empeora cuando se presentan las cifras del estudio realizado por la central de riesgo TransUnion donde puso al descubierto que el 30 por ciento de las personas que usan el internet y las redes en Colombia fueron víctimas de fraude digital, nueve puntos porcentuales por encima del registro del año anterior, siendo Bogotá, Pereira y Cúcuta las ciudades con mayores ataques fraudulentos.

Según este estudio de los grupos generacionales, el más afectado con este fenómeno digital en tiempos de pandemia es la generación X (nacida entre 1965 y 1979) con 35 por ciento; seguido por los millennials (nacidos entre 1980 y 1994), al que se han dirigido el 32 por ciento de los ataques.

Asobancaria por su parte no tiene una cifra consolidada de cuánto dinero han perdido las personas y las propias entidades en el último año por cuenta del accionar de los ciberdelincuentes, pero sí advierte que, por cada 100.000 pesos transados en el sistema financiero en general, 4,9 pesos fueron reclamaciones por fraude en el 2020, indicador que fue de 4,3 en el 2019. Solo en los canales digitales, ese indicador pasó, en el mismo periodo, de 2,7 a 3,5 pesos por cada 100.000 pesos transados.

- **Respecto a la ciberdelincuencia, ¿cuáles delitos son los más denunciados?**

Los tipos penales que más se denunciaron fueron: La suplantación en sitios web para capturar datos personales (346%), la interceptación de datos informáticos (204%), la violación de datos personales (151%), la obstaculización ilegítima de sistemas informáticos (123%) y el daño informático (113%).

- **¿Cuál ha sido la respuesta institucional respecto a estas denuncias?**

La realidad es que no hay una correlación entre los delitos denunciados y los delitos esclarecidos, las cifras de impunidad siguen en alza. Con corte al 17 de noviembre se habían realizado 135 capturas por estos delitos. Esta cifra, en comparación con las 231 capturas realizadas en el mismo periodo de 2019, representa una caída de 42%.

Lo anterior, explicó el Mayor Ramírez, obedece a dos factores, que no solo se presentaron en Colombia sino también a nivel global. “En primer lugar, la pandemia ocasionó traumatismos en muchos sectores, entre ellos el judicial y el carcelario, lo que ha generado una dilatación en el desarrollo de actividades en contra de los cibercriminales. En segundo lugar, la complejidad en la investigación de los delitos informáticos, ya que el anonimato en un factor que en muchos casos está presente a favor de los cibercriminales.”

- **¿Qué efectos tiene la sanción de los tipos penales objeto de investigación en relación a la prevención general?**

Dentro de los delitos informáticos creados por la Ley 1273 (2009) y adicionados a la Ley 599 (2000), los de mayor ocurrencia son, el hurto por medios electrónicos y la suplantación de personas y entidades. Según la Dijín, en el segundo semestre de 2020 se registraron 18.255 delitos por canales informáticos. Esta cifra representa casi el doble de los casos reportados en 2019, los cuales llegaron a 9.300.

Según Colombia Fintech los delitos informáticos se han incrementado en un 409% esto producto precisamente del confinamiento como consecuencia del covid-19, según esta investigación los más afectados con este accionar delincuencial son los micro y macro empresarios y personas naturales, esto se debe principalmente a los fraudes y a la suplantación de identidad que se hace a través de canales digitales. (ver figura 3)

Asuntos legales (2020). Siguiendo con este análisis estadístico se tiene que los ciberdelitos de mayor ocurrencia durante el presente son; Hurto por medios informáticos y semejantes con 11.372 casos, violación de datos personales con 8.940 casos y acceso abusivo a un sistema informático con 5.477 casos. Así lo explicó el teniente coronel Julián Ricardo Buitrago, jefe del Centro Cibernético de la Policía.

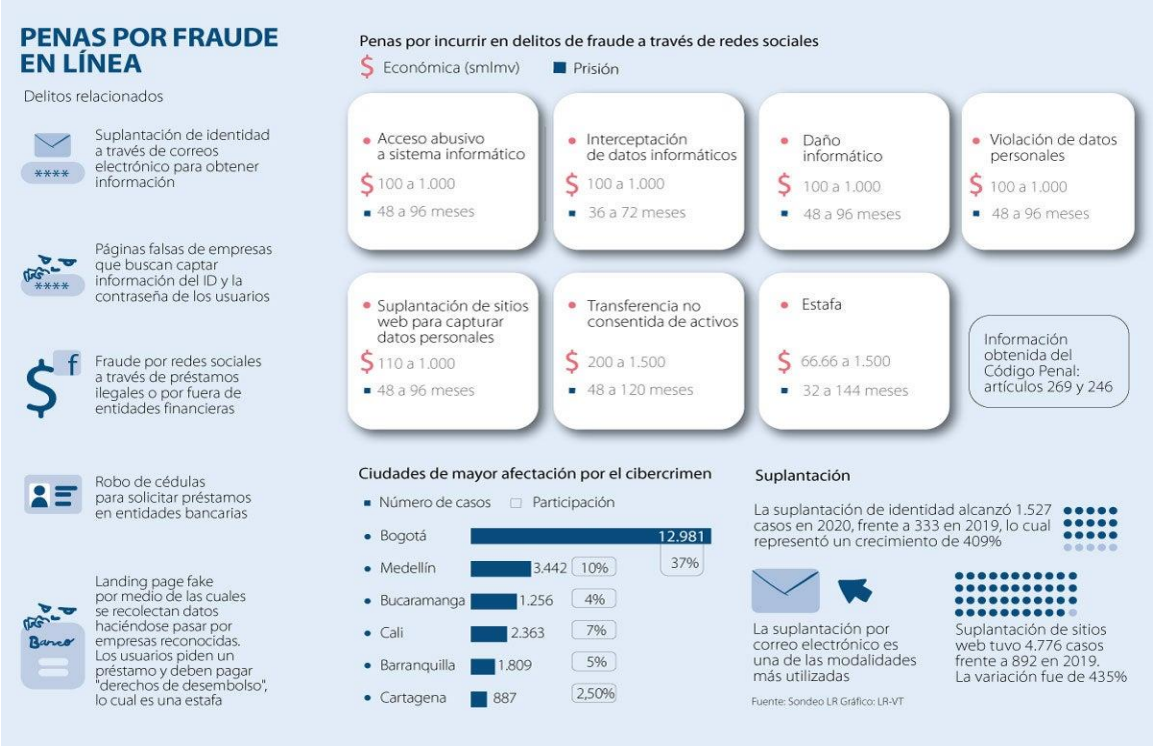

figura 3 Asuntos legales. (2020).

Conclusiones:

1.- El bien jurídicamente tutelado en los delitos de Hurto por Medios Informáticos y Traslado no consentido de activos. Art. 269I y 269J es el patrimonio económico. Así estos hagan parte del bien jurídico de la protección de la información y de los datos. Título VII Bis.

2.- En la comisión de estos dos delitos siempre se utilizan métodos y herramientas tecnológicas para ingresar a través de su punto neurálgico que son las redes interconectadas.

3.- En el modus operandi de estos dos delitos siempre se identifica la participación de una pluralidad de personas ya sea en calidad de autores o calidad de participes que se conciertan para ello.

4.- Estos tipos penales no admiten culpa.

5.- La comisión de estos dos delitos está en apogeo dentro y fuera del país, generando detrimento económico a personas naturales o jurídicas que muchas veces no se atreven a denunciar por la complejidad en la forma como ocurren y por la sofisticación de los instrumentos que se usan para su comisión aunado al descuido por parte de las víctimas en el uso de las redes y medios informáticos.

6.- Generar mecanismos de seguridad en estas plataformas, protegiendo la información personal y proporcionando un sistema de seguridad para los usuarios al ingreso a estas plataformas. Educando de manera más eficiente al usuario para con esto evitar que sea víctima de los ciberdelitos.

7.- En esta investigación se pudo evidenciar que en nuestro país las personas o entidades encargadas de prevenir este tipo de conductas, no cuentan con las herramientas o material necesario para el análisis interpretación y la forma adecuada para la obtención

completa de todos aquellos elementos probatorios y poder juzgar de manera eficiente estos comportamientos delincuenciales.

8.- Con fundamento a lo investigado y analizado en este trabajo, consideramos que no era necesario la creación de estos tipos penales, toda vez que en nuestra codificación penal existían normas que, a través de otros tipos penales existentes podrían ser tomados en cuenta como referencia.

9.- El Art. 269J. a nuestro modo de apreciar constituye un verdadero tipo penal de Estafa, aunque sin ningún tipo de contacto directo con la víctima, debido a que todo ocurre a través de la red sin haber una comunicación directa con el ente afectado y el perpetrador de la acción, y consideramos que esta modalidad sí es un verdadero delito informático pues todos sus elementos normativos y descriptivos, así como los supuestos fácticos consultados lo demuestran.

10.- Este tipo de conductas son difíciles de investigar debido a la forma como se cometen, a la falta de personal debidamente capacitado para tal fin, a la falta de herramientas o instrumentos tecnológicos que permitan detectar la forma como ocurren estas conductas, todo esto genera dificultades a la hora de obtener material probatorio que permita enjuiciar a los responsables.

11.- Los cambios que se han dado durante los últimos años en cuanto a los avances tecnológicos han hecho que estos se globalicen trayendo para la humanidad con su aplicabilidad avances a pasos agigantados, generando grades ventajas al diario vivir de la sociedad, pero también se debe tener claro que cuando estos avances tecnológicos son utilizados para a través de ellos cometer conductas delictivas ya dejan de ser ventajas y se convierten en un problema de difícil solución y por eso la necesidad de generar conciencia frente al buen manejo de estas tecnologías tendientes a impedir ser víctimas de la delincuencia especializada en este accionar.

12.- Los delitos informáticos de mayor ocurrencia son: el cambiazo de tarjeta, la clonación de tarjetas, el phishing, el Software espía – Spyware, y el Key Logger.

Referencias.

- CSJ, CORTE SUPREMA DE JUSTICIA. SALA DE CASACION PENAL (2015). Sentencia SP1245-2015. M. P. Eyder Patiño Cabrera. https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf

- CSJ, CORTE SUPREMA DE JUSTICIA. SALA DE CASACION PENAL (2013). Sentencia Rad. 40830. M. P. Gustavo Enrique Malo Fernández. https://vlex.com.co/vid/-440201698.

- CSJ, CORTE SUPREMA DE JUSTICIA. SALA DE CASACION PENAL (1999). Sentencia 10644. M. P. Carlos Augusto Gálvez Argote. https://xperta.legis.co/visor/jurcol/jurcol_759920419445f034e0430a010151f034

- CSJ, CORTE SUPREMA DE JUSTICIA. SALA DE CASACION PENAL (2005). Sentencia 21558. M. P. Yesid Ramírez Bastidas. https://www.redjurista.com/Documents/corte_suprema_de_justicia,_sala_de_casacion_penal_e._no._21558_de_2005.aspx#/

- CSJ, CORTE SUPREMA DE JUSTICIA. SALA DE CASACION PENAL (2019). Sentencia 45272. M. P. EUGENIO FERNÁNDEZ CARLIER. https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1dic2019/SP2288-2019(45272).PDF

- CSJ, CORTE SUPREMA DE JUSTICIA. SALA DE CASACION PENAL (2005). Sentencia 21474. M. P. Marina Pulido de Barón. https://vlex.com.co/tags/sentencia-21474-enero-26-2005-227707

- CSJ, CORTE SUPREMA DE JUSTICIA. SALA DE CASACION PENAL (2015). Sentencia 42724. M. P. Eyder Patiño Cabrera. https://www.ambitojuridico.com/noticias/penal/penal/reparacion-de-hurto-por-medios-informaticos-da-lugar-rebaja-de-pena

- CSJ, CORTE SUPREMA DE JUSTICIA. SALA DE CASACION PENAL (2015). Sentencia SP1245-2015. M. P. Eyder Patiño Cabrera. https://vlex.com.co/vid/562269070

- ACUARIO DEL PINO. S. (2010). Delitos Informáticos, Generalidades. Obtenido de Acuario del Pino Santiago.

- ALDAMA-BAQUEDANO. C. (1993). Los medios informáticos. Poder Judicial (30), 9-26.

- BECERRA GALLARDO, N. C., Botello Gómez, Nerys & Rincón Rodríguez, M. M. (2011).

- BELTRAMONE. G.; Herrera-Bravo, R. & Zabale, E. (1998). Nociones básicas sobre los delitos informáticos. http://rodolfoherrera.galeon.com/delitos.pdf

- BUENO ARUS. F. (1994). “El delito informático”, Actualidad Informática Aranzadi Nº 11, abril.

- CAMACHO LOSA. L. (1987). Delito Informático. Madrid: Gráficas Cóndor.

- CARRACA. F. (s/a). Teoría de la amotio o remoción. En: Inseguridad en Bosa. http://hurtoenbosa.blogspot.com.co/2011/11/marco-teorico.html

- CARRASCO HERNANDEZ J.M. (s/a). Robo en General. En: Inseguridad en Bosá. http://hurtoenbosa.blogspot.com.co/2011/11/marco-teorico.html

- CASTILLO. J. L. Blanco Parra, B., y Pérez Flórez, R (2010). La protección de la información y los datos como delito informático en Colombia: sanciones penales.

- CASTRO OSPINA. S. J. (2002). La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano. Universidad Externado de Colombia.

- DANE. Departamento Nacional de Planeación. (2011). Conpes 3701. Lineamientos de política para ciberseguridad y ciberdefensa.

- CONSTITUCION POLITICA. (1991). http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

- CONGRESO DE COLOMBIA. (2007). Proyecto de Ley No. 042. “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”. https://vlex.com.co/vid/informe-ponencia-debate-ca-mara-senado-451332546

- CONGRESO DE COLOMBIA. (2007). Gaceta del Congreso No. 355 del 30 de julio. https://vlex.com.co/vid/gaceta-congreso-30-07-766870417.

- CONGRESO DE COLOMBIA. (2007). Proyecto de Ley No. 123. “por medio de la cual se adopta el Código de Ética de los técnicos electricistas y se dictan otras disposiciones”. https://vlex.com.co/vid/proyecto-ley-senado-451457682

- CONGRESO DE COLOMBIA. (2007). Gaceta del Congreso No. 455 del 17 de septiembre. http://svrpubindc.imprenta.gov.co/senado/.

- CONGRESO DE COLOMBIA. (2007). Gaceta del Congreso No. 528 del 18 de octubre. http://svrpubindc.imprenta.gov.co/senado/.

- CONGRESO DE COLOMBIA. (2008). Gaceta del Congreso No. 275 del 22 de mayo. http://svrpubindc.imprenta.gov.co/senado/.

- CONGRESO DE COLOMBIA. (2009). Gaceta del Congreso No. 93 del 26 de febrero. http://svrpubindc.imprenta.gov.co/senado/.

- CONGRESO DE COLOMBIA. (2008). Gaceta del Congreso No. 953 del 19 de diciembre. http://svrpubindc.imprenta.gov.co/senado/.

- CONGRESO DE COLOMBIA. (2000). Ley No. 599. “Por la cual se expide el Código Penal”. Diario Oficial No. 44.097 de 24 de julio de 2000. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

- CONGRESO DE COLOMBIA. (2009). Ley No. 1273. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.”. Diario Oficial No. 47.223 de 5 de enero de 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- CONSEJO EUROPEO. (2001). Convenio sobre la Ciberdelincuencia. Budapest. https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

- CUERVO A. J. (1999). Delitos Informáticos: Protección Penal de la Intimidad, Revista Electrónica de Derecho Informático, No. 6, enero. http://www.derecho.org

- DAVARA. M. Á. (2002). Fact Book del Comercio Electrónico, Ediciones Arazandi, Segunda Edición.

- DE CEA JIMENEZ. A. (2012). Los delitos en las redes sociales: aproximación a su estudio y clasificación. Universidad de Salamanca, España.

- DIAZ VARGAS. M. F. & Acuña Moreno, W. A. (2006). Los delitos informáticos en Colombia y su penalización. Universidad Libre, Seccional Bogotá.

- DIAZ GARCIA. A. (2013). En busca de cura para los delitos informáticos. XVII congreso Iberoamericano de Derecho e Informática. Santa Cruz, Bolivia. http://fiadi.org/congresos/

- GERVEZ PIZA. J. A., Serrano Romero, L. C., y Uribe Celis, L. M. (2012). La lenta adecuación en Colombia del derecho penal frente a nuevas conductas derivadas del mal uso de los avances informáticos. Universidad Libre, Seccional Cúcuta.

- GIRALDO ANGEL. J. & Giraldo López, O. (2013). Metodología y técnica de la investigación jurídica. 11ª edición.

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

- GRISALES PEREZ. G. S. (2013). Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (Art. 269I) y Transferencia no consentida de activos (Art. 269j) Ley 1273 de 2009. Universidad Eafit, Medellín, Antioquia.

- HERNANDEZ SAMPIERI. R. & Fernández Collado, C. (2010). Metodología de la Investigación. Mc Graw Hill. México, Quinta Edición.

- HUERTA. M. y Líbano. C. (1996). Delitos informáticos. Ed. Conosur Ltda, Santiago.

- MARTA y MARTIN. R. M. (1997). Bienes jurídicos intermedios y delitos de peligro -Aproximación a los presupuestos de la técnica de peligro para los delitos que protegen bienes jurídicos intermedios. Granada, Comares.

- OJEDA-PEREZ. J. E. Rincón-Rodríguez. F. Arias-Flórez M. E. & Daza-Martínez L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66. Universidad Santo Tomás de Aquino.

- PARRA SEPULVEDA M. A. & Lamus Vargas. H. D. (2012). Análisis jurídico de las conductas de la organización Wikileaks frente a los delitos informáticos y a los derechos de libertad de expresión, recibir y publicar información. Universidad Libre, Seccional Cúcuta.

- PICOTTI L. (2013). Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales. Revista de Internet, Derecho y Política, núm.

16, enero-junio, 2013, pp. 76-90. Universitat Oberta de Catalunya. Barcelona, España.

- PIATTINI-VELTHUIS M. G. & Peso-Navarro, E. (2001). Auditoría informática. Madrid: Alfaomega.

- QUIÑONES G. G. (1989). Cibernética Penal. El Delito Computarizado. Gráficas Capitolio, Caracas (Venezuela).

- RIASCOS GOMEZ L. O. (2010). El delito informático contra la intimidad y los datos de la persona en el Derecho Colombiano. Facultad de Derecho de la Universidad de Nariño (Pasto-Colombia).

- RODRIGUEZ ARBELAEZ J. D. (2012). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. Universidad CES. http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

- SUAREZ SANCHEZ. A. (2009). La estafa informática. Bogotá: Grupo Ibáñez

- SUAREZ SANCHEZ. A. (2010). El hurto por medios informáticos y semejantes a través de la utilización de tarjeta magnética falsa o ajena en cajero automático. En: Estudios de derecho penal I. Universidad de Bogotá Jorge Tadeo Lozano. Recuperado: http://avalon.utadeo.edu.co/servicios/ebooks/derecho_penal_I/files/assets/basic-html/page237.html

- TELLEZ VALDES. J. (1996). Derecho Informático. Ed. McGraw-Hill, México.

- TORRES. H. W. (2002). Derecho informático. Medellín: Ediciones Jurídicas.

- SOTOMAYOR. J. O. (2012). Curso de Derecho Penal I. Medellín, Antioquia.

- SUAREZ SANCHEZ. A. (2000). Delitos contra el patrimonio económico, 2ª ed., Universidad Externado de Colombia, Bogotá.

- ACOSTA ARGOTE. (2021). Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis. Recuperado de https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

- PORTAFOLIO (2020). Delitos informáticos, la otra pandemia en tiempos del coronavirus. Recuperado de https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

- EL TIEMPO. (2021). Cuatro de cada 10 fraudes en la banca se hacen por canales digitales. Recuperado de https://www.eltiempo.com/economia/sector-financiero/asi-estan-robando-los-ciberdelincuentes-a-los-clientes-de-los-bancos-601247

- VITA MESA Laura. (2020). Los delitos cometidos por medios informáticos crecieron 83% por cuenta de la pandemia. Recuperado de

https://www.asuntoslegales.com.co/consumidor/los-delitos-cometidos-por-medios-informaticos-crecieron-83-por-cuenta-de-la-pandemia-3099101