MIGUEL HERNANDO RIVERA FLOREZ

LA TENTATIVA EN EL DELITO DE HURTO MEDIANTE MEDIOS INFORMÁTICOS

(Maestría en Justicia y Tutela de los Derechos, con énfasis en Derecho Penal y Ciencias Criminológicas)

Bogotá D.C., Colombia

2020

LA TENTATIVA EN EL DELITO DE HURTO MEDIANTE MEDIOS INFORMÁTICOS

MIGUEL HERNANDO RIVERA FLOREZ

DARÍO BAZZANI
Director

UNIVERSIDAD EXTERNADO DE COLOMBIA
FACULTAD DE DERECHO PENAL
MAESTRÍA EN JUSTICIA Y TUTELA DE LOS DERECHOS CON ÉNFASIS EN DERECHO PENAL Y CIENCIAS CRIMINOLÓGICAS
Bogotá D.C., Colombia
2020

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

MAESTRÍA EN JUSTICIA Y TUTELA DE DERECHOS CON ÉNFASIS EN CIENCIAS PENALES Y CRIMINOLÓGICAS

Rector:	**Dr. Juan Carlos Henao Pérez**
Secretaria General	**Dra. Martha Hinestrosa Rey**
Decana Facultad de Derecho:	**Dra. Adriana Zapata Giraldo**
Director Departamento Derecho Penal:	**Dr. Jaime Bernal Cuellar**
Director de Tesis:	**Dr. Darío Bazzani**
Presidente:	**Dr. Darío Bazzani**
Examinadores:	**Dr. William Monroy** **Dr. Carlos Arturo Gómez**

AGRADECIMIENTOS

Agradezco a mi director de tesis Dr. Bazzani, por enfocar sus esfuerzos en contribuirme de manera personal y profesional en la realización de mi investigación, la cual va más allá de una tesis, ya que la misma generó diversos interrogantes frente a la formación y realización penal de los delitos informáticos.

Agradezco inmensamente a mi familia quien apoyó el encause académico con la finalidad de buscar nuevos horizontes e interrogantes jurídicos para mi vida académica presente y futura.

A todos mis más grades agradecimientos.

DEDICATORIA

Dedico el presente trabajo de investigación a mi esposa, quien es mi compañera de lucha inalcanzable, quien da todo de sí para brindarme la oportunidad de realizar mis sueños académicos, doy mis más gigantescas gracias, no solo a ti por estar presente, sino a Dios por darme la oportunidad de que me impulses en mi vida profesional académica, la cual considero llena de vacíos y expectativas, siempre con el fin loable de seguir en la búsqueda. *Gracias infinitas gracias.*

CONTENIDO

INTRODUCCIÓN

Este trabajo se realizó con la finalidad de hacer un estudio acerca de los delitos informáticos y el dispositivo amplificador del tipo, la tentativa, investigación enfocada o más bien acercamiento al mismo, frente a la presentación de la tentativa y la consumación de delito informático o más bien frente al bien jurídico tutelado *"de la información y de los datos",* los cuales desde mi punto de vista profesional pueden recaer en el dispositivo amplificador del tipo.

La presente investigación se enfocó en tratar de estudiar a profundidad el presente fenómeno, el cual de raíz ha sido excluido por parte de la jurisprudencia nacional, sin embargo, el mismo fenómeno a través del derecho comprado presenta diferentes rasgos frente a la apreciación del mismo, por ejemplo en el cual España en su línea de derecho penal, aprueba la concurrencia del fenómeno del tipo penal, aceptada la tentativa y a pesar de poseer diversos artículos frente a la realización del hecho doloso a través de diferentes medios y técnicas informáticas en su consumación, por esta razón se realiza el presente estudio frente al fenómeno elegido.

Como se puede observar dentro del desarrollo del texto de este trabajo de investigación a través del derecho comparado su aceptación o más bien la aplicación de dispositivo amplificador del tipo penal *Tentativa*, es aplicado en diferentes países frente a la realización de delitos de carácter informático, si bien es cierto y se desarrolla dentro del presente texto la recolección de la evidencia o prueba del mismo se hace extremadamente compleja sin embargo no es óbice para dejar y descartar de plano como lo realizan las políticas criminales en nuestro estado.

La aplicación de la modalidad de tentativa en los delitos informáticos en nuestro país no se acoge la tesis y se descarta de plano el mismo con la finalidad de

encajar o encuadrar dentro de los demás tipos penales creados por el legislador no significa que el mismo no se presente en la realización del hecho reprochable, por esta razón realizó la presente exposición acerca de un tema que personalmente me genera gran curiosidad legal en la aplicación de casos concreto orientados específicamente al delito informático o *ciber-crimen.*

CAPITULO I

1. DESARROLLO TÍPICO DE DELITOS INFORMÁTICOS EN EL DERECHO COMPARADO

1.1. Legislación Española

El concepto de delito informático en la legislación española, se encuentra comprendido como; todo ilícito que se ejecute a través de medios informáticos con el fin de amparar los bienes jurídicos vinculados con la tecnología.

En cuanto a su desarrollo evolutivo, comenzó a evidenciarse esta figura en el Código Penal de 1995 en los artículos 197 y 198, en donde estableció modalidades delictivas, como el descubrimiento y revelación de secretos.[1] En esta figura, quien incurriera en la vulneración de la intimidad del otro sin su consentimiento, ya sea en el apoderamiento de documentos, interceptación de comunicaciones, utilización de datos reservados de carácter personal o familiar, u otros; será castigado con pena privativa de la libertad y pecuniaria. Además, de ser realizados estos actos por una autoridad o funcionario público, éste será castigado con las mismas penas y con inhabilidad absoluta entre seis a doce años.[2]

De igual forma, se desarrolla en el Código las penas concernientes a la revelación de secretos ajenos propios del oficio o relaciones laborales, así como el incumplimiento de la obligación de sigilo y reserva. Denotándose en lo anterior, la protección al bien jurídico de la intimidad que puede ser vulnerado con el uso indebido de la tecnología.

[1] GARCÍA NOGUERA, Noelia. Delitos, Delitos Informáticos en el Código Penal Español. 2002. Recuperado de https://www.delitosinformaticos.com/delitos/codigopenal.shtml

[2] JEFATURA DEL ESTADO «BOE». Ley Orgánica 10, Código Penal, 1995. núm. 281, de 24 de noviembre de 1995 Referencia: BOE-A-1995-25444

Ahora bien, en la legislación española, la tentativa o el acceso a algún portal con el fin de obtener la contraseña sin realizar alguna actividad posterior con esta información, no se encuentra tipificado en el código y se conoce como hacking indirecto, lo que sí está tipificado, son las acciones subsiguientes a la obtención de dicha información.

En el artículo 278 del Código Penal español se desarrolla el espionaje informático empresarial, siendo el secreto empresarial el bien jurídico protegido, pues la información supone un valor económico para la empresa que la pone en ventaja frente a otras.[3]

Así mismo, se tipifican los daños informáticos o el sabotaje, artículo 264 numeral 2, mostrando mejora frente al Código Penal anterior que solo preveía la destrucción de bienes materiales.[4]

Otro de los avances del Código Penal actual es el delito de estafa informática. Si bien, el Código Penal anterior a 1995 si lo tipificaba en su artículo 528, para la generación del mismo se requerían dos elementos claros: la utilización de engaño y la producción de un error en la víctima. La concurrencia de estos elementos impidió en muchas ocasiones la calificación de un hecho como estafa cuando ésta se realizaba a través de medios informáticos, es el caso de la transferencia bancaria utilizando otro computador, con lo que no se podía evidenciar el engaño a la víctima y, por tanto, tampoco el error de la misma.

Ante la gran cantidad de defraudaciones informáticas se hizo un intento de acomodar las figuras ya existentes, a través de la doctrina y la jurisprudencia, sin embargo, no era viable. Con el nuevo Código Penal en su artículo 248 numeral 2,

[3] Ibídem, Ley Orgánica 10, 1995.
[4] Ibídem, Ley Orgánica 10, 1995.

se estableció el concepto de estafa y luego las conductas defraudadoras llevadas a cabo mediante manipulaciones informáticas, dando así, cobertura a las actuaciones delictivas que el anterior código no contenía. De igual forma, se pueden presentar casos en el que exista el concurso de delitos de estafa informática con otras figuras tipificadas como, el concurso de estafa con el delito de sabotaje; o concurso de delito de estafa y falsificación documental.[5]

En cuanto a la pornografía infantil, el nuevo Código Penal incluyó la expresión "el que por cualquier medio", para así incluir internet como mecanismo para cometer el delito (Ley Orgánica 10 de 1995 Código Penal, 1995, art. 189). Igualmente, existen delitos tradicionales los cuales son de perfecta aplicación por la posibilidad de cometerse a través de medios informáticos, tal es el caso de la difusión y exhibición de material pornográfico de menores, artículo 186, que puede darse a través de redes sociales o correo electrónico [6].

Como ejemplo de lo anterior, se presenta el caso de un hombre de 50 años, abogado, detenido en Madrid, por presunto delito relacionado con la prostitución y corrupción de menores. El hombre solicitaba contacto con niñas entre los 13 y 15 años, a través de una página web. La policía madrileña, por medio de los agentes de la Unidad de Delitos Tecnológicos detuvo al hombre a raíz de una denuncia presentada por un programa de investigación sobre pornografía infantil por medio de internet. Si bien, el abogado sabía que el sexo consentido con una menor entre 13 y 15 años no es delito, cometió el error de enviarle contenido pedófilo (víctima, 2002).

Por otro lado, los delitos de calumnia e injuria, artículos 205 al 209, también pueden ser llevados a cabo a través de medios tecnológicos, como lo es la

[5] Ibidem, Ley Orgánica 10, 1995.
[6] GARCÍA NOGUERA, Noelia. Delitos, Delitos Informáticos en el Código Penal Español. (200). Recuperado de https://www.delitosinformaticos.com/delitos/codigopenal.shtml

difusión de mensajes con contenidos calumniosos o injuriosos a través de internet, o la utilización y radiodifusión entre otros. Para lo cual, se puede establecer una responsabilidad civil solidaria para la persona natural o jurídica que preste el medio de propagación.[7]

Así mismo los delitos de hurto y robo, artículo 234 y 237, se pueden incluir, cuando son llevados a cabo con la falsificación de tarjetas, y la manipulación de los mandos o instrumentos de apertura a distancia.[8]

Finalmente, las defraudaciones de fluido eléctrico y de equipo terminal de comunicaciones, artículos 255 y 256; los delitos de propiedad intelectual, artículo 279; los delitos contra la propiedad industrial, artículo 273; publicidad ilícita, artículo 282; falsedad de documento público y privado, artículos 390 y 395, se incluyen cuando son realizados a través de medios informáticos, pues vulnera el amparo de bienes jurídicos relacionados con la tecnología.[9]

Posteriormente, el 27 de noviembre de 2009 el gobierno presenta un proyecto con el fin de reformar la Ley Orgánica 10 de 1995, esto es, el Código Penal vigente. El propósito de dicha reforma fue dar aplicación a los tratados internacionales y llenar los vacíos legales que se estaban presentando en la práctica.

En cuanto a la criminalidad informática, se previó castigar el fraude informático cometido mediante tarjetas de crédito y las nuevas formas relativas a los ataques contra los sistemas de información y los daños informáticos.

[7] Ley Orgánica 10, Código Penal, 1995
[8] Ibídem, 1995
[9] ZDENKO Seligo. Legislación sobre delitos informáticos España. Recuperado de https://delitosinformaticos.com/legislacion/espana.shtml

Es así como la Ley Orgánica 5 del 22 de junio de 2010, introdujo las modificaciones al Código Penal, las cuales entrarían en vigencia el 23 de diciembre de 2010.

Los nuevos delitos informáticos que introdujo la Ley Orgánica 5 de 2010 son aquellos cometidos a través de redes informáticas como el child grooming o ciber acoso contenido en el artículo 183 el Código Penal y la utilización ilícita de tarjetas de crédito, artículo 248 numeral 2 del Código Penal.

No obstante, con esta Ley Orgánica, el legislador español prefirió modificar y extender el ámbito de aplicación de los delitos tradiciones como el de estafa y daños, que presentaban analogías con las nuevas formas de cometer delitos a través de nuevas tecnologías. La extensión de estos delitos tradicionales se realizó, por un lado, introduciendo subtipos autónomos para castigar las nuevas modalidades ilícitas, y por otro, ampliando los objetos materiales de los delitos que presentaban analogías con los nuevos hechos delictivos, tutelando de esta manera los nuevos objetos informáticos.

Un ejemplo de lo anterior, es el delito de fraude informático, el cual sigue la línea adoptada en 1995 en el que coloca los nuevos delitos informáticos que se refieren a la tutela de la confidencialidad, integridad, disponibilidad de datos y sistemas informáticos al lado de los delitos delictivos tradicionales que presentan analogía.

La Ley Orgánica 5 de 2010 introduce los nuevos delitos de daños informáticos dentro de un tipo penal autónomo, en lugar de ponerlos al lado (artículo 263 del Código Penal). Sin embargo, esta ubicación queda idéntica a la norma en el capítulo IX del título XIII, entre los delitos contra el patrimonio y el orden socioeconómico. El nuevo delito de acceso no autorizado a datos y programas informáticos (artículo 197 del Código Penal), buscó cubrir las lagunas legales que impedían castigar el hacking y el cracking introduciendo una disposición para

sancionar el acceso no autorizado a programas informáticos, para lo cual se requiere que la introducción no autorizada se realice mediante la violación de medidas de seguridad destinadas a impedir el acceso sin la autorización debida. Lo anterior, evidencia que el legislador evito una excesiva extensión del tipo delictivo al poner la condición de que en el sistema hubiese una protección. Además de castigar la conducta activa del acceso, también castiga la conducta omisiva de mantenerse en un sistema en contra de la voluntad del titular, lo cual supone, el sistema debería tener una protección.

Por lo tanto, el nuevo delito de daños informáticos consagrado en el artículo 264 numeral 1 del Código Penal queda *"…por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave…".* En efecto no se trata de un delito de resultado de conducta libre, pues está vinculada a la interrupción o interferencia del correcto funcionamiento de un sistema, a su vez los ataques físicos pueden ser subsumidos en el numeral 2 del mismo artículo, pero solamente, si causan de manera indirecta un daño a datos y a programas informáticos contenidos en el mismo sistema. No obstante, los daños a la parte física o hardware de un sistema que no afecten su normal funcionamiento, serán subsumidos por el delito de daño.[10]

En cuanto a la responsabilidad penal de las personas jurídicas por los delitos informáticos, el legislador en el 2010 introduce la responsabilidad penal de las personas jurídicas. El artículo 31 del Código Penal prevé un doble criterio de imputación de responsabilidad penal de las personas jurídicas, basándose en la comisión del delito por parte de una o más personas pertenecientes a una entidad, entonces, la persona jurídica es responsable de los delitos cometidos por su representante o administrador, así como los delitos cometidos por sujetos

[10] Artículo 263 del Código Penal.

subordinados cuando los hechos se hayan realizado por falta de control de la persona jurídica sobre su actuación. Por ejemplo, si la persona natural actúa en nombre o por cuenta de una persona jurídica cometiendo un delito de daño informático y este es castigado con pena privativa de la libertad superior a dos años, a la persona jurídica se le aplicara una multa del doble hasta el cuádruplo del perjuicio causado.[11]

Si bien, incluir la responsabilidad penal para las personas jurídicas ha sido un avance, esto solo se ha dado parcialmente, debido a que la responsabilidad penal no ha sido prevista por todos los delitos informáticos, pues solo concierne a aquellos que han sido introducidos por la Ley Orgánica de 2010, esto es, el acceso no autorizado a datos y programas informáticos (Artículo 197 Código Penal) y los daños informáticos (Artículo 264 numerales 1 y 2 de Código Penal).

Por otro parte, queda un vacío legal en cuando al cracker que ingresa a un sistema informático ajeno para instalar un programa espía que le permita tomar control del sistema, pues esta conducta que representa una peligrosa amenaza a la integridad y disponibilidad de datos no es relevante en el artículo 197 numeral 3 del Código Penal, puesto que no implica necesariamente un acceso a datos informáticos contenidos en el sistema violado.

Es claro que el legislador español ha dado un avance a la legislación en materia de delitos informáticos. Sin embargo, estas han sido decisiones marco, perdiendo así la ocasión para dar plena ejecución a las demás importantes disposiciones del Convenio del Consejo de Europa sobre el cibercrimen, destacándose la falta de una norma directa a castigar, en línea con el artículo 3 del Convenido de Consejo de Europa sobre el cibercrimen, esto es, las conductas de interceptación de datos informáticos, que solo fueron subsumidas de manera parcial en los artículos 197

[11] Artículo 264 numeral 4, Ley Orgánica 5, Código Penal, 2010

numeral 1 y 2 y 278 numeral 1 del Código Penal. A su vez, la falta de previsión de una norma clara para castigar el abuso de los dispositivos, es decir, la producción, posesión, venta, importación, distribución, puesta a disposición de un dispositivo, programa informático, código de acceso o palabra clave con la finalidad de cometer un delito contra la confidencialidad, disponibilidad o integridad de datos o sistemas informáticos, sigue siendo un gran vacío legal. Por lo que resulta importante que el legislador de efectiva actuación sobre las disposiciones del Convenio para así abarcar a plenitud todo en materia de delitos informáticos.

1.2. Legislación Estados Unidos de América

El delito informático se ha incluido en figuras típicas de carácter tradicional, como hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes, entre otros, debido a la evolución de las tecnologías junto con las técnicas informáticas y el uso indebido de las mismas, lo que crea la necesidad de regulación en el derecho.

Del mismo modo, es difícil tener una definición universal del delito informático, en razón a que se alude a una situación especial que necesita ser tipificada de forma clara en los códigos penales.

Desde 1983 la Organización de Cooperación y Desarrollo Económico (OCDE)[12] ha estudiado y ha buscado la posibilidad de armonizar las leyes internacionales penales con el fin de luchar contra el uso indebido de la tecnología, realizando una publicación sobre delitos informáticos y un análisis de la normativa jurídica, en donde define el de delito informático como: *"cualquier comportamiento*

[12] La Organización para la Cooperación y el Desarrollo Económico es un Organismo Internacional de carácter intergubernamental del que forman parte 37 países miembros. La OCDE fue creada en 1960 con sede en París, para dar continuidad y consolidar el trabajo realizado por la antigua Organización Europea de Cooperación Económica (OECE) que se había constituido para canalizar la implementación del Plan Marshall. La OCDE sustituyó a ésta en la tarea de impulsar la reconstrucción y el desarrollo en el continente tras la Segunda Guerra Mundial. Tomado de: Gobierno de España. Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. 2018. Disponible en http://www.exteriores.gob.es/RepresentacionesPermanentes/OCDE/es/quees2/Paginas/default.aspx

antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos". Concepto que es utilizado en todos los ámbitos penales, económicos y legales. La OCDE ha desarrollado un conjunto de normas para la seguridad de los sistemas de información con el fin que sirva de guía para la legislación de los países, haciendo énfasis que quien atenta contra el hombre no es la tecnología o los medios informáticos, sino el mismo hombre, que actúa sin escrúpulos y por tanto, se debe estar a la vanguardia de los actos criminales, dando cobertura a las perspectivas civiles, comerciales y administrativas, creando una protección global para alcanzar la eficiencia en la defensa de los bienes jurídicos.

En la actualidad se está frente a un sin número de nuevas formas de comisión de delitos informáticos, tal como las bombas lógicas, cuya detonación puede programarse para que cause el máximo daño en cualquier tiempo, a su vez, puede utilizarse como instrumento de extorsión. Es innegable que el acceso no autorizado a sistemas informáticos cada día está siendo más utilizado, desde la simple curiosidad, hasta el sabotaje o espionaje como tal. A su vez, es común, hablar de hacker o piratas informáticos, cuyo acceso se efectúa desde el exterior aprovechando la falta o deficientes medidas de seguridad para hacerse pasar por usuarios legítimos del sistema y tener acceso a toda la información; igualmente, el tráfico de reproducciones no autorizadas a través de las redes sociales cada vez se vuelve más cotidiano.

Es así, como la Organización de Cooperación y Desarrollo Económico (OCDE) en 1983 comenzó a trabajar por la posibilidad de aplicar y armonizar en el plano internacional de las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales. Teniendo en cuenta que las implicaciones económicas de la delincuencia informática tienen un carácter internacional, incluso transnacional y, por tanto, se hace necesario, una protección jurídico penal integral. Logrando de esta forma unas conclusiones

políticas jurídicos que desembocaron en una lista de acciones que fueran consideradas por los Estado como merecedoras de pena[13].

Luego, en 1986 la OCDE publicó un informe titulado “Delitos de Informática: análisis de la normatividad jurídica”, en el cual se hace un estudio de las normas vigentes y las propuestas presentadas por los Estados miembros y se recomendaba una lista mínima de ejemplos como el fraude y falsificación, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

Por su parte, el Consejo de Europa inició su propio estudio sobre esta temática con el fin de crear directrices que ayuden al legislador a determinar qué tipo de conductas debían prohibirse en el ámbito penal. Con esto, la lista mínima de la OCDE se amplió considerablemente, y se ocupó de la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Desarrollado lo anterior, el Consejo de Europa aprobó la recomendación R9 sobre delitos informáticos en donde recomiendan a los Estados Miembro revisar su legislación y actualizarla frente a las nuevas comisiones de delitos informáticos. Dicha recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Posteriormente, en 1992 la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, tanto para los Estados como para el sector privado. Estas reconocían el uso cada vez mayor de las redes informáticas, el carácter internacional de los sistemas de información y su proliferación en todo el mundo, así como en la vida social, cultural y política; con

[13] Ibídem, 2018

lo que se hacían necesario aumentar la conciencia de los riesgos recaídos sobre los sistemas de información y de las posibilidades para cubrir estos riesgos y reconocer que las medidas no satisfacían los problemas planteados. Para lo cual, se crearon definiciones unificadas de algunos conceptos informáticos, como: datos informáticos, sistemas de información, disponibilidad, integridad o confidencialidad de los datos informáticos. Además, consagra nueve principios: responsabilidad, concienciación, ética, multidisciplinario, proporcionalidad, integración, velocidad, revaluación y democrático.

De igual modo, en 1992 la Asociación Internacional de Derecho Penal, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas, la modificación de ser el caso, de los textos penales con el fin de proteger los bienes jurídicos a cabalidad. La Organización de las Naciones Unidas ONU define los delitos informáticos como aquellos que implican*: "un comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos"*[14]*.*

Finalmente, en el 2002 la OCDE actualizó las directrices elaboradas en 1992 para acomodar los nuevos problemas de la época, esto es, los derivados del internet y sus abusos. Del mismo modo, se realizaron algunas adaptaciones de los principios originales, la integración de varios de ellos y la aparición de tres nuevos: el principio de evaluación del riesgo, de diseño y realización de la seguridad y el de gestión de la seguridad.

Adicionalmente, la ONU ha elaborado un catálogo de delitos, estableciendo una sub-clasificación:

[14] ORGANIZACIÓN DE LAS NACIONES UNIDAS – ONU. Definición y tipos de delitos informáticos. 2011. Disponible es https://delitosinformaticoscipa.blogspot.com/2011/02/definicion-y-tipos-de-delitos.html

1. Acceso no autorizado: Acceso no autorizado violando las medidas de seguridad, teniendo la variación moderna a la intromisión a sitios web.
2. Daño a los datos o programas informáticos: Borrar, descomponer, deteriorar o suprimir los datos o programas informáticos sin derecho a ellos.
3. Sabotaje informático: Introducción, alteración, borrado, supresión de datos o programas, interferencia en sistemas informáticos con la intención de obstaculizar el funcionamiento de un sistema de computadoras o de telecomunicaciones.
4. Interceptación no autorizada: Captación, realizada sin autorización, y por medios técnicos, de comunicaciones destinadas a un sistema o red informática, provenientes de ese sistema o red, o efectuadas dentro de dicho sistema o red.
5. Espionaje informático: Adquisición, revelación, transferencia o utilización de un secreto comercial sin autorización, con la intención de causar una pérdida económica a la persona que tiene derecho a dicho conocimiento, o de obtener un beneficio ilícito para sí mismo o una tercera persona.[15]

La ONU posteriormente, reconoció los delitos informáticos:

- ✓ Manipulación de los datos de entrada: o sustracción de datos, el cual no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona.
- ✓ Manipulación de programas: Requiere de conocimientos técnicos informáticos, modificando los programas existentes en el sistema o insertando nuevos programas.
- ✓ Manipulación de los datos de salida: Se fija un objetivo al funcionamiento del sistema informático, un ejemplo de ello, es el fraude que se realiza en los cajeros automáticos.

[15] Ibídem, 2011.

Siendo las falsificaciones informáticas usadas, como objeto, cuando se alteran datos de los documentos almacenados en forma computarizada; y, como instrumento, cuando las computadoras se utilizan también para efectuar falsificaciones de documentos de uso comercial.

El trabajo de la ONU siguiendo una línea similar al de la OCDE resulta una herramienta importante a nivel internacional en la lucha contra los delitos informáticos. La delincuencia informática sufre novedades con el uso del internet a diario, y los trabajos deben estar a la vanguardia de la comisión de los delitos. Es así como en el 2005 se realizó una visión panorámica de algunas nuevas formas de delincuencia informática junto con el crecimiento del internet, al igual que en las ediciones anteriores, se insiste en la necesidad de colaboración entre Estados, pero también entre empresas privadas y, por primera vez, se celebra la aprobación del Convenio sobre la Ciberdelincuencia de Budapest de 23 de noviembre de 2001. Finalmente, en el 2010 aunque no se hicieron muchas novedades se menciona por vez primera la posición de vulnerabilidad en la que se encuentran ante este tipo de delitos los países en vía de desarrollo y se urge a los países desarrollados a prestar su colaboración a aquellos.

En cuanto a la clasificación y tipificación de los delitos, no hay duda que nace por la necesidad de proteger los bienes jurídicos que se veían afectados con el uso indebido de la tecnología. Frente a lo cual, Estados Unidos fue el primer país en tener una regulación de ámbito estatal, pues ha sido importante para el país mantener una amplia protección frente a los delitos informáticos a través de una política legislativa nacional en el Derecho Penal Estadounidense.[16]

[16] OFICINA DE INFORMACIÓN DIPLOMÁTICA DEL MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN. Estados Unidos. 2013.p. 1- 27. Disponible en http://www.exteriores.gob.es/documents/fichaspais/estadosunidos_ficha%20pais.pdf

Estados Unidos, es pionero en la materia, con el concepto del cybercrime; comprendiendo que tanto aquellas situaciones en que el elemento informático se encuentra en el objeto de la conducta penada como es el caso de la intromisión ilegal a bancos de datos; o en aquellas situaciones en que dicho elemento es el medio para realizar un fin ilícito como es el caso de estafa vía Internet, son consideradas delito y es crimen cibernético.

Para comprender un poco más del avance de Estado Unidos en esta materia, se hace necesario un recuento histórico. El primer abuso de este tipo se registró en 1958, cuando se reportaron los primeros casos de sabotaje; posteriormente, en 1966 se adelantó el primer proceso por la alteración de datos en un banco en Minneapolis. En la década de los 70´s, los ataques informáticos se hicieron más frecuentes, además que en el Pentágono, la OTAN, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos. Sin embargo, es en 1976 cuando el FBI comienza a entrenar a sus agentes sobre delitos informáticos.[17]

Luego, se aprueba la Counterfeit Access Device and Abuse Act en 1984, ya que hasta este momento las conductas delictivas en esta materia se recogían en leyes estatales de limitada aplicación y se presenta la Ley Federal de Protección de Sistemas de 1985.

Al respecto de la Counterfeit Access Device and Abuse Act, fue un hito en la regulación penal de los crímenes informáticos, no sólo en Estados Unidos, sino a nivel mundial, al ser la primera ley que se centraba en la persecución de estos delitos. La misma establece diferentes delitos federales a partir del título "fraude y actividades relacionadas en la conexión entre ordenadores" para enjuiciar la actividad criminal informática. Sin embargo, fue insuficiente, pues en el primer caso de condena por este delito en Texas, no pudo ser aplicada por no verse

[17] Ibídem, p. 1-27

comprometidos los sistemas informáticos objeto de protección de la ley, la cual era una lista cerrada y limitada. La enmienda aprobada en 1986, además de cambiar el nombre a denominarse Computer Fraud and Abuse Act su ámbito de aplicación se generalizaba y ampliaba respecto a la ley de 1984. Esta ley ha sido modificada en múltiples ocasiones cada vez complementándola a mayor medida.

En 1994 se adoptó el Acta Federal de Abuso Computacional que contempla la regulación de los virus, conceptualizándolos; además, establece que modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito, siendo este un gran adelanto en contra de los ataques tecnológicos que cada vez iban en aumento (Unidos). En 1998 se adoptó la Ley de Usurpación de Identidad, la cual establece como crimen federal utilizar ilegalmente un medio de identificación de otra persona para cometer medios delictivos. Y en 2001 la ley USA Patriot como reacción al terrorismo extendió la aplicación de la misma más allá de la jurisdicción de Estado Unidos[18].

Luego y conforme al aumento de casos de hacking y la sensación de inseguridad se crean el FCIC (Federal Computers Investigation Commitee), que es la organización más importante e influyente en lo referente a delitos computacionales y la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias[19].

Entonces, las leyes federales que protegen contra el ataque a computadores, invasiones electrónicas de privacidad y otras transgresiones son: 18 USC,

[18] *TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996.*

[19] SEGÚN-INFO. Seguridad de la información. Legislación y Delitos Informáticos - La Información y el Delito. Recuperado de https://www.segu-info.com.ar/legislacion/?pais=17

Capítulo 47, sección 1029, y sección 1030, de 1994 que modificó al Acta de Fraude y el Acta Federal de Abuso Computacional de 1986.

1.2.1. Sección 1029[20]

1. Prohíbe el fraude y cualquier actividad relacionada que pueda realizarse mediante el acceso o uso de dispositivos falsificados como: Pins, tarjetas de crédito, números de cuentas, y demás identificadores electrónicos. La sección 1029 cubre nueve áreas de actividad criminal, las cuales requieren que el delito implique comercio interestatal o extranjero.
2. Producción, uso o tráfico de dispositivos de acceso falsificados.
3. Uso u obtención sin autorización de dispositivos de acceso para obtener algo de valor totalizando $1000 o más, durante un periodo de un año.
4. Posesión de 15 o más dispositivos de acceso no autorizados o falsificados.
5. Fabricación, tráfico o posesión de equipo de fabricación de dispositivos de acceso ilegales.
6. Realización de transacciones con dispositivos de acceso pertenecientes a otra persona con el objetivo de obtener dinero o algo de valor totalizando $1000 o más durante un periodo de un año.
7. Solicitar a una persona con el objetivo de ofrecerle algún dispositivo de acceso o venderle información que pueda ser usada para conseguir acceso a algún sistema.
8. Uso, producción, tráfico o posesión de instrumentos de telecomunicación que hayan sido alterados o modificados para obtener un uso no autorizado de un servicio de telecomunicaciones.
9. Uso, fabricación, tráfico o posesión de receptores-escaneadores o hardware o software usado para alterar o modificar instrumentos de

[20] RODRIGUEZ, Jesús. Ponencia Ciber Crimen. 2016. Disponible en https://issuu.com/joserangelbaron/docs/presentacio__n_del_dr._jesus_rodrig

telecomunicaciones para obtener acceso no autorizado a servicios de telecomunicaciones.

10. Hacer creer a una persona el delincuente es un miembro de su compañía de tarjeta de crédito o su agente para obtener dinero o realización de transacciones hechas con un dispositivo de acceso y viceversa.

1.2.2. Sección 130[21]

1. Prohíbe el acceso no autorizado o fraudulento a ordenadores gubernamentales, y establece diversas condenas para esa clase de accesos. Esta ley es una de las pocas piezas de legislación federal únicamente referidas a ordenadores. Bajo la Ley de Abuso y Fraude Informático, el Servicio Secreto americano y el F.B.I. tiene jurisprudencia para investigar los delitos definidos en este decreto. La sección 1030 cubre seis áreas de la actividad criminal:
2. Adquisición de información restringida relacionada con defensa nacional, asuntos exteriores o sobre energía nuclear con el objetivo o posibilidad de que sean usados para dañar a los Estados Unidos o para aventajar a cualquier otra nación extranjera.
3. Obtención de información en un registro financiero de una institución fiscal o de un propietario de tarjeta de crédito; o de información de un cliente en un archivo de una agencia de información de clientes.
4. Atacar un ordenador que sólo corresponda ser usado por algún departamento o agencia del gobierno de los EEUU, para el caso de que no sólo puede ser usada por esta agencia, atacar un ordenador usado por el gobierno en el que la intrusión producida afecte el uso que el gobierno hace de él.

[21] Ibídem, 2016.

5. Promover un fraude accediendo a un ordenador de interés federal y obtener algo de valor, a menos que el fraude y la cosa obtenida consistan solamente en el uso de dicho ordenador.
6. A través del uso de un ordenador utilizado en comercio interestatal, transmitir intencionadamente programas, información, códigos o comandos a otro sistema informático.
7. Promover el fraude traficando con passwords o información similar que haga que se pueda acceder a un ordenador sin la debida autorización. Todo esto si ese tráfico afecta al comercio estatal o internacional o si el ordenador afectado es utilizado por o para el Gobierno[22].

Siendo estos los principales elementos legislativos aplicables a los delitos informáticos y representando, un adelanto al ir en contra de los actos de transmisión de virus.

De igual forma, cabe destacar que existe una abundante legislación que ha sido modificada dentro de las diferentes enmendáis aprobadas en los años 1.988, 1.989, 1,994, 1,996, 2,001, 2,002 y 2,007 donde se amplían las protecciones y se endurecen las penas; en cada uno de los que abarcan la tipificación de los delitos, como en materia procesal. Esto, a causa de que la organización estatal es federativa, lo cual implica que cada estado es parte de la unión, pero dicta y aplica sus propias leyes y regulaciones, todo, sin perjuicio de la Constitución. Pues, la legislación estatal ha jugado un rol importante en la persecución de los delitos como fraude y acceso ilegal cuyo origen está en el common law.

Es así, como el delito informático o cybercrime en Estado Unidos abarca tanto delitos comunes que se ejecutan a través de la tecnología, como los delitos que

[22] Código Penal Internacional contra delitos informáticos. Legislación Informática de Estado Unidos. 2014. Disponible en http://catherinpacheco01.blogspot.com/2014/11/ legislacion-informatica-de-estado-unidos.html

son posibles gracias a la existencia de la misma. Implicando la respuesta tanto de la aplicación de las leyes generales, como de las específicas de cada estado.

Entonces, un delito informático quebranta las leyes federales cuando: implica el compromiso o robo de información que pueda afectar la defensa nacional; involucra información de agencias del gobierno; entidades financieras; entidades interestatales o extranjeras; y afecta a poblaciones en otros países o estados.

Otros delitos tipificados en la legislación estadounidense son: las obscenidades, la producción y su distribución por cualquier medio; la pornografía infantil a lo cual se creó la Ley de Protección de los Niños de Internet (CIPA) que prohíbe a las bibliotecas públicas la adquisición de ordenadores con acceso a Internet, salvo cuando cuenten con tecnología que permita filtrar contenido inapropiado para menores. Esta norma es utilizada para perseguir a los pedófilos que utilizan Internet; y, la protección del copyright o derechos de autor.[23]

1.3 Legislación Chilena

Los delitos informáticos en la legislación de Chile están consagrados en la Ley No. 19.223, que tipifica estas figuras penales, distinguiendo entre, sabotaje, espionaje y fraudes informáticos. Esta legislación, se enfoca en proteger el nuevo bien jurídico que surge del uso de la tecnología propendiendo la calidad, pureza e idoneidad de la información. Por eso es importante la identificación del mismo, la intimidad, la propiedad de la información nominativa, la información personal registrada, la información en sí misma y la pureza de la técnica que supone la informática, cosa que la Ley en mención no deja claro. No obstante, la redacción de las disposiciones de la Ley 19.223 permite calificar a los delitos allí tipificados

[23] BCN Informe. Biblioteca Nacional del Congreso. Los delitos cibernéticos en la legislación estadounidense. Disponible en https://www.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf

como pluriofensivos, admitiendo la aplicación de sus normas en resguardo de bienes jurídicos distintos, como el patrimonio o la intimidad, según el caso.

De su articulado puede inferirse el propósito de la Ley enfocada al resguardo de los datos informáticos y los sistemas que lo contienen, pero a su vez, no se hace cargo de las vías tecnológicas como medio de comisión de los delitos comunes. No obstante, la legislación chilena habla de los delitos informáticos haciéndolo en referencia a la protección mediante el derecho penal de los datos y sistemas informáticos, mas no de los delitos cibernéticos en general, siguiendo el concepto restringido de delito informático.

Es evidente que esta Ley no se adecua a las nuevas formas de comisión de estos delitos que día a día avanzan con el desarrollo tecnológico, pues se presentan conflictos procesales en cuanto a la competencia cuando los delitos son cometidos desde el extranjero, sumado a que la interpretación de la norma presenta un grado de confusión importante[24].

Si bien es cierto, Chile se acoge a las recomendaciones internacionales del Consejo de Europa y la Unión Europea, no lo hace en su totalidad, puesto que, en Chile, no se incrimina el simple acceso no autorizado a un computador o a sus datos por medios informáticos.

Haciendo un análisis más profundo de los tipos penales de la Ley No. 19.223, se contempla dos figuras delictivas. Por un lado, el sabotaje informático, y, por el otro el espionaje informático.
El sabotaje informático:

[24] BCN Informe. Biblioteca Congreso Nacional de Chile. Delitos Informáticos Chile y la legislación extranjera. 2019. Disponible en https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=11020

El sabotaje informático se entiende, según la ley, como “El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento…” (Ley No. 19.223 Delitos informáticos y sistemas de información, 1993, art. 1), así mismo los castigos frente a este delito se encuentran en el artículo 3 de la misma ley y no exige la concurrencia de ningún requisito especifico, se contempla un agravante cuando la persona que vaya a cometer el delito pueda proveer el daño que causaría; el problema que se presenta es determinar la intensidad en la afectación, ya que la norma se enfoca más a castigar el daño si este es irreversible.

En cuanto a las conductas que son tipificadas como sabotaje informático, se engloban todos aquellos atentados realizados en contra de un sistema de tratamiento de información, cuya finalidad es destruir o causar daño a los datos, soportes o contenidos de un computador afectando el hardware de una entidad.

Sin embargo, se presenta un problema cuando se destruyen los soportes físicos del sistema, pues aquí concurrirían leyes penales de tipo común, como el delito de daños, debiendo ser resuelto por el Tribunal en base a los principios de especialidad, accesoriedad, o subsunción. Igualmente, otra dificultad relacionada, es la extensión del daño punible, frente al sistema como a sus partes o componentes. ¿Si se llevará a un extremo, sería posible sostener que cabe considerar la destrucción de un teclado como un delito informático?

Frente a la interceptación, interferencia, acceso o no autorizado, son conductas asociadas con el espionaje informático, aun cuando corresponda a hechos distintos, por una parte, el conocimiento y uso de datos; y por otra, la revelación maliciosa de estos. Así, la penalización de las hipótesis de interceptación, interferencia o acceso a sistemas informáticos requiere una intención de uso de los datos excesivamente amplia, más allá de lo que requiere o necesita un tipo

que busque la penalización del hacking, haciendo difícil la asociación de ambos. Por su lado, la ONU hace una definición más completa al involucrar dos elementos que a la normatividad nacional le faltan, estas son, la necesidad de haber provocado un perjuicio pecuniario, o al menos el haber logrado un beneficio económico para quien ha cometido el ilícito.

En lo que respecta a los datos, no establece criterios claros a la hora de discriminar la titularidad, importancia o sensibilidad de la información que es objeto de acceso o interceptación indebida. Lo que da brecha a que todos los datos se protegen igual, incluso si estos se obtuvieron mediante la interceptación de algún dato de público conocimiento, siendo necesaria una distinción, ya sea para la construcción de los elementos del tipo o para establecer distinta penalidad.

Finalmente, la Ley tipifica la revelación o difusión de datos de un sistema informático en general, sin importar si éstos son públicos, y sin exigir que estén bajo secreto, reserva o encriptación, o penando incluso si ya son del conocimiento de quien los recibe. Extremando el caso, bastaría sólo el dolo, o al menos la presencia de un ánimo lucrativo, para configurar el ilícito.

La Ley contempla tres modos que afectan el normal funcionamiento informático de una entidad. *Primero:* Impedir el funcionamiento del sistema; *Segundo:* Obstaculizar el funcionamiento; y, *tercero:* Modificar el funcionamiento. Siendo clara la intención de la Ley al propender cubrir las necesidades de proteger los programas por no ser posible su debida tutela bajo los tipos penales comunes, pero, presenta falencias al dejar varios vacíos legales.

El espionaje informático

La Ley 19.223 establece dos modalidades distintas bajo la denominación de espionaje informático. Por un lado, “El que, con ánimo de apoderarse, usar, o conocer indebidamente de la información contenida en un sistema de tratamiento

de la misma, lo intercepte, interfiera o acceda a él…" y "El que maliciosamente revele o difunda los datos contenidos en un sistema de información…"[25]

Lo anterior, genera una división penal en dos grupos:

- ***Delitos de apoderamiento, uso, o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información.***

Cometidos por sujetos sin autorización cuya finalidad es interceptar, interferir o acceder a datos informáticos. Sin embargo, no basta con que el sujeto activo intercepte, interfiera o acceda a un sistema informático, también, se deben realizar esas conductas con el objetivo de apoderarse, usar, o conocer indebidamente la información. La tipificación de este delito no exige que para su configuración deba ir acompañado el ánimo de lucro, sino que basta con que se utilice la misma para cualquier fin.

- ***Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información.***

La comisión de estos delitos se restringe solo a los sujetos que tengan acceso a los sistemas informativos, diferenciándose del anterior y teniendo agravantes, pues la connotación "revelación indebida" está dirigida a sujetos que tienen la obligación de reserva frente a la información que se encuentra en el sistema y, esa obligación es emanada de un vínculo previo entre el sujeto activo y el afectado. Así, la norma castiga las conductas de revelación y difusión maliciosa de datos, lo que permite proteger la fidelidad en el cuidado de la información[26].

[25] Ley No. 19.223 Delitos informáticos y sistemas de información, 1993, art. 2 y 4.
[26] BCN Informe. Biblioteca Congreso Nacional de Chile. Delitos Informáticos Chile y la legislación extranjera. 2019. Disponible en https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=11020

Entonces, los elementos del delito informático son: Las modificaciones en el sistema de procesamiento de datos; el ánimo de lucro o de obtención de beneficios ilícitos; y, la utilización de elementos propios del fraude.

La carga probatoria sobre el dolo recae sobre la parte que lo alega, esta debe rendir las pruebas necesarias para acreditar el conocimiento e intención de realizar una determinada figura delictiva y querer la consecución de su resultado. Por lo que, en estos casos, se habla de un dolo directo quedando excluidos el dolo de consecuencias seguras o necesarias y el dolo eventual. Si bien es cierto, una conducta puede iniciarse sin la concurrencia de dolo directo, los actos que componen el hecho pueden adquirir dolo directo, tal es el caso de un hacker que acceda a un sistema informático sin la intensión de apoderarse de la información y termina haciéndolo.

En 2018, se realiza un proyecto de ley que ingresó al Senado de Chile, a través del Boletín 12.192-25 de noviembre, y que deroga la Ley No. 19.223 el cual modifica el delito de destrucción o inutilización de sistema de datos y tipifica nuevos delitos, como son: acceder a un sistema informático sin autorización, impedir a otro el acceso por vía informática a sus datos personales, alterar, dañar o destruir los datos contenidos en un sistema informático, cualquier forma de puesta a disposición de elementos informáticos que permitan o faciliten la comisión de delitos y el delito de exacción patrimonial, que incluye un agravante en el artículo 1 referente a las personas que tengan acceso a este tipo de información; y a su vez, se crea un agravante general, que consiste en emplear medios informáticos para la comisión de estos delitos.[27]

En este proyecto, además, se sanciona la tentativa y se modifica el Código Penal para introducir normas que fortalezcan el Ministerio Público y la Policía, pues solo

[27] Delitos Informáticos. Chile y legislación extranjera.

se exige que el acceso a un sistema informático se haga de forma indebida, independiente de si este acceso se realiza de buena o mala fe, o con la intención de apoderarse o conocer indebidamente la información ahí contenida.

No obstante, el proyecto se encuentra mal encaminado en materia de uso de tecnologías como el cifrado al ser considerado como un agravante de cualquiera de los delitos contenidos en la ley, olvidándose que este tipo de tecnologías han sido clave para combatir el delito en la ciberseguridad.

No hay duda que este proyecto de ley utiliza un vocabulario más acorde a las necesidades actuales del país, además, busca cumplir con los compromisos internacionales adquiridos por Chile al ratificar el convenio de Budapest, instrumento internacional que busca homogenizar la regulación de los delitos informáticos a nivel internacional y mejorar las capacidades de colaboración de los distintos países en la persecución del crimen en línea. Sin embargo, sigue siento responsabilidad del gobierno proteger los derechos de los ciudadanos y aprovechar la flexibilidad que otorga el convenio para la implementación de sus obligaciones (Viollier, 2018).[28]

2. Desarrollo doctrinario en el derecho comparado del bien jurídico tutelado delito de hurto por medios informáticos en el derecho comparado

2.1. Doctrina Española

Es incorrecto hablar de delito informático, cuando en la actualidad este es un término que abarca una pluralidad cuya única común vinculación son los computadores de una u otra forma. El bien jurídico protegido no siempre es de la

[28] BCN Informe. Biblioteca Congreso Nacional de Chile. Delitos Informáticos Chile y la legislación extranjera. 2019. Disponible en https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=11020

misma0 naturaleza y la comisión del delito presenta características similares. El computador es en ocasiones el medio para la comisión del hecho, y en otras, es el objeto de la agresión en sus diversos componentes. Por lo cual, es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información.

Así las cosas, y de acuerdo a la incidencia en la delincuencia informática, los bienes jurídicos objetos de este tipo de delitos son cada vez más variados y en ocasiones, las conductas afectan intereses públicos.[29]

La intimidad y dignidad de la persona natural, se ve lesionada, cuando aspectos de su vida privada son revelados por personas diferentes de las autorizadas para ello. Por otra parte, los bienes jurídicos patrimoniales son los más vulnerables para este tipo de delitos.[30]

La doctrina española distingue los siguientes supuestos, tomando como ejemplo el uso de tarjetas bancarias en cajeros:

1. En el caso de robo en cajero automático cuando se usa la tarjeta de un tercero. Se podría considerar como un robo con fuerza al presuponer la falta de voluntad del banco en entregar el dinero a una persona no autorizada. Sin embargo, se debe ir más allá, al considerar la necesidad de crear un tipo específico entre las defraudaciones que recoja los supuestos de legitimidad de tarjetas, ya que la pulsación del número personal del titular crea una apariencia de legalidad en el ejercicio del derecho frente al banco, acercándose más esta acción a las de tipo defraudatorio.

[29] ACURIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. 2016. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
[30] Ibídem, 2016

2. Utilización abusiva del cajero por el titular de la tarjeta magnética. El cual no es un comportamiento típico de estafa, si bien es desleal por el titular obligar al banco a pagar obligaciones no contraídas, el titular no está obligado a cuidar los intereses del banco.[31]
3. Acceso al cajero mediante tarjeta falseada o alterada. Para la doctrina, este caso no entra dentro de la manipulación informática, ni dentro del robo con fuerza en las cosas ni del hurto. [32]

2.2. Doctrina Estados Unidos de América

El origen de una protección amplia contra los delitos informáticos ha tenido punto de partida desde la política legislativa nacional al ser incluido en el Derecho Penal estadounidense. Con lo que se hace interesante señalar la primera condena en Estados Unidos por realizar actos concretos de daños informáticos sobre sistemas ajenos. Este fue el resultado del procedimiento penal del Estado de Texas contra Donald Gene Burleson en 1988. Aquí se condenó al acusado por introducirse sin autorización y borrar datos del sistema luego de ser despedido en 1985, recibió una condena de siete años de libertad condicional y debió indemnizar a la empresa afectada con 11.800 dólares. Para la época, estaba en vigencia la Ley Federal Counterfeit Access Device and Abuse Act de 1984, que si bien, supone un hito en la regulación penal de los abusos informáticos al ser la primera legislación de carácter nacional que se centraba directamente en la persecución de este tipo de acciones, estableciendo diferentes delitos federales a partir del título "fraude y actividades relacionadas en la conexión entre ordenadores" para enjuiciar la actividad criminal informática, la misma, fue insuficiente a la hora de su aplicación, pues en el caso de Donald Gene Burleson no fue empleada por no verse

[31] ACURIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[32]GARCÍA CERVIGÓN, Josefina. (s.f). El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. Recuperado de https://revistas.upcomillas.es/index.php/revistaicade/article/download/357/283.

comprometidos los sistemas informáticos objeto de protección de la ley (la lista que contiene la Ley es muy cerrada y limitada). Surgiendo entonces, la necesidad de enmiendas, como la de 1986 que cambio el nombre de la Ley a Computer Fraud and Abuse Acty, la cual pretendía ser una herramienta legal general para combatir el ataque a sistemas y hacer frente a los delitos federales cometidos por medios informáticos.

Bajo esta nueva legislación, en 1991, se produce el primer gran juicio por la comisión del delito federal de daños informáticos en Estados Unidos. Es el caso de la Nación contra Robert Tappam Morris, el cual fue condenado por introducir un virus en la red de Internet en 1986 que provocó el colapso de diversos sistemas informáticos que vieron interrumpido su normal funcionamiento. Esta sentencia es interesarse al mencionarse por primera vez en una Corte Nacional, la existencia del internet y la necesidad de mejorar la seguridad en estos sistemas.

Posteriormente, Estados Unidos adoptó en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

Esta ley es un avance por estar directamente en contra de los actos de transmisión de virus, pues diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. Igualmente, el creador de un virus no puede escudarse con el hecho de que no conocía que daño iba a causar.

Adelanto que evidencia un acercamiento más responsable frente a los virus informáticos, así mismo, la nueva ley da lugar a que se contemple, qué se debe entender como acto delictivo.

Es así, como conforme a los avances informáticos, la legislación ha sido modificada con el fin de cubrir todos los posibles vacíos legales, ampliando los sistemas que iban a estar protegidos y endureciendo las penas, además de incorporar conceptos derivados del Derecho Internacional. De tal forma que a través de estas regulaciones normativas queda configurada la protección sobre los denominados Computer Crimes, delitos cometidos mediante, o contra, ordenadores o dispositivos informáticos en general.

El caso norteamericano más importante ha sido el denominado Estados Unidos contra David Lee Smith en 2002 por crear y distribuir el virus Melissa en Internet que afectaba archivos de Microsoft Office. Este virus provocó el mayor caso conocido de infección masiva en la historia, porque no sólo provocó daños en sistemas informáticos, sino que también paralizo la mayoría de las empresas del mundo, como Intel y Microsoft.

Por su parte, cada Estado crea su normatividad frente al delito informático. En 1992 en california, por ejemplo, se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos, pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de la misma.

También es importante las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos, en donde se amplía los sujetos susceptibles de verse afectados por estos delitos y la creación de sanciones pecuniarias. Esto con el fin de aumentar la protección a las personas, negocios y entidades gubernamentales, debido a que los legisladores se dieron cuenta que la proliferación de la tecnología al igual que los delitos informáticos han ido en aumento.[33]

[33] ACURIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. 2018. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

En la actualidad se destaca, en Estados Unidos, la cantidad de agencias y otras instituciones públicas y privadas que han aparecido con el fin de proteger los sistemas de los delitos informáticos. El Instituto de Seguridad en Computadora (CSI) realiza informes anuales denominados “Estudios de Seguridad y Delitos Informáticos” desde hace más de una década. A su vez la institución del Centro de Quejas de Delitos por Internet o IC3, es una entidad gubernamental que establece la colaboración del FBI, el NW3C y el BJA con el objetivo de servir como un vehículo para recibir, elaborar y remitir las denuncias penales teniendo en cuenta la rápida expansión de la delincuencia cibernética. El IC3 proporciona a las víctimas de los delitos cibernéticos un cómodo y fácil mecanismo de denuncia de actividades sospechosas relacionadas con internet, que alerta a las autoridades de presuntas violaciones penales o civiles.

Por otro lado, la Organización de Estados Americanos (OEA) reconoce la importancia del internet y las nuevas tecnologías en el crecimiento de las economías mundiales. Lamentablemente, Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial por la indebida manipulación de la misma, los hackers son una amenaza latente, más cuando se ven amenazados los ciudadanos, las economías y servicios esenciales, a lo que se hace necesario una estrategia con enfoque de protección integral, internacional y multidisciplinario.

Una muestra del compromiso de la OEA con el desarrollo de la estrategia, celebró una Conferencia sobre Seguridad Cibernética (Buenos Aires, Argentina, del 28 al 29 de julio de 2003) en la que evidencio las amenazas cibernéticas y la necesidad de crear una cultura de seguridad informática. Para lo cual, seria óptimo proporcionar información a la población para asegurar sus computadoras incrementando la educación sobre el tema y promoviendo la adopción de políticas sobre el delito informático. Considerando a los sistemas informáticos como una

gran amenaza a los países desarrollados, por lo que el terrorismo informático, es un acto de guerra y deben tomarse las medidas pertinentes al respecto.[34]

2.3 Doctrina Chilena

Algunos autores chilenos, señalan que para definir los delitos informáticos se debe realizar desde una percepción en derecho, siendo esta la ciencia que se encarga de tipificar los delitos. Esto debido a que el derecho es la que regula las conductas de la vida en sociedad, entre las que se incluye la actividad informática que hoy en día tiene tanta trascendencia social y económica.

Así las cosas, algunos autores definen los delitos informáticos como:

> "Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro"[35]

Definición amplia que aborda las realidades actuales, comprendiendo que las acciones ilícitas tradicionales se realizan con el auxilio de medios informáticos. Acciones estas socialmente peligrosas y antijurídicas que implementan la tecnología como medio u objeto ante la comisión de un delito.

---

[34] Ibídem, 2018

[35] HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur. 1999

Esto no sólo dio para a la creación de la ley No. 19.223, sino también, a la introducción en el artículo 248 del Código Penal numeral 3 en el año 2003 (Ley 20.526 Código Penal, 1978). Numeral, directamente vinculado con el fraude informático al sancionar la fabricación, introducción, posesión o el facilitar programas específicamente destinados a la comisión de estafas prevista en el artículo, entre las cuales se encuentra el fraude informático.[36]

Además, en el proyecto de la Ley No. 19.223, se evidencia la finalidad de proteger un nuevo bien jurídico que ha surgido con el uso de las tecnologías computacionales. Sin embargo, no solamente es ese bien el que se propende proteger, sino también, otros bienes como el patrimonio, la privacidad, la seguridad y el derecho de propiedad intelectual. Siendo conscientes de que el nacimiento de esta nueva tecnología, proporciona nuevos mecanismos para atentar contra bienes jurídicos ya existentes (Delitos Informáticos. Chile y legislación extranjera, s.f).[37]

Respecto al sabotaje informático en la Ley 19.223 en particular el primer artículo referente a la destrucción o inutilización del sistema de tratamiento de datos, o de sus partes o componentes, nace una crítica frente a la cobertura del tipo penal, o sea, al objeto de ataque, ya que, por un lado, la destrucción de un sistema de tratamiento de datos puede ser subsumible en el tipo penal de daño convencional, y, por otro, la extensión del daño punible, pues cubre la hipótesis de daño a los datos o programas informáticos a partir de la destrucción o inutilización de los elementos que componen el sistema informático para su aplicación.

[36] ACUARIO DEL PINO, Santiago. (s.f). Delitos Informáticos: Generalidades. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[37] BCN Informe Biblioteca Nacional del Congreso de Chile, Delitos Informáticos. Chile y la legislación extranjera. Recuperado de https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIÓN CUENTA&prmID=11020

En cuanto al artículo 2 respecto a la interceptación, interferencia o acceso no autorizado, conductas asociadas por la jurisprudencia en conjunto al artículo 414 como correspondientes a espionaje informático, le falta a la normatividad nacional dos elementos, estos son: la necesidad de haber provocado un perjuicio pecuniario, o al menos el haber logrado un beneficio económico para quien ha cometido el ilícito, elementos que la ONU destaca en su definición de espionaje informático.

La Ley 19.223, tampoco establece criterio alguno para distinguir los datos, por su titularidad, importancia o sensibilidad. Y, finalmente, el artículo 4 tipifica la revelación o difusión de datos de un sistema informático en general, sin importar si éstos son públicos, y sin exigir que estén bajo secreto, reserva o encriptación.

Si bien, el resguardo de la información es el propósito de la legislación, con la redacción de las disposiciones de la Ley 19.223 permite calificar a los delitos allí tipificados como pluriofensivos, admitiendo la aplicación de sus normas en resguardo de bienes jurídicos distintos, como el patrimonio o la intimidad.

Luego, en junio de 2005, se crea la Ley 20.009, se hace cargo de la imposibilidad de aplicación de tipos penales de fraude a las defraudaciones cometidas por medios informáticos sobre tarjetas de crédito, cubriendo un gran vacío legal que antes existía.

3. Desarrollo jurisprudencial en el derecho comparado del bien jurídico tutelado delito de hurto por medios informáticos en el derecho comparado

3.1 Jurisprudencia Española

- **Sentencia Penal No 446 del año 2012. Audiencia Provincial de Madrid, Sección 16. Ref. 420/2011 de 08 de junio de 2012.**[38]

Es el caso de una mujer que accedió de manera fraudulenta a la cuenta bancara de otras personas y realizó disposiciones de dinero a favor de terceros, comisionándose el delito de estafa. La principal prueba en su contra fue el informe de la Policía Nacional que investiga delitos informáticos en el que explicaba la modalidad de este tipo de delitos.

En la apelación, alega el apelante error en la valoración de la prueba, y vulneración del principio de presunción de inocencia, ya que eran otros los autores que habían hecho la transferencia de manera fraudulenta. Transferencia de la que ella desconocía los detalles. Igualmente, alega que ella no realizó el engaño, ni hizo la manipulación informática con ánimo de lucro, añadiendo que la actuación de su parte fue un error invencible al desconocer de esta manipulación.

El Juzgado Penal No. 2 de Móstoles en Juicio Oral, procede a resolver la apelación quien confirma lo indicado por el Juzgado de lo Penal, el cual dictó sentencia el día 29 de julio de 2011, cuyo fallo decretó condenar a Gema, como autora, por cooperación necesaria, de un delito de estafa del artículo 248.2 del Código Penal, con la concurrencia de la circunstancia modificativa de la responsabilidad criminal, consistente en atenuante, simple, de dilaciones

[38] MADRID. Sentencia Penal Nº 446/2012, Audiencia Provincial de Madrid, Sección 16, Rec 420/2011 de 08 de junio de 2012. Recuperado de https://www.iberley.es/jurisprudencia/sentencia-penal-n-446-2012-ap-madrid-sec-16-rec-420-2011-08-06-2012-11043761?voces%5B0%5D=Delito+inform%C3%A1tico&noIndex

indebidas, a la pena de veintiún mes de Prisión, con inhabilitación especial para el ejercicio del derecho de sufragio pasivo por el tiempo de esa condena. Además de ser condenada a la mitad de las costas del proceso.[39]

3.2 Jurisprudencia Estadounidense

- **Sentencia a ciudadano ruso Maxim Senakh culpable de conspiración para cometer fraude electrónico y violar la Ley de abuso y fraude informático.**

Es el caso de un ciudadano ruso que participó en una empresa criminal que instalaba y explotaba software de computadora malicioso en decenas de servidores a nivel mundial para general millones de dólares en pagos fraudulentos. El acusado y sus co-conspiradores buscaron convertir una red de miles de computadoras infectadas en los Estados Unidos y en todo el mundo en sus cajeros automáticos personales, creando una infraestructura sofisticada que afecto a miles de usuarios de internet. El malware conocido como Ebury obtenía credenciales de inicio de sesión de servidores afectados lo que les permitida generar y redirigir el tráfico de Internet en la promoción de varios esquemas de correo electrónico de spam y fraude de clics, con lo que recaudaron dólares en ingresos

Sin embargo, las acciones de la División Criminal del Departamento de Justicia y el FBI dejaron claro que los ciberdelincuentes no son inmunes a la persecución de los Estados Unidos solo porque operan desde lejos o detrás de un velo de tecnología. Pues el FBI tiene la capacidad y la determinación de identificarlos, encontrarlos y llevarlos ante la justicia.

[39] IBERRLEY COLEX. Jurisprudencia sobre delito informático. 2012. Recuperado de https://www.iberley.es/jurisprudencia/delito-informatico.

La sentencia proferida el 3 de agosto de 2017, envía un fuerte mensaje a los ciberdelincuentes internacionales que creen erróneamente que pueden atacar al pueblo estadounidense con impunidad.

Maxim Senakh, de 41 años, de Veliky Novgorod, Rusia, fue sentenciado a 46 meses de prisión y será deportado luego de ser liberado. Senakh se declaró culpable el 28 de marzo de conspiración para cometer fraude electrónico y violar la Ley de abuso y fraude informático.[40]

- **Sentencia a Hackers Hamza Bendelladj y Aleksandr Andreevich Panin por conspiración para cometer fraude bancario, fraude electrónico, conspiración para cometer fraude y abuso de computadoras.**

Estos hackers desarrollaron el malware malicioso SpyEye, con el objetivo de robar dinero de cuentas bancarias de individuos e instituciones al infectar a millones de computadoras en los Estados Unidos y en todo el mundo, causando un billón en daños financieros a individuos e instituciones financieras de todo el mundo.[41]

Bendelladj, de 27 años, fue condenado a 15 años de prisión y Andreevich a 9 años de prisión, al declararse culpables de un cargo de conspiración para cometer fraude bancario, 10 cargos de fraude electrónico, un cargo de conspiración para cometer fraude y abuso de computadoras y 11 cargos de fraude y abuso de computadora.

[40] THE UNITED STATES DEPARTMENT OF JUSTICE. Justice News. Russian Citizen Sentenced to 46 Months in Prison for Involvement in Global Botnet Conspiracy. 2017. Recuperado de https://www.justice.gov/opa/pr/russian-citizen-sentenced-46-months-prison-involvement-global-botnet-conspiracy

[41] DEPARTMENT OF JUSTICE. U.S. ATTORNEY'S OFFICE. Two Major International Hackers Who Developed the "SpyEye" Malware get over 24 Years Combined in Federal Prison. 2016. Recuperado de https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined

Este caso es de gran importancia al llevar a la justicia a unos piratas informáticos prolíficos y además prevenir inconmensurables pérdidas financieras a nivel mundial. Al realizarse estos arrestos el riesgo de la sofisticada versión de SpyEye se redujo a cero, demostrando el poder de las investigaciones del FBI enfocadas a desmantelar el delito informático.

SpyEye fue diseñado para automatizar el robo de información confidencial personal y financiera, como credenciales de banca en línea, información de tarjetas de crédito, nombres de usuario, contraseñas, PIN y otra información de identificación personal. Al infectarse la computadora, estaba bajo su control lo cual les permitía el acceso a la información personal y financiera de las víctimas.

El FBI descubrió a los pocos meses de su arresto, que estos delincuentes planeaban lanzar una nueva versión de SpyEye más poderoso, cuyas consecuencias serían inmensurables.

Este caso fue investigado por Agentes Especiales de la Oficina Federal de Investigaciones. El FBI interrumpió y desmanteló la estructura organizativa detrás de SpyEye utilizando niveles de cooperación sin precedentes con la industria privada y 26 agencias internacionales de cumplimiento de la ley, entre las que se encuentran ellas la Agencia Nacional de Delitos del Reino Unido, la Policía Real de Tailandia, la Policía Nacional de los Países Bajos - Unidad Nacional de Delitos de Alta Tecnología (NHTCU), el Departamento Nacional de República Dominicana. Investigaciones (DNI), el Departamento de Delitos Cibernéticos de la Agencia Estatal de Seguridad Nacional de Bulgaria y la Policía Federal de Australia (AFP). Demostrando que las fronteras internacionales ya no ofrecen refugios seguros para los delincuentes cibernéticos.[42]

[42] YOUNES ALI. News. Hacker Hamza Bendelladj. Sentenced to 15 years. 2016 Recuperado de https://www.aljazeera.com/news/2016/04/hacker-hamza-bendelladj-sentenced-15-years-160422104149553.html

Ante lo anterior, es importante resaltar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030). Esta elimina argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, entre otros. Siendo esta Ley un adelanto al estar directamente en contra de los actos de transmisión de virus. El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos, definiendo dos niveles para quienes crean el virus con el fin de causar daño y para aquellos que lo transmiten de manera imprudencial. Aclarando a su vez que el creador de un virus no puede escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que solo quería enviar un mensaje.

Esta Ley constituye un acercamiento importante a la problemática de los virus informáticos, específicamente no definiéndolos sino describiendo su actuar y su peligrosidad, entendiéndose este como un acto delictivo.

Reconociéndose, el objetivo del legislador, al querer aumentar la protección a los individuos, negocios, y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas informáticos creados legalmente. Teniendo claro que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos.

3.3 Jurisprudencia Chilena

Análisis jurisprudencial chileno con énfasis en el artículo 1 de la Ley No. 19.223 de delitos informáticos, en el que se demuestran los vacíos de la norma.

- **Sentencia, caso Hipermercado Curicó Limitada con Lizama Ponce, María de las Nieves y otros.**

La cajera trabajadora del supermercado, se aprovecha del sistema de venta de tarjetas electrónicas de saldo para telefonía móvil para venderlas sin registrar la venta en el sistema interno de cajas, por lo que los movimientos no se visualizan en el sistema, a pesar de entregar el código de carga de la compañía celular.

Entre los cargos que se le formularon se encuentra el contenido en el artículo 1 de la Ley No. 19.223, por cuanto impide, obstaculiza o modifica el funcionamiento de un sistema de tratamiento de información. Sin embargo, la Corte de Apelaciones de Talca, conociendo de la sentencia condenatoria de primera instancia, concede recurso de nulidad entendiendo que no concurre el delito informático pues no existió modificación o alteración alguna que permitiera configurar el delito, sino que fue un aprovechamiento de la mala programación del sistema.[43] Quedando claro que la interceptación debe ser realizada por un medio técnico, vacío legal de la Ley 19.223 y por lo tanto, no hubo condena por otro delito en reemplazo.

- **Sentencia, caso de la modificación de los datos de las tarjetas de decodificadores de señales televisivas satelitales, a fin de tener acceso a mayor cantidad de canales.**

En Sky Chile CPA, el imputado Pablo Andrés, vendía tarjetas de codificación para receptores de señal satelital modificadas, con el fin de obtener acceso a más canales sin pagar a sus operadores. Éste, fue condenado por los delitos en la Ley de Telecomunicaciones y también por el artículo 1 de la Ley No. 19.223, al modificar el funcionamiento del sistema de tratamiento de información.

[43] LARA, Juan Carlos, MARTINEZ, Manuel y VIOLLIER Pablo. Hacia una regulación de los delitos informáticos basada en la evidencia. Revista Chilena de Derecho y Tecnología. 2014. p. 114. Recuperado de https://rchdt.uchile.cl/index.php/RCHDT/article/download/32222/34151/

Para la comisión del delito, Pablo se valió de programas informáticos que descargo gratuitamente en internet. No obstante, la Corte Suprema señala que no se puede condenar por el artículo 1 de la Ley No. 19.223, debido a que el programa no fue creado por el imputado y no se puede condenar, cuando solo hizo uso de las fallas de sistema.[44]

Se hace continuidad del análisis jurisprudencial chileno, al artículo 2 de la Ley No. 19.223 de delitos informáticos, demostrando los problemas en torno al significado de "indebido".

- **Sentencia, caso base de datos, Compañía Sudamericana de Vapores con Jans Vásquez.**

Un individuo es inculpado de tomar las bases de datos de su antiguo trabajo, a las que tenía acceso, para llevarlas a un nuevo empleo. En primera instancia, quedo absuelto. Para lo cual se realizó la apelación de la sentencia absolutoria. Ante esto, la Corte de Apelaciones de Santiago, entendió que existía una tesis de apoderamiento y uso indebido de bases de datos a partir de lo mencionado en el artículo 2 de la Ley 19.223, por cuanto la información fue enviada al correo personal para su uso posterior, a lo que se evidencia que existió por parte del inculpado una apropiación indebida de esos datos.

Pues si bien es cierto, el sujeto tenía acceso a esa información, dicho acceso se limitaba solo al uso dentro de la empresa, por tanto, su uso posterior es indebido y, por tanto, típico.[45]

[44] Ibídem, p. 114
[45] Ibídem, p. 116

Así, el concepto de “indebido” alcanza al uso de datos que, incluso habiendo autorización para conocer en determinado contexto, quedan exentos de esa autorización para un uso posterior, que es entonces indebido y, por tanto, típico.

- **Sentencia, caso Polincay Export y Comercial Polincay Limitada con Pérez Rodríguez, Raúl Ignacio.**

En este caso, el imputado había obtenido la contraseña de acceso al correo electrónico de su jefe, a fin de acceder al contenido de su computador, obteniendo información de su empleador y sus negocios, cometiendo un abuso de confianza. Además, dicho acceso se mantuvo aun cuando el dejo de trabajar para la empresa.

La Corte de Apelaciones de Santiago, consideró que la participación y consiguiente responsabilidad criminal del procesado como autor del delito por el cual se le ha acusado, se encontraba suficientemente acreditada, y, por lo tanto, el imputado se apropió indebidamente de la información reservada contenida en las bases de datos informáticas de su empleadora. No obstante, la Corte Suprema en casación, absuelve al imputado por cuanto considera que la intromisión no fue indebida, y, establece la responsabilidad plena de la víctima por haber puesto en peligro sus propios datos.[46]

Por último, análisis jurisprudencial chileno, al artículo 4 de la Ley No. 19.223 de delitos informáticos.

[46] Ibídem, p. 117

- **Sentencia, caso Vargas Mayorga, Marisol con Valenzuela Cruz, Sergio y otros.**

El caso hace referencia a la obtención de imágenes íntimas de una teniente del Ejército de Chile por parte de dos compañeros de tropa. Los imputados encontraron las imágenes en un dispositivo USB de la víctima, al cual accedieron sin su consentimiento, y tras lo cual compartieron esas fotos.

Este caso fue llevado en primera y segunda instancia dentro de la jurisdicción de los tribunales militares, condenando a los imputados por el delito contemplado en el artículo 4 de la Ley No. 19.223, por la revelación maliciosa de datos contenidos en el sistema de información. Igualmente, la Corte Suprema en casación, señalo que el legislador protege los datos sensibles y la intimidad personal por lo que la sentencia condenatoria era la correcta.[47]

Sin embargo, el voto minoritario sostuvo que, al no tener relación con los sistemas de información o sus datos, su indemnidad o uso indebido, el fallo recurrido incurre en infracción de la ley.

Siendo este caso más relacionado con la idea de protección de la intimidad de la víctima, que con la afectación misma de datos como delito informático. Dejando clara la Corte, la existencia de otros bienes jurídicos protegidos, externos al objeto de protección perseguido por la Ley 19.223. Asimismo, evidenciando la insuficiencia de los tipos penales en resguardo del derecho a la vida privada o a la intimidad en el Código Penal Chileno.

Sin duda, uno de los elementos más discutibles de las normas en la Ley 19.223 es frente a la expresión “maliciosamente” para referirse al ánimo en que han de cometerse los ilícitos informáticos. A lo cual la Corte Suprema rescata la

[47] Ibídem, p. 118

conclusión a la que se ha llegado con el transcurso del tiempo de la misma Ley, y en tanto, la expresión se refiere a la existencia y prueba de dolo específico, necesario para la configuración del tipo establecido en dichas hipótesis contenidas en la Ley.

Con lo anterior, queda claro que la Ley No. 19.223, con su reducido articulado y cuestionada redacción, revela ciertas falencias a la hora de ser aplicada por los tribunales de chile.

CAPITULO II

1. DESARROLLO LEGISLATIVO DEL BIEN JURÍDICO TUTELADO EN EL DELITO DE HURTO POR MEDIOS INFORMÁTICOS EN COLOMBIA

1.1 El Hurto calificado como primera estructuración típica

En el último siglo la teoría del delito ha tenido una evolución fundamental, radicada en la imputación objetiva, frente al accionar de delitos que ocurren en el medio real o en el mundo exterior para ser más exacto, como por ejemplo el hurto, el homicidio, delitos de carácter administrativos, a estos delitos los denominares analógicos o clásicos, los cuales han surtido una gran transformación por cuenta de la imputación objetiva[48], este tipo de delitos puntualizan la imputación a realizar sobre el mismo y el nexo de causalidad en los delito dolosos e imprudentes, sin embargo los delitos de digitales o la idea de proteger bienes ideales o inmateriales es la tendencia mundial como por ejemplo los delitos que protegen la propiedad intelectual[49] (CP, artículos. 270 y ss.) o industrial.

Finalizando los años sesenta, nacen para el mundo jurídico la realización de los delitos informáticos o cyber-crimenes (daños informáticos, trasferencias no autorizadas de activos, obstaculización de datos e infraestructuras informáticas), este surgimiento de una nueva clase de delitos ha generado una serie de nuevos estudios legales o jurídicos, y categorización dogmática frente a los esquemas tradicionales del delito clásico. Este replanteamiento jurídico y dogmático permitirá una nueva ventana jurídica frente a la realización de este tipo de delitos

[48] Frisch, Wolfg ang, *La imputación objetiva del resultado,* Barcelona, Atelier, 2015, pp. 41 y ss., y 56 y ss.; Jescheck, Hans Heinrich / Weigend, Thomas, *Tratado de Derecho Penal*, Granada, Comares, 2002, pp. 307 y ss.; Roxin, Claus, *Derecho Penal, Parte General*, Tomo 1, Madrid, Editorial Civitas, 1997, pp. 362 y ss.; Welzel, Hans, *Derecho Penal alemán: Parte General,* Santiago, Jurídica de Chile 1997, pp. 66 y ss. (tipo y adecuación social).

[49] GRACIA MARTÍN, Luis, Prolegómenos*,* Madrid, Civitas, 2001, p. 88. Señala*: con claridad la insuficiencia dogmática de los nuevos delitos en la era del riesgo.*

cibernéticos, los cuales se caracterizan por el empleo de medio electrónicos, inicialmente computadores y redes de conexión para una sociedad que se modifica cyber-digitalmente. Estos delitos lesionan y ponen en peligro la confiabilidad, integridad, acceso a datos informáticos y redes de seguridad informática, las cuales según la evolución digital son necesarias para la sociedad global desde su inicio cibernético y que a hoy son más requeridas y necesarias para lograr una interacción social, lo interesante de estos comportamientos es que, en una minuciosa investigación político-criminal, son conductas punibles (CP, artículo 9), que tienen su realización en un espacio, *sin espacio físico,* estas conductas se desarrollan en el cyber-espacio o en la web4, realidad simulada a través de la cual se accede a través de un computador o una red de conexión digital5, no es de olvidar que estos elementos favorecen a la socialización global y no solo frente a los aspectos de comunicación sino políticos, sociales y económicos, estos elementos también favorecen a la reproducción de una sociedad conectada, digitalizada, mediática y altamente vulnerable por su analfabetismo digital hacia el mismo componente y utilización de medios electrónicos. Estos riesgos se caracterizan por ser extremadamente técnicos y masivos, elementos que no caracterizan los delitos tradicionales de cuyo estudio y aplicación −difícilmente− se satisface con la teoría del "delito analógico". Como lo precisa Miró Llinares.

El crimen informático, sitúa a la doctrina jurídico-penal contemporánea frente a varias transformaciones de *Delito y de Pena*, los cuales a medida de los avances tecnológicos deben ser analizados con urgencia [50].

[50] Predicament, Durham, Cole, "The emerging structures of criminal information law: Tracing the contours of a new paradigm" en: *Information, Technology, Crime.* National legislation and international initiatives, Ius informationis, Vol. 6, Köln-Berlín-Bonn-München, Heymann, 1994, pp. 546. Señala que *"The challenge of post-modern society is to make certain that the Enlightenment values of classical criminal law are not eroded by the demands of increasing complexity or alternatively, that such values are transformed and adapted that will provide protections appropriate to the new historical context in which they are being applied"*

Primero, definición, delito más especializado frente a la noción general del mismo, debido a que este delito se realiza en diferentes realidades informáticas en el cybe –espacio y exige herramientas tecnológicas especializadas, adicionado a esto la clasificación de comportamiento en una realidad virtual involucran una transformación compleja de elementos típicos objetivos y subjetivos, sobre todo de la acción y sus 'resultados' de acuerdo con este nuevo fenómeno social[51]; lo que genera una enorme incertidumbre dogmática.

Segundo, la sociedad actual, obedece al funcionamiento de la gestión de la información, datos y las infraestructuras informáticas necesarias para la subsistencia e interacción de sus miembros.

Es una realidad que la sociedad actual basa sus cimientos en datos informáticos, influencia de primer orden para el interactuar de una sociedad moderna y como se relacionan con el medio circundante, se puede concluir que pasamos de una época análoga a un resurgimiento social digital, el cual se caracteriza por hiperconexiones y colonias virtuales que permiten el ejercicio del control no institucional a las instancias públicas (Facebook, Twitter, etcétera)[52]. De estos resurgimientos digitales se permite establecer que se generan nuevos bienes jurídicos tutelados estatalmente y seguido a esto nuevos bienes jurídicos la

[51] PÉREZ LUÑO, Enrique Antonio. Manual de informática y derecho, Barcelona, Ariel, 1996, p. 75. Habla de nuevas versiones de los delitos tradicionales.

[52] POSADA MAYA, Ricardo, "Libertad de información e independencia judicial", en *Discriminación, principio de jurisdicción universal y temas de derecho penal,* Bogotá, Uniandes, 2013, pp. 682-683, advierte que: "La fácil acogida de los mensajes mediáticos por parte de la opinión pública obedece, en gran medida, a la influencia de las nuevas generaciones en la construcción de una sociedad altamente mediática y tecnológica, que debe ser apreciada en el contexto de la globalización comunicacional. Un contexto en donde la opinión, a través de las redes sociales como Facebook, Twitter y Messenger, etcétera, resulta el mecanismo más fácil para participar en los asuntos de interés general, en particular para aquellos grupos que tradicionalmente no han tenido un acceso material a las discusiones que deciden el frágil equilibrio de las expectativas sociales; pero también porque dichos escenarios cumplen, como ninguno, o bien la reivindicación cierta del derecho a la administración de justicia, o el clásico recurso al "pan y circo", al "desquite" o a la "venganza social", como fórmulas de reafirmación y optimización subjetiva (no necesariamente objetiva o legítima) de las libertades constitucional de quien participa en este tipo de escenarios" (cursivas por fuera del texto original).

exigencia por parte de la sociedad a los diversos estados en su protección, como: patrimonio (digital), intimidad y autodeterminación informática[53].

Tercero, estos avances tecnológicos hacen cada vez más difícil la delimitación de las categorías dogmáticas de la conducta punible, como estructuras jurídicas que permitirían explicar mejor estas nuevas formas de criminalidad[54]. Por ejemplo, comisión tecnológica, la conexión cibernética, la virtualidad, la deslocalización y los datos inmateriales, no son conceptos que se encuadran con una teoría del delito análoga o desactualizada, como lo señala Miró Llinares, no se estaba pensando en la ciberdelincuencia "[…] cuando se desarrollan prácticamente todas las teorías criminológicas, y tampoco cuando lo hacen las teorías del crimen, pues los presupuestos negados y los datos aportados para hacerlo se refieren siempre a la delincuencia 'física' […]"[55].

Como conclusión, no es posible a través de la dogmática clásica del delito, resolver o explicar todos los elementos que conforman una realidad simulada o múltiples realidades generadas en un espacio infinito de datos o realidad cibernética, debido a que las mismas se generaron de manera análoga o para una realidad física con efectos físicos y no digitales, debido a que no fue pensado en

[53] SATZGER, Helmut, "La protección de datos y sistemas informáticos en el derecho penal alemán europeo.Tentativa de una comparación con la situación legal en Colombia", en: *Derecho penal y nuevas tecnologías,* Bogotá, Universidad Sergio Arboleda, 2016, p. 19, dice que: "En esencia –tanto el ordenamiento jurídico colombiano, como en el sistema jurídico alemán– existen sobradas razones para reconocer en el derecho penal de la información el novedoso bien jurídico, pues, a diferencia de la sociedad industrial que se basa en gran medida, en los objetos de derecho físicos, tangibles, la sociedad de la información se afinca, casi exclusivamente, en datos e información prácticamente intangibles".

[54] POSADA MAYA, Ricardo, "Una Aproximación a la Criminalidad informática en Colombia", en *Revista de Derecho Comunicaciones y Nuevas Tecnologías*, 2006, p. 15, indica lo siguiente: "Así las cosas, la fenomenología criminal ha variado como secuela del cambio informático global; pues la primera se ha adaptado al segundo, con el efecto previsible de que los mecanismos institucionalizados de regulación de la vida social han transformado –no siempre de manera adecuad – sus propias perspectivas y criterios de imputación. Especialmente el Derecho penal, con el fin de mejorar sus herramientas de prevención, control y sanción. Y ello es así, pues se afirma que las técnicas jurídicas de control tradicionales resultan cada vez menos eficaces –aunque ello sea discutible– para prevenir o someter formas de criminalidad masificadas, especializadas, continuas, lesivas, muy difíciles de descubrir, rastrear y criminalizar; por oposición a la progresiva vulnerabilidad de las víctimas y de las funciones protegidas".

[55] MIRÓ LLINARES, Fernando, "La cibercriminalidad 2.0: Falacias y realidades", cit, p. 72.

ese momento y la tecnología no existía, por esto es escasa y debe desarrollarse a medida del surgimiento de las diversas tecnologías informáticas que aceleran el mundo actual, no se resuelven de forma hábil y práctica todos los problemas que se producen a partir de la informática en la realidad criminal[56].

Cibercrimen y teoría de la tipicidad

En el año 2009 surge la ley 1273 de 2009, la cual adiciona un nuevo capítulo al código penal, ley 599 de 2000, "*De la protección de la información y de los datos"* capítulo VII Bis[57],con el fin de proteger un nuevo bien jurídico[58], en el cual se generan nuevas conductas delictivas artículos 269ª y SS, con la finalidad de tipificar y hacer prevalecer el bien jurídico tutelado "*De la protección de la información y de los datos*" informáticos, (confidencialidad/confiabilidad, disponibilidad, integridad, no repudio y recuperación de datos)[59].

[56]Bien señala ZAGREBELSKY, Gustavo, *El derecho dúctil: Ley, derechos, justicia,* 5ª edición, Editorial Trotta, Madrid, 2003, p. 122, cuando se refiere al carácter práctico de la ciencia del derecho, que "[…] Naturaleza práctica del derecho significa también que el derecho, respetuoso con su función, se preocupa de su idoneidad para disciplinar efectivamente la realidad conforme al valor que los principios confieren a la misma. Así, pues, las consecuencias prácticas del derecho no son en modo alguno un aspecto posterior, independiente y carente de influencia sobre el propio derecho, sino que son un elemento cualificativo del mismo. No se trata en absoluto de asignar a lo "fáctico" una prioridad sobre lo "normativo", sino de mantener una concepción del derecho que permita que estos dos momentos no sean irrelevantes el uno para el otro […]".

[57] Dicho título se compone de dos capítulos: el primero está referido a "Los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" (a las cuales se deben agregar el no epudio y la recuperación de información), artículos 269A a 269H; y el segundo, atiende a "Los atentados informáticos y otras infracciones", artículos 269I, 269J y el artículo 105 de la Ley 1453 de 2011 (que resulta innominado o incluido en el artículo 269J de manera absolutamente antitécnica).

[58] MATA Y MARTÍN, Ricardo, *Bienes jurídicos intermedios y delitos de peligro,* Granada, Comares, 1997, pp. 23 y ss.

[59] Sobre las funciones informáticas en sentido estricto, véase Cano Martínez, Jeimy, *Manual de un Chief Information Security Officer,* Bogotá, Ediciones de la U, 2016, pp. 96 y 97; Pomante, Gianluca, *Internet e criminalità,* Torino, Giappichelli Editore, 1999 pp. 109 y 113; Posada Maya, Ricardo, "Una Aproximación a la criminalidad informática en Colombia", cit., p. 22; Posada Maya, Ricardo, "El delito de transferencia no consentida de activos", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* Bogotá, 2012, pp. 215-216; Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos,* en *Estudios de Derecho penal* No. 33, Comares, Granada, 2002. pp. 67 y 69 y ss.; id., *Delincuencia informática y fraudes informáticos,* p. 72.

Este nuevo capítulo introduce modalidades tentadas frente a la vulneración "seguridad de la información informatizada" y los sistemas e infraestructuras informáticas, en particular de naturaleza patrimonial. Dicho título tomó como referencia técnica internacional la Convención contra la Cibercriminalidad de 2001 (Budapest)[60].

Esta clasificación de comisión dolosa, que se introducen en el nuevo capítulo al código penal Colombiano, Ley 599 de 2000, introducen una nueva técnica de reconocimiento del cibercrimen, categorización dogmática, nexo de causalidad, riesgo y dominio del hecho, resultan herramientas necesarias para categorizar y entender los crímenes digitales o cibercrimen[61] del derecho penal.

Veamos las principales diferencias entre los elementos propios de la teoría de la tipicidad para delitos clásicos y para los cibercrímenes o crímenes digitales.

La definición de *cibercrimen*

La doctrina especializada sostiene que los *cibercrímenes* (o delitos informáticos en sentido *estricto* o *propio*), castigan los comportamientos que lesionan o ponen en peligro de manera ilícita la seguridad de las funciones informáticas; sin perjuicio de que ello implique la lesión o la puesta en peligro de otros bienes jurídicos tutelados.

[60] LEZERTUA, Manuel, "El proyecto del convenio sobre el Cybercrimen del Consejo de Europa", en: *Internet y derecho penal, uadernos de Derecho judicial X,* Madrid, Consejo General del Poder Judicial, 2001 pp. 15-62; Morales García, Oscar, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cyber-Crimen", En: *Delincuencia informática, Cuadernos de derecho judicial IX,* Madrid, Consejo General del Poder Judicial, 2002, pp. 11-34. Recuperado de http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS _ 185 _ spanish.PDF

[61] DURHAM, Cole, "The emerging structures of criminal information law: Tracing the contours of a new paradigm", en: *Information, Technology, Crime: National legislation and international initiatives,* Ius informationis, Vol. 6, Köln-Berlín-Bonn-München, Heymann, 1994, pp. 533-542.

La definición del cibercrimen, anteriormente mencionada, no es rígida en su definición, es un sentido amplio de la misma, debido a que la utilización de medios informáticos y telemáticos son elementos instrumentalizados en la ejecución de los cibercrímenes[62], incluso equiparando estos últimos a los *delitos computacionales o de conexidad medial* a la red para el tratamiento de datos, información y sistemas informáticos (utilización de elementos incorporales)[63]. Recuérdese que los delitos vinculados al internet, a diferencia de los cibercrímenes, protegen en primera medida otros bienes jurídicos tutelados como la intimidad o el patrimonio económico, antes que la seguridad de la información, los datos y los sistemas informáticos, que se protegen de manera indirecta.

Precisamente, atendiendo a estas diferencias, la Ley 1273 de 2009, artículo 2, adicionó un numeral 17 al artículo 58 del CP, por medio del cual se agrava la pena de los delitos no informáticos: "*Cuando para la realización de las conductas*

[62]MATELLANES, Nuria, "Algunas notas sobre las formas de delincuencia informática en el Código penal", en: *Hacia un Derecho penal sin fronteras,* XII Congreso Universitario de Alumnos de Derecho penal, Madrid, Colex, 2000, p. 130; Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos,* cit, pp. 65, 130 y 131; id, "Hacia una expansión doctrinal y fáctico del fraude informático" en *Revista Aranzadi de derecho y nuevas tecnologías,* Nº3, 2003, p. 118; UIT, *Understanding Cybercrime: phenomena, challenges and legal response,* Ginebra, UIT, 2012, p. 11; Wall, David, *Cybercrime: The Transformation of Crime in the Information Age,* Cambridge: Polity Press, 2007, p. 221.

[63]CONPES 3701 (2011-2014) define el ciberdelito como una "Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)", definición que infortunadamente no distingue entre el delito informático en sentido amplio y en sentido estricto; De La Cuesta Arzamendi, José Luis / De La Mata Barranco, Norberto, *Derecho penal informático,* Madrid, Civitas-Thomson Reuters, 2010, pp. 31 y 159; Fernández García, Emilio Manuel, "Fraudes y otros delitos patrimoniales relacionados con la informática e internet", en: *Estudios Jurídicos*, IV , Madrid, Consejo General del Poder Judicial, 1999, p. 391; Galán Muñoz, Alfonso, *El fraude y la estafa mediante sistemas informáticos: Análisis del artículo 248.2 C.P.,* Valencia, Tirant lo Blanch, 2005, pp. 29 y ss.; Miró Llinares, Fernando, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio,* cit, pp. 33 y ss.; Satzger, Helmut, "La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia", en: *Derecho penal y nuevas tecnologías,* Bogotá, Universidad Sergio Arboleda, 2016, p. 12; Sieber, Ulrich, *Computerkriminalität und Strafrecht: Neue Entwicklungen in Technik und Recht,* 2da ed., Köln-Berlin-Bonn-München, Heymanns, 1980 p. 39; id, "Criminalidad informática. Peligro
y prevención", pp. 29 y ss.; id. "Documentación para una aproximación al delito informático" en *Delincuencia informática,* 1992, pp. 65-90; Tiedemann, Klaus, "Criminalidad mediante computadoras", en: *Nuevo Foro Penal* No. 30, octubre–diciembre de 1985, Bogotá, Temis, pp. 481 a 492; id., *Poder económico y delito,* Ariel, Barcelona, 1985, p. 122.

punibles se utilicen medios informáticos, electrónicos o telemáticos" (cursivas por fuera del texto original). Una circunstancia de mayor punibilidad que recoge un *desvalor de acción en la ejecución de los delitos clásicos*, y que debe ser considerada al momento de la individualización judicial de la pena (CP, artículo 61; CPP, artículo 447).

El cibercrimen, no trata de delitos tradicionales o comunes, sino de tipos penales y conductas especiales, que se realizan a través de procedimientos informáticos, cuya riqueza técnica, su contexto virtual, la afectación de objetos inmateriales[64] y su deslocalización en el *ciberespacio*, rompen los esquemas teóricos y las dinámicas probatorias propias de los delitos comunes.

1.2. Referencia de otros tipos penales que protegen los sistemas informáticos.

Antes de la expedición de la Ley 1273 de 2009, el Código Penal, hacía referencia a conductas punibles cometidas con medios informáticos. Sin embargo, estas conductas no estaban contenidas en un solo título, lo cual hacía difícil la sanción de estos delitos, y su definición no había sido determinada por el legislador.

---

[64] POSADA MAYA, Ricardo, "Una Aproximación a la criminalidad informática en Colombia", cit., pp. 19 y 20; id., Posada Maya, Ricardo, "El delito de transferencia no consentida de activos", cit., p. 214, señala que "la *cibercriminalidad* cubre aquellas conductas punibles realizadas con fines ilícitos, no consentidas (facultadas) por el titular de la información o los datos, o abusivas de este consentimiento (facultad), que se orientan 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 privada o semiprivada), empresarial, comercial o pública, que pongan en peligro o lesionen (C.P., artículo 11) la
seguridad de las funciones informáticas en sentido estricto, esto es, la confiabilidad (calidad, pureza, idoneidad y corrección), la integridad y la disponibilidad de datos o información, y de los componentes lógicos de la programación de los equipos informáticos o de los programas operativos o aplicativos *(software)* […]. *Por consiguiente, no se trata de delitos comunes sino de tipologías especiales realizadas a través de procedimientos informáticos, que gozan de cierta riqueza técnica, aunque no abandonan los tipos penales ordinarios como referentes dogmáticos y criminológicos"* (cursivas por fuera del texto original). Por otro lado, Rovira del Canto, Enrique, *Delincuencia informática y fraudes informáticos,* cit, pp. 130. Meek Neira, Michael, *Delito informático y cadena de custodia,* niversidad Sergio Arboleda, Bogotá, 2013, pp. 59.

Algunos doctrinantes, entre ellos el profesor Ricardo Posada Maya, da una definición de los delitos informáticos:[65]

> "El 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…".

Las conductas mencionadas en la definición del profesor Ricardo Posada Maya eran perseguidas utilizando algunos tipos penales, consagrados en el Código Penal Colombiano, como:

- Hurto calificado, artículo 240, numeral 4.
- Falsedad ideológica en documento público, artículo 286.
- Falsedad en documento privado, artículo 289.
- Uso de documento falso, artículo 291
- Destrucción Supresión y ocultamiento de documento público, artículo 292.
- Destrucción Supresión y ocultamiento de documento privado, artículo 293.
- Falsedad personal, artículo 296.
- Entre otros.

Los cuales se podían cometer a través de medios informáticos, lo que conlleva a una defraudación potencial no consentida a los intereses económicos de las víctimas, en provecho de terceros.

[65] Ibídem, 2006, p. 21

No obstante, y aunque el artículo 195 del Código Penal hablara del acceso abusivo a un sistema informático, esta norma no poseía un contenido completo y suficiente para las necesidades actuales frente a los delitos informáticos (Ley 599 Código Penal, 2000). Demostrando entonces, la necesidad de regular las conductas con fines ilícitos que constituyen delito informático, las cuales son realizadas a través de medios tecnológicos y /o con la utilización de internet, con el propósito de dañar, suprimir, defraudar, falsificar o modificar datos informáticos con ánimo de lucro.

Por consiguiente, con la ley 1273 de 2009, se modifica el Código Penal y se crea un nuevo bien jurídico tutelado, denominado “de la protección de la información y de los datos”, además, se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Ley 1273 , 2009).[66]

1.3. Decreto que dio origen a la introducción de este tipo penal.

En el Congreso de la República, surgió una primera iniciativa - Proyecto de Ley No. 042 de 2007 Cámara - destinada a modificar y adicionar algunos tipos penales regulados en el capítulo VII del Código Penal, relativos a la "Violación a la intimidad, reserva e interceptación de comunicaciones", cuya finalidad era en su momento endurecer las penas del hurto calificado, el daño en bien ajeno, la violación de reserva industrial o comercial y el espionaje, cuando quiera que se ejecuten *utilizando medios informáticos o se vulneren las seguridades informáticas de las víctimas*.

[66] GRISALES PÉREZ, Giovanni Stalin. Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes. Universidad EAFIT. 2013. Recuperado de https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf?sequence=1

La exposición de motivos fue expresa en señalar que, de los tres modelos legislativos posibles, a saber, i) ley especial -no integrada al Código Penal-, ii) capítulo especial -incorporado al Estatuto Sustantivo- y iii) modificación de los tipos penales existentes, se optó por el tercero a fin de garantizar la protección de otros bienes jurídicos distintos al de la información que también podían resultar lesionados con actividades relacionadas con la cibercriminalidad. Posteriormente, surgió una segunda iniciativa legislativa -Proyecto de Ley No. 123 de 2007 Cámara, la cual propuso la creación de un nuevo bien jurídico para la protección de la información. En esta segunda iniciativa legislativa se enfatizó en la necesidad de mayor protección al patrimonio y a los sistemas informáticos, propuestas legislativas en el Proyecto de Ley No. 042 Cámara, 123 Cámara y Senado, dando lugar a la proposición de crear un Título VII Bis al Código Penal, destinado, esencialmente, a la salvaguarda de la información y los datos, tomando como base, las conductas reguladas en el Convenio sobre la Ciberdelincuencia de Budapest y algunas que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, las cuales fueron ubicadas en el capítulo I y un segundo grupo de punibles definidos bajo el rótulo de “otras infracciones”, concretamente, el hurto por medios informáticos y semejantes, la transferencia no consentida de activos, la falsedad informática, el espionaje informático, la violación de reserva industrial o comercial valiéndose de medios informáticos (capítulo II).

El modelo adoptado en el proyecto original -042- debido a que contraía la dificultad de permitir la dispersión de esta problemática a lo largo del articulado lo que le quita fuerza y coherencia a la materia, (…) amén de que (sic) dificulta en extremo la precisión del bien jurídico que se debe proteger en estos casos, esto es, la Protección de la Información y de los Datos".

Una afirmación como la recién transcrita podría sugerir un único valor jurídico a ser protegido: la información y los datos, pero son las mismas ponencias las que

precisan frente a los punibles de hurto por medios informáticos y semejantes y transferencia no consentida de activos, que el primero procura «completar las descripciones típicas contenidas en los artículos 239 y siguientes del Código Penal, a las cuales se remite expresamente» y el segundo busca variar la estafa clásica por la figura de la estafa electrónica.

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

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

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

Particularmente, en cuanto se refiere al injusto de hurto por medios informáticos y semejantes, descrito en el artículo 269I, la ponencia señaló que se asimila al reato de hurto agravado y agregó que "si se observan los actuales artículos 239 y 240

de la (sic) C.P., dicha relación se establece sin ninguna modificación, pues el numeral cuarto del artículo 240 agrava el hurto con ganzúa, llave falsa superando seguridades electrónicas u otras semejantes. En consecuencia, no es correcto recalcar la relación ya existente."

Sometido este informe a la aprobación de la Comisión Primera del Senado, se llegó al acuerdo de no archivar el proyecto, siempre que se hicieran algunos ajustes a los tipos penales, teniendo en cuenta, la creciente necesidad de regular las defraudaciones patrimoniales a los ahorradores de los sistemas financieros.

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

En este punto, es bueno precisar que ante las preocupaciones por la confusión que podría suscitarse en la definición del bien jurídico protegido en aquellos casos en que además de la información y los datos se atenta contra el patrimonio económico y la solución propuesta de agregar a los tipos básicos la modalidad informática, en la norma que se pretende aprobar, quedan debidamente protegidos, tutelados, los derechos de los ciudadanos, usuarios del sistema financiero, personas naturales y/o jurídicas, que sean objeto o víctimas de transacciones financieras, a través de la tecnología, a través de la utilización indebida, por parte de organizaciones criminales en la Internet.

El anterior recuento, permite establecer, objetivamente, que el nuevo título -VII bis, se dirigió a regular, en esencia, el tema de los delitos informáticos y a proteger la información y los datos de carácter electrónico. No obstante, el legislador

colombiano utilizó esta oportunidad para enfatizar en la represión del apoderamiento ilícito, a través de mecanismos informáticos, de los dineros confiados al mercado financiero.

Hurto por medios informáticos y semejantes -Acentúa el reproche jurídico-social de los delitos informáticos: pues dicha conducta ya estaba sancionada en el art. 240 núm. 4, sin embargo, no son análogas.

La Corte argumenta que el propósito del órgano legislativo fue acentuar y no regular, por primera vez, el reproche jurídico-social respecto de dicha actividad ilegal porque ésta ya venía siendo sancionada conforme al punible de hurto, previsto en el artículo 239 del Código Penal, calificado por la circunstancia descrita en el numeral 4 del precepto 240 ibídem.

Antes de la expedición de la Ley 1273 de 2009, el estatuto sustantivo sancionaba, de esta manera, la modalidad de sustracción de una cosa mueble ajena -el dinero- para provecho propio o de un tercero a través de la ruptura de las barreras de protección informáticas o electrónicas dispuestas por el titular del bien jurídico del patrimonio económico. Pero, aprovechando la coyuntura legislativa, que solicitaba la regulación de los delitos informáticos, en el artículo 269 I, el legislador quiso redefinir o enriquecer con mayor precisión idiomática, si se quiere, el mecanismo de desplazamiento ilícito de la cosa mueble desde el titular del derecho hacia el sujeto activo, más no creó una nueva acción objeto de juicio de desvalor, porque, se insiste, ella ya estaba tipificada en la conducta simple de hurto y en la circunstancia calificante, al punto que no consagró un nuevo verbo rector sino que, al respecto, se remitió al canon 239 y en función de la pena, al precepto 240 ibídem.

No pretende sostener la idea categórica de que el tipo penal de hurto por medios informáticos es necesariamente análogo al de hurto calificado, pues, como resulta

obvio, éste no está dentro de la esfera de protección de la información y los datos o la intimidad, como si lo está el punible que nos ocupa; pero lo que sí se encuentra sujeto al criterio analógico, en cuanto resulta ser benigno al procesado, es la posibilidad de otorgar a un supuesto de hecho similar (protección del bien del patrimonio económico), la misma consecuencia jurídica que le imprime el artículo 269 ajusten a los delitos rubricados bajo los capítulos comprendidos en el Título VII.

Esta postura es compatible y fiel al interés del legislador por entregar una ventaja punitiva a aquel que repare en términos económicos el daño causado por delitos que agredan el patrimonio de las personas.

La Ley 1273 de 2009, fue creada para contrarrestar una nueva conducta delictiva que se venía dando en Colombia, pues, existía el vacío jurídico. Con lo que nace la necesidad de tipificar el delito, y así, darles herramientas a los jueces y fiscales cuando estén frente a este tipo de conducta. Además, teniendo en cuenta el auge que tiene la tecnología en la sociedad, es necesaria una regulación para las acciones inescrupulosas que se presentan día a día y que vulneran bienes jurídicos tutelados.

Por lo tanto, el día 5 de enero de 2009 el congreso de la república de Colombia promulgo la ley contra los delitos informáticos, la cual modifico el Código Penal Colombiano, Ley 599 de 2000, y creó un nuevo bien jurídico tutelado como la protección de la información y de los datos y se preserva integralmente los sistemas que utilicen las tecnologías de la información y comunicaciones. Cuya exposición de motivos resaltaba la importancia de regular y sancionar una serie de conductas que no estaban bien determinadas en la legislación colombiana y por lo que se hace necesario la tipificación penal.

Para lo cual, se considera en detalle los delitos informáticos y se expone la legitimidad del documento electrónico, el dato y la información en Colombia, lo que permite diferenciar un delito informático de un hecho punible para su consumación.

Entonces para hablar de delito informático se necesitan dos presupuestos: por un lado, que la conducta constitutiva del mismo esté tipificada por la Ley, y, por otro, que medie una sentencia condenatoria en la cual el funcionario judicial, haya declarado probada la existencia concreta de una conducta típica, antijurídica y culpable del delito informático. Ante esto, es importante analizar el bien jurídico tutelado.

Entiéndase por bien jurídico tutelado como los bienes que son protegidos por el derecho. El interés social no se convierte en bien jurídico hasta que es protegido jurídicamente. En otras palabras, el bien jurídico es la elevación a la categoría del bien tutelado o protegido por el derecho, mediante una sanción para cualquier conducta que lesione o amenace con lesionar este bien protegido. Esta característica proteccionista, se nota mayormente en el ámbito del Derecho Penal.

Al ser Colombia un estado social democrático de derecho, se propende amparar la vida en sociedad, y a su vez regular las acciones cuando estas perturben el sistema social. Sin embargo, los bienes serán jurídico penales si tienen una importancia fundamental. Al determinar cuáles son los bienes jurídicos que merecen tutela penal, siempre se tendrá en cuenta el principio de tener al Derecho penal como última opción para la protección de un bien jurídico, ya que, éste afecta otros bienes jurídicos, con el fin de proteger otros de mayor valor social.

Exponiéndose el menester de tipificar el delito informático, al vulnerar bienes jurídicos con conductas nocivas y peligrosas.[67]

1.4 Descripción típica en el código (bienes jurídicos que se protegen)

Con la modificación de la Ley 1273 de 2009 al Código Penal en el artículo 269 I, se propendió comprender las nuevas conductas que protegen el nuevo bien jurídico tutelado, para lo cual se analiza cada uno de ellos.

El artículo 269 I del Código Penal consagra el hurto por medios informáticos y semejantes, así:

> El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este código.[68]

El anterior artículo es subordinado a la conducta típica de hurto, así mismo se aplica el principio de lesividad al verse en peligro un bien jurídico tutelado, por lo que es necesario que a la realización de esa figura se consume un daño al bien tutelado, esto es, afectación patrimonial. Es una conducta instantánea debido a que la acción típica se agota al momento en que la víctima es despojada de su dinero a través de medios informáticos. Además, presenta una pluralidad de acciones con las que se puede configurar el delito tales como, manipulación del sistema informático o de las redes y suplantación de usuario ante sistemas de

[67]ARZUAGA HERRADA, Toyber S. y Guevara Medina, Elkin. La Ley 1273 DE 2009 y los delitos informáticos en Santiago de Cali. 2013. Recuperado de http://bibliotecadigital.usb.edu.co:8080/bitstream/10819/1891/1/la%20Ley1273_ Delitos%20 InformaticosSantiago%20de%20Cali_Arzuaga_2013..pdf

[68] Ley 1273 de 2009.

autenticación y autorización. También es de medio determinado por cuanto se exige para su realización, la afectación por medio de un mecanismo informático, electrónico o telemático, de ahí entonces su especificidad.

Los elementos de tipo penal que enmarca la norma son:

- **Sujeto - Activo**: Esta norma no exige una calidad específica para quien cometa la conducta, ya que con la expresión “el que” indica que cualquier persona natural puede cometer el ilícito. Y el sujeto es activo inmediato ya que es quien realiza la acción ilegal. Seria mediato, quien ejerce el dominio de la voluntad de un tercero para que actúe como autor; y es coautor quien ejerce dominio funcional del hecho, pero no tiene el dominio sobre la voluntad de quienes lo causan, por lo que su aporte es concurrente para la realización de delito.

Por ejemplo: Es autor directo quien se dirige al cajero con la tarjeta clonada y retira el dinero. Quien participa en la clonación de la tarjeta, seria cómplice si solo es quien tiene el dispositivo para la clonación de las tarjetas. Caso contrario sería, si quien clona la tarjeta participa activamente en compañía de quien va al banco a realizar los retiros, por lo que, en este caso, sería coautor.

- **Sujetos - Pasivos:** Son aquellas personas naturales o jurídicas que padecen el detrimento económico y perjuicio en sus intereses patrimoniales. Es quien tiene la titularidad del interés o bien jurídico que se encuentra tutelado por un determinado tipo penal, bien que es amenazado con la realización de la acción típica.

Por ejemplo: La persona a la que le fue sustraída su tarjeta o robada su clave y quien es titular de la cuenta bancaria, fue poco diligente con el cuidado de los mismos y, por lo tanto, sería el sujeto pasivo. No lo es el banco ya que es software

del mismo, ante la utilización de estos elementos, permite que cualquier persona que los posea ingrese al sistema y realice los movimientos bancarios hasta el tope asignado. Sin embargo, si un sistema de clonación es instalado en un cajero que está bajo la custodia del banco, se reconoce como sujeto pasivo, la persona jurídica. Por ello, en ciertas oportunidades las entidades reconocen el dinero a los afectados, una vez se ha desarrollado su investigación interna.

- **La acción o conducta**: Es aquella conducta que es tipificada como prohibida en el ordenamiento jurídico. Para que una conducta sea catalogada como delito, se debe acudir a las prohibiciones que señala el artículo 239 de Código Penal, cuya acción es "apoderarse". Esto es, que el apoderamiento sea ilícito. La norma es subordinada al tipo básico de hurto y fue creada para evitar el apoderamiento no solo de dinero, sino de información privilegiada de personas naturales o jurídicas que tiene un gran valor en el mercado. En este caso se exige la alteración del bien jurídico tutelado a través de medios informáticos que vulneran la seguridad informática.

La seguridad informática es definida por el profesor Ricardo Posada Maya, 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) …"[69]

Es esta seguridad informática la que se ve afectada, pues los delincuentes realizan maniobras fraudulentas, como manipulación o suplantación, para ingresar el sistema informático de las entidades o personas y hurtar dinero o información.

[69] 2006, p. 26

- **El objeto material**: Se refiere a un bien corporal, como el dinero; o incorporal como la información privilegiada.

Ambos bienes muebles, el primero es tangible; y el segundo, tiene una utilidad en el mercado.

La jurisprudencia ha desarrollado cada uno de los elementos del tipo penal a través de la sentencia SP1245-2015, Magistrado Ponente Dr. Eyder Patiño Cabrera, en esta sentencia se desglosan los elementos del tipo, a saber: "**HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES** - Elementos: sujeto activo indeterminado / **HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES** - Tipo penal de medio concreto o determinado: establece modalidades o mecanismos específicos de apoderamiento.

El precepto examinado, solamente se ocupa de establecer el sujeto activo indeterminado -no cualificado o común y un subjetivo- del punible y de consagrar unos específicos ingredientes normativos, que lo identifican como un tipo de medio concreto o, si se quiere, determinado, por cuanto estructura una modalidad o mecanismo específico de desapoderamiento de la cosa mueble ajena, a saber, superar las seguridades informáticas mediante i) la manipulación del sistema informático, la red de sistema electrónico, telemático u otro semejante o ii) la suplantación de una persona ante los sistemas de autenticación y de autorización establecidos.

Dolo, dicha remisión al artículo 269I abarca el ingrediente especial subjetivo necesario para su comisión, como lo es, el animus lucrandi o la finalidad o propósito doloso de obtener un provecho o utilidad -propio o en favor de un tercero- de carácter patrimonial.

Tipo penal de resultado, es de lesión porque exige el efectivo menoscabo del interés jurídicamente tutelado, que para el caso lo son el patrimonio económico y

la seguridad en el tráfico a través de los sistemas informáticos; pero también es de resultado, como quiera que para la consumación del desvalor total del injusto requiere el desapoderamiento del dinero con el subsecuente perjuicio, estimable en términos económicos, para quien tenga la relación posesoria con la cosa.

Ejecución instantánea, Es de conducta instantánea toda vez que el agotamiento del comportamiento típico se perfecciona cuando la víctima es desposeída de su dinero vulnerando los sistemas de protección informáticos dispuestos para su resguardo.

Sujeto pasivo, el usuario financiero o la persona jurídica que custodia el dinero, dependerá de la barrera informática, telemática o electrónica comprometida, lo será el titular del derecho patrimonial o poseedor del dinero sustraído, que, según el caso, podrá serlo el usuario financiero y/o la persona jurídica que lo custodia.

Objeto material del delito, cosa mueble ajena. En cuanto al objeto, la distinción doctrinal entre objeto jurídico y/o material de protección, obliga a determinar, en el caso concreto, que, si bien el delito se ubica dentro del título que protege la información y los datos, el bien material del delito no puede ser otro que la cosa mueble ajena que sufre un apoderamiento por parte de un extraño.

Bienes jurídicos tutelados: patrimonio económico de forma inmediata y la información y datos de forma mediata. Como lo concibió la exposición de motivos del Proyecto de Ley 042 Cámara-, de naturaleza meramente intermedia, pues el interés superior protegido de manera directa es el patrimonio económico, entendido como ese conjunto de derechos y obligaciones, susceptible de ser valorado en términos económicos, más concretamente, en dinero. El mentado ilícito tiene la virtualidad de lesionar tanto la seguridad y la confianza de las personas naturales y jurídicas en los sistemas informáticos, telemáticos, electrónicos o semejantes, con sus componentes de software y hardware,

implementados por las entidades encargadas de custodiar el capital de sus usuarios, como los intereses individuales de contenido económico del titular de la cosa ajena, cuestión que ubica al tipo penal examinado en el contexto de los delitos típicamente pluriofensivos por afectar más de un interés jurídico, el descrito expresamente en la legislación penal codificada - en este caso, el título VII bis- y el que surge de manera remota, pero directa, de la realización de la acción injusta.

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

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

2. Desarrollo doctrinario del bien jurídico tutelado por el delito de hurto por medios informáticos en Colombia

2.1. El delito de hurto por medios informáticos como un tipo penal pluriofensivo:

Es necesario establecer el bien jurídico que se pretende proteger, entiéndase por bien jurídico como aquellos valores que por su importancia en la sociedad son objeto de protección mediante el Derecho Penal.

Se reconocen 3 teorías sobre el bien jurídico protegido mediante el delito de hurto por medios informáticos:

- ***La primera teoría, en la que el bien jurídico protegido sería la confidencialidad, integridad y disponibilidad de la información.***

Esta teoría resulta de la falencia legislativa al ubicar el tipo penal de hurto por medios informáticos dentro el título de los delitos contra la información y los datos, lo que se deduce de una interpretación exegética del Código Penal. Esta interpretación la manejó el Tribunal Superior del Distrito Judicial de Neiva, cuando dicha corporación afirmó que el hurto por medios informáticos no era un delito en contra del patrimonio económico, y por ende no podía ser objeto de la rebaja por reparación integral consagrada en el artículo 269 del Código Penal, y, fue precisamente por esta razón que la Corte Suprema de Justicia en sentencia 42724 del 11 de febrero de 2015, revocó la decisión del Tribunal Superior del Distrito Judicial de Neiva, afirmando que la rebaja era completamente procedente por tratarse de un delito en contra del patrimonio económico. Lo que muestra que la ubicación del tipo penal es sólo un dato indiciario del bien jurídico protegido por el tipo penal específico. Para lo cual, se debe entender que el bien jurídico protegido de manera directa es el patrimonio económico, o sea, el conjunto de derechos y

obligaciones, susceptible de ser valorado en términos económicos, más concretamente, en dinero.

- ***La segunda teoría, en la que el bien jurídico protegido sería el patrimonio económico.***

El bien jurídico protegido es el patrimonio económico, lo que resulta claro por varias razones. Primero, porque existe remisión de la conducta a realizar por parte del tipo penal de hurto por medios informáticos al tipo penal básico de hurto; lo que concluye que se trata del clásico delito de hurto, sólo que cometido a través de un medio informático. Y, por ende, al tratarse de una modalidad de hurto, el bien jurídico es el mismo, el patrimonio económico.

De lo cual, resulta concluir, que el tipo penal de hurto por medios informáticos no solo está circunscrito al ámbito de punibles contra la información y los datos, sino, esencialmente a la esfera de los lesivos del patrimonio económico, por causar un detrimento en el mismo.

Y, Segundo, porque existe remisión a la sanción a imponer. Esto debido a que el tipo penal remite a la pena del hurto calificado, artículo 240 del Código Penal (Ley 599 Código Penal, 2000).

- ***La tercera teoría, en la que el bien jurídico protegido es la protección penal dual de las dos teorías antes mencionadas.***

La doctrina ha señalado que existen posturas mixtas, que atribuyen como objeto de protección, tanto un carácter individual, como lo es el patrimonio económico, y el segundo, colectivo referente a la protección de la información y los datos. Ante lo cual muchos defensores están de acuerdo respecto de la dualidad de protección

de estos dos bienes jurídicos, pero, en desacuerdo con la determinación de su consideración como delito pluriofensivo, o como bien jurídico intermedio.

Esta interpretación dual del bien jurídico significaría que la comisión de un delito de hurto por medios informáticos produce, no solo la pérdida patrimonial al individuo, sino también, lesiona la seguridad y confianza de los ciudadanos a los sistemas informáticos.

No obstante, al manejarse la tesis de los tipos penales intermedios en los que se causa la inmediata lesión de un bien jurídico de naturaleza individual, el patrimonio, y ocasiona, además, la mediata y abstracta puesta en peligro de otro bien jurídico de naturaleza colectiva, surgen críticas sobre la misma. Suárez Sánchez (Suárez Sánchez, 2010, p. 239) formula las siguientes: "…Se denota una esforzada argumentación al indicar que los sistemas de información son bienes jurídicos de peligro abstracto; además, es una postura en la que prevalece el patrimonio económico; en vez de determinar de forma precisa el bien jurídico tutelado, justifica la ubicación del tipo penal en los delitos informáticos; y por último, no explica porque la información y los datos son considerados como un bien jurídico colectivo".[70]

2.2. El bien jurídico del patrimonio económico en el delito de hurto por medios informáticos

Para iniciar con el estudio del bien jurídico del delito de hurto por medios informáticos se debe precisar si se trata de naturaleza individual o colectiva, o sea, que no solo protege el patrimonio individual de un determinado sujeto, sino que

[70] MAJER, Abushihab. Hurto por medios informáticos ¿un delito informático? 2016. Recuperado de https://repository.usta.edu.co/bitstream/handle/11634/9259/AbushhMajer2017.pdf?sequence=1&isAllowed=y

tutela otro bien jurídico de característica colectivo, lo que refleja el interés social en la seguridad de la información.

Según Tiedemann (Lecciones de derecho 1993, p. 35 y ss) al estudiar el delito de estafa informática, éste es un delito de naturaleza compleja, pues, protegía tanto el patrimonio individual como el colectivo de la seguridad en el tráfico realizado mediante los sistemas informáticos.

Conforme a lo anterior, no bastar la sola lesión o la puesta en peligro del bien jurídico individual, o sea el patrimonio, sino que se exige también que el resultado cause peligro para un bien jurídico de carácter colectivo, la seguridad de los medios informáticos. Tratándose, entonces, de los bienes jurídicos intermedios.

Para poder calificar el delito de hurto como protector de un bien jurídico intermedio hay que aceptar que la conducta típica se dirige a lesionar de manera inmediata un bien jurídico individual, lo que provoca la puesta en peligro del bien jurídico colectivo.

Conforme a esta interpretación ha de afirmarse que el delito de hurto por medios informáticos y semejantes propende proteger los sistemas informáticos con trascendencia patrimonial. Al ser el hurto por medios informáticos y semejantes un delito de peligro de lesión, bastar probar el daño del bien jurídico de patrimonio individual, para concretar el momento en que ha de apreciarse la pena.[71]

[71] SUÁREZ SÁNCHEZ, Alberto. El hurto por medios informáticos y semejantes a través de la utilización de tarjeta magnética falsa o ajena en cajero automático. Estudios de Derecho Penal I.p. 237-240. Recuperado de http://avalon.utadeo.edu.co/servicios/ebooks/derecho_penal _I/files/assets/basic-html/page240.html

2.3. El bien jurídico de la información en el delito de hurto por medios informáticos

En la tesis en donde el bien jurídico protegido es el de la información y los datos, no existe un sector doctrinario que defienda esta postura, por el contrario, se considera una falencia legislativa, en razón de la ubicación dada por el legislador al tipo penal de hurto por medios informáticos dentro del título de los delitos contra la información y los datos, que aunque se encuentre ubicado allí, el verdadero bien jurídico que se propende proteger es el patrimonio económico.[72]

Así las cosas, 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. Estas normas hacen referencia a los elementos normativos encontrados en el artículo 239 del Código Penal, el cual remite al ánimo de lucro que se obtiene a través de la transferencia no consentida de activos, tipo penal que se asemeja a la estafa.

Ahora bien, nace la necesidad de definir el delito informático, para lo cual se referencia al jurista español Camacho Losa,[73] el cual considera que es "…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".

El Consejo de Europa por su parte incluye una lista de actos que deberían o podrían ser objeto de sanción penal, los cuales son:

---

[72] MAJER, Abushihab. Hurto por medios informáticos ¿un delito informático? 2016. Recuperado de https://repository.usta.edu.co/bitstream/handle/11634/9259/AbushhMajer2017.pdf?sequence=1&isAllowed=y

[73] ARIZAMENDI & DE LA MATA BARRANCO. Derecho Penal Informático. 2010, pág. 25 y ss.

- Fraude en el campo informático mediante la inserción, alteración, borrado o supresión de datos, con ánimo de lucro y daño a terceros.
- Falsificación en materia informática.
- Daños causados a datos o programas informáticos.
- Sabotaje informático.
- Acceso no autorizado.
- Interceptación no autorizada.
- Reproducción no autorizada de un programa informático protegido.
- Reproducción no autorizada de una topografía.
- Alteración de datos o de programas informáticos.
- El espionaje informático.
- La utilización no autorizada de un ordenador.
- La utilización no autorizada de un programa informático protegido.
- Tráfico de claves (passwords) obtenidas ilegalmente.
- Obtención de un acceso no autorizado a sistemas informáticos.
- La distribución de virus o de programas similares.

Y por su parte, en la Convención de Cibercriminalidad, realizada en Budapest en 2001 (Europa, 2001) definieron una serie de conductas que deben ser catalogadas como delitos informáticos para los estados parte, entre ellos:

- Acceso ilícito.
- Interceptación ilícita.
- Ataque a la integridad de datos.
- Ataques a la integridad del sistema
- Falsificación informática
- Fraude informático
- Entre otros.

Ahora bien, si se analizan los conceptos dados no solo por la doctrina, sino también por los instrumentos internacionales, se observa que las conductas punibles consagradas en los artículos 269I y 269J del Código Penal, el objeto de ataque o bien jurídico vulnerado no es otro que la información que se encuentra en la red y el medio para la comisión del delito son los programas informáticos, todo esto conforme a la nueva era de la tecnología digital.

En resumen, quien realiza los tipos penales de la Ley 1273 de 2009, no está atentando contra un medio informático, sino que utiliza este medio para llevar a cabo la ejecución del delito, pues una vez tenga la información privilegiada procederá a realizar la afectación a su patrimonio a través de la transferencia de dinero o hurto por medio informáticos. Reafirmando, que el bien jurídico que se protege es el patrimonio económico de los sujetos, además de la información personal y privada.[74]

- **Dispositivo Amplificador del Tipo**

El artículo 27 del Código Penal señala que quien iniciare la ejecución de una conducta punible y ésta no se produjere por circunstancias ajenas a su voluntad, incurrirá en pena (Ley 599 Código Penal, 2000). Por lo que es necesario el inicio o ejecución de la conducta punible, es decir que el bien jurídico tutelado se vea en peligro. Lo cual se produce en el instante en que se ingresa al sistema informático. Teniendo así a una persona con una idea criminal, realizando actos preparativos para cometer hurto a través de medios informáticos, sin embargo, no ha iniciado la ejecución de la acción ilícita con lo que no se podría sancionar conforme al artículo 269I a título de tentativa, pero si está en curso del tipo penal descrito en el artículo 269F, esto es violación de datos personales, ya que se puede compilar,

[74] GRISALES PÉREZ, Giovanni Stalin. Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (Art. 269i) y Transferencia no consentida de activos (Art. 269j) Ley 1273 de 2009. Universidad EAFIT. 2013. Recuperado de https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf?sequence=1

interceptar, o emplear códigos o datos personales contenidos en una base de datos (Ley 1273 , 2009).[75]

3. Dispositivos amplificadores del tipo penal

El legislador sanciona no solo las conductas humanas consumadas, sino todos aquellos elementos puestos a disposición de la realización de la conducta punible, para estos se generaron dos hipótesis que merecen un reproche judicial, primero aquella que por diversas circunstancias no logran su objetivo delictual y otra la realización del mismo por varias personas, la tipicidad como elemento del delito lleva consigo la singularidad sin embargo a través del desarrollo típico se generaron por parte del legislador los dispositivos amplificadores del tipo penal. Se generan o desarrollan dos elementos a saber, *la tentativa y coparticipación,* los cuales se originaron con la finalidad de resolver el problema jurídico de avance sin establecer el fin de consecución que es la realización de un hecho reprochado jurídicamente y dos la participación de dos o más personas en la realización de este hecho doloso, estos elementos figuran en el Código Penal (art. 27 y 28), a estos se les denominó por parte del profesor Reyes Echandía “dispositivos amplificadores del tipo penal” y el profesor Jiménez Huerta “dispositivos legales amplificadores del tipo”.

De esta manera se resuelven por parte de legislador los problemas generados por la no consumación de ciertas conductas, tentativa y la realización de un hecho por más de dos personas en su realización, debido a que ciertos tipos penales en su mayoría se desarrollan de manera singular, pero como sostiene Reyes Echandía “este procedimiento, sin embargo, hubiera resultado demasiado prolijo y engorroso por lo casuístico; mucho más lógico y adecuado era consagrar como tipos autónomos en la parte general estos dispositivos, de tal manera que pudiesen predicarse de todos los esquemas típicos de la parte especial”.

[75] Ibídem, 2013.

3.1. La Tentativa

En la realización del hecho reprochado jurídicamente, el sujeto activo de la conducta penal a realizar puede dar inicio a los actos preparatorios en su realización sin embargo frente al elemento de consumación no se obtiene el resultado del mismo debido a circunstancias ajenas a su voluntad. Este es el caso de la tentativa, del delito frustrado o del conato de delito, como se conoce en la doctrina.

El artículo 27 del Código Penal colombiano consagra esta figura amplificadora de los tipos delictivos de la parte especial del estatuto punitivo cuando dice:

> […] el que iniciare la ejecución de una conducta punible mediante actos idóneos e inequívocamente dirigidos a su consumación, y esta no se produjere por circunstancias ajenas a su voluntad, incurrirá en pena no menor de la mitad del mínimo ni mayor de las tres cuartas partes del máximo de la señalada para la conducta punible consumada. Cuando la conducta punible no se consuma por circunstancias ajenas a la voluntad del autor o partícipe, incurrirá en pena no menor de la tercera parte del mínimo ni mayor de las dos terceras partes del máximo de la señalada para su consumación, si voluntariamente ha realizado todos los esfuerzos necesarios para impedirla.[76]

La tentativa es pues un grado de lo cuantitativo del hecho típico es, como decía Carrara, “un pedazo o fragmento de hecho descriptivo, que en la figura típica aparece completo o consumado, indicado por el verbo rector”. Se trata de factores en los cuales el sujeto activo de la realización de la conducta punible no realiza el resultado, no alcanza a cumplir la realización del hecho, sin estas figuras de la

[76] REPUBLICA DE COLOMBIA. Código Penal colombiano. Artículo 27. Tentativa.

tentativa y la coparticipación, estarían por fuera del ámbito legal sin reproche judicial. Por esta razón se hace necesario a través de la historia y las diferentes escuelas del delito estudiar los comportamientos frente a la acción y ejecución de los delitos.

Se hace indispensable reconocer el camino del delito, la sucesión de acciones predelictivas o el iter criminis como se conoce en la doctrina. El iter criminis tiene cinco fases: ideación, preparación, ejecución, consumación y agotamiento. La idealización del ser humano o el sujeto activo del hecho reprochado legalmente es el inicio o la fuente inicial para la realización de un comportamiento criminal que obedece al fuero interno, este primer elemento dentro del estudio del comportamiento criminal se le ha denominado como designio criminal porque permanece en el fuero interno del hombre. Una vez este fuero interno constituye la idea criminal debe realizar diversos actos preparatorios para la realización del crimen estos actos iniciales o preparatorios son actos inidóneos o ineficaces por sí mismos, debido a que los mismos permanecen en el fuero interno del actor y aun no llegan a ser proyectados en el mundo exterior, para Carrara, son actos inidóneos o ineficaces, por sí solos, para obtener el resultado punible. Una vez se inicia la exteriorización de los actos preparatorios se inicia la idea de ejecución del hecho reprochado jurídicamente, estos actos que son exteriorizados en el mundo real, son actos eficaces o idóneos por sí mismos, los cuales pueden poner en riesgo el bien jurídico tutelado. Una vez recorrido los actos internos a actos preparatorios afectación a un bien jurídico tutelado accedemos al elemento de consumación los cuales el sujeto activo del actuar reprochado desencadena diversos elementos con la finalidad de concretar con la obtención de un resultado jurídicamente reprochable.

Inicio de la tentativa, Carrara decía que la tentativa comienza cuando se realizan actos unívocamente dirigidos a producir un cierto resultado, ya que estos actos son realizados de manera inequívoca en a producción de un resultado

jurídicamente reprochado no cabe duda alguna que se dirige a causar determinado resultado punible.

3.2. Clasificación de la tentativa

La tentativa puede ser simple, frustrada, desistida e inidónea. Es necesario considerar de las diversas especies de tentativa, no solo por la determinación y clasificación legal sino por los diversos elementos que la componen en el mundo físico. Son muchas las clasificaciones que la doctrina presenta sobre este tema, según el fundamento real del resultado imperfecto y así, se realiza un alcance de clasificación de la tentativa. Tentativa por falta involuntaria de consumación, tentativa por idoneidad de los medios utilizados, tentativa por arrepentimiento eficaz del agente (desistimiento) y tentativa por inexistencia de sujeto pasivo.

Clasificación y modalidades de la tentativa.

3.2.1. Tentativa Simple

La tentativa simple se presenta cuando la ejecución de la acción típica se interrumpe por la irrupción de un factor extraño al querer del agente que le impide la consumación de la conducta.

3.2.2. Tentativa Frustrada

Se presenta la tentativa frustrada, cuando el agente a pesar de haber realizado todo lo que estaba a su alcance, no logra la producción del resultado por circunstancias ajenas a su voluntad, mientras que en la tentativa simple el agente apenas se encuentra en el umbral de la ejecución, en la frustrada realiza todo lo que está a su alcance para la consecución del resultado, ejemplo de esta última tentativa se da con el ladrón que huye con la cosa y el policía lo detiene, quien

hace seis disparos a su víctima, pero los médicos le salvan la vida, la mujer que toma la píldora abortiva, pero se le practica un lavado intestinal.

3.2.3 Tentativa Desistida

La tentativa desistida existe cuando el agente, a pesar de haber comenzado la ejecución del hecho o haberlo completado mediante actos inidóneos encaminados a su consumación, de manera voluntaria decide poner fin al actuar criminal, el desistimiento no es arrepentimiento, este último se da cuando el hecho ya está consumado y sirve como atenuante o eximente punitiva. En la tentativa simple y frustrada lo decisivo para la no consumación son los factores extraños a la voluntad del agente, en la tentativa desistida lo determinante es la propia voluntad del agente. Para que pueda hablarse de tentativa desistida deben reunirse unos requisitos que se deducen del inciso segundo del artículo 27 del código penal, tales requisitos son: en primer lugar, es indispensable el abandono de la voluntad delictiva por parte del agente, esto es, que medie de su parte la decisión de no persistir más en la realización de la idea criminosa; en segundo lugar, el abandono debe ser definitivo, no provisional, porque estaríamos en presencia de una postergación de la idea criminal; en tercer lugar, el abandono debe ser voluntario, esto es de suma importancia porque el autor puede abandonar el hecho motivado en reacciones primitivas, en supersticiones, en sentimientos de carácter irracional ajenos ciertamente a su voluntad y, en cuarto lugar, el desistimiento debe impedir la consumación.

3.2.4 Tentativa Inidónea

Cuando el autor comienza a ejecutar el hecho, pero este no se consuma en virtud de que los actos no son idóneos para su logro, sea que ello acontezca por razones fácticas o jurídicas. También se le denomina tentativa imposible o delito imposible, ya que el hecho punible no se realiza por idoneidad de la conducta, de los medios

utilizados, del sujeto pasivo o del objeto jurídico. En el derecho nacional no es punible la tentativa inidónea o imposible, porque el legislador, entendió desde el código penal de 1980 que tal figura se corresponde con una concepción subjetivista del derecho penal, para lo cual lo trascendental es la lesión de los valores ético-sociales, que ve en la supuesta peligrosidad del agente su criterio de punición.

4. Desarrollo jurisprudencial del bien jurídico tutelado por el delito de hurto por medios informáticos en Colombia

4.1. El derecho a la información en la Jurisprudencia Constitucional Colombiana

En el proyecto de ley, de la Ley 1273 de 2009, define al operador informático, como aquella persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por lo que éste se sujeta al cumplimiento de los deberes y responsabilidades para garantizar la protección de los derechos del titular de la información.

Un ejemplo de un operador informático es el B.C.R.A, que se ha estructurado con base en los datos que proveen las entidades financieras, las entidades no financieras emisoras de tarjetas de crédito y el propio B.C.R.A. Tiene por objeto brindar información sobre los deudores del sistema financiero a los bancos y demás instituciones que intermedian en el crédito, para facilitar la toma de decisiones en materia crediticia.

En la Ley 1266 de 2008 desde un principio se enfatizó en el concepto de fuente de información de carácter financiero ya sea que actúe como tal o como fuente operador. Siendo la fuente de información como la persona, entidad u organización que recibe o conoce datos personales de los titulares de la

información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si esta fuente, entrega la información directamente y no a través de un operados, cumplirá el rol de fuente y operador por lo que asumirá los deberes y responsabilidades de ambos.

Es así como en la Ley 1266 de 2008

> Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones", en su artículo 3 literal b, estableció una serie de derechos que tienen los titulares de la información frente a los operadores de los bancos de datos (Ley 1266, 2008). Por lo que la administración de datos semiprivados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones establecidas en la ley. Estos mismos derechos quedaron plasmados en el artículo 6º, numeral 2, de la Ley de Habeas Data colombiana.[77]

4.2. Jurisprudencia de la Corte Suprema de Justicia

Si bien es cierto la tipificación de hurto por medio informáticos se consagro en el artículo 269I, este delito se encuentra directamente subordinado al tipo penal básico de hurto, en cuanto a la descripción típica; y al tipo penal de hurto calificado, en cuanto a la pena. Por lo cual, es y siempre será subordinado, tan así

[77] CONGRESO DE LA REÚBLICA. Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Revista UPTC. Realidad. Recuperado de https://revistas.uptc.edu.co/index.php/derecho_realidad/article/download/.../3960/

que, si se realiza algún cambio en el tipo penal básico de hurto, implicaría un cambio en el hurto por medios informáticos.[78]

Lo anterior, se evidencia en la jurisprudencia analizada a continuación:

- **Sentencia SP1245-2015 de febrero 11 de 2015. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. SP1245-2015. Radicación 42.724. Magistrado Ponente: Dr. Eyder Patiño Cabrera.**

La tipificación del delito de hurto por medios informáticos nació frente a la creciente criminalidad en materia informática, con lo cual, Colombia se vio en la necesidad de sancionar las infracciones referentes al abuso de los sistemas informáticos y datos personales.

Con este ideal surgió el Proyecto de Ley 42 de 2007 destinada a modificar y adicionar algunos tipos penales regulados en el capítulo VII del Código Penal relativos a la "Violación a la intimidad, reserva e interceptación de comunicaciones" y a endurecer las penas cuando se vulneren las seguridades informáticas de las víctimas. Se parte de la base de la elevación a bien jurídico tutelado el derecho a la información, buscándose salvaguardar la seguridad informática ante los ataques en contra de otros bienes como la intimidad, la propiedad, la libre competencia y hasta la misma seguridad del Estado. Siendo esta la razón, por la que algunos doctrinantes catalogan el derecho a la información o seguridad informática como bien jurídico intermedio. Es así, como la iniciativa, lo que busca es agravar conducta tipificadas y solo en algunos casos tipificar comportamiento no contemplados en la ley penal, pues, si bien varias conductas utilizan medios informáticos para cometer el delito, estos no se pueden

[78]MAJER, Abushihab. Hurto por medios informáticos ¿un delito informático? 2006. Recuperado dehttps://repository.usta.edu.co/bitstream/handle/11634/9259/AbushhMajer2017.pdf?sequence=1&isAllowed=y

denominar delitos informáticos sino delitos tradicionales con nuevas formas de comisión y que ameritan una tipificación en la ley penal.

Posteriormente surgió el Proyecto de Ley 123 de 2007 Cámara, la cual propuso la creación de un nuevo bien jurídico para la protección de la información.

Generando la acumulación de las dos propuestas legislativas que dan lugar a la proposición de crear un título VII bis al Código Penal, destinado a salvaguardar la información. Dividiendo las conductas en dos grupos, por un lado, aquellos que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos informáticos, y, por otro lado, concretamente, el hurto por medios informáticos y semejantes, la transferencia no consentida de activos, la falsedad informática, el espionaje informático, la violación de reserva industrial o comercial valiéndose de medios informáticos.

Sin embargo, el proyecto fue archivado, al considerarlo innecesario frente a la regulación penal existente. Por lo que no deben crearse tipos con nuevas denominaciones, ya que preexisten tipos que genéricamente recogen el comportamiento a reprimir.

No obstante, y ante la exposición del ponente la Comisión Primera del Senado, llegó al acuerdo de no archivar el proyecto siempre y cuando se le hicieran algunos ajustes, teniendo en cuenta la necesidad de regular las defraudaciones patrimoniales.

Finalmente, el proyecto, fue aprobado conservando como únicos delitos del capítulo II, los de hurto por medios informáticos y semejantes y transferencia no consentida de activos. Aclarando que, aunque el bien jurídico protegido es el de la protección a la información, la nueva ley procuraba amparar al sistema financiero y a sus usuarios de las defraudaciones patrimoniales.

La Corte, entonces, argumenta que el propósito del legislativo fue la de acentuar el reproche frente a esa actividad ilegal, pues ya venía siendo sancionada conforme al punible de hurto consagrado en el artículo 239 del Código Penal.

Es así, como con la expedición de la Ley 1273 de 2009, lo que el legislador quiso fue enriquecer con mayor precisión idiomática el mecanismo de desplazamiento ilícito de la cosa mueble desde el titular del derecho hacia el sujeto activo, mas no creo una nueva acción.[79]

[79] Legis. (2019). Sentencia Corte Suprema de Justicia, delitos informáticos. Recuperado de https://legal.legis.com.co/document/Index?obra=jurcol&documnt=jurcol_107dd927623e0146e0530a0101510146

CAPITULO III

1. LA TENTATIVA EN EL DELITO DE HURTO MEDIANTE MEDIOS INFORMÁTICOS

En la legislación Penal Colombiana la tentativa se encuentra determinada en el artículo 27 del código penal, Ley 599 de 2000, determina “el que iniciare la ejecución de una conducta punible mediante actos idóneos e inequívocamente dirigidos a su consumación, y esta no se produjere por circunstancias ajenas a su voluntad, incurrirá en pena no menor de la mitad del mínimo ni mayor de las tres cuartas partes del máximo de la señalada para la conducta punible consumada” “cuando la conducta punible no se consuma por circunstancias ajenas a la voluntad del autor o participe, incurrirá en pena no menor de la tercera parte del mínimo ni mayor de las dos terceras partes del máximo de la señalada para su consumación, si voluntariamente a realizado todos los esfuerzos necesarios para impedirla”. Como podemos observar realizando un análisis normativo del artículo 27 de la Ley 599 de 2000, encontramos la tentativa dentro del título III capitulo único “*De La Conducta Punible”*, en este articulo la legislación colombiana recopila dentro de la clasificación anteriormente realizada en el capítulo dos, la clasificación de la tentativa, la cual se clasifica según el legislador en *Tentativa Acabada Y Tentativa Inacabada.*

Para el caso que nos ocupa hurto mediante medios informáticos, el hurto en su clasificación más básica, requiere de un resultado, el cual es el retiro de la órbita de dominio patrimonial del sujeto pasivo del injusto, exigiendo así un resultado, en estos casos de manera general, la pérdida o el menos cabo del patrimonio económico, de forma general cada caso en concreto presentaría diversos interrogantes en el mundo fenomenológico, por ejemplo la clonación de una tarjeta débito, exige como mínimo la utilización de un medio tecnológico para extraer el código de seguridad, trasladar el mismo a una tarjeta matriz, insertar un código

digital y extraer dinero de una cuenta bancaria, sin embargo el sujeto activo del injusto puede realizar todos y cada uno de los pasos requeridos para lograr su objetivo sin embargo si al momento de realizar o extraer el dinero el cajero automático no posee saldo o por desperfectos de la maquinaria no puede realizar la transacción se recaería obligatoriamente en la tentativa, la cual sería de estudio en su clasificación según nuestra legislación. Recayendo en la tentativa dependiendo de la sub-clasificación realizada por el artículo 27 del Código Penal, se castigaría el injusto, pero no en la totalidad de la regulación penal que daría para la conducta penal consumada bien como lo determina el código penal, sin recaer o subsumir el comportamiento injusto en otra conducta penalmente reprochable. El Dr. Alberto Suarez Sánchez en su libro *Manual De Delito Informático En Colombia* determina "se da la tentativa de este delito cuando el sujeto activo ejecuta acción idónea para apoderarse de la cosa mueble ajena y no logra adueñarse de la misma…", en este caso se está bajo el dispositivo amplificador del tipo penal.

Concurso real o aparente del delito de hurto por medios informáticos con el acceso abusivo a un sistema informático.

El concurso esta defino en el artículo 31 del código penal colombiano y reza "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, quedara sometido a la que establezca la pena más grave según su naturaleza, aumentada hasta en otro tanto, sin que fuere superior a la suma aritmética de las que correspondan a las respectivas conductas punibles debidamente dosificadas cada una de ellas. En ningún caso, en los eventos de concurso, la pena privativa de la libertad podrá exceder de sesenta años"

Acceso abusivo a un sistema financiero, artículo 269A determina "el que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema

informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de 48 a 96 meses de prisión y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes" articulo adicionado por la ley 1273 de 2009.

Se exponen a continuación los dos elementos determinantes para realizar el análisis referente al concurso de delitos, frente al hurto por medios informáticos y el acceso abusivo de un sistema financiero. Referente al concurso podemos encontrar dos elementos del mismo o una subdivisión relativa a la procedencia del mismo, como lo es el concurso *ideal o formal*, una conducta varios delitos o *el real o material* varias conductas varios delitos.

El concurso de delitos dentro de sí mismo conlleva ciertos criterios o principios que rigen el mismo como lo son: especialidad, consunción, subsidiaridad y alternatividad, procederemos entonces a realizar una descripción de cada una de los principios para abordar el concurso de conductas:

> ***Principio de especialidad***: ley general retrocede a la ley especial.
> ***Principio de consunción***: si un delito es más grave que otro se aplica el más gravoso.
> ***Principio de subsidiaridad***: aplicación auxiliar de un tipo penal cuando no existe uno que rija la conducta.
> ***Principio de alternatividad***: dos tipos penales son paralelos pero excluyentes por tener elementos incompatibles.

Se describen los principios que rigen los elementos esenciales frente al concurso de delitos, para el caso concreto se estudiara *el hurto y el acceso abusivo*, el acceso abusivo determina varios aspectos integrantes del tipo penal, acceso abusivo, mantenerse dentro del mismo en contra de la voluntad y la manipulación

del mismo con la finalidad de apoderarse de cosa mueble ajena, estos elementos recopilan la descripción integral del tipo penal de acceso abusivo con una única finalidad el apoderamiento sin embargo el hurto a través de medios informáticos subsume todos y cada uno de los aspectos generales y especiales del acceso abusivo el cual tienen por sí misma la única finalidad el apoderamiento de cosa ajena. Frente al concurso de delitos entre el hurto a través de medios informáticos y el acceso abusivo solo se puede describir o desarrollar dentro de su génesis un concurso aparente debido a que los dos tipos penales se subsumen en general en el hurto a través de medios informativos los cuales están íntimamente ligados y no darían lugar a un concurso real o material según la clasificación desglosada con anterioridad. El Dr. Suárez Sánchez determina "este concurso aparente se soluciona a través del principio de consunción por que el delito de hurto por medios informáticos y semejantes recoge en su descripción los elementos del tipo de acceso abusivo a un sistema informático".[80]

Como conclusión, siguiendo los lineamientos determinados por los principios que rigen el concurso de conductas punibles, no existe o existe por así decirlo un concurso aparente de delitos entre el hurto y el acceso abusivo a un sistema informático, el hurto a través de medios informáticos tiende en su genealogía a recopilar todos los aspectos de manera más amplia a la especificidad de cada uno de los tipos penales que presenta el título VII Bis, de la Protección de la Información y de los datos.

[80] SUAREZ SANCHEZ, Alberto. Manual de Delito Informático en Colombia. Análisis Dogmático de La Ley 1273 de 2009. 2016

1.1 Análisis comparativo (*derecho comparado*) del bien jurídico tutelado, configuración de tentativa y concurso de conductas punibles.

Se presenta un análisis de derecho comparado frente a la apreciación de diversos países y su evolución actual frente al cibercrimen.

España: En España como en todos los países en general, surtieron y modificaron su legislación penal con la finalidad de adecuarlo a las nuevas tecnologías y a las nuevas conductas punibles que se iban presentando a través del desarrollo sistemático de las redes de información. Sin embargo y a pesar de tener los mismos respaldos de origen como es la Convención Del Consejo De Europa sobre Delincuencia Informática Del 23 De noviembre De 2003 En Budapest, cada país ha desarrollado su propia adecuación y metodología integral a su política criminal orientada específicamente en delitos informáticos.

El legislador español decide adecuar los tipos penales existentes a los problemas penales que surgen en las redes de información, como un elemento de estafa y lo subdivide en dos bienes jurídicos, aquellos delitos que afectan el patrimonio económico y los delitos que afectan a las personas, catalogados los mismos a través del artículo 248.2 del código penal español. Considerado por el legislador español como un tipo de estafa, la cual está tipificada en el código penal español de 1995 en el artículo 248[81] *fraude informático*. La legislación española recopila los aspectos dogmáticos de la tentativa sin embargo para las defraudaciones informáticas o estafas informática España accede a la modalidad de tentativa dentro de estos comportamientos reprochables.

[81] GARCIA GARCIA-CERVIGON, Josefina. El fraude informático en España e Italia. Tratamiento jurídico penal y criminológico. 2008. Recuperado de https: https://revistas.comillas.edu/index.php/revistaicade/article/view/357/283.

El artículo 16 del Código Penal español, dice que "hay tentativa cuando el sujeto da principio a la ejecución del delito directamente por hechos exteriores, practicando todos o parte de los actos que objetivamente deberían de producir el resultado, y sin embargo este no se produce por causas independientes de la voluntad del autor".[82]

Dentro de la definición presentada, la figura de la tentativa juega un papel importante frente al fraude informático y condena o reprocha a través de su política criminal la modalidad de tentativa acabada e inacabada.

Ahora bien, lo que no comparte la Sala es la condena de Lorenzo como cooperador necesario de un delito consumado, sino de un delito en grado de tentativa, pues el delito no llegó a consumarse en cuanto el acusado no se quedó con la comisión pactada ni envió a Ucrania el resto de la cantidad ilícitamente ingresada en su cuenta, sino que después de retirarla de su cuenta, como reconoció en el acto del juicio, la volvió a ingresar en la entidad bancaria, tras recibir una llamada del director de la entidad bancaria alertándole de su ilícita procedencia. Tal circunstancia, apreciada en la sentencia de instancia como atenuante de reparación del daño en delito consumado, entiende la Sala que debe apreciarse como comisión del delito en grado de tentativa.[83]

Como razona la ya citada sentencia de la Audiencia Provincial de Madrid, sec. 27a, de 15-11-2010: "Así, y tras la promulgación del vigente Código Penal de 1.995, desapareció de la parte general del Código la figura, clásica en nuestro derecho penal del delito frustrado, para quedar englobadas tales acciones en el

[82] CONSEJO GENERAL DEL PODER JUDICIAL. Jurisprudencia. ID Cendoj 26089370012014100232 Audiencia Provincial. Recuperado de https: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7095915&links=%22phishing%22&optimize=20140613&publicinterface=true

[83] CONSEJO GENERAL DEL PODER JUDICIAL. Jurisprudencia. ID Cendoj 26089370012014100232 Audiencia Provincial. Recuperado de https: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7095915&links=%22phishing%22&optimize=20140613&publicinterface=true

nuevo concepto más amplio de tentativa, que abarca tanto la frustración del Código anterior como la tentativa propiamente dicha. Se ha diferenciado ambas figuras indicando que la antigua frustración sería una suerte de tentativa acabada, es decir, aquel caso en el cómo dispone el artículo 16, el autor realiza todos los actos que objetivamente deberían de producir el resultado, mientras que la llamada tentativa inacabada, se refiere a los supuestos en los que el autor realiza solo parte de los actos que deberían de producir el resultado. La diferenciación ente ambas modalidades, presenta su mayor relevancia a la hora de individualizar la pena, por cuanto que, si bien el Código Penal en su artículo 62 dispone que a los autores de tentativa de delito se les impondrá la pena inferior en uno o dos grados a la señalada por la Ley para el delito consumado, es importante que dicho precepto añade que para ello deberá de atenderse al peligro inherente al intento y al grado de ejecución alcanzado. Así, la Jurisprudencia viene admitiendo de manera pacífica que en los casos de la llamada tentativa acabada, procede la reducción en un solo grado, mientras que en los casos de tentativa inacabada, procede la reducción en dos grados, y ello sin perjuicio de particulares circunstancias que pudieran concurrir en cada caso particular".[84]

Como podemos apreciar dentro del extracto sugerido por parte de la jurisprudencia española frente al fraude informático, la tentativa realmente tiene aplicabilidad en el contexto de la defraudación informática sin subsumirla en otro tipo penal.

1.2 Estado Unidos

Estados Unidos es uno de los pioneros en legislación informática, sin embargo se deben tener en cuenta varios aspectos relevantes frente a su aplicación, el

[84] CONSEJO GENERAL DEL PODER JUDICIAL. Jurisprudencia. ID Cendoj 26089370012014100232 Audiencia Provincial. Recuperado de https: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7095915&links=%22phishing%22&optimize=20140613&publicinterface=true

primero es la legislación en sentido estricto combinado con el common law, o la ley común, adicionado a esto Estados Unidos, está dividido en un estado federal en cual se componen de varios estados y cada uno de estos estados que la compone determina una diversidad de legislaciones internas teniendo como base el respeto a la ley federal, hay varios un alcance a la división de delitos informáticos como lo son: fraude y acceso ilegal, terrorismo, obscenidades, copyright, amenazas y acoso cibernético.

En general, un delito informático quebranta las leyes federales cuando entra en alguna de las siguientes categorías:

- ✓ -Implica el compromiso o el robo de información de defensa nacional, asuntos exteriores, energía atómica u otra información restringida.
- ✓ -Involucra a un ordenador perteneciente a departamentos o agencias del gobierno de los Estados Unidos.
- ✓ -Involucra a un banco o cualquier otra clase de institución financiera.
- ✓ -Involucra comunicaciones interestatales o con el extranjero.
- ✓ -Afecta a gente u ordenadores en otros países o estados.

La Sección 1029 prohíbe el fraude y cualquier actividad relacionada que pueda realizarse mediante el acceso o uso de dispositivos falsificados como PINs, tarjetas de crédito, números de cuentas, y algunos tipos más de identificadores electrónicos. Las nueve áreas de actividad criminal que se cubren en la Sección 1029 están listadas abajo. Todas *requieren* que el delito implique comercio interestatal o con el extranjero[85].

Se aplica a través del common law el grado de tentativa, el cual implica el acceso abusivo sin ocasionar ningún daño, con el solo actuar se tipifica la conducta a

[85] Código penal internacional-delitos informáticos. Recuperado de https: http://catherinpacheco01.blogspot.com/2014/11/legislacion-informatica-de-estado-unidos.html

través de la ley federal sin embargo la legislación frente a delitos informáticos es extremadamente amplia debido a que cada estado rigiéndose por la legislación federal puede generar nuevos hechos reprochables en la realización de comportamientos reprochados por la ley federal o estatal.

1.3 Chile

En Chile existe solo una ley vigente hasta la fecha que regula materias relativas a los delitos informáticos, esta es la ley 19.223, la cual solo está compuesta de cuatro artículos, a continuación.[86]

"Artículo 1°. - El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo. Artículo 2°. - El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio. Artículo 3°. - El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
Artículo 4°. - El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."[28]

[86] BUSTOS BOBADILLA, Álvaro Francisco & ZUÑIGA SANCHEZ, Carlos Alberto. Análisis de los delitos informáticos en el derecho chileno y comparado. Santiago de Chile. 2013.

La penalidad asignada a las figuras de ejecución imperfecta va a estar determinada según el modelo de justificación de la punibilidad que se adopte. De este modo, según el modelo subjetivo, al que le basta la persecución del ánimo rebelde o peligroso, la tendencia va a ser la equiparación de las penas del delito consumado y la tentativa en la medida que el dolo del sujeto activo es el mismo en uno y otro caso al estar dirigido a la consumación del delito. El modelo objetivo en cambio, aboga por una penalidad inferior o atenuada respecto del delito consumado debido a que en la tentativa o frustración no se concretó la lesión al bien jurídico.

El Código Penal Chileno hace punibles, mediante una formula general contenida en su artículo 7, la tentativa y frustración de crímenes y simples delitos, excluyendo en su artículo 9 las faltas, que solo se castigan consumadas. figuras típicas que conceptualmente no admiten estas etapas como los delitos culposos y otros ya señalados.

En conformidad al inciso 2 del artículo 50 del mismo cuerpo legal, “siempre que la ley designe la pena de un delito, se entiende que la impone al delito consumado”.

Partiendo de la pena asignada al delito consumado, el Código Penal reconoce la menor irreprochabilidad de estas conductas que no implican la completa ejecución de las actividades destinadas a la lesión o puesta en peligro de un bien jurídico protegido y atendiendo al modelo objetivo y a la tradición jurídica liberal a la que adhiere nuestro derecho penal a este respecto, señala en los artículos 51 a 54 las penas asignadas a los crímenes y simples delitos que se encuentren en grado de tentativa o frustración. Distingue además entre los grados de participación del sujeto activo (autor, cómplice o encubridor), asignando penas que van desde el grado inmediatamente inferior a la correspondiente para el delito consumado en caso del autor de crimen o simple delito frustrado hasta una pena inferior en cuatro

grados en caso de encubridores de tentativa[87]. Determinado lo anterior, cada caso concreto frente a la realización del hecho reprochable se establecerá el grado de ejecución y la modalidad tentada para así cuantificar la pena de la conducta penalmente reprochada muy similar a nuestra legislación penal.

Jurisprudencia chilena-cibercrimen.

II. LOS HECHOS

Entre los días 28 de diciembre de 2001 y 8 de enero de 2002, un ex empleado de la empresa ATI Chile, realizó diversas intromisiones ilegales al servidor de ésta, alterando, dañando y conociendo indebidamente información contenida en éste. Los sitios Web afectados fueron: www.guestbook.cl y www.metabuscador.cl

El imputado era un joven de 19 años, conocido en el Chat IRC con el seudónimo «P0key», el cual habría actuado por «venganza» en contra de la empresa, pues había sido despedido de ésta.

El «cracker»[3] al ingresar ilegalmente a estos sitios, alteró el contenido de éstos, creando una nueva página Web (index.html) en reemplazo de la existente, que mostraba mensajes ofensivos[4] hacia la empresa e indicaba que el sitio había sido hackeado.

El fiscal jefe de la ciudad de Talca don Carlos Olivos Muñoz, realizó una clara exposición respecto de los hechos, la investigación realizada, todos los medios de prueba reunidos durante ocho meses de investigación y solicitó la aplicación de una pena de 3 años y un día de presidio, por tres delitos informáticos: artículos 1, 2 y 3 de la Ley 19.223.

[87] ORELLANA VALENCIA, Juan Pedro. Desarrollo jurisprudencia de la tentativa y frustración. Corte de Apelaciones de Valdivia. 2007.

El querellante, abogado Alberto Contreras Clunes, ratifica todo lo señalado por el fiscal y recalca la gravedad de los delitos imputados, los perjuicios ocasionados a la empresa y el actuar malicioso del acusado. También resalta el hecho que el acusado confiesa su participación en su declaración policial y el jactarse de ello en la entrevista del diario *El Centro.*

Importante resulta la inclusión de un peritaje informático realizado por la Brigada del Ciber Crimen de la Policía de Investigaciones de Chile. En efecto, se realizó un peritaje a la computadora que ocupaba el acusado en el Ciber Café, como a su computadora personal. Por medio de un sofisticado programa, inaugurado en esta ocasión, se logra recuperar diversos archivos borrados del disco duro de la CPU del Ciber Café. Merece especial atención uno, consistente en un correo electrónico enviado por el acusado a su pareja en el cual le cuenta: *«estoy borrando unas («weas») que me pueden comprometer en los asuntos judiciales …»,* enviado precisamente en la tarde del día anterior al que prestó declaración policial.

En sus conclusiones el peritaje señala que: *«El computador en cuestión cuenta con las capacidades técnicas necesarias y los programas adecuados tanto para navegar por Internet como para efectuar daños a sistemas informáticos».* En efecto, se pudo determinar que el disco duro contenía 24 programas: *«… de uso frecuente por los Hackers, Crackers o Criminales Informáticos».*

Finaliza el querellante señalando la importancia que tiene la informática en la actualidad, las potenciales víctimas de este tipo de delitos y los graves perjuicios que se causan a las empresas, pudiendo éstas llegar a quebrar económicamente por el desprestigio que estos delitos le provocan, solicitando la imposición de una pena de cinco años de presidio, en atención a tratarse de reiteración de delitos, contemplados en los artículos 1, 2 y 3 de la Ley 19.223.

Por su parte el defensor penal público don Joaquín Lagos León, alegó indicando que no se encontraba acreditada la participación de su defendido en los hechos, negándole valor a la declaración policial.

Introdujo una novedosa jurisprudencia del derecho norte americano, en la cual se penaliza a las empresas que ofrecen servicios de seguridad informática y son víctimas de «hackers», puesto que no dan cumplimiento a los servicios ofrecidos[6].

IV. EL FALLO

Al finalizar la audiencia, la Juez de Garantía dicta su veredicto: Culpable por los delitos N°1, 2 y 3 de la Ley 19.223, fijando la fecha de la lectura del fallo para el día 11 de abril de 2003.

El fallo consta de 13 fojas en las que pormenorizadamente se analizan todos los medios de prueba, describiendo en forma precisa el actuar delictivo y la forma en que éste se encontraba acreditado.

Al fijar la pena, la Juez advierte que tratándose de reiteración de delitos resulta más beneficioso aplicar una pena única conforme al artículo 351 del Código Procesal Penal. Señala también que lo dispuesto en el inciso cuarto de dicho artículo, es: *«una facultad para el Tribunal»* en consideración a que el querellante solicitó una pena superior a la del fiscal.

Por otra parte, afirma que: *«la entidad de las atenuantes[7] no nos convence, teniendo presente que según quedó establecido se trata de delitos reiterados, por lo que la pena que se impondrá en el grado señalado se considera más condigna con el actuar ilícito del acusado».*

En atención a ello aplica la pena de tres años y un día de presidio, que es el mínimo de la escala penal de presidio menor en su grado máximo[88].

1.4 Argentina

Los delitos informáticos fueron introducidos y desarrollados a través de la legislación interna por medio de la Ley 26.388 en este país, el cual conculca los siguientes hechos reprochables dentro del ciber crimen o brinda protección legal penal frente a los siguientes derechos fundamentales, a saber:

Delitos contra la integridad sexual-pornografía infantil, reprocha las siguientes conductas a través de estos verbos rectores, Producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir por cualquier medio, cualquier representación de una persona menor de 18 años dedicado a actividades sexuales explícitas o de sus partes genitales.

- Tener representaciones de personas menores de edad para distribuirlas o comercializarlas.
- Organizar espectáculos en vivo de representaciones sexuales explícitas en las que participan persones menores de edad.
- Facilitar el acceso a espectáculos pornográficos o dar material pornográfico a personas menores de 14 años.

[88] CONTRERAS CLUNES, Alberto. Ius et praxis, versión on line ISSN 0718-0012. Delitos informáticos: un importante precedente. Recuperado de https: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122003000100023.

Violación de secretos y de la privacidad.

- Abrir o acceder indebidamente una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido.
- Apoderarse indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado.
- Suprimir o desviar de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
- Interceptar o captar comunicaciones electrónicas o telecomunicaciones de carácter privado o de acceso restringido.

La pena se agrava si el autor comunica o publica el contenido de la carta, escrito, despacho o comunicación electrónica y esto causa perjuicio. Si el hecho lo comete un funcionario público que abusa de sus funciones, sufre, además, inhabilitación.

Acceso a sistema informático. El código penal de este país sanciona la intromisión a cualquier acceso informático con un agravante adicional si es en perjuicio de un organismo de carácter público.

Acceso a banco de datos. Acceder ilegítimamente a un banco de datos personales. Proporcionar o revelar información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a guardar por ley.

Publicación de Comunicaciones electrónicas. sanciona todos los elementos de comunicación no destinados a publicidad.

Fraude informático. sanciona cualquier defraudación mediante la utilización de medios electrónicos

Daño informático. Alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos. Vender distribuir, hacer circular o introducir en un sistema informático, cualquier programa destinado a causar daños.

Conductas agravadas destinadas a servicios públicos como la salud, energía, transporte y comunicaciones.

La tentativa en el derecho penal Argentino y su tratamiento: Jorge Eduardo Buompadre expresa que esta nueva modalidad constituye una figura especializada en relación a la estafa prevista en el art. 172, por el medio empleado (un sistema informático), aunque con anterioridad ya se había contemplado la posibilidad de defraudar con tarjetas de compra, débito o crédito sustraídas o extraviadas incluso si se lo hacía mediante operaciones automatizadas (art. 173, inciso 15, incorporado por la Ley 25.390).[89] [90]

CONCEPTO DE TENTATIVA, expresa que "Tentativa es comienzo de ejecución de un delito determinado con dolo de consumación y medios idóneos, que no llega a consumarse por causas ajenas a la voluntad del autor." Las ideas no son punibles por el principio *cogitationis poenam nemo patitur* (nadie sufre pena por su pensamiento). Por lo tanto, no entran dentro del concepto de tentativa. Con la consumación del delito termina toda posibilidad de tentativa ya que en está la conducta de individuo encuadra perfectamente en el tipo, en cambio la tentativa lo que hace es ampliar el tipo para poder llegar a la punición de conductas que no llegan a consumarse. Entonces lo que nos queda por analizar son los actos que se exteriorizan, dentro de estos encontramos los actos preparatorios y los de ejecución.

[89] ROIBON, María Milagros. La estafa informática en el código penal argentino.
[90] BUOMPADRE. Manual de Derecho Penal. Parte especial. 3ª reimpresión. Editorial Astrea. 2017, p. 476

ACTOS PREPARATORIOS Y EJECUTIVOS, Los actos preparatorios no son punibles, porque estos no son suficientes para demostrar su vinculación con el propósito de ejecutar un delito determinado y para poner en peligro un bien jurídico; pero hay algunos casos que excepcionalmente la ley castiga en la parte especial, como el art. 189bis que se refiere a la tenencia de explosivos y armas de guerra; el art. 210 que pena la asociación ilícita; el art. 216 que castiga la conspiración para la traición; el art. 299 sanciona la tenencia de instrumentos conocidamente destinado a cometer falsificaciones; también debe agregarse a esta lista el art. 6 de la ley 20771, que reprime la tenencia de estupefacientes.

Estos actos son punibles ya que su celebración está directamente vinculada con la realización de un delito y pone en peligro un bien jurídico determinado, "Sin embargo, moderadamente se ha manifestado la tendencia a extender la punibilidad a los actos preparatorios, como expresión de una forma de estado autoritario".[91]

Como podemos observar el tratamiento dado por la legislación argentina al dispositivo amplificador del tipo penal, la tentativa, es un desarrollo similar al interno de nuestra legislación, ahora lo pertinente es verificar la modalidad tentada en los delitos informáticos, en su mayoría de doctrinantes y autores referentes a las conductas sancionadas penalmente a través del hecho reprochado por medios electrónicos, admiten la modalidad de tentativa, se esboza particularmente la orientación de diversos escritores orientados a la violación de libertades sexuales y a su protección informática visto anteriormente, los cuales tutelan y conculcan la tentativa específicamente frente a pornografía infantil por ejemplo *"es la relativa a la publicidad o puesta en circulación de imágenes, filmaciones de menores establecidas en el primer párrafo. Allí, el delito se consuma una vez realizadas las tomas o filmaciones, sin necesidad de que se acredite su divulgación a terceras*

[91] SOLER, Sebastián. Derecho penal argentino. Tomo 2. 1953.

personas, más allá de las que participaron en la toma de las imágenes"[92]*.* Sin embargo, la legislación argentina fue un poco más allá de lo estipulado en la Doctrina frente a la modalidad de tentativa, debido a que en cada caso concreto y a cada delito informático se realiza el correspondiente estudio frente a la modalidad de su realización, por ejemplo "*la tentativa en este delito, al igual que en todos los delitos en los cuales el bien jurídico es la privacidad, la prueba en el grado de tentativa es sumamente difícil comprobarlo. El porqué de tal afirmación se debe a que la tentativa se produce al momento en que un tercero toma conocimiento del secreto, aunque no se produzca el daño, porque si se produce el daño salimos de la figura de la tentativa. Desde este punto de vista, si el secreto "continúa guardado" en el tercero que no debe conocerlo y de ninguna manera se puede probar que ese secreto fue suministrado por el funcionario público, entonces es imposible probar el delito".*[93]

[92] RIQUERT, A. Marcelo. Cibercrimen y delitos informáticos – los nuevos tipos penales en la era de internet Tenencia simple de pornografía infantil. 2018.

[93] SORBO HUBO, Daniel. Doctrina penal delitos informáticos. Utsupra. Editorial jurídica. Edición 2013.

CONCLUSIONES

Realizada la correspondiente investigación, puedo determinar como elemento base, excluyendo a EEUU, las modalidades y criterios del dispositivo amplificador del tipo, elemento presente en nuestra legislación, legislaciones penales suramericanas y europeas.

La tentativa es aplicada a los delitos de carácter informático o ciber-crimen. Como en otros muchos tipos penales. Tiene una aplicación en el ámbito de la tentativa acabada e inacabada.

Procede la aplicación de la misma de manera general como la aplicación en diversos ámbitos penales, generando beneficios en el quantum punitivo.

Por principio de favorabilidad de la ley penal, beneficiaria su ámbito de aplicación para este tipo de tipos penales, los cuales generarían una mayor aplicación frente al dispositivo amplificador del tipo penal y se evitaría subsumir en otros delitos que afectarían la gravosidad del sujeto activo del injusto.

Favorabilidad al momento de aplicación de dosificación de la pena.

Quedarían sujetos del ámbito penal todos aquellos actos tendientes a la realización de cualquier actividad criminal en la realización de delitos informáticos, según el tipo de tentativa a aplicar en nuestro ámbito penal.

Una vez analizado el concurso de delitos entre el hurto a través de medios informáticos y el acceso abusivo, como conclusión el hurto a través de medios informáticos subsume todos y cada uno de los elementos en la realización de la conducta punible, por esta razón el concurso no procede y es solo aparente,

siendo así admitiría la tentativa debido a que el delito fin es el apoderamiento de la cosa ajena.

Desde el derecho comparado la tentativa procede para los delitos informáticos y castiga la modalidad de tentativa, obteniendo así un reproche penal más universal. Las políticas político-criminales deben enmarcar los ámbitos penales desde su base general, queriendo esto decir que el legislador al momento de estudiar la constitución de los delitos informáticos, subsumió conductas realizando su estudio desde un punto de vista práctico y no geológico del delito, excluyendo de por si en nuestro ámbito penal la tentativa para delitos informáticos. Los cuales y una vez estudiado y analizado el derecho penal comprado en diversos estados los mismo admiten el estudio de la tentativa.

Para determinar la constitución de un delito informático el mismo se debe acercar desde el inicio del estudio de la teoría del delito siendo este procedente para todas las modalidades delictivas encausadas, a futuro se realizaran o generaran nuevas conductas que serán excluidas dentro del estudio penal sin embargo, al momento de la tipificación de estos posibles comportamientos el legislador debe abarcar mayores estudios frente a la realización de este tipo de comportamientos sin excluir la base y fundamentos del derecho penal.

BIBLIOGRAFÍA

BCN Informe. Biblioteca Nacional del Congreso. Los delitos cibernéticos en la legislación estadounidense. Recuperado de https://www.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/

BUSTOS BOBADILLA, Álvaro Francisco & ZÚÑIGA SÁNCHE, Carlos Alberto. Análisis de los delitos informáticos en el derecho chileno y comparado. Santiago de chile, 2013.

CONSEJO GENERAL DEL PODER JUDICIAL. Jurisprudencia. Id Cendoj 26089370012014100232 audiencia provincial.

DE LA CUESTA ARZAMENDI, José Luis; DE LA MATA BARRANCO, Norberto. *derecho penal informático,* Madrid, Civitas-thomson Reuters, 2010, pp. 31 y 159;

DURHAM, Cole. The emerging structures of criminal information law: tracing the contours of a new paradigm", en: *information, technology, crime: national legislation and international initiatives,* ius informationis, vol. 6, köln-berlín-bonn-münchen, heymann, 1994, pp. 533-542.

EZERTUA, Manuel. El proyecto del convenio sobre el cybercrimen del consejo de europa", en: *internet y derecho penal uadernos de derecho judicial x,* Madrid, consejo general del poder judicial, 2001 pp. 15-62; Morales García, Oscar, "apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del consejo de europa sobre cyber-crimen", en: *delincuencia informática, cuadernos de derecho judicial ix,* madrid, consejo general del poder judicial, 2002, pp. 11-34.

FERNÁNDEZ GARCÍA, Emilio Manuel. fraudes y otros delitos patrimoniales relacionados con la informática e internet", en: *estudios jurídicos*, iv, Madrid, consejo general del poder judicial, 1999, p. 391.

FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf

FRISCH, WOLFG ANG, *La Imputación Objetiva del Resultado,* Barcelona, Atelier, 2015, p. 41 Y SS., Y 56 Y SS.; JESCHECK, HANS HEINRICH / WEIGEND, THOMAS, *Tratado de Derecho Penal*, Granada, Comares, 2002, p. 307 y ss.; ROXIN, CLAUS, *Derecho Penal, Parte General*, Tomo 1, Madrid, Editorial Civitas, 1997, pp. 362 y ss.; WELZEL, HANS, *Derecho Penal Alemán: Parte General,* Santiago, Jurídica de Chile 1997, pp. 66 y ss. (Tipo y Adecuación Social).

GALÁN MUÑOZ, Alfonso. El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 c.p., valencia, tirant lo blanch, 2005, pp. 29 y ss.; MIRÓ LLINARES, Fernando. El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio, cit, pp. 33 y ss.

GARCÍA NOGUERA, Noelia. Delitos: Delitos Informáticos en el Código Penal Español. 2002. Recuperado de https://www.delitosinformaticos.com/delitos/codigopenal.shtml

GOBIERNO DE ESTADOS UNIDOS. Código Penal Internacional contra Delitos Informáticos. Legislación informática de Estado Unidos. 2014. Recuperado de http://catherinpacheco01.blogspot.com/2014/11/

GRACIA MARTÍN, Luis. *Prolegómenos*, Madrid, Civitas, 2001, p. 88

GRISALES PÉREZ, Giovanni Stalin. Análisis dogmático de las conductas de hurto por medios informáticos y semejantes (art. 269i) y transferencia no consentida de activos (art. 269j), Ley 1273 de 2009. Universidad Eafit. 2013.

LEGIS. Sentencia Corte Suprema de Justicia. Delitos informáticos. 2019 legislacion-informatica-de-estado-unidos.html

MAJER, Abushihab. Hurto por medios informáticos ¿un delito informático? 2016

MATA Y MARTÍN, Ricardo. Bienes jurídicos intermedios y delitos de peligro, Granada, Comares, 1997, pp. Sobre las funciones informáticas en sentido estricto, véase Cano Martínez, Jeimy, *Manual de un chief information security officer,* Bogotá, ediciones de la u, 2016, pp. 96 y 97; POMANTE, Gianluca, *internet e criminalità,* Torino, Giappichelli editore, 1999 pp. 109 y 113; POSADA MAYA, Ricardo, "una aproximación a la criminalidad informática en Colombia", cit., p. 22;

POSADA MAYA, Ricardo, "el delito de transferencia no consentida de activos", en *revista de derecho, comunicaciones y nuevas tecnologías,* Bogotá, 2012, pp. 215-216; Rovira del canto, enrique, *delincuencia informática y fraudes informáticos,* en *estudios de derecho penal* no. 33, Comares, Granada, 2002. Pp. 67 y 69 y ss.; id., *delincuencia informática y fraudes informáticos,* p. 72.

MATELLANES, Nuria. Algunas notas sobre las formas de delincuencia informática en el código penal, en: *Hacia un derecho penal sin fronteras,* xii congreso universitario de alumnos de derecho penal, Madrid, Colex, 2000, p. 130; Rovira del Canto, enrique, *delincuencia informática y fraudes informáticos,* cit, pp. 65, 130 y 131; id, "hacia una expansión doctrinal y fáctico del fraude informático" en *Revista Aranzadi de derecho y nuevas tecnologías,* nº3, 2003, p. 118; Uit, *understanding cybercrime:* Conpes 3701 (2011-2014).

MIRÓ LLINARES, Fernando. La cibercriminalidad 2.0: falacias y realidades. 5ª edición, editorial Trotta, Madrid, 2003, p. 122.
MUNICACIONCUENTA&prmID=11020

ORELLANA VALENCIA, Juan Pedro. Desarrollo jurisprudencia de la tentativa y frustración. Corte de Apelaciones de Valdivia, 2017.

PÉREZ LUÑO, Enrique Antonio. Manual de informática y derecho, Barcelona, Ariel, 1996, p. 75.

POSADA MAYA, Ricardo. Libertad de información e independencia judicial, en discriminación, principio de jurisdicción universal y temas de derecho penal, Bogotá, Uniandes, 2013, p. 682-683.

POSADA MAYA, Ricardo. Una aproximación a la criminalidad informática en Colombia. Revista de derecho comunicaciones y nuevas tecnologías, 2006, p. 15.

POSADA MAYA, Ricardo. Una aproximación a la criminalidad informática en Colombia", cit., pp. 19 y 20; id., POSADA MAYA, Ricardo, "el delito de transferencia no consentida de activos", cit., p. 214.

RIQUERT, Marcelo A. Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet tenencia simple de pornografía infantil, 2018.

ROIBON, María Milagros. La estafa informática en el código penal argentino.

ROVIRA DEL CANTO, Enrique. Delincuencia informática y fraudes informáticos, cit, pp. 130. MEEK NEIRA, Michael. Delito informático y cadena de custodia, Universidad Sergio Arboleda, Bogotá, 2013, pp. 59.

SATZGER, Helmut. La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia, en: derecho penal y nuevas tecnologías, Bogotá, Universidad Sergio Arboleda, 2016, p. 19.

SEGU.INFO. Seguridad de la información. Legislación y Delitos Informáticos - La Información y el Delito. Recuperado de https://www.segu-info.com.ar/legislacion/?pais=17

SIEBER, Urich. Computerkriminalität und strafrecht: neue entwicklungen in technik und recht, 2da ed., köln-berlin-bonn-münchen, heymanns, 1980 p. 39; id, "criminalidad informática. Peligro y prevención", pp. 29 y ss.; id. "documentación para una aproximación al delito informático" en delincuencia informática, 1992, pp. 65-90.

SOLER, Sebastián. Derecho penal argentino. Tomo 2. 1953.

SORBO, Hugo Daniel. Doctrina penal delitos informáticos. Utsupra. Editorial jurídica. Edición, 2013.

SUÁREZ SÁNCHEZ. Manual de delito informático en Colombia. Análisis dogmático de la ley 1273 de 2009.

TIEDEMANN, Klaus. Criminalidad mediante computadoras, en: *nuevo foro penal* no. 30, octubre–diciembre de 1985, Bogotá, Temis, pp. 481 a 492; id., *poder económico y delito, A*riel, Barcelona, 1985, p. 122.

ZDENKO, Seligo. Legislación sobre delitos Informáticos. España. Recuperado de https://delitosinformaticos.com/legislacion/espana.shtml

ACURIO DEL PINO, Santiago. Delitos Informáticos: Generalidades. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

GARCÍA CERVIGÓN, Josefina. El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. Recuperado de https://revistas.upcomillas.es/index.php/revistaicade/article/download/ 357/283.

IBERRLEY COLEX. Jurisprudencia sobre delito informático. 2012. Recuperado de https://www.iberley.es/jurisprudencia/delito-informatico.

ARZUAGA HERRADA, Toyber S. & GUEVARA MEDINA, Elkin. La Ley 1273 de 2009 y los delitos informáticos en Santiago de Cali. 2013) Recuperado de http://bibliotecadigital.usb.edu.co:8080/bitstream/10819/1891/1/ la%20Ley1273_ Delitos%20 InformaticosSantiago%20de%20Cali_Arzuaga_2013..pdf}

BLOGSPOT. Código penal internacional-delitos informáticos. Recuperado de http://catherinpacheco01.blogspot.com/2014/11/legislacion-informatica-de-estado-unidos.html

CONSEJO GENERAL DEL PODER JUDICIAL. Jurisprudencia. ID Cendoj 26089370012014100232 Audiencia Provincial. Recuperado de https: http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7095915&links=%22phishing%22&optimize=20140613&publicinterface=true

CONTRERAS CLUNES, Alberto. Lus et praxis, versión on line ISSN 0718-0012. Delitos informáticos: un importante precedente. Recuperado de https: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122003000100023.

DEPARTMENT OF JUSTICE. U.S. ATTORNEY'S OFFICE. Two Major International Hackers Who Developed the "SpyEye" Malware get over 24 Years Combined in Federal Prison. 2016. Recuperado de https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined.

GARCIA GARCIA-CERVIGON, Josefina. El fraude informático en España e Italia. Tratamiento jurídico penal y criminológico. 2018. Recuperado de https: https://revistas.comillas.edu/index.php/revistaicade/article/view/357/283.

GRISALES PÉREZ, Giovanni Stalin. Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes. Universidad EAFIT. 2013. Recuperado de https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf?sequence=1

LARA, Juan Carlos, MARTÍNEZ, Manuel y VIOLLIER, Pablo. Hacia una regulación de los delitos informáticos basada en la evidencia. Revista Chilena de Derecho y Tecnología. 2014. Recuperado de https://rchdt.uchile.cl/

MAJER, Abushihab. Hurto por medios informáticos ¿Un delito Informático? 2016. https://repository.usta.edu.co/bitstream/handle/11634/9259/AbushhMajer2017.pdf?sequence=1&isAllowed=y

SUÁREZ SÁNCHEZ, Alberto. El hurto por medios informáticos y semejantes a través de la utilización de tarjeta magnética falsa o ajena en cajero automático. Estudios de Derecho Penal I. p. 237-240. Recuperado de http://avalon.utadeo.edu.co/servicios/ebooks/derecho_penal _I/files/assets/basic-html/page240.html

THE UNITED STATES DEPARTMENT OF JUSTICE. Justice News. Russian Citizen Sentenced to 46 Months in Prison for Involvement in Global Botnet Conspiracy. 2017, Recuperado de https://www.justice.gov/opa/pr/russian-citizen-sentenced-46-months-prison-involvement-global-botnet-conspiracy

YOUNES, Ali. News. Hacker Hamza Bendelladj sentenced to 15 years. 2016. Recuperado de https://www.aljazeera.com/news/2016/04/hacker-hamza-bendelladj-sentenced-15-years-160422104149553.html