Universidad EAFIT

Escuela de Derecho

Maestría en Derecho Penal

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

Autor:
Giovanni Stalin Grisales Pérez

Asesora:
Dra. Diana Restrepo Rodríguez

Jurado:
Dr. Fernando León Tamayo Arboleda

Medellín, Antioquia

Julio de 2013

Contenido

Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (art. 269 I) y Transferencia no consentida de activos (art. 269 J), introducidos al Código Penal Colombiano por la Ley 1273 de 2009[G]

GIOVANNI GRISALES[**]

Resumen: La razón de este documento, surge del incremento desmesurado de los delitos informáticos a nivel mundial, conductas como el hurto por medios informáticos y la Transferencia no consentida de activos, afectan en nuestro país, tanto a personas naturales como jurídicas, padeciendo cada una de ellas en su medida, graves detrimentos patrimoniales a través de la perdida de sus bienes económicos e información privada a la que acceden de manera ilegal los delincuentes cibernéticos. Esa razón, llevó a que se hiciera un estudio dogmático de ambas conductas punibles, tomando como referencia los cientos de casos que mes a mes ingresan a los despachos de las Fiscalías de Medellín y que fueron muchos de ellos analizados con el fin de ilustrar de una manera clara, sencilla y comprensible a Jueces, Fiscales, funcionarios de Policía Judicial, abogados, estudiantes de derechos y todos aquellos que quieran conocer desde lo jurídico el amplio y complicado mundo de los delitos informáticos en Colombia.

Palabras Clave: derecho penal, delitos informáticos, transferencia no consentida de activos, hurto por medios informáticos, Ley 1273 de 2009.

Abstract: The reason for this document stems from the disproportionate increase of cybercrime worldwide, behaviors such as theft by computer and nonconsensual transfer of assets affect our country, both natural and legal persons, suffering from each in its measure, serious economic detriment through the loss of economic assets and private information to illegally accessing cybercriminals. That reason was that a study be made of both dogmatic criminal conduct by reference to the hundreds of cases every month enter the offices of the Prosecutor of Medellín and many of them were analyzed in order to illustrate a clear, simple and understandable to judges, prosecutors, judicial police officers, lawyers, law students and all those who want to know from the legal the vast and complicated world of cybercrime in Colombia

Key Words: criminal law, computer crime, unauthorized transfer of assets, theft by computer, Act 1273 of 2009

[*] Este texto es el resultado de la investigación desarrollada dentro de la temática de los "delitos informáticos", adelantada durante la Maestría en Derecho Penal en la Universidad EAFIT, entre los años 2011 al marzo de 2013, bajo la asesoría de la profesora Diana Restrepo Rodríguez. Esta investigación se encuentra registrada en la base de datos de la Biblioteca de la Universidad EAFIT.

[**] Abogado de la Universidad de Antioquia, Fiscal Delegado ante el Circuito de Medellín, candidato a Licenciado en Derecho Penal en la Universidad EAFIT.

Elementos típicos del art. 269 J CP. 7.1. Clasificación de la conducta del art. 269J CP. 7.2. Los sujetos activo y pasivo. 7.3. La acción. 7.4. El objeto material. 7.5. Elementos subjetivos, descriptivos y normativos del tipo. 7.6 Dispositivo Amplificador del Tipo: La Tentativa 8. Problemas de concursos y su resolución a través de los principios de subsidiariedad, consunsión, alternatividad y especialidad. 9. Conclusiones. 10. Bibliografía. 11. Anexo: Glosario.

1. Introducción.

Motiva la presente investigación el continuo incremento de conductas delictivas cometidas a través de la red de comunicaciones conocida como Internet - Informe de fecha 01 de junio de 2012, suscrito por el Investigador Criminalístico del CTI Jorge Andrés Osorio Cano, el cual analiza la variable de los delitos informáticos de 2007 a 2012-, así como el poco desarrollo de la doctrina e incluso la jurisprudencia sobre dichos temas, por lo que se busca aportar unos conceptos básicos y prácticos a través del estudio dogmático de dos de las conductas que más afectan a los usuarios de la red en nuestro país y que son el Hurto por Medios Informáticos y Semejantes (Art. 269 i) y la Transferencia No Consentida de Activos (Art. 269J) de la Ley 1273 de 2009.

Ese auge delictual se presenta por el avance de la tecnología y el aprovechamiento de la globalización de la información, la cual es promocionada continuamente a través de las políticas de Estado, los medios de comunicación y las empresas privadas - bancos y telecomunicaciones– para que se utilicen de manera masiva todos aquellos recursos digitales que son ofrecidos actualmente buscando que las personas tengan una mejor calidad de vida, pues acceden más fácilmente a educación, recreación digital, comunicación personal, conectividad instantánea y continua, negocios a nivel nacional e internacional y todo tipo de información en tiempo real.

Sin embargo, ese desarrollo tecnológico, que buscaba mejorar la calidad de vida de los ciudadanos y dinamizar la información de manera veloz e instantánea a través de la red, encontró en los delincuentes informáticos un novedoso y lucrativo nicho para explotar, gracias al desconocimiento casi total de las funciones de los lenguajes de programación y de las diferentes técnicas de intrusión por la mayoría de los usuarios de la red. Esto ha creado nuevas dinámicas delictivas dirigidas a “hurtar” o “apoderarse” de esa información privilegiada –bancaria, personal, privada, secreta, empresarial, política, etc.-, de cada una de las personas y organizaciones, para explotarla en beneficio económico propio.

Basta con mirar algunos ejemplos nacionales e internacionales documentados por diferentes medios de comunicación sobre el avance casi imparable de los delitos informáticos, su impacto a nivel social, el monto de las ganancias obtenidas por quienes a ellos se dedican, el perjuicio económico para los Estados y el peligro que puede acarrear a las políticas internacionales de seguridad, para comprender que es un tema en el que la justicia, especialmente en nuestro país, ha avanzado muy poco.

Sólo por mencionar algunos casos de la actualidad nacional, se puede mencionar, en primer lugar, el siguiente reporte del diario El Espectador.com, de 23 de abril de 2012: “Delitos informáticos causan pérdidas millonarias a bancos y empresas. De acuerdo con el estudio del ciberdelito desarrollado por el Registro de Direcciones de Internet para América Latina y Caribe (Lacnic), el phishing o robo de datos personales significa pérdidas anuales por unos US$93 mil millones de dólares, y afecta a unos 2.500 bancos que operan en la región, en tanto los robos a cuentas de

clientes suman otros US$761 millones de dólares. / Asimismo, según cifras del estudio de McAfee Inc. y Science Applications International Corporation, 25% de las organizaciones han sufrido la paralización o atraso de una fusión o adquisición, o bien de la implementación de un nuevo producto o solución, a causa de una filtración de datos o por una amenaza creíble de filtración de datos. / Cabe mencionar que empresas e instituciones de todo el mundo gastaron 338 mil millones de dólares en 2011, para combatir ataques cibercriminales, dos tercios de los cuales fueron delitos de fraude económico, de acuerdo con números ofrecidos durante el Programa de Ciberseguridad y Cibercrimen de la ONU…"

Por su parte, la Revista Semana señala en un reportaje del martes 14 de agosto de 2012: "El boom de los mercenarios de la red. ¿Quieres saber qué trama tu competencia? ¿Fisgonear en los emails de tu mujer? ¿Obtener datos de tarjetas de crédito? Hay un mercado negro muy lucrativo de este tipo de servicios y cada vez es más descarado, explicó a BBC Mundo el informático forense y presidente de la Federación de Ingenieros Informáticos de España. Kapersky Labs ha cuantificado cuánto dinero puede hacer un pirata informático vendiendo en el mercado negro la información que extrae de internet. De acuerdo a los cálculos realizados por la firma, un pirata informático puede llegar a vender los datos de una tarjeta de crédito por US$10, la imagen de un pasaporte escaneado por US$25 y un pasaporte hecho en base a ese escaneo por US$1.000. Las cifras se multiplican a medida que los cibercriminales infectan no cientos sino miles de computadoras. "Todos ganan excepto la víctima", explica Bestuzhev".

Tomando como referencia nuestro país, tenemos que la ASOBANCARIA se ha preocupado altamente por el tema, dada la insidia económica que éste trae. En su reporte económico semanal –de fecha 29 de octubre de 2012- señala:

> "…Las tipologías de fraude que afectan al sector bancario y a sus clientes van desde el fleteo y el taquillazo hasta complejos delitos informáticos. Dentro de estos últimos se puede hacer referencia a modalidades como el *phishing* (suplantación de sitios web), instalación de troyanos o software espía para el hurto de información, el acceso abusivo a sistemas informáticos y la clonación de tarjetas débito y crédito.
>
> El uso cada vez mayor de los canales electrónicos para la realización de operaciones bancarias y los avances tecnológicos, que le facilitan al delincuente adquirir herramientas y establecer contacto con organizaciones ilegales de otros territorios, son factores que han llevado a una tendencia creciente de los ataques tecnológicos o informáticos contra los establecimientos de crédito.
>
> En Colombia también ha ocurrido un incremento rápido de los canales electrónicos. De acuerdo con el Informe de Inclusión Financiera de Asobancaria del primer semestre de 2012, entre junio de 2009 y el mismo período de este año su crecimiento fue del 3,8%. Esto se explica por canales como internet, que en junio de 2009 participaba con el 6,5% y ahora el 9,5% de las transacciones monetarias se realiza por este medio. Algo similar aconteció con el uso de los datafonos.
>
> En relación con el cibercrimen, según el reporte "Symantec Internet Security Threat" publicado en 2011, en el año 2010 se encontraron 4.989 nuevas vulnerabilidades en elementos tecnológicos (es decir, 95 por semana) y existen más de 403 millones de variantes de malware. Además, la alta penetración de la telefonía celular ha llevado a un incremento de ataques hacia dispositivos móviles. De acuerdo con ese mismo estudio, el año pasado se identificó un 93% más de

> vulnerabilidades y un 1.116% de malware en celulares respecto de la vigencia anterior.
>
> Algunos datos adicionales ilustran también esta situación. El costo anual de los cibercrímenes en el mundo se calcula en USD 114 billones, el 69% de los adultos ha sido víctima de un cibercrimen en su vida, cada 14 segundos hay una víctima (es decir, más de un millón de víctimas por año) y el FBI habla de USD 400 billones de estafas en estas modalidades anualmente.
>
> En Colombia los mayores retos de mitigación del fraude en las transacciones financieras se encuentran en las operaciones que se realizan en ambientes no presenciales como la internet, la banca móvil, la audio-respuesta y principalmente el comercio electrónico. Esta tendencia se acentúa por dos razones. En primer lugar, por el proceso de migración a tecnología EMV -mejor conocida como tarjeta con chip- en el que se encuentra nuestro país. Y en segundo lugar, por el vertiginoso crecimiento del comercio electrónico…"

Finalmente, y para cerrar así este apartado que pretende ilustrar el contexto en el que se establecen los delitos que se examinarán, el periódico El Colombiano en un amplio reportaje del 24 de marzo de 2013 (Rojas Arboleda, 2013), realizado como consecuencia de los ciberataques actualmente conocidos entre Estados Unidos y China, realiza un completo análisis de las implicaciones políticas y económicas y la forma fácil como aquellas intrusiones se realizan: "…La primera finta vino de parte de EEUU, donde se publicó un informe de la empresa especializada en seguridad informática Mandiant, calificado como el más detallado hasta la fecha que reveló una serie de ataques sistemáticos a compañías de EE.UU en un periodo de 7 años. El rastreo hecho por la firma ubicó en un barrio de Shanghái un edificio de 12 pisos dirigido por la "Unidad 61398" que a su vez hace parte del Ejército Popular de Liberación chino, como fuente de las violaciones informáticas. Han robado sistemáticamente cientos de terabytes de información de por lo menos 141 organizaciones. Según nuestras observaciones, este es uno de los grupos más prolijos de espionaje cibernético en términos de la cantidad de información robada".

Este panorama, entonces, fue lo que motivó esta investigación, buscando conocer cómo enfrenta el sistema judicial de nuestra ciudad los delitos informáticos, a través del estudio dogmático que me ha permitido la realización de una Maestría en Derecho Penal, de la cual este escrito es el trabajo de grado, y de mi experiencia investigativa adquirida en los años en que me he desempeñado como Fiscal Delegado en Medellín, adscrito a la Unidad de Estructura de Apoyo de la Fiscalía General de la Nación, encargada de documentar, investigar y desarticular organizaciones criminales, entre ellas las dedicadas a esta tipología delictiva. La intención es explicar cómo se descomponen y encajan las dos conductas punibles más frecuentemente denunciadas ante el ente investigador, cuáles son los supuestos fácticos más comunes, qué se busca tutelar con la tipificación de los delitos informáticos, cómo participan sus intervinientes, cuáles son las modalidades delictivas, la figura del concurso en la Ley 1273 de 2009, la tentativa, qué ocurre con el dinero transferido a empresas privadas o públicas para pagar deudas de terceros bajo esa modalidad, entre muchas otras preguntas e interrogantes que se buscar resolver a través de la lectura del presente trabajo.

Esperamos que sea un aporte importante a la doctrina de nuestro país, y que sirva como herramienta de consulta para Jueces, Fiscales, abogados, investigadores judiciales y todos aquellos que de una u otra forma están vinculados con el derecho penal informático.

2. El bien jurídico protegido en los tipos penales estudiados.

El primer concepto que debe ser abordado en este documento responde a las preguntas: ¿qué es el bien jurídico? ¿De dónde surge el bien jurídico? Y, por último, ¿cuál es el bien jurídico que se protege a través de la comisión de estos delitos?

Es necesario definir, en primer lugar, qué es bien jurídico de manera general, para luego de manera particular dar respuesta a los demás interrogantes. Varios autores entregan en sus textos una definición general muy similar sobre lo que es este concepto.

El texto de derecho penal general, escrito por Santiago Mir (Puig, 2003), define el bien jurídico desde el punto de vista dogmático como el "objeto de tutela jurídica", y pone de ejemplo la vida, la propiedad, la libertad, el honor, etc., indicando que la legislación penal castiga los ataques contra esos bienes protegidos.

El profesor Velásquez (2007), al hablar del bien jurídico señala: "…consecuencia de una de las funciones de la norma penal es la protección de bienes jurídicos, exigencia según la cual todo tipo penal contiene en su aspecto objetivado un determinado objeto de protección denominado "bien jurídico" o "bien jurídicamente tutelado" (p. 274), pasando luego a referir que ese bien jurídico es un "…concepto abstracto que en ningún caso puede ser confundido con el objeto sobre el cual recae la acción del agente como se verifica… " (p. 274). Y trae como ejemplo de esto, el hecho de que en el hurto el objeto es la cosa mueble y el bien jurídico es el patrimonio económico.

A su vez, Fernández (2004), en su libro "Bien jurídico y sistema del delito", lo define como "…aquel núcleo de cualidades esenciales de las personas, las cosas o las instituciones, que sirven al libre desarrollo del individuo en un Estado constitucional, social y democrático de derecho y, justamente de ese valor social especial que revisten devienen objetos de tutela penal…" (p. 149).

También Hefendehl (2007) hace una comparación entre la teoría del "principio del daño" (*harm principle*) que rige el derecho angloamericano y el término "bien jurídico" usado por la teoría alemana, y también la colombiana. Así, indica lo siguiente: "…el bien jurídico es algo independiente: no el fin de protección, sino ese "algo" que se halla tras el fin de protección. Pero ¿qué es ese "algo"? La respuesta podría encontrarse en esa noción de recurso que late tras el interés, definiéndolo como un medio o una capacidad que, en el caso normal, posee un cierto valor para el mantenimiento de un estándar de calidad de vida. Como ejemplos podrían citarse la propiedad, que proporciona los medios para satisfacer las necesidades materiales, o la integridad corporal, en tanto constituye un requisito previo para la consecución de otros intereses…" (pág. 42). Y más adelante agrega: "La teoría alemana del bien jurídico otorga un considerable valor a la concreción de los bienes merecedores de protección, pero desatiende el hecho de que ello por sí mismo no es suficiente. Por regla general, los bienes jurídicos no están protegidos frente a todas las modalidades de acción posibles, sino sólo frente a aquellas que lo ponen en peligro o lo menoscaban…" (pág.46).

Teniendo entonces una noción del bien jurídico, y retomando a Mir Puig (2003), vemos que este autor le asigna, además, unas funciones, que aparte de señalar el límite que se impone a los legisladores, tiene también la función sistemática de interpretación y de medición de la pena, desarrolladas de la siguiente manera:

> Función sistemática. El Código penal, parte de los distintos bienes jurídicos protegidos en cada delito o falta – vida, integridad física, libertad sexual, propiedad (pág. 91).

Significa ello que la legislación penal recoge ese grupo de faltas a través de las cuales se puede vulnerar un determinado bien jurídico, ya sea la vida e integridad personal, el patrimonio económico, la dignidad humana, etc. El autor continúa explicando las demás funciones del bien jurídico, así:

> Función de guía de interpretación: una vez determinado el bien jurídico protegido en un delito, la interpretación (teleológica) podrá excluir del tipo respectivo las conductas que no lesionen ni pongan en peligro dicho bien jurídico, esto es, aquellas conductas que son inocuas para afectar el conjunto de bienes jurídicos que se protegen.
>
> Función de criterio de medición de la pena. La mayor o menor gravedad de la lesión del bien jurídico, o la mayor o menor peligrosidad de su ataque, influyen decisivamente en la gravedad del hecho. Dentro del margen de arbitrio judicial que la ley concede ello puede servir de base a la concreta determinación de la pena… (págs. 137-138). Obviamente esto lo determina el juzgador al momento de emitir una sentencia condenatoria.

De las anteriores nociones surgen esos bienes jurídicos cuyas características y funciones son asignadas para reglamentar el control social tendiente a proteger los intereses de una determinada clase social, afectada por las conductas de aquellos ciudadanos que van en contra de sus intereses, en nuestro caso patrimoniales, y cuyas funciones ya están determinadas por la dogmática.

Como acaba de afirmarse, el bien jurídico tutelado en los delitos que nos ocupan es el patrimonio. Ahora bien, sobre el interrogante acerca de dónde surge el bien jurídico, Mir Puig (2003) también hace aportes muy significativos de política criminal, indicando que: "…*esa determinación de los bienes a proteger penalmente depende de los intereses y valores del grupo social que en cada momento histórico detenta el poder político*…" (pág. 137) y sobre esa evolución de los bienes jurídicos toma como fundamento la legislación española y señala: "…*los códigos españoles, como los del mundo occidental… parten de la protección de intereses y valores predominantemente burgueses. Las modificaciones que entretanto ha ido experimentado el capitalismo y el modelo de Estado en nuestro ámbito cultural van determinando o exigiendo ciertos cambios en los bienes jurídicos del derecho penal*…". Idea que es relevante para dar respuesta a nuestros interrogantes.

Desde el Código de Napoleón se protegía el patrimonio económico, un título de dicha codificación era dedicado exclusivamente a la propiedad; esa normatividad, que hace referencia al derecho civil, demuestra el interés de los legisladores de todas las épocas por proteger el derecho a la propiedad, tomándolo como uno de los más preciados del hombre (2003).

Capella (1997) señala que la creación de un bien jurídico surge de esa "…institucionalización de la fuerza cultural-militar de una forma de organización social incapaz de reproducirse por el mero despliegue de su lógica económica… El Estado detenta la suprema capacidad de violencia; sostiene

la reglamentación social y puede incluso innovarla, mediante la amenaza de la coerción –el derecho- es originariamente una reglamentación coercitiva; y subordina a la suya, la capacidad de reglamentación y de violencia de la sociedad… ” (pág. 128).

Así mismo, indica que dentro de las funciones del Estado moderno está la de “…*reprimir las amenazas al modo de producción dominante procedente de las clases subalternas o de ciertos sectores de las clases dominantes mismas para mantener la existencia social del capital*…” (Capella, 1997, pág. 129). Conforme a lo anterior y bajo la teoría del funcionalismo desarrollada entre otros por Luhmann, quien demuestra cómo la expansión del derecho penal lleva a que cada sistema (jurídico, económico, moral, etc.), construya su propio modelo de lo que le sirve para mantener su control social, es de donde surgen las normas de los arts. 269 I y 269 J de la Ley 1273 de 2009, 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, vemos que el derecho penal tradicional no alcanzaba a controlar actos reales como los que se cometen utilizando los medios informáticos, por lo que ello llevó a 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. Así, el bien jurídico tutelado en los artículos que nos interesan es definido por el legislador como “*de la protección de la información y de los datos*”, pero se encuentra adicionado como título Bis, a la parte del Código que protege el patrimonio económico.

Encontramos entonces que los delitos que nos ocupan pretenden tutelar el patrimonio económico aunque, como veremos más adelante, de unas específicas y novedosas formas de lesión que implican el empleo de medios informáticos. Es fundamental, entonces, aclarar en qué consiste ese bien jurídico. Al respecto, Suárez Sánchez (2003, pág. 747) indica que el patrimonio de las personas lo constituye la universalidad de sus bienes, incluye derechos subjetivos que se tenga sobre ellos y aún las expectativas de contenido patrimonial, y continúa su exposición indicando que el bien jurídico es el conjunto de relaciones posesorias legítimas. Se trata, dice, “…de la relación del hombre con las cosas, servicios o derechos con significado económico, la cual debe ser material y voluntaria...” (pág. 747).

En su texto, este autor incluye dentro del patrimonio esos bienes materiales, indicando que la relación material no es sólo sobre bienes sino también sobre las cosas incorporales que son los derechos de diversa índole, entendiendo dentro de esos derechos de diversa índole la conservación, el uso, el goce y la disposición (pág. 748).

Por otra parte, Cerezo A. y Choclan Montalvo (2001) traen la misma definición de patrimonio realizada por Bustos Ramírez en su Manual de Derecho Penal (1991), acogiendo un concepto mixto jurídico-económico. Consideran pues que el patrimonio económico es el bien jurídico que se protege en los delitos contra la propiedad (hurto, robo y daños) y que es también el bien jurídico que se afecta en el delito de estafa. Indican además que el patrimonio está integrado por tres elementos: “a) Los bienes dotados de valor económico que constituyen su objeto material, excluidos por consiguiente los que tengan mero valor afectivo; b) La existencia de una relación con los bienes protegibles por el ordenamiento jurídico, o al menos, que no sea disconforme con el mismo (la mera tenencia por el sustractor de la cosa hurtada) y c) causación real o potencial de un

perjuicio patrimonial, entendido como disminución económicamente evaluable del acervo patrimonial…" (pág. 220).

Estas definiciones textuales de los diferentes autores, en un comienzo permiten ubicarnos dentro de lo que la teoría define como bien jurídico, y es aquello protegido a través del Derecho penal, concluyendo que bien jurídico es ese conjunto de cosas que tienen una relación jurídica con un individuo en particular y son protegidas por la legislación penal a través de una sanción a quien se atreva a vulnerarlos. Sin embargo, recordando a Welzel, mencionado por Fontan Balestra (2004) "…la misión primaria del derecho penal no es el amparo actual de los bienes jurídicos; es decir, el amparo de la persona individual, de la propiedad, etc., pues es allí, precisamente, a donde, por regla general, llega su acción demasiado tarde. Por encima del amparo de los bienes jurídicos individuales concretos, está la misión de asegurar la validez real (la observancia) de los valores del actuar humano según el pensamiento jurídico..." (pág. 379).

Por último, tenemos que en Colombia el bien jurídico del patrimonio económico, ha sido definido bajo ciertos parámetros ya claros para la jurisprudencia y la doctrina.

En un compendio sobre el tratamiento del tema en la jurisprudencia, Sanguino Madarriaga (2007), haciendo referencia a Pacheco Osorio, pág. 42, indica: "…nuestro derecho civil no limita, pues, el concepto de propiedad o dominio a la facultad de gozar o disponer arbitrariamente de las cosas materiales, sino que lo extiende a todos los derechos que forman parte del activo patrimonial de una persona natural o jurídica. Así se tiene que, en Colombia, el poseedor es titular del derecho de posesión, el tenedor es propietario del derecho de tenencia, el acreedor es propietario de la acreencia, etc. Así las cosas me parece claro que el bien jurídico protegido mediante la incriminación de estos delitos es el derecho de propiedad, tomada esta expresión en el sentido amplio que le asigna el derecho civil…" y agrega el autor que parte de la doctrina critica arduamente el concepto de patrimonio como bien jurídicamente tutelado, pues si este es una "… universalidad de derechos materiales e inmateriales, pertenecientes a personas naturales o jurídicas, poseídos actualmente o a la espera de una posesión, resulta inadmisible que puedan constituir sobre ellos una clase especial de tipos penales cuya naturaleza está lejos de ser abstracta o en proyecto de formación. Por el contrario, los bienes tutelados por la norma represora han de ser actuales, concretos, físicamente apreciables, susceptibles de valuación…" y señala además, que para algunos autores "… la denominación de delitos contra el patrimonio económico indica que el objeto de protección no es solamente la propiedad, entendida como " el derecho real en una cosa corporal, para gozar y disponer de ella arbitrariamente, no siendo contra ley o contra derecho ajeno" (Código Civil, art. 669), sino también la posesión, o sea la tenencia de una cosa determinada con ánimo de señor y dueño (art. 762 Ibídem) y la mera tenencia es la que se ejerce sobre una cosa, no como dueño, sino en lugar o a nombre del dueño (Art. 775 ibidem).

Doctrinantes colombianos como Alfonso Reyes Echandía (Pérez Pinzón, 1987), Pedro Alfonso Pabón Parra (Pabón Parra, 2002) entre otros, concluyen que el patrimonio económico está conformado por ese conjunto de relaciones jurídicas legítimas y valuables entre el sujeto y sus bienes – o valores económicos tangibles e intangibles-que están bajo su poder y tienen protección jurídica.

Lo anterior, entonces, permite responder el último interrogante y demostrar que aquello que se busca proteger con el nuevo bien jurídico integrado a la Legislación penal por la Ley 1273 de 2009,

es **el patrimonio económico de las personas existentes en las diferentes entidades bancarias,** quienes custodian a través de cuentas asignadas a miles de sus afiliados el dinero por ellos depositado allí; dinero que es sustraído luego de apoderarse, a través de diferentes medios ilegítimos –y en los casos que nos interesan informáticos- de la información privilegiada de cada cliente; información necesaria para ingresar a los sistemas bancarios y que consiste en datos, tales como códigos, claves, números de cuentas bancarias, números de tarjetas de crédito, números de identificación personal, en fin, toda aquella secuencia numérica o alfanumérica necesaria para que las personas tengan acceso a las diferentes actividades comerciales, personales y de comunicaciones que surgen de la utilización de los sistemas informáticos, bien jurídico patrimonio que está para este caso íntimamente ligado a ese nuevo bien construido por los legisladores como es "…**la protección de la información y de los datos**" y que protege ya desde un perfil más amplio la información personal y privada del conglomerado social, sean personas naturales o jurídicas quienes utilizan la red conocida como Internet.

3. ¿Por qué se trata de delitos informáticos?

Para responder a este segundo interrogante debemos destacar la conclusión a la que se llegó en el capítulo anterior, indicando que el bien jurídicamente protegido con la creación de los dos tipos penales descritos en los artículos 269I y 269J, no es otro que el patrimonio económico. Las mismas normas hacen referencia en su contenido a los elementos normativos descritos en el artículo 239 CP, al cual remite expresamente uno de ellos y al ánimo de lucro que se obtiene a través de la transferencia no consentida de activos, tipo penal que se asemeja, como se explicará más adelante, a la figura jurídica de la estafa.

Ahora bien, existe la necesidad de identificar a través de la doctrina qué es un delito informático.

En el texto Derecho Penal Informático (Arizamendi & De la Mata Barranco, 2010), haciendo referencia al jurista español Camacho Losa (pág. 25 y ss), se ha considerado como delito informático "…toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas".

Por su parte, el profesor Posada Maya (2006) en su texto *Aproximación a la criminalidad informática*, define así el delito informático: "…se entiende cualquier conducta con fines ilícitos, ello es, no autorizada por el titular del bien jurídico afectado o abusiva de dicho consentimiento, dirigida a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación y ejecución automática de programas de datos o información informatizada reservada o secreta de naturaleza personal, empresarial, comercial o pública. Ello, con independencia de que los resultados o los actos de agotamiento de dicha conducta punible de emprendimiento constituyan una conducta delictiva independiente…"

Ahora bien, a nivel internacional, el Consejo de Europa, asumiendo las recomendaciones descritas en la **R (89) 9**, incluye una lista de actos que deberían o podrían ser objeto de sanción penal, esto es, actos que para ese organismo pueden ser considerados como un delito informático, señalando los siguientes:

"…

1. Fraude en el campo de la informática mediante la "inserción, alteración, borrado o supresión de datos o de programas de informática, o de cualquier otra interferencia en el desarrollo del tratamiento de los datos informáticos", con ánimo de lucro y daño a terceros;
2. Falsificación en materia informática.
3. Daños causados a datos o programas informáticos (borrado, daño, deterioro o supresión ilegal de datos o programas informáticos).
4. Sabotaje informático.
5. Acceso no autorizado.
6. Interceptación no autorizada.
7. Reproducción no autorizada de un programa informático protegido.
8. Reproducción no autorizada de una topografía.
9. Alteración de datos o de programas informáticos.
10. El espionaje informático.
11. La utilización no autorizada de un ordenador.
12. La utilización no autorizada de un programa informático protegido.
13. Tráfico de claves (*password*) obtenidas ilegalmente.
14. Obtención de un acceso no autorizado a sistemas informáticos
15. La distribución de virus o de programas similares…" (pág. 60).

Por último, tenemos la Convención de Cibercriminalidad, realizada en Budapest en 2001 (Europa, 2001), como instrumento internacional que define una serie de conductas que deben ser catalogadas como delitos informáticos dentro de los estados parte, señalando entre ellos el acceso ilícito, interceptación ilícita, ataque a la integridad de los datos, ataques a la integridad del sistema, falsificación informática y fraude informático, entre otros.

Ahora bien, si tomamos como delito informático las definiciones, no sólo de la doctrina sino lo que consideran los instrumentos internacionales relacionados, podemos observar que las conductas punibles estudiadas – arts. 269I y 269J del CP-, por el objeto inicial del ataque que no es otro que la información de los usuarios de la red; el medio comisivo con que se comete – software o programas especializados-; y el ámbito de la informática, aunado todo ello al mundo de la tecnología digital, llegamos a la conclusión de que necesariamente estos tipos penales son cometidos utilizando para ello los medios informáticos.

Según parte de la doctrina española, entre ellos el Profesor González Rus (1999), los delitos informáticos se subdividen en dos grupos: uno que puede ser aquel que atenta contra la intimidad de las personas ante el gran cúmulo de datos que mantienen en sus correos electrónicos, redes sociales o discos personales de sus computadores, y otro que se compone de aquellos que atentan contra el patrimonio económico, y que se cometen utilizando las nuevas tecnologías informáticas. Además, señala que los delitos contra el sistema informático se pueden catalogar como los "…referidos tanto a sus elementos físicos como lógicos, incluyendo aquí los delitos de hurto, hurto de uso, robo, apropiación indebida, estafa, daños…", así como "…los delitos cometidos "por medio" del sistema informático", distinguiendo a su vez, dentro de éstos, aquellos en los que el uso del modo informático no es absolutamente necesario, pudiéndose cometer el delito por un medio no informático si el autor así lo hubiere decidido, y los que únicamente pueden ser cometidos por medios informáticos. De este modo no sólo concluye sobre cuáles son los delitos informáticos, sino también acerca de aquellos que se cometen contra los sistemas informáticos.

Analizando todo lo anterior, vemos que quien realiza los tipos penales de la Ley 1273 de 2009, en general no está atentando contra un medio informático como tal, sino que está utilizando precisamente ese medio informático para llevar a cabo la ejecución de los mismos, bien sea para conectarse a la red y desde allí obtener la información previa que requiere para la realización de una de las dos conductas punibles o para ejecutar, una vez se tenga la información personal o privilegiada del ciudadano, una afectación a su patrimonio a través de la transferencia de activos o el hurto por medios informáticos. Si se estuviera atentando contra un medio informático, se debería definir cuál es ese medio informático para establecer el tipo de conducta a investigar, pues podríamos encontrarnos en una situación como el hurto de un computador, una terminal de comunicaciones digital, un disco duro con información confidencial de personas naturales o jurídicas, una CPU o, el borrado, alteración o limitación al ingreso de un programa de computación, lo que podría tratarse ya como un posible daño en bien ajeno.

Visto lo anterior, y teniendo en cuenta que el bien jurídico que se protege es el patrimonio económico de los sujetos, y la información personal y privada, podemos concluir que en el caso objeto de estudio estamos enfrentados a unas conductas que se cometen utilizando esos medios informáticos existentes y que pueden ser computadores portátiles, teléfonos inteligentes, computadores de oficina, todos ellos sí, con una conexión obligatoria a la red de datos conocida como Internet. Medios estos que, aunados a los conocimientos especiales de los autores, son utilizados para apropiarse de los activos de sus víctimas bajo una de las dos modalidades descritas en los artículos 269I y 269J CP.

4. ¿Antes de la existencia de estos tipos penales qué pasaba en nuestra legislación penal?

Antes de la expedición de la Ley 1273 de 2009, nuestro Código Penal, en varias normas, hacía referencia a la descripción de conductas punibles cometidas utilizando medios informáticos, no expresamente dentro de un título como tal, sino que éstas se encontraban diseminadas por varios de ellos. Retomando al profesor Posada Maya (2006, pág. 21), describe para ese momento histórico de la política criminal, cómo se podían sancionar penalmente aquellos supuestos fácticos cometidos por quienes se valían de las tecnologías digitales para afectar bienes jurídicos utilizando normas vigentes en la legislación penal. Dicho doctrinante definía lo siguiente: "…delito informático propiamente dicho, se entiende cualquier conducta con fines ilícitos, ello es, no autorizada por el titular del bien jurídico afectado o abusiva de dicho consentimiento, dirigida a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación y ejecución automática de programas de datos o información informatizada reservada o secreta de naturaleza personal, empresarial, comercial o pública. Ello, con independencia de que los resultados o los actos de agotamiento de dicha conducta punible de emprendimiento constituyan una conducta delictiva independiente…".

Y a continuación subdividía esos supuestos fácticos recurrentes que constituían delitos informáticos, en: el **espionaje informático, el sabotaje informático, fraude informático y la falsedad informática,** cada una de esas conductas descritas tenían como particularidad para su realización la utilización de internet, y eran ejecutadas a través de programas maliciosos los cuales buscaban en todo momento la intrusión de los computadores de personas naturales y jurídicas, para alterar, dañar, inutilizar, suprimir, defraudar, falsificar, adulterar, modificar o crear imitaciones parciales de información, con el fin de capturar datos, copiar imágenes, archivos de sonidos, archivos secretos, archivos personales o institucionales e información bancaria, en fin, todo aquello que pudiera representar ganancias económicas para los delincuentes tecnológicos.

Estas conductas que eran perseguidas utilizando algunos tipos penales, entre ellos los artículos 239, 240 – 4 Hurto Calificado, Artículo 286 - Falsedad ideológica en documento público-, artículo 289 - falsedad en documento privado -, como la falsedad en documentos privados, artículo 291 – Uso de documento falso -, Artículo 292 - Destrucción Supresión y ocultamiento de documento público, Artículo 293 - Destrucción Supresión y ocultamiento de documento privado -, y artículo 296 –Falsedad Personal– entre otros.

El autor señalaba, además, que "…los delitos informáticos en sentido estricto implican hipótesis especiales de apoderamiento o sustracción de datos o información con ánimo de lucro genérico… o de defraudación informática en las que no existe inducción o mantenimiento en error de una persona, sino más bien la manipulación, introducción, alteración, borrado o supresión de datos, sistemas, redes, programas, bases de datos o de los resultados del procesamiento de datos con *ánimo de lucro o de beneficio*, que conllevan una defraudación potencial no consentida a los intereses económicos de las víctimas, en provecho de los defraudadores o terceros…" , significando con ello la necesidad de reglamentar aquellos supuestos fácticos descritos como conductas ejecutadas de manera digital.

Para el caso que nos ocupa estrictamente, esto es, las conductas descritas en los artículo 269 I y 269 J, las acciones dolosas que traen el contenido de dichas normas, desde esa época, ya se encontraban cobijadas por la ley penal, recordemos que existía y aún hoy tienen vigencia los artículos 239 y 240 numeral 4, "Con llave sustraída, o falsa, o violando o superando seguridades electrónicas u otras semejantes…" que hacen innecesaria la creación del tipo penal de "hurto por medios informáticos y semejantes"; igualmente, la estafa, descrita en el artículo 246, que permite sancionar lo que en aquella época Posada Maya llamó fraudes informáticos, y que corresponde a la misma conducta de transferencia no consentida de activos aunada a esa falsedad en documentos, a través de la cual se sancionarían las falsedades cometidas utilizando para ello la red de datos, ello sí, con una aplicación analógica, interpretativa y amplia de las definiciones, sin desbordar el principio de legalidad impuesto por el legislador.

Sin embargo, debe resaltarse que las demás conductas de ese Título VII bis, esto es, aquellas que atentan contra el nuevo bien jurídico de *"la protección de la información y de los datos"* sí era necesaria su regulación, pues para enfrentar la realización de la mismas sólo existía el artículo 195 CP, cuyo título era **acceso abusivo a un sistema informático,** norma que no poseía un contenido tan rico en elementos descriptivos ni normativos como aquellos que abarcan todos los supuestos genéricos creados en los artículos 269 A a 269 G de la Ley 1273 de 2009.

En conclusión, entonces, tenemos que dichos preceptos penales - los artículos 269 I y 269J - no era necesario que nacieran a la vida jurídica, pues el primero es una extensión del artículo 240-4 CP y el segundo, una extensión del artículo 246 CP. Otra solución posible hubiese sido la creación de agravantes o calificantes con elementos normativos de contenido informático a través de las cuales se sancionara la comisión de las conductas utilizando internet, solución que fue tomada por el derecho comparado - Legislación Española – tal y como se puede ver del contenido del artículo referente a la estafa: "…Art. 248. Numeral 2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero". Norma que, como vemos, fue recogida literalmente por nuestros legisladores y bautizada con el *nomen iuris* de Transferencia no consentida de activos.

5. Ejemplos de Hurto por medios informáticos y semejantes (art. 269 i) y Transferencia no consentida de activos (art. 269J) del Código Penal.

Se relacionaran las modalidades más recurrentes, según la información consultada en la Fiscalía General de la Nación, Unidad de estructura de Apoyo de Medellín, para los años 2011 y 2012.

Ejemplo Hurto por medios informáticos y semejantes - Art. 269I (caso del cambio de tarjeta débito en cajero electrónico):

A hace fila en un cajero electrónico en determinado sector de la ciudad, detrás suyo dos hombres hacen igualmente la fila. Cuando corresponde el turno a A de ingresar al cajero y se encuentra realizando su transacción bancaria, uno de los hombres, B, entra y le pregunta si le puede ayudar a manejar el cajero. A, un poco intimidada acepta y el hombre B toma su tarjeta, le indica cómo debe pasarla por el lector y le pide que digite la clave, luego de ello le regresa su tarjeta, ella en presencia del extraño digita su clave y realiza el retiro, el cajero arroja su dinero y la mujer sale de allí con la tarjeta débito y la suma que extrajo.

Una hora más tarde empieza a recibir comunicaciones vía teléfono celular de la oficina de seguridad bancaria donde la interrogan si ella estaba en ese momento realizando unos retiros de su cuenta. A niega estas transacciones y le piden que revise su tarjeta débito. Al observarla detenidamente se da cuenta que la tarjeta poseída no es la suya, por lo que solicita al funcionario que de manera inmediata congele su cuenta hasta el día siguiente hábil.

Para el instante en que se congela su cuenta, ya los delincuentes habían retirado la suma de un millón doscientos mil ($ 1.200.000) pesos en efectivo y realizaron transferencias a otras cuentas de terceras personas, en ciudades de Bogotá y Cali por un monto cercano a los quince millones de pesos ($15.000.000), dinero que fue retirado a través de oficina bancaria, dándose la consumación del hecho punible en el instante mismo en que los autores se apoderan del dinero entregado por el cajero automático, así como en el instante en que éste es transferido de la cuenta del titular a la del receptor ilegítimo del dinero, pues en ese momento sale de la órbita de custodia del propio banco.

Ejemplo de Hurto por medios Informáticos y semejantes (Art. 269I). El caso de la clonación de tarjeta débito o crédito.

Un hombre adulto A se encuentra frente a un cajero electrónico con la finalidad de hacer un retiro de su cuenta de ahorros; una vez ingresa al cajero e introduce su tarjeta y hace un retiro en efectivo, otro hombre B entra y le dice que la transacción le quedó mal realizada, le pide que inserte nuevamente su tarjeta, pero antes de hacerlo, hábilmente el delincuente se apodera de ella y la introduce él mismo en el lector del cajero, luego le pide al hombre A que digite su clave y cuando está realizando esta acción, el hombre B con un dispositivo manual clona la banda magnética de su tarjeta y como ha observado plenamente la clave termina su actividad. El cliente recibe el dinero pedido en la transacción y ante lo extraño de la situación se dirige a otro cajero ubicado cerca y consulta nuevamente su saldo, encontrando todo correcto.

Sin embargo, horas más tarde recibe señales de alerta del sistema de seguridad del banco, donde le indican que se habían realizado dos transferencias de su cuenta por un monto de ocho millones de pesos ($8.000.000), el cliente se dirige al banco, consulta las últimas transacciones y niega las

transferencias de su cuenta a la de terceros por el monto estipulado. Presenta su tarjeta original a la entidad bancaria. Al observar el video de la cámara de seguridad se puede apreciar cuando el ciudadano A recibe ayuda de un tercero B, digita su clave en presencia de aquél, e igualmente cómo el victimario al tomar la tarjeta con ágiles maniobras la pasa por un dispositivo manual de copiado de información. En este supuesto, igualmente la consumación se presenta en el instante en que se apoderan del dinero entregado por el cajero electrónico y en el instante en que se realizan las transferencias desde la cuenta del titular a la cuenta del receptor ilegitimo, pues en esos momentos salen de la órbita de custodia del banco.

Ejemplo de transferencia no consentida de activos. Art. 269J CP.

Un sujeto activo conocido como hacker, diseña unos programas maliciosos llamados troyanos, virus, gusanos, o páginas falsas, etc., los cuales son implantados en la red de internet y dirigidos a buscar computadores con fallas de seguridad para "infectar". La finalidad de aquél software maliciosos es extraer la información financiera - números de cuentas bancarias y claves e información personal de quienes utilizan dichos dispositivos de comunicación para efectuar transacciones electrónicas.

Es así que una vez obtenida la información bancaria por parte del delincuente informático a través de los ataques o técnicas descritas, esta información correspondiente a números de cuentas bancarias y claves personales es vendida al mejor postor, quien es el sujeto activo de la conducta o – Sujeto B-, personaje que no domina el conocimiento de los lenguajes de programación y sólo se limita a comprar la información ya recolectada por los hackers. Luego de ello y a través de terceros el sujeto B busca deudores del mismo sistema financiero, de empresas de servicios públicos, o de cualquier tipo de deuda que pueda ser pagada a través de la red para que aporten su factura – Sujeto C -.

Al encontrar un deudor – Sujeto C-, dispuesto a prestarse para continuar con el *iter criminis*, se llega a un acuerdo entre ambos sobre el pago virtual de las mismas, por lo que éste entrega el documento con código de banco, número de identificación personal y valor a pagar, para que el Sujeto B - ejecute su cancelación. Con el anterior documento y la información comprada al hacker el sujeto activo B ingresa ilícitamente vía internet a las cuentas de los titulares de las mismas y una vez allí de manera digital ingresa la información correspondiente al número de la factura, su valor y Código y desde su PC transfiere el dinero del saldo que posee el titular de la cuenta a la empresa privada o pública para realizar el pago previamente facturado. Es entonces cuando culmina la cadena delictiva y se consuma para el primero de ellos, esto es el hacker, el delito de Violación de datos personales - artículo 269F - y para los Sujetos A y B la transferencia no consentida de activos.

6. Hurto por medios informáticos y semejantes. Elementos típicos del art. 269 I CP.

Con la finalidad de comprender cada una de las nuevas conductas creadas por la legislación penal, en procura de proteger ese bien jurídicamente tutelado del patrimonio económico y la protección de la información y de los datos, es necesario descomponer sistemáticamente las conductas prohibidas descritas en los artículos 269I y 269J CP.

Art. 269 i. Hurto por medios informáticos y semejantes. *El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el art. 240 de este código.*

6.1. Clasificación de la conducta del art. 269 I CP.

Uno de los objetivos del desarrollo de la presente investigación tiene que ver con la clasificación de los tipos penales estudiados. Pues bien, veamos dicha clasificación en su orden, según los parámetros que ofrece el Profesor Juan Oberto Sotomayor (Sotomayor, 2012) en su curso de Derecho penal I de 2012.

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" (2012, pág. 5). 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 están enmarcadas 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 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, como se ha expuesto, 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.

Continuando con la clasificación abordaremos la **tipicidad** desde el **artículo 10** del CP, donde señala la norma: "*La ley penal definirá de manera inequívoca, expresa y clara las características básicas estructurales del tipo".*

Pabón Parra (1999, pág. 105) define el concepto de tipicidad como aquella "…adecuación plena de la conducta a la descripción abstracta contenida en el precepto legal, tanto en referencia a todos y cada uno de sus elementos o presupuestos objetivos, como a los componentes subjetivos inmersos en el precepto – tipicidad objetiva y subjetiva…". Por su parte, Fernández (2002, pág. 250) lo define así: "…el tipo es la descripción de la conducta hecha por el legislador…" y agrega, trayendo el concepto de Zaffaroni, que "…es un instrumento legal, lógicamente necesario y de naturaleza predominantemente descriptiva, que tiene por función la individualización de conductas humanas…" (pág. 250).

Y entra el autor a desarrollar cada uno de los anteriores conceptos, indicando que "…es *legal* dado que es un dispositivo plasmado en la ley; es *lógicamente necesario* porque para saber si una conducta es delictuosa no puede prescindirse de tal herramienta; es *descriptivo* porque a la hora de consignar las conductas el legislador suele acudir a "descripciones" valiéndose de figuras lingüísticas apropiadas, o elementos descriptivos como " matar", " falsificar", "cosa"; en otras oportunidades, sin embargo utiliza dicciones que se remiten o sustentan – en gran medida- en juicios de valor de carácter jurídico, como "título no traslativo de dominio", "ajena", "servidor público", "documento público"; o elementos de índole subjetivo como "ánimo de lucro", propósito de obtener provecho" y tiene la *función de individualización* de conductas humanas penalmente prohibidas porque es el encargado de otorgar relevancia penal a los diversos comportamientos valorados de manera negativa por el legislador (pág. 251).

Con base en las anteriores definiciones, entraremos a realizar el análisis de los diferentes elementos del tipo penal que nos ocupa, empezando por:

6.2. Los sujetos activo y pasivo.

Sujetos Activos:
La definición que el Código Penal trae de autor (*art. 29 C. Penal. Es autor quien realiza la conducta punible por sí mismo o utilizando a otro como instrumento. Son Coautores los que mediando acuerdo común, actúan con división del trabajo criminal atendiendo a la importancia del aporte)*, y que describe en el art. 269 i, 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 en todas las ocasiones estudiadas en denuncias facilitadas por la Fiscalía General de la Nación, la acción es desplegada por varios sujetos que comparten la autoría (coautoría) o participan del hecho punible. Veamos cómo se desarrolla:

Con los supuestos fácticos atrás relacionados, encontramos que las modalidades identificadas permiten determinar que si se ejecutan hurtos por medios informáticos y semejantes, bajo la manera de clonación de tarjetas, los autores suelen ser varios, uno de ellos como se dijo 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 tantos

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.

Tomando como base la tesis de **Claus Roxin** (Roxin, 1998)**,** posición que sustentamos y compartimos, por brindar mayor seguridad jurídica, es a través del dominio del hecho que se desprenden las figuras por el expuestas, veamos. Quien domina la acción directamente y realiza el verbo rector es **autor único inmediato**; quien ejerce el dominio de la voluntad de un tercero para que actúe como autor es conocido como **autor mediato**; es **coautor** quien ejerce ese dominio funcional del hecho y **participe** quien no obstante concurrir en la realización del hecho es ajeno a ese control de la acción causante del resultado, así como de ese dominio funcional que se pregona pues ni siquiera tiene el dominio sobre la voluntad de quienes lo causan por lo que su aporte es considerado como concurrente para el alcance del delito.

En la coautoría, según la doctrina, las personas que concurren a la realización del delito deben acordar previamente la ejecución del mismo y comprometerse a aportar a través de su acción de manera individual y necesaria para que se concrete el ilícito, es por tanto sobre esos sujetos que se subdivide en partes iguales el control o dominio funcional de ese hecho causante de un resultado delictivo.

Teniendo como base lo anterior, es autor directo quien ejecuta el verbo rector, esto es, quien tiene el dominio de la acción típica. Para el presente caso, 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 - Primer ejemplo-, 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 estaríamos 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 ó 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:
Ahora bien, retomemos otro de los elementos que para este tipo de conductas punibles es bien importante de conocer y que corresponde al ***sujeto pasivo,*** persona natural o jurídica, pues son aquellos que padecen el desmedro económico y perjuicio en sus intereses patrimoniales.

Veamos una definición de sujeto pasivo. Víctimas, según el Código de Procedimiento Penal, en su artículo 132, son: las personas naturales o jurídicas y demás sujetos de derechos que individual o colectivamente hayan sufrido algún daño como consecuencia del injusto. Según la doctrina, el **sujeto pasivo** es definido como aquél que tiene la titularidad del interés o bien jurídico primordialmente tutelado por un determinado tipo penal, bien que es amenazado o vulnerado con la realización de la acción típica (Pabón Parra, 2002, pág. 831).Por su parte, Fernández (2002, pág. 260) define el sujeto pasivo como "…el titular del bien jurídico protegido en cada caso concreto y que puede resultar o no perjudicado con la conducta del sujeto activo…".

Debe advertirse igualmente, que 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.

Para tener una idea de cómo resolver este asunto, 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. Si aceptamos este planteamiento, que corresponde a lo ocurrido en muchos de 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 269 i CP.

Sin embargo, ¿qué ocurre cuando 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? Esa es otra posibilidad. ¿Recae la responsabilidad en la entidad bancaria encargada de la seguridad de sus cajeros automáticos o se traslada al cliente? Aquí surge otro planteamiento y es el hecho de conocer que en el lugar se vulneró la seguridad del cajero electrónico. Si ello ocurre, es decir, si se establece un cajero como punto de compromiso, no debe ser sujeto pasivo –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".

La discusión jurídica sobre quién se afecta con la pérdida del dinero es ardua, respecto a este tipo de conductas punibles de hurto por medios informáticos y hasta ahora, esa devolución de lo hurtado bajo esas modalidades, no es en favor de los titulares de las cuentas bancarias, quienes casi siempre resultan siendo víctimas del delito. Sin embargo, en las pocas oportunidades en que la entidad bancaria devuelve al cliente la suma hurtada, sería en ella en la que confluirían las calidades de sujeto pasivo y víctima a la vez.

6.3. La acción o conducta.

Tomamos **la acción** desde el concepto finalista utilizado por Mir Puig (2003, pág. 162): "… el derecho penal de un Estado Social y democrático de derecho sólo puede prohibir comportamientos voluntarios finales. En un derecho penal las normas se justifican por su necesidad para evitar de sus destinatarios determinados comportamientos indeseables. Las normas penales no tienen entonces sentido en orden a evitar comportamientos que no puedan ser evitados mediante su motivación normativa…". Por tanto**,** la acción típica es aquella conducta prohibida por el ordenamiento jurídico. Fernández (2002, pág. 261), la define en los tipos dolosos como "… acciones en sentido estricto, para lo cual se vale generalmente de una inflexión verbal, de un verbo encargado de regir la acción o *verbo rector* que es concreción de una prohibición…".

La acción entonces es un comportamiento prohibido para el ciudadano, elevado por el legislador a la categoría de norma penal y cuyo elemento principal prohibitivo está definido en el verbo rector que concreta esa prohibición (o mandato, si se trata de tipos omisivos), tenemos entonces que en los delitos estudiados las acciones prohibitivas son las siguientes:

El verbo rector consagrado en el art. 269 i CP, implica que para ser catalogada la conducta como delito hay que acudir a la prohibición señalada en el artículo 239 del Código Penal, 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, no sólo en dinero, que es retirado de las cuentas de los clientes bancarios, sino también en 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.

La norma, sin distinción, es subordinada del tipo básico del hurto descrito en el 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, es así que retomando el concepto descrito en el numeral 6.1 y lo que ha definido 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.

Para comprender mejor que es Seguridad Informática y Manipulación de un sistema informático, pasaremos a su definición:

¿Qué es la SEGURIDAD INFORMÁTICA? Señala el profesor Posada Maya (2006.pdf, pág. 26): "…la seguridad informática puede ser definida como aquellos programas eficaces diseñados e implementados en los servidores de las empresas o entidades bancarias, que busca limitar el ingreso o acceso a un sistema, además de ellos, para evitar exponer la integridad, confidencialidad, o disponibilidad de los datos o la información de naturaleza reservada al riesgo de intrusión (suicidio informático)…" la seguridad informática, indica "…contienen, además, los ataques de otros programas maliciosos (virus, gusanos, bombas lógicas, troyanos)… que buscan acceder a las bases de datos donde reposa la información privilegiada y valiosa para el hacker…".

Superar esas medida de seguridad, no es más que realizar una intrusión, para este caso, - art. 269i - a través de maniobras fraudulentas utilizadas por los delincuentes, al sistema informático de las entidades bancarias o empresas a las cuales se les pretender hurtar su información.

Diferente es el caso de la transferencia no consentida de activos, que se analizará más adelante, donde a través de la utilización de virus, gusanos, troyanos, bombas lógicas y programas espías se logra ingresar hacer una intrusión a los computadores de las víctimas para sustraer de ellos la información privilegiada que se requiere a fin de vulnerar el patrimonio económico o la información personal privilegiada.

Ahora bien, ¿qué es manipular un sistema informático?

Existen muchas definiciones de sistema informático, una de las más sencillas es quizás la siguiente: "…Un **sistema informático**, es un "…conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales… (Acuario del Pino, 2010)" como todo sistema tiene un conjunto de partes interrelacionadas, esto es hardware y software, así como recurso humano que permite almacenar y procesar información. El hardware incluye computadores de cualquier tipo y dispositivo electrónico inteligente, que consisten en procesadores, memoria, y sistemas de almacenamiento externo, etc. El Software incluye el sistema operativo siendo especialmente importante los sistemas de gestión de bases de datos. Por último el soporte humano incluye al personal técnico que crea y mantiene el sistema, entre ellos están los analistas de sistemas, programadores y operarios.

Otro de los ingredientes de la conducta es lo que definiremos como **manipular**, y esto corresponde según la Real Academia de la Lengua, "…manejar cosas, controlar cosas, situaciones". Uniendo así los dos conceptos, tenemos que ese elemento del tipo "manipular un sistema informático", corresponde al manejo o control del hardware que incluye computadoras – para este caso los cajeros electrónicos-, y sistemas de almacenamiento externo de información – bandas magnéticas o chips de las tarjetas electrónicas que almacenan o conservan información-, a través de las cuales se accede a una pequeña parte del sistema o a la información a la que tiene acceso el cliente del banco a quien le hurtaron su "llave" de ingreso al mismo, permitiendo ello manipular el sistema con la finalidad de acceder a la cuenta del cliente y desde allí realizar retiros a través de cajeros o transferencias electrónicas de su dinero.

Así mismo definiremos lo que es "… suplantar a un usuario ante los sistemas de autenticación y de autorización establecidos…". Siguiendo la metodología anterior, se descompondrá la oración y se definirán cada uno de los conceptos.

Suplantar, según la real academia de la lengua es sustituir ilegalmente a una persona u ocupar su lugar para obtener beneficios.

El Sistema de autenticación, por su parte, tomándolo en términos de seguridad de redes de datos o sistemas informáticos, podemos deducir de las diferentes lecturas que es aquel proceso de verificación de la identidad digital de quien remite una comunicación como una petición para conectarse. El usuario remitente puede ser una persona, un computador o un programa elaborado bajo un lenguaje especial y enviado desde el computador o dispositivo de comunicación. En un sitio web de confianza – página de banco o de compras -, la autenticación es el modo de asegurar que los usuarios son quien ellos dicen que son, esto es que el usuario que intenta ingresar al sistema a realizar funciones es de hecho el usuario que tiene la autorización para hacerlo, si está plenamente identificado por el sistema. Este proceso de autenticación, en el sistema financiero inicia desde el momento en que se introduce la tarjeta al lector, para que el sistema identifique la información allí contenida como válida y se digita la clave o password, al autenticarse al usuario se le permite ingresar al sistema.

El Sistema de autorización, ligado a la autenticación, es un proceso digital – una vez digitada la clave o password - por el cual una red de datos autoriza a un usuario previamente identificado a acceder a determinados recursos de la misma.

Según lo anterior, al combinarse ambos, esto es autenticación y autorización, ello le permite al usuario del sistema informático realizar una comunicación entre usuario y sistema para ejecutar una determinada operación dentro del mismo, ya sea realizar retiros, transferencias, pagos, cambiar claves, inscribir cuentas relacionadas, etc.

Los factores de seguridad informática están íntimamente ligados al momento de solicitar el ingreso a un sistema informático, según el profesor JEIMY CANO, (J., 2009) los sistemas informáticos están diseñados bajo unos estrictos controles de seguridad, controles que deben estar relacionados con el funcionamiento de la infraestructura, para garantizar una mayor confiabilidad, disponibilidad, trazabilidad e integridad de la información requerida por el usuario, y cuyo riesgo principal al momento del ingreso al sistema es la impericia y falta de cuidado de los usuarios finales que lo utilizan, tomando lo anterior como base y reforzándolo con lo señalado por (Hernández Orallo) en su texto digital Seguridad y privacidad en los sistemas informáticos , "…es importante remarcar que la seguridad supone un coste y que la seguridad absoluta es imposible. Por lo tanto, hay que definir cuáles son nuestros objetivos y a qué nivel de seguridad se quiere llegar…" para establecer, conforme dicho texto, los controles que deben existir para ingresar al sistema, indicando que estos comprenden medidas de seguridad basadas en un estudio de coste/beneficio, que conlleve a la ejecución protección física de las instalaciones – Guardianes de seguridad-, medidas tales como soluciones informáticas que aumenta la seguridad de los sistemas, lo que incluye cifrado de la información, cortafuegos, antivirus, detectores de intrusos, cursos de formación sobre seguridad a los usuarios del sistema, auditorías informáticas, y lo

principal, para los usuarios, criptografía y autenticación como elementos indispensable para ingresar al sistema a través de claves secretas, algoritmos de encriptación y seguridades internas que permitan determinar que quien efectivamente ingrese al sistema es la persona autorizada para ello bajo los parámetros y privilegios acordados entre el administrador del sistema y el usuario.

Para hacer más comprensible lo anterior, hay que significar que la mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de auditoría oportunos.

Con base en ello el primer elemento necesario y suficiente estrictamente hablando, por tanto para la autenticación es la existencia de identidades biunívocamente identificadas con un identificador único. Los identificadores de usuarios pueden tener muchas formas siendo la más común, según la literatura sobre informática una sucesión de caracteres conocida comúnmente como **login**, **password** o **clave personal**

Descifrando entonces lo anterior tenemos que el proceso general de autenticación en un sistema consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

Al cumplir así con los requisitos exigidos por el sistema, para autorizar y autenticar, el sistema habilita al usuario para que ingrese y realice las acciones permitidas según su perfil, dentro de aquél, esto es en palabras sencillas retiros de dinero, transferencias, pagos, consultas etc.

Vemos entonces, que cuando alguien vinculado a las organizaciones dedicadas a la clonación de tarjetas débito y crédito y obtención de sus claves, ingresa al sistema, con una banda magnética o chip utilizando estos dispositivos de almacenamiento o conservación de información, y digita la clave, esto es se autentica ante el sistema como la persona titular de la cuenta, - sin serlo- el sistema autoriza su ingreso y es allí donde automáticamente se está suplantando al titular de la misma, por lo que se cumple con ese elemento normativo del tipo.

6.4 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.

6.5 Dispositivo Amplificador del Tipo: La Tentativa.

A pesar de la claridad del momento en que se produce el apoderamiento del objeto material, ha surgido en la práctica un interrogante a resolver y es: ¿Qué ocurre cuando por información de la ciudadanía o de empleados de seguridad de los bancos se captura un ciudadano con un aparato de copiado de tarjetas débito y crédito – Skimmin o Skimer - o con varias tarjetas de diferentes entidades bancarias a nombre de terceras personas? ¿Se puede hablar allí de apoderamiento de "cosa mueble ajena" u objeto material del delito del artículo 269 i CP? Y otra pregunta más, ¿si el objeto material es el dinero ("cosa mueble") que persigue el autor de la conducta punible, la apropiación del skimmin con la información de las bandas magnéticas o las solas tarjetas débito o crédito a nombre de terceras personas, puede configurar una tentativa de hurto por medios informáticos y semejantes?

La respuesta, desde nuestro punto de vista, es que esos elementos – skimmin y tarjetas - , como se ha descrito, son medios utilizados para llegar a un determinado fin, dado que es necesario no sólo su posesión, sino los demás actos ejecutivos que permitan el desarrollo de la conducta punible y esos otros actos, son: trasladar la información del aparato clonador a una nueva banda magnética, y la utilización de esa nueva banda, con la clave personal en un cajero automático para proceder a identificarse, autenticarse e ingresar al sistema telemático o informático y así ejecutar ese apoderamiento del dinero disponible. Igual sucedería cuando se logra acceder a claves o información digital de una persona para ser utilizada con la finalidad de sustraer de manera ilegítima datos privilegiados de un cliente, una empresa o institución.

Para aclarar esta constante duda que surge, de si hay tentativa o no cuando se presenta esa incautación de elementos para clonar tarjetas débito o crédito, debe analizarse un aspecto dogmático fundamental que está descrito en la definición de Tentativa.

Art. 27. El que iniciare la ejecución de una conducta punible mediante actos idóneos e inequívocamente dirigidos a su consumación, y ésta no se produjere por circunstancias ajenas a su voluntad, incurrirá en pena…

Cuando la conducta punible no se consuma por circunstancias ajenas a la voluntad del autor o partícipe, incurrirá en pena no menor…

Vemos así que una exigencia de la norma es iniciar la ejecución de la conducta. Se debe recordar que el *iter criminis* tiene cuatro componentes que son: idea criminal, actos preparatorios, actos ejecutivos y consumación.

Además de la idea criminal y de que el medio sea idóneo para su comisión, también es necesario el inicio o ejecución de la conducta punible, es decir, esa puesta en peligro del bien jurídicamente tutelado a través del comienzo de la acción típica; acción que inicia en el momento de ingresar al sistema a través de la autenticación y autorización, pues sin ello, sólo nos quedaríamos en los actos preparatorios y para que se configure el tipo penal exige la manipulación del sistema o la suplantación de un usuario ante el mismo con la finalidad de apoderarse (art. 239 CP) del bien mueble - dinero- y, ¿cómo se producen éstas? La respuesta es desde el instante en que se ingresa al sistema informático.

Siendo ello así, tenemos una persona con una idea criminal, realizando actos preparativos para una acción determinada -Hurto por medios informáticos-, con unos medios idóneos –componentes que almacenan datos personales, cuentas y claves -, pero que aún no ha iniciado los actos de ejecución para afectar ese bien jurídicamente tutelado del patrimonio económico, al cual dirige su acción. Por tanto, no se podría sancionar conforme lo dispone el artículo 269i a título de tentativa, sin embargo, esa acción no es atípica y quien es capturado en posesión del dispositivo de almacenamiento con la información compilada, **sin estar facultado para ello,** queda incurso en el tipo penal descrito en el artículo 269F, esto es Violación de datos personales, por configurarse allí varios verbos rectores como pueden ser compilar, interceptar, o emplear códigos personales, datos personales contenidos en un archivo, o base de datos.

7. Transferencias no consentidas de activos. Elementos típicos del art. 269 J CP.

Siguiendo la metodología anterior, pasaremos a descomponer sistemáticamente la conducta prohibida descrita en el artículo 269J CP.

*Art. 269 j. 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.

7.1. Clasificación de la conducta del art. 269J CP.

Ahora bien, siguiendo los lineamientos del anterior delito, definiremos cuál es la caracterización del tipo penal. Nos encontramos ante un **tipo básico**, pues se aplica sin depender de ningún otro, su contenido describe de manera independiente el comportamiento que se prohíbe, el cual corresponde a la transferencia no consentida de activos. Es de ***lesión,*** dado que al seguir el principio de lesividad descrito en el artículo 11 CP, estamos ante un tipo que exige el daño al bien jurídicamente tutelado, de ***resultado*** por cuanto ese daño se presenta al concretarse la transferencia de activos de la cuenta de la víctima a otra, sin su consentimiento, y de ***conducta instantánea*** por cuanto la acción típica 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.

7.2 Los sujetos activo y pasivo.

Sujetos Activos:

Igual que el anterior artículo 269 i CP, no exige a quien comete la conducta punible calidad especial alguna, por lo que autor es "el que" la ejecute. Esto es, cualquier persona natural puede ser responsable de ella. Sin embargo, 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, tal y como ha quedado claro.

Es necesario, por tanto, referirnos a sujetos activos de la conducta, en sentido plural, tal y como se hizo con el artículo anterior, pues de la lectura de cientos de casos adelantados en la Fiscalía de Medellín, Unidad Estructura de Apoyo, de los años 2011 y 2012, esta conducta punible no es ejecutada por un solo individuo, sino por un grupo de personas concertadas previamente para realizarla, recordemos el ejemplo descrito en el numeral 5 donde se detallan sus intervinientes:

1) Hacker (sujeto activo A).
2) Comprador de información al hacker (sujeto activo B).
3) Deudor del sistema financiero o entidades públicas o privadas (sujeto activo C) quien facilita su factura para que el sujeto activo B, la pague a través de medios virtuales.
4) Víctima, a quien a través de manipulaciones informáticas o artificios la desapoderaron de su información bancaria – número de cuenta y clave personal- y dinero.

Retomando la teoría de Roxin, ya expuesta, es necesario hacer el siguiente análisis respecto a la forma participación de cada uno de los Sujetos en la comisión del hecho, y que no son otros que el hacker (Sujeto A), Sujeto B y Sujeto C.

Empezando por el hacker (Sujeto A), debemos decir que su actividad se concentra en obtener a través de las diferentes técnicas de intrusión la información bancaria de los titulares de las cuentas. Su accionar entonces llega hasta allí, sin ejecutar el verbo rector descrito en el artículo 269J, esto es la transferencia del activo. Siendo ello así quedan dos caminos para resolver el

interrogante sobre su responsabilidad y son los siguientes: a) debe este interviniente responder a título de cómplice necesario, conforme lo señala Roxin, por aportar una información sin la cual no sería posible el acceso a unas cuentas de titulares de activos? ó ¿debe responder como autor del ilícito descrito en el artículo 269F, esto es la conducta típica de violación de datos personales?

Consideramos que su acción dolosa estuvo dirigida solamente a realizar las intrusiones ilegitimas buscando obtener la información personal y bancaria de los clientes, información que no emplea posteriormente para vulnerar un sistema e ingresar a realizar transferencias electrónicas, sino que es vendida al mejor postor para que aquél la aproveche lucrándose ilegalmente al realizar el verbo rector del tipo. Por ello su responsabilidad debe ser a título de autor conforme lo señala el artículo 269F, pues compiló información personal, no autorizada y secreta, dicho tipo penal describe perfectamente su accionar antes de la comisión del segundo hecho punible, además de ello, no hace un aporte esencial en la parte ejecutiva de la acción que se inicia cuando se ingresa al sistema y se termina con las transferencias no consentidas de activos. Además del argumento anterior, existen otros dos más que fortalecen esta posición, el primero de ello dentro de la misma redacción del artículo 269J que dice "…siempre que la conducta no constituya delito sancionado con pena más grave…" y el segundo que se expondrá más adelante y tiene que ver con el tema del concurso de conductas punibles, permitiendo a través del principio de la especialidad fortalecer los argumentos sobre la responsabilidad del Sujeto A o hacker.

Ahora bien ¿a qué título responde el Sujeto B? No hay duda alguna que es la persona que tiene un dominio total del hecho, por tanto es un autor de la conducta punible descrita en el artículo 269J, basta con repasar la descripción fáctica, para determinar que es él quien ejecuta íntegramente el verbo rector, eso sí, previa consecución de la información bancaria y las facturas o pagos a realizar vía internet.

¿Y el Sujeto C? Retomando lo dicho por Roxin (1998, págs. 166 y ss.), tenemos que indicar que es un cómplice necesario, pues sin su ayuda o entrega de los documentos con número de referencia, nombre de la entidad a la que se le debe hacer el pago, fecha de pago y valor a pagar al Sujeto B, no se podría llevar a cabo la realización de la conducta delictiva que se analiza y es necesario, por cuanto su aporte, esencial para la comisión de esta conducta, no se presenta en la fase ejecutiva de la realización del delito, limitándose a hacer entrega de su documento y desconociendo el momento en que este se llevará a cabo, lo que hace que pierda cualquier tipo de dominio sobre el hecho.

Sujetos Pasivos:

Se debe definir quién puede ser en este caso. Si tomamos la definición de sujeto pasivo, como aquel titular del bien jurídico tutelado perjudicado con la conducta, tenemos que analizar lo siguiente:

Es claro que el ingreso que ejecutan los delincuentes informáticos para cometer este tipo penal es a través del sistema digital protegido por el banco y allí directamente a la cuenta del titular desde donde ejecutan las transferencias no consentidas de activos. También es claro que la información obtenida para acceder ilegalmente a la cuenta se consiguió por el hacker a través de maniobras de engaño, tales como phishing, pharming y otras modalidades delictivas, sin embargo es necesario definir quién tiene la custodia del dinero, y del sistema o programa digital que permite ejecutar las transacciones electrónicas autorizadas para el cliente. Esa custodia la tiene directamente el banco;

es esta entidad quien monitorea continuamente los ingresos desde las diferentes IP de donde se realizan los movimientos bancarios y ese monitoreo le da el privilegio de impedir la entrada de una dirección electrónica utilizada para la comisión de transferencias no consentidas de activos. Igualmente, es el banco quien, una vez reportado el fraude por parte del titular de la cuenta, puede dar aplicación al Acuerdo Interbancario, vigente desde el pasado 01 de enero de 2011 el cual fue expedido por la Asobancaria, y que le permite al usuario del sistema financiero reversar una transacción no consentida por ellos y realizada desde su cuenta vía internet, cajero electrónico o cualquier tipo de anal electrónico, y solicitar como consecuencia de ello la **reversión** de la misma a su cuenta personal, teniendo presente sí, que debe cumplirse con unos sencillos requisitos buscando exonerar a la entidad de cualquier tipo de reclamación civil en caso de que la solicitud no sea cierta. De esos argumentos se desprende que ante la custodia, no sólo del dinero, sino del sistema, y los movimientos bancarios desde las cuentas de las víctimas de este tipo de conductas punibles, sea la entidad bancaria la víctima del hecho y no el titular de la cuenta en ella registrada.

Sin embargo, la discusión puede presentarse álgida en cuanto a quién se señala como víctima, pues 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. Tema que queda abierto para una futura discusión.

7.3. La acción.

Descomponiendo el tipo como en el análisis anterior, tenemos que el artículo 269 J posee un verbo rector principal y es **transferir**, y cuatro más 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, sin embargo, nuestra investigación sólo se centra en el primero de los verbos.

Ese 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.

Una vez descrito lo anterior, tenemos que **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.

Siguiendo con el inciso final, tenemos que **fabricar** no es más que hacer o construir una cosa a partir de una combinación de componentes. Para el caso que nos ocupa 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, por su parte, 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, ó 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.

Hay que señalar que las acciones descritas anteriormente, en nuestro país, son difíciles de demostrar en los estrados judiciales dada la falta de preparación de los funcionarios públicos 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.

7.4. El objeto material.

Resulta necesario, para entender este apartado, definir 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, en su lección - Estructura del Tipo Penal – pág. 199, dice lo siguiente: "…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)…"

El profesor Fernando Velásquez, por su parte, 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…" (Manual de Derecho Penal, parte General, pág. 276).

Tal y 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 el caso de las transferencias no consentidas de activos, tenemos, según lo investigado, que el dinero es el principal activo que buscan los autores de la acción ilícita. Sin embargo, recordemos que también hay activos intangibles que como en el caso anterior del artículo 269 i, pueden ser la información privilegiada de personas naturales o jurídicas.

7.5 Elementos subjetivos, descriptivos y normativos del tipo.

Por elementos subjetivos, según VELASQUEZ (2002, pág. 277) se entiende el *dolo* y aquellos otros *elementos subjetivos distintos al dolo*

Por elementos normativos y descriptivos en cambio se entienden los primeros como aquellos pueden referirse a una significación cultural o significación jurídica o normativa y los segundos, aquellos, que el autor puede conocer sin hacer una especial valoración, como por ejemplo en el hurto la cosa mueble.

1. Teniendo las anteriores definiciones, tenemos que 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. 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. Y efectivamente 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 artículo 269 J.
3. Debe igualmente el sujeto activo valerse de una "**manipulación informática"**. Término que ya fue descrito en el análisis del capítulo correspondiente al hurto por medios informáticos y semejantes.
4. 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 electrónicos a través de los cuales se instalan los programas espías en sus ordenadores.

Retomando el ánimo de lucro que tiene que tener el delincuente informático, el cual recae sobre el objeto material – que no es otro que el dinero como activo, existe una fuerte discusión jurídica a nivel de la judicatura, respecto al siguiente problema jurídico: ¿qué ocurre cuando ese activo es transferido ilícitamente como pago de una factura, servicio o deuda a una entidad pública -Empresa de servicios públicos domiciliarios, impuestos predial, impuesto de vehículos, pagos de multa de tránsito -, o privada -Empresas de telefonía celular, empresas de servicios públicos privados, empresas de financiamiento, entidades bancarias-, desde una cuenta que ha sido vulnerada a través de artificios o manipulaciones informáticas? ¿Puede ese objeto material, ser legitimado por ese tercero, que lo recibe como pago de una deuda legítima o un servicio público prestado?

La discusión en los estrados judiciales es ardua y las soluciones no son pacíficas por lo siguiente. Se ha debatido en la praxis judicial por parte de pocos Fiscales de ciudades como Cali y Medellín, en audiencias preliminares, llamadas de restablecimiento del Derecho -art. 22 CPP-, dentro de diferentes indagaciones, si el receptor debe o no devolver el dinero con el que se pagó ilícitamente desde una cuenta bancaria a través de transferencias no consentida de activos, una factura. En la ciudad de Cali, dentro de los siguientes casos se ha dispuesto en favor de las víctimas titulares de las cuentas, **REVERSAR** los pagos fraudulentos a su cuenta original; veamos en qué casos: radicados SPOA 760016000193201014684 de fecha 08 de febrero de 2011, emitido por el Juzgado 26 de Control de Garantías; 760016000193201022150 de febrero 11 de 2011, emitido por el Juzgado 20 de Control de Garantías; 760016000193201018801 de Marzo 02 de 2011, emitido por el Juzgado 29 de Control de Garantías; 760016000193201019616 de marzo 08 de 2011, emitido por el Juzgado 28 de Control de Garantías 760016000193201000912 de marzo 10 de 2011, emitido por el Juzgado 13 de Control de Garantías; 760016107110201000440 de marzo 15 de 2011, emitido por el Juzgado 4 de Control de Garantías; 760016000193201026717 de marzo 15 de 2011, emitido por el Juzgado 21 de Control de Garantías; 760016000193201016553 de marzo 16 de 2011, emitido por el Juzgado 2 de Control de Garantías todos ellos de la ciudad de Cali, en cada una de esas decisiones se dispuso la **reversión** del dinero por pagos ilícitos transferidos vía electrónica como pago de facturas a entidades financieras, de servicios públicos y otros.

En la ciudad de Medellín, por su parte, dentro del radicado 050016000206201012563, en agosto de 2011, se adelantó audiencia de restablecimiento del derecho y el Juez Octavo de Control de Garantías, así como el 15 Penal del Circuito - en segunda instancia-, negaron el restablecimiento de ese derecho a la víctima argumentando la buena fe de la empresa privada que recibió el pago desde una cuenta ajena al titular del deudor. Sin embargo, posteriormente ha ido cambiando esa visión procesal y constitucional y dentro de la indagación que se adelantó en el proceso donde figura como víctima el señor SERVIO EDISSON BASTIDAS ALVAREZ en contra de las empresas COMCEL, CODENSA Y ETB por pagos realizados a través de transferencias no consentidas de activos, los Jueces 10 y 18 Penal Municipal de Control de Garantías y 18 Penal del Circuito de Conocimiento en segunda instancia, en Febrero y Junio de 2012 ordenaron que se **reversaran** esos pagos ilegítimos efectuados a través de transferencias electrónicas a las cuentas de origen, con el fin de restablecer el derecho del denunciante titular de la cuenta de origen.

Por su parte, el Tribunal Superior de Bogotá, - Sala Civil – con decisión de fecha 18 de diciembre de 2009, Magistrada Ponente LUZ MAGDALENA MOJICA RODRIGUEZ, en proceso ordinario que adelantó la señora TERESA DE JESUS RODRIGUEZ DE GORDILLO contra el Banco de Bogotá, por unos pagos electrónicos realizados desde su cuenta bancaria a través de Internet, decidió condenar a la entidad Bancaria por el dinero que debía custodiar debidamente en la cuenta de aquella y reintegrarle la suma que salió ilícitamente de su saldo, la cual fue transferida al pago de cuentas de telefonía celular de personas ajenas a ella.

Aunque también es necesario indicar que las decisiones de los Funcionarios Judiciales han sido rebatidas por los defensores de las empresas desde el punto de vista de la buena fe, señalando que reciben pagos electrónicos en grandes cantidades, de los cuales no pueden rastrear su procedencia, simplemente aplican el principio de que quien les paga, les paga con dinero legal pues proviene de una transferencia electrónica que debe ser controlada por la entidad bancaria de donde proviene el dinero y quien tiene los recursos humanos y tecnológicos para su control; por tanto, si ella falló en esos controles, debe ser ella quien responda a su cuenta habiente y no ellos

como receptores de un pago "legítimo" por una venta de artículos o servicio prestados de manera legal.

Como se dijo, las decisiones de los operadores jurídicos no han sido unánimes, pero sí han sentado precedentes en las ciudades señaladas, allí Jueces de la República, en etapa de indagación, esto es, aún sin vincular a ninguna persona al caso, han ordenado a ese tercero – entidad pública o empresa privada – la devolución del dinero sustraído a la cuenta de origen, esto es a la cuenta cuyo dinero estaba custodiado por la entidad bancaria, por cuanto ese activo provenía de una conducta delictiva previamente demostrada.

Consideramos que si esta tesis de la Fiscalía y los Jueces que han tomado las decisiones de devolver el dinero se impone, ello redundaría en la reducción de las miles de denuncias que atiborran las Fiscalías, pues se estaría rompiendo esa cadena delictual que inicia con el ingreso ilícito al computador del titular de la cuenta bancaria de donde sustraen la información y culmina con la legalización del dinero recibido como pago de una factura por parte de la empresa o entidad que lo recibe. Sin embargo, hay que considerar otros aspectos que deben ser tenidos en cuenta y que corresponden al debate de quien es víctima en estos hechos, situación ya expuesta en el numeral 7.2 – Sujeto pasivo – y donde se planteó la posible responsabilidad que en los mismos pueda tener el titular de la cuenta que realiza transacciones continuamente por internet, ingresando su información bancaria en cualquier computador y sin las previsiones de seguridad recomendadas.

Al estudiar esta situación dentro de las investigaciones penales analizadas, se pudo ver que son muy pocas las decisiones de **reversión** de pagos al titular de la cuenta por parte de aquellos terceros que lo reciben a través de transferencias no consentidas, incluso del desconocimiento de la gente y la falta de información por parte del banco para que conozcan el contenido del Acuerdo Interbancario que permitiría en primera medida repudiar esos pagos no consentidos por ellos, llevando siempre la peor parte el cliente bancario, quien en definitiva es el perdedor de un dinero que no está bajo su custodia. De esta manera, entonces, queda abierta la discusión de si se deben o no reversar esos pagos, de manera voluntaria o por orden de una autoridad judicial, y si quien los recibe, - empresa pública o privada-, recibe pagos fraudulentos que puede legitimar a través del principio de la buena fe, o en definitiva debe devolverlos.

7.6 Dispositivo Amplificador del Tipo: La Tentativa.

Ahora bien, analizando el dispositivo amplificador del tipo de la tentativa, para determinar si se presenta o no dicha figura jurídica en esta conducta punible, debe indicarse, tomando como base los presupuestos de la misma señalados en relación con el delito anterior, lo siguiente:

Por ser de resultado y conducta instantánea se presenta el fenómeno de la tentativa, sin embargo, tal y como ocurre con el artículo 269i 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. Se resalta sí, que dicho momento fáctico es difícil de determinar, por cuanto, igual que la anterior conducta, 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.

Quienes sí pueden detectar esas intrusiones son las entidades bancarias, por cuanto registran todo tipo de movimiento en las cuentas de los usuarios y utilizando la tecnología, informan de los mismos vía correo electrónico, o por mensaje de texto al cliente a fin de conocer lo que ocurre en su cuenta en tiempo real. Sin embargo, sólo se detectará que una intrusión es ilegítima una vez se haya realizado la afectación patrimonial al cliente, ya sea a través de un retiro o una transferencia de dinero no consentido, por lo que las intrusiones previas para realizar cualquier otra actividad digital como cambiar privilegios en la red, esto es – inscripción de cuentas para realizar transferencias de dineros, aumento de montos a transferir, creación de nuevo usuarios, registro de cuentas para recepcionar pagos electrónicos, etc., no son reportados por el cliente y menos monitoreados por el banco, quedando ello en actos preparativos impunes a la luz del artículo aquí analizado, pero que pueden ser sancionados bajo los parámetros del artículo 269 A – Acceso Abusivo a un sistema informático.

8. Problemas de concursos y su resolución a través de los principios de subsidiariedad, consunción, alternatividad y especialidad.

Sin que se pretenda agotar toda la problemática que los delitos aquí estudiados pueden presentar en algunos casos, por configurar un concurso de delitos aparente o real, interesa en este punto aclarar el tratamiento que se debe dar al hecho de que un único autor despliegue una conducta que se ajuste a varios tipos penales: el de Acceso abusivo a un sistema informático (art. 269ª), y el Hurto por medios informáticos o semejantes (Art. 269I), o la Transferencia no consentida de activos (Art. 269J).

¿Cuándo se presenta un delito de Hurto por medios informáticos y semejantes (Art. 269 i) o una Transferencia no consentida de activos (art. 269 j), concursan aquellas conductas con el tipo penal descrito en el artículo 269 A, esto es el Acceso abusivo a un sistema descrito en el mismo Título VII Bis?

El art. 31 del Código Penal señala expresamente: "Concurso de conductas punibles. El que con una sola acción u omisión o con varias acciones u omisiones infrinja varias disposiciones de la ley penal o varias veces la misma disposición, quedará sometido a la que establezca la pena más grave, según su naturaleza…"

Para llegar a una conclusión sobre si se presenta un concurso aparente o real, y si este último es ideal o material, lo primero que se debe hacer es definir lo que significa **unidad de acción**.

El profesor Fernando Velásquez diferencia la unidad de acción de la pluralidad de acciones. En su texto (Manual de derecho Penal, Parte General, Editorial Temis, 2002, pág. 469), define el primer aspecto como aquél "…criterio ontológico-normativo en cuya virtud, para saber si hay una o varias acciones, se debe partir del concepto final de acción al cual se añade el enjuiciamiento jurídico social, mediante los tipos penales correspondientes; por ello, pues, deben, examinarse tanto **la finalidad concreta trazada por el autor**, **su plan**, **como el tipo penal correspondiente**, que debe ser interpretado, desde el punto de vista social. En otras palabras: la unidad de acción jurídico penal se establece, así, por dos factores (al igual que urdimbre y trama); por la proposición de un fin voluntario y por el enjuiciamiento normativo jurídico social en razón de los tipos…".

Retrotrayendo entonces los supuestos fácticos en que se desarrollan las dos conductas punibles analizadas y teniendo como fundamento la definición planteada por la doctrina sobre la **unidad de acción**, ello nos arroja una primera pauta para resolver el problema jurídico planteado, que consiste en que al analizar la acción desplegada por los autores de las conductas punibles de Hurto por medios informáticos o la Transferencia no consentida de activos, estamos en presencia de una única acción que en su recorrido trasiega como actos preparativos por otras conductas punibles como son el acceso abusivo a un sistema informático (art. 269F) y/o una Violación de datos personales (Art. 269F), sólo que esa unidad de acción lleva implícita una finalidad concreta y la ejecución de un plan determinado, esto es, el apoderamiento a través de un Hurto o una Transferencia de un activo, de dinero o información privilegiada de una persona natural o jurídica.

Otro recurso que coadyuva a resolver el problema planteado tiene que ver con lo que es un concurso y cuáles son los tipos de ellos, conforme lo señala artículo 31 ibídem.

Según lo dispuesto por Velásquez, esta figura jurídica del concurso aparente debe ser resuelta pues de aplicarse ambos tipos penales a la vez, se estaría vulnerando el principio de la prohibición de doble sanción por los mismos hechos – *non bis in ídem* – y resalta en su texto:

"…En efecto, puede ocurrir que el funcionario judicial observe, al analizar la conducta concreta a la luz del catálogo de delitos, que ésta se ajusta a lo dispuesto en varios tipos penales a la vez, pero, estudiando más a fondo el asunto, concluya que en realidad solo se trata de una adecuación perfecta, bien porque una de las normas contentivas del comportamiento es más específica que la otra; porque una absorbe el desvalor de la otra; porque una solo se aplica en defecto de la otra ; o porque una de ellas se muestra inaplicable, en síntesis, porque una excluye a la otra…" (pág. 320).

Esa figura del concurso aparente se resuelve según la doctrina y la jurisprudencia utilizando los criterios de especialidad, subsidiariedad, consunción y alternatividad. Para el caso que nos ocupa, el principio que se debe aplicar es el de **especialidad,** el cual lo define la doctrina así: "…cuando un supuesto de hecho reproduce los elementos típicos de otro más general y caracteriza de manera más precisa al hecho o al autor añadiendo elementos adicionales, es este el que se aplica y no aquél" (pág. 477). Sampedro Arrubla, por su parte, añade a lo anterior, la indicación de que "…un tipo penal excluye a otro por especialidad cuando, a más de contener las mismas características básicas del subordinado, contiene una o más que aparecen presentes en el hecho concreto".

Lo que puede llegar a causar esa confusión en el intérprete de la norma al estudiar estos delitos informáticos, tiene que ver con esos actos preparatorios para la consumación de una de las dos conductas estudiadas, pues esos preparativos a medida que se ejecutan contienen elementos que encajan en conductas típicas tal y como lo describen los artículos 269 A – Acceso abusivo a un sistema informático - Art. 269 E – Uso de software malicioso -, Art 269 F – Violación de datos personales - , actos que deben ejecutarse para llegar al fin propuesto por el autor que es, en el caso del Hurto informático, el apoderamiento del activo o, en el caso del 269J, la transferencia no consentida del mismo.

Vemos que para configurar el acceso abusivo sólo se requiere que la persona sin autorización, o por fuera de ella, acceda al sistema o una parte de él en contra de la voluntad del titular del mismo, para el hurto, además de ese acceso, se debe ejecutar una conducta de apoderamiento de un activo o una transferencia del mismo, mientras que para la transferencia no consentida, además del acceso abusivo, el empleo de software malicioso y la violación de datos personales, medio comisivo e información obtenida que son indispensables para llegar al fin propuesto en la conducta, como es la transferencia de un activo

vía electrónica. Así pues, ese principio de especialidad permite observar que las dos conductas estudiadas poseen elementos que caracterizan de manera más amplia el hecho, añadiendo elementos adicionales -manipulación informática, medidas de seguridad informáticas, suplantación de usuarios ante la red, etc., que lo enriquecen y lo hacen más especial que el general.

En conclusión, entonces, por existir unidad de hecho, según Mir Puig, o de acción según Velásquez, y entonces tratarse de un concurso aparente de tipos que se resuelve a través del principio de especialidad, es que la tipicidad de los supuestos de hecho en los casos donde se presenten alguna de las dos conductas punibles relacionadas, no es otra que el Hurto por medios Informáticos y/o la Transferencia no consentida de activos, ello en procura de proteger la prohibición constitucional del *non bis in ídem.*

9. Conclusiones.

Varias son las conclusiones a las que se llega luego de este primer estudio sobre las conductas delictivas más frecuentemente denunciadas en la Fiscalía Seccional de Medellín, como delitos informáticos consagrados en los artículos 269I y 269 J CP.

Como conclusiones generales tenemos que:

1. El bien jurídicamente tutelado en ambas conductas es el patrimonio económico.
2. Estas conductas siempre son cometidas utilizando medios informáticos, esto es, las redes o sistemas de comunicación (internet), entre ellos podemos incluir los cajeros electrónicos los cuales están interconectados a un determinada red.
3. Los ejecutores de este tipo de conductas siempre son un grupo determinado de personas que se asocian para ello.
4. La comisión de las mismas es en todo momento bajo la modalidad dolosa.
5. Ambas conductas van en aumento tanto a nivel nacional como internacional, causando un perjuicio económico robusto que pocas veces es informado a la comunidad en general para evitar emitir mensajes de desconfianza respecto a lo que ocurre en el sistema bancario, lo anterior producto del desconocimiento de la utilización de los medios informáticos por parte de los usuarios, así como de la falta de precaución y protección de los sistemas para evitar caer en las modalidades de estafa que circulan en la red.
6. Existe una debilidad manifiesta en cuanto a la protección personal, no sólo al realizar transacciones en cajeros electrónicos y puntos de pago, sino, además, en toda la información personal y confidencial que las personas suben a las redes sociales.
7. En ambos delitos, la recuperación del dinero sustraído al cliente de sus cuentas bancarias es exigua, comparada con las sumas de las que se apoderan los delincuentes informáticos al ejecutar ambas modalidades frente a diversos clientes del sistema bancario.
8. Existe un gran desconocimiento por parte de muchos de los funcionarios públicos encargados de investigar, acusar y juzgar estas conductas delictivas, así como la dogmática de ellas, lo técnico del lenguaje que se utiliza, y el análisis, interpretación y obtención de los elementos materiales de prueba que deben ser recolectados.
9. Con base en lo investigado y analizado, no se hacía necesaria la creación de ambos tipos penales, pues en nuestra legislación ya existían normas que, como se dijo, ejerciendo una interpretación amplia de los tipos penales de Hurto calificado y Estafa, encuadrarían perfectamente en ellos. Aunque sí era necesario, para sancionar la transferencia no consentida de activos, incluir un agravante que trajera esa figura jurídica.
10. En cuanto al Concurso de conductas punibles entre las aquí analizadas y las figuras de los arts. 269 A-269 F, es necesario resaltar que éste no se configura cuando existe ese acceso abusivo al sistema informático y el hurto o transferencia electrónica no consentida de activos, y ello se resuelve por el principio de la especialidad, pues estas conductas tienen un fin determinado que es apoderarse de un activo y, para lograrlo, hay inevitablemente que ingresar ilícitamente al sistema personal y bancario, lo que, de manera independiente, sería considerado constitutivo de los delitos de los arts. 269A-269F en mención.
11. En cuanto a la Transferencia no consentida de activos, es un tipo penal de Estafa, sin ningún tipo de contacto directo con la víctima, pues todo ocurre a través de la red, esta modalidad sí es un verdadero delito informático pues todos sus elementos normativos y descriptivos, así como los supuestos fácticos consultados lo demuestran.
12. A pesar de exponerse en estas líneas la discusión que se está presentando entre Fiscalía, Judicatura y defensores entorno a si el dinero que ingresa a las cuentas como pagos de

deudas de terceros es legal o no, quedan varios interrogantes para responder sobre esta postura jurídica, que incluso daría para una nueva investigación tendiente a establecer, a través de un recorrido jurídico de normas penales, civiles y comerciales, cuál debe ser la decisión más ajustada a derecho, dejando aquí planteado que sería ésta una manera de romper ese círculo delictivo que se cierra al ser legalizado el dinero que reciben las empresas como parte de pagos, ya que su devolución al titular de origen – dueño de la cuenta bancaria-, ocasiona un recobro a quien jurídicamente es el deudor.

13. La transferencia no consentida de activos es un delito complejo de investigar, pues como se ha indicado su ejecución se presenta sólo a través de la red y la consecución de los elementos materiales de prueba son digitales y volátiles, lo que permite que quienes se dedican a estas modalidades delictivas adquieran grandes ganancias económicas con unos mínimos riesgos de ser capturados en nuestro país aumentando con ello el número de intrusiones ilícitas y de investigaciones por dichas conductas delictivas.

10. Bibliografía.

Gonzáles de Lemos, Maria del Pilar , 29418 (Corte Suprema de Justicia - Sala de Casación Penal - 23 de 02 de 2009).

Acuario del Pino, S. (2010). *Delitos Informáticos, Generalidades*. Obtenido de Acuario del Pino Santiago.delitos informáticos generalidades.pdf.

Arboleda Vallejo, M. (2012). *Código Penal y de Procedimiento Penal.* Bogotá D.C.: Leyer.

Arizamendi, D. l., & De la Mata Barranco, N. J. (2010). *DERECHO PENAL INFORMATICO.* PAMPLONA - ESPAÑA: CIVITAS - THONSON REUTERS.

ASOBANCARIA. (29 de 10 de 2012). *asobancaria.com*. Recuperado el 16 de 11 de 2012, de http://www.asobancaria.com

ASOBANCARIA, Acuerdo Interbancario, enero 01 de 2011

Cano Martínez, J. J. (2009). *Computación Forense, Descubriendo los rastros infromáticos.* México: ALFA OMEGA GRUPO EDITOR S.A. DE C.V. .

Cano Martinez, J. J. (2010). *El peritaje informático y la evidencia digital en Colombia.* Bogotá D.C.: Kimpres Ltda.

Capella, J. R. (1997). *La fruta prohibida.* Madrid: Trotta.

Cerezo A., C., & Choclan Montalvo, J. (2001). *Derecho penal, parte especial* (2 ed., Vol. Tomo II). Madrid, España: Bosch.

Cerezo A., C., & Choclan Montalvo, J. (2001). *Derecho penal, parte especial* (2 ed., Vol. Tomo II). Madrid, España: Bosch.

El Espectador.com. (23 de 04 de 2012). *elespectador.com*. Recuperado el 26 de Julio de 2012, de elespectador.com: htttp://www.elespectador.com

Europa, C. d. (23 de 11 de 2001). *Convenio sobre la Ciberdelincuencia.* Obtenido de Convencion de cibercrminalidad budapest 2001. PDF.

FERNANDEZ, D. G. (2004). *Bien Jurídico y Sistema del Delito.* Montevideo - Buenos Aires: Editorial B de F.

Fontan Balestra, C. (s.f.). Tratado de Derecho Penal Tomo V, Parte Especial. En C. Fontan Balestra, *Tratado de Derecho Penal* (págs. 377-387). Buenos Aires: Abeledo - Perrot.

García Conlledo, M. d. (2001). La Coautoría en el Código Penal Colombiano. *Huellas*, 138 .

González Rus, J. J. (1999). Protección penal de sistemas elementos, datos, documentos y programas informáticos. En J. J. González Rus. Madrid.

Hefendehl, R. (2007). *La Teoría del Bien Jurídico. ¿Legitimacion del Derecho Penal o Juego de abolorio Dogmático?* Madrid: Ediciones Jurídicas y Sociales.

Hernández, Orallo E. (2012), Seguridad y Privacidad en los sistemas Informáticos, www.disca.upv.es/enheror/pdf/ACTASeguridad.pdf

MIR PUIG, S. (2003). DERECHO PENAL, Parte General . En S. MIR PUIG, *DERECHO PENAL, Parte General* (págs. 134, 135, 136). Barelona: REPPERTOR SL.

Pabón Parra, P. A. (2002). *Manual de Derecho penal.* Bogotá D.C.: Ediciones Doctrina y Ley ltda.

Pérez Pinzón, A. O. (1987). Delitos contra el Patrimonio económico. En A. e. Reyes Echandía, *Derecho Penal, Parte Especial Tomo I* (págs. 373-381). Bogotá D.C.: Universidad Externado.

Posada Maya, R. (2006). Aproximación a la Criminalidad Informática. Medellín. Recuperado el 13 de noviembre de 2012

Revista Semana. (14 de 08 de 2012). *semana.com*. Recuperado el 12 de 10 de 2012, de semana.com: http://www.semana.com

Rojas Arboleda, D. (24 de 03 de 2013). Ciberataques, una amenaza que tiene en vilo al mundo. *El Colombiano*, pág. 2 y 3.

Rojas Arboleda, Daniel. (24 de 03 de 2013). Ciberataques, una amenaza que tiene en vilo al mundo. *Ciberataques, una amenaza que tiene en vilo al mundo*, págs. 2-3.

Roxín, C. (1998). Autoria y dominio del hecho en derecho penal. En C. J. Contreras. Madrid: Ed Marcial Ponis.

Sanguino Madariaga, A. (2007). *Delitos contra el Patrimonio económico en la Jurisprudencia.* Bogotá D.C.: Librería Jurídica Sánchez Ltda.

Sotomayor, J. O. (2012). Curso de Derecho Penal I. Medellin, Antioquia.

Suárez Sánchez, A. (2003). Delitos contra el patrimonio económico. En AA.VV., *Lecciones de Derecho penal, parte especial.* Bogotá: Universidad Externado de Colombia.

Suárez Sánchez, A. (2009). *La estafa Informática,2009.pdf.* Recuperado el 23 de 09 de 2012.

Suarez Sanchez; Alberto. (2011). Delitos contra el Patrimonio económico. En U. E. Colombia, *Lecciones de Derecho Penal* (pág. 793 a 839). Bogotá D.C.: Universidad Externado de Colombia.

Velasquez, V. F. (2007). Manual de Derecho Penal, Parte General. En V. F. VELASQUEZ, *Manual de Derecho Penal - Parte General* - (pág. 274). Medellín: Temis.

11. Anexo: Glosario.

Backdoor (Puerta trasera). Que permite a un atacante tomar el control remoto del sistema infectado para llevar a cabo una gran diversidad de acciones; espiar el escritorio remoto realizar capturas de pantalla, o de la web cam, subir, descargar archivos, alterar el funcionamiento normal del sistema, etc. (Arizamendi, D. l., & De la Mata Barranco, N. J., 2010, pág., 203).

Bomba Lógica (Arizamendi, D. l., & De la Mata Barranco, N. J., Pág. 162, 203) Son rutinas introducidas en un programa para que al realizar una determinada acción – por ejemplo copia del mismo-, se produzcan alteraciones o daños en el programa. Las bombas de tiempo como las lógicas, son rutinas introducidas en programas o archivos, pero para que se produzca una alteración del programa o daño al mismo en un momento determinado, al llegar a una fecha concreta o pasar un plazo de tiempo establecido al efecto.

Correo spam Se llama **spam**, **correo basura** o **mensaje basura** a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La palabra spam proviene de la segunda guerra mundial , cuando los familiares de los soldados en guerra les enviaban comida enlatada, entre estas comidas enlatadas, estaba una carne enlatada llamada spam, que en los Estados Unidos era y sigue siendo muy común.

DNS: Domain Name System o **DNS** (en español: **sistema de nombres de dominio**) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a internet o a una red privada. Este sistema asocia información variada con nombres de dominio asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza unas bases de datos distribuidas y jerárquicas que almacena información asociada a nombres de dominio en redes como internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Fleteo: (Según la definición de Asobancaria). Modalidad de hurto a personas que sucede después de haber realizado un retiro en una oficina bancaria y en la que el delincuente utiliza la intimidación y/o violencia para apoderarse del dinero.

Gusano: Este tipo de software no busca principalmente la destrucción de datos, sino su autorreplicación y transmisión para interferirla función informática de otros ordenadores. Su campo de actuación es la Red

Hacker: En informática, un **hacker** o pirata informático es una persona que invade computadoras, usando programas, esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("White hats.)

Dirección IP: una **IP** es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del modelo OSI. Los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán, ya que seguirán accediendo por el nombre de dominio.

Malware: (Del inglés malicious software), también es llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar un computador o sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término malware incluye virus, gusanos, troyanos.

Página WEB: una **página web** es el nombre de un documento o información electrónica adaptada para la world wide web y que puede ser accedida mediante un navegador. Esta información se encuentra generalmente en formato html o xhtml, y puede proporcionar navegación a otras páginas web mediante enlaces de hipertexto. Las páginas web frecuentemente incluyen otros recursos como hojas de estilo cascada, quiones (*scripts*) e imágenes digitales entre otros.

Pharming: es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su expolrador de internet a la página web que el atacante haya especificado para ese nombre de dominio. La técnica de pharming se utiliza normalmente para realizar ataques de phishing, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

Phishing: es un tipo de estafa informática que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta, esto es, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas, a fin de adquirir una contraseña o información detallada sobre tarjetas de crédito o números de cuentas **bancarias.**

Reversión: según la Asobancaria es la anulación del registro contable de una transacción y de los efectos que esta produjo.

Skimmin o Skimer: Dispositivo para copiar información de las tarjetas débito o crédito que se instala en los cajeros electrónicos y posee un lector de tarjeta y una memoria para guardar la información

Software espía: El **spyware** o **programa espía** es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.

Taquillazo: (Según definición de Asobancaria). Es el nombre con el que se conoce a la modalidad de hurto a oficinas bancarias en las que los delincuentes entran fuertemente armados e intimidan a los cajeros para que les entreguen el dinero del que se dispone en las cajas

Troyano: programa informático malicioso para robar contraseñas (Arizamendi, D. l., & De la Mata Barranco, N. J. 2010, págs. 81, 202) Son un software malicioso que, oculto en un programa benigno o útil, se introduce en el sistema informático (incluso en teléfonos móviles o PDA´s) una vez dentro del sistema, pueden generar un gran número de disturbios o daños en el mismo (borrado, o daño en los datos o programas, utilizar el sistema para realizar ataques de denegación de servicios, robar contraseñas y datos, abrir puertas traseras para permitir a los atacantes controlar el sistema y convertir el ordenador en un ZOMBI al servicio de estos). Actualmente son las principales amenazas sobre los ordenadores.

Virus informático: es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.