Universidad de Chile, Facultad de Derecho
Escuela de Postgrado
Magíster en Derecho Penal 2011 Magallanes

APROXIMACION A LA PROBLEMÁTICA DE LA DELINCUENCIA INFORMATICA , PUNIBILIDAD Y LEY APLICABLE

Alejandra Verónica . Guevara Mendoza
RUT Nº 12.792.579-8
Profesor Guía : Germán Ovalle Madrid

APROXIMACION A LA PROBLEMÁTICA DE LA DELINCUENCIA INFORMATICA , PUNIBILIDAD Y LEY APLICABLE

1.- RESUMEN

El presente trabajo tiene por objeto dar una visión global de los problemas que se presentan al juzgador al momento de enfrentarse con la delincuencia informática, abarcando en primer lugar las consideraciones en cuanto a lo que debemos entender por delincuencia informática, las dificultades reales que presenta tanto su descubrimiento como su investigación y prueba, para luego abordar la forma en que estos hechos deben ser tratados penalmente, para lo cual se trabajará en poder responder a la principal pregunta en la materia, esto es: si en nuestro país los delitos que conforman la delincuencia informática y en particular el fraude informático se encuentran regulados en la legislación penal o no; para lo cual se analizarán las principales leyes, doctrina y jurisprudencia _ esencialmente Chilena _ existentes sobre este punto, abordando las dos principales posturas al respecto, esto es, la de aquellos que responden afirmativamente, con exposición de sus argumentos y la legislación especial aplicable, como la postura de aquellos que responden negativamente y en tal evento se abordarán las soluciones que ante este vacío legal nos entregan para evitar la impunidad de tales hechos, analizando en ambos casos el bien jurídico protegido y los principios generales del derecho vinculados a ello, pasando por el análisis de las reglas y teorías que determinan - ya sentada la posibilidad de sancionar estas conductas_ el tribunal llamado a conocer de ellas . Finalizando el presente trabajo con la conclusión arribada por quien suscribe luego de este estudio en orden a tomar posición por una de estas posturas y los lineamientos que la sustentan.

(Delincuencia informática – fraude informático- ley penal – competencia – bien jurídico – principios generales de derecho)

INDICE

Páginas

I.- INTRODUCCION

El desarrollo de la informática trae gran desarrollo a una sociedad, pero a su vez abre las puertas a técnicas nuevas de criminalidad, más rápidas y con mayores dificultades de represión penal. Estos avances han significado en estos últimos años el cambio de visión en materia de valoración de la información, pasando la información a ser considerada en la actualidad como un bien de alto valor económico digno de protección legal y por sobre todo de protección a nivel penal, surgiendo con estos avances de la tecnología novedosos bienes jurídicos.

La delincuencia informática como se ha venido indicando, surge y se mantiene en una estrecha relación con los avances tecnológicos, principalmente por el desarrollo que en materia computacional a nivel mundial se produjo en la década de los sesenta, pudiendo indicarse que no es un fenómeno que se delimite claramente sino que seguirá en constante evolución, lamentablemente en forma más rápida que el desarrollo del derecho llamado a reprimirlo y sancionarlo, lo cual se traduce en una gran ventaja para el delincuente informático, siendo factores relevantes en la proliferación de los mismos, entre otros, la necesidad de tener conocimientos especiales en materia informática para entender estos ilícitos y poder enfrentarlos en forma, la insuficiencia de los sistemas de seguridad para impedir su ejecución, la carencia de leyes especiales que aborden globalmente esta delincuencia, que por sus especiales características requiere un tratamiento diverso a los tipos comunes [1].

Nuestro sistema penal, como es sabido, se basa principalmente en el principio de legalidad, consagrado básicamente a nivel de nuestra Carta Fundamental en el artículo 19 N º 3 inciso 8º, derecho penal que tiene como objetivo proteger bienes jurídicos de relevancia, sean individuales o colectivos pero trascendentes de protección para la comunidad y que justifiquen la existencia de un reproche y un castigo.

[1] Marcelo Huerta Mirada, Claudio Líbano Manssur. “Delitos Informáticos”, segunda edición complementada y actualizada a 1998. Editorial Jurídica Cono Sur Ltda. pág.105-108.

Un derecho penal que no es estático sino que más bien obedece necesariamente a los aspectos y evolución de la sociedad en la que debe aplicarse tendiendo en la búsqueda de sus objetivos y como lo reconoce la mayoría de la doctrina nacional a privilegiar el respeto y la protección de la seguridad ciudadana mediante la creación de tipos penales que se ajusten a estas nuevas necesidades [2].

El derecho penal debe adecuarse a la necesidad y realidad del dinamismo de lo que con él se pretende proteger, y que dado el avance de nuestro desarrollo social ya no puede quedar limitada esta protección a los clásicos bienes jurídicos individuales u orientados exclusivamente a la persona como individuo, sino que debe extenderse al reconocimiento de la existencia de bienes jurídicos supraindividuales que han surgido precisamente, como se indicó, de la evolución socioeconómica de los países [3], no obstante lo cual se debe reconocer que tratándose de delitos socio-económicos deben ser sancionados bajo la premisa de la " extrema ratio" o de " absoluta necesidad de la intervención punitiva del Estado", para aquellos casos en que principalmente exista abuso de poder que implique una grave interferencia en el funcionamiento del sistema económico y dejar el resto a lo infraccional administrativo [4]. Pues bien a lo largo de este trabajo iremos dando a conocer los aspectos y problemática más relevante que en materia penal han surgido en los últimos años a consecuencia del aparecimiento de nuevas formas de criminalidad, partiendo por abordar lo que debe entenderse como tal, para esbozar las principales y mas frecuentes modalidades de comisión, para luego entrar de lleno a la problemática central, cual es la de determinar si este tipo de conductas son o no punibles, dando los lineamientos de las dos grandes posiciones al efecto para luego analizar la legislación existente en nuestro país sobre la materia y conocer algunos ejemplos de las soluciones jurisprudenciales que se han dado a lo largo del tiempo, incluso con antelación al surgimiento de leyes que abordan especialmente el tema como lo fue la dictación de la Ley N º19223 sobre Delitos

[2] Sergio Politoff, Jean Pierre Matus, Maria Cecilia Ramírez. " Lecciones de Derecho Penal Chileno, parte general, Editorial Jurídica de Chile año 2004, pág. 19-53.

[3] Juan Bustos Ramírez, Obras Completas . Derecho Penal Parte General Tomo II, Editorial Ara Editores, año 2005 pág. 181.

[4] Juan Bustos Ramírez, ob. Cit. Pág. 603.

Informáticos y la Ley Nº 20009 sobre Tarjetas de Crédito, no sin antes al menos mencionar para conocimiento general, cuál ha sido la realidad en los países cuyas legislaciones han servido de modelos o referentes para nuestra legislación. Hecho lo anterior y ya partiendo del entendido que existe legislación aplicable a la materia haremos un alcance a la problemática que origina este tipo especial de delincuencia por sus características de comisión para la determinación del tribunal competente y las posibles soluciones que se pueden dar en estos casos, todo ello con el objeto de poder dar a conocer al lector la existencia de este problema penal real, actual y que seguirá en amplio crecimiento y por ende digno de ser tratado con mayor profundidad a fin de motivar soluciones claras y que permitan mantener incólume la seguridad jurídica tan preciada en estos tiempos.

II.- ASPECTOS GENERALES

II.1.- Aspectos generales de la delincuencia informática en general y sus formas particulares, en especial, el fraude informático

Concepto y alcance de la delincuencia informática

Suelen existir confusiones de términos ya que se habla indistintamente de delito informático y delincuencia informática para hacer mención a conductas ilícitas realizadas por medios tecnológicos, pero conforme a nuestro derecho penal y al principio de legalidad que nos rige no podemos encuadrar todas las conductas posibles de cometer mediante el uso de medios informáticos en el término delito informático ya que para ser delito debe estar expresamente tipificado en la ley y ello resulta imposible ya que existirían tantas modalidades de comisión como el avance de la informática lo permita por lo cual hay autores como Claudio Magliona y Macarena

Lopez que optan por seguir la denominación genérica de delincuencia informática aunque reconocen que su definición no es unánimemente aceptada en la doctrina [5].

Cuando hablamos de informática en general estamos hablando de tratamientos y manejo de la información por medio principalmente de computadores. En materia internacional se acepta mayoritariamente el concepto dado por la Academia Francesa de la Lengua desde el año 1966 que indica que la informática "es la ciencia de tratamiento sistemático y lógico, especialmente por medio de máquinas automáticas, de la información, entendida ésta como el soporte de los conocimientos y de las comunicaciones humanadas en su contexto económico y social [6]".

Por su parte y a fin de entender en general de qué estamos hablando cuando hablamos de sistemas de tratamiento de la información se puede indicar que son sistemas automatizados, programas o soportes lógicos y los datos contenidos en ellos, debiendo entenderse excluido el soporte material mismo, como lo sería físicamente el disco, el cual estaría protegido por las figuras clásicas, lo cual se desprende de la historia legislativa en la materia como se verá más adelante.

Para la Organización para la cooperación Económica Europea y Desarrollo (OCDE) el delito informático es "Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos, y/o la transmisión de los mismos", aunque es una definición que se le critica por no ser comprensiva en forma precisa de sus elementos [7].

---

[5] Claudio Paul Magliona Markovicth- Macarena López Medel. " Delincuencia y Fraude Informático" Derecho Comparado y Ley N º 19223. Editorial Jurídica de Chile, año 1999 pág.35-37.

[6] D. S. Nº 887 de 03 de julio del año 1975 publicado en el Diario Oficial el 18-08-1975 citado por Vera Quilodrán, Alejandro en su obra Delito e Informática (La Informática como fuente del delito) Ediciones Jurídicas La Ley, Santiago Chile 1966, pág. 19, citado a su ves por Magliona Markovich, Claudio Paul y López Medel, Macarena, "Delincuencia y Fraude Informático" Derecho Comparado y Ley N º 19223. Editorial Jurídica de Chile año 1999, pág. 19.

[7] Organization For Economic Cooperation Anual Development , " Computed Related Crime : Analisys of legal Polito; Paris, France, 1986, pág.7 citado por los autores Claudio Magliona y Macarena López, ob. Citada página 37.

Para el profesor Chileno Hernando Morales Ríos, delito informático es una "acción delictiva en la cual el computador es el instrumento u objeto del hecho" [8], pero también se le critica la falta de especificación de que debe entenderse por tal, siendo entre nuestra doctrina una de las definiciones más aceptadas y la cual comparto, la definición que de delitos informáticos se entrega en la obra de Marcelo Huerta y Claudio Líbano, para quienes delito informático … "son 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 [9]". Sin perjuicio de lo cual no debe entenderse que toda utilización de un sistema informático deba necesariamente considerarse delito informático, dada su especialidad, pudiendo perfectamente presentarse casos de delitos comunes cuya ejecución, si bien puede cometerse por otros medios, se facilita o mejora con la utilización de un computador.

Para los autores Marcelo Huerta y Claudio Líbano, la delincuencia o criminalidad informática es el género, dentro de los cuales, cuando se encuentra expresamente tipificada la conducta se puede hablar de delito informático en particular, siendo el fraude una especie. El término Delito Informático abarca o comprende diversas conductas ilícitas, y no una única general, y la definición que se pretenda efectuar de los mismos necesariamente debe ser una definición operativa y flexible, que permita en definitiva ir cubriendo el avance de los medios de comisión de conductas delictuales

---

[8] Morales Rios, Hernando, Ponencia en Congreso para la Enseñanza del Derecho, Madrid España, mayo de 1989 citado por Abedrapo Bustos, Eduardo, ley N º 19223 sobre Delitos Informáticos. Memoria elaborada en 1996 para optar al grado de Licenciado en Ciencias Jurídicas y Sociales de la Universidad de Chile, página 34.

[9] Marcelo Huerta Mirada, Claudio Líbano Manssur. Ob cit. Pág.116.

en uso de las nuevas técnicas de la informática que vayan surgiendo con el desarrollo de la tecnología [10] .

Se debe tener presente eso si que no es exclusivamente el uso de computadores lo que caracteriza la delincuencia informática, en el sentido que da lo mismo si el computador es el medio, instrumento u objeto material del delito, sino que lo trascendente es precisamente la especificidad de los medios tecnológicos involucrados, siendo los delitos que con mayor frecuencia se dan en la criminalidad informática los de sabotaje informático, alteración de datos, espionaje informático, fraude informático (pharming), piratería informática (phishing, vishing), delitos de hacking directo e indirecto, entre otros y que se verán más adelante en mayor detalle.

Por su parte el autor Gustavo Balmaceda Hoyos rechaza la utilización de la nomenclatura "delito informático" que se utiliza por la doctrina para referirse a las conductas desarrolladas por medios informáticos, por cuanto indica que no se puede definir lo que comprende cabalmente la informática y porque el tipo penal en sí no existe a su juicio, prefiriendo elegir más bien un concepto funcional y de criminología como el de los que hablan de "criminalidad informática". Sostiene que no puede ser llamado delito porque no hay texto legal expreso que lo tipifique como tal, y por las innumerables formas de comisión no podrían expresarse claramente en un tipo penal definido[11].

Cabe mencionar que el origen general de las figuras constitutivas de la delincuencia informática esta dado por el mal uso o abuso de los sistemas informáticos y que surgen principalmente a partir de la década de los ochentas con el incremento de los avances tecnológicos[12] y con surgimientos de nuevos perfiles de

[10] Marcelo Huerta Mirada, Claudio Líbano Manssur. Ob cit. Pág.110-111.

[11] Gustavo Balmaceda Hoyos. El delito de Estafa Informática . Ediciones Jurídicas de Santiago, año 2009, páginas 60 y stgs.

[12] Hernán Silva Silva. Las Estafas. Doctrina y jurisprudencia y derecho comparado. Editorial Jurídica de Chile año 1996. Pág. 228.

delincuentes, los que por lo general y por las particularidades de esta delincuencia son sujetos instruidos, con amplios conocimientos en materia informática y económica.

Bien jurídico protegido

Como señala el profesor Juan Bustos Ramírez [13] el bien jurídico "es una fórmula sintética de lo que se protege realmente" siendo sus presupuestos las relaciones sociales, las posiciones que en ellos ocupan los individuos, su intermediación con las cosas y otros entes y la interacción que se produce entre ellos, reconociéndose que se trata de una relación dinámica. Esta protección de un bien jurídico puede darse de variadas formas y no solo en el ámbito penal, lo cual claramente dependerá de las políticas criminales del lugar, lo que implica que puede existir un bien jurídico digno de protección sin la existencia de un delito, pero todo delito debe tener un bien jurídico preciso y concreto que proteger, lo cual implica la necesidad de una revisión constante de los tipos penales especiales e ir analizando si requieren en un tiempo o sociedad determinada de recurrir para su protección o no de las herramientas de protección penal, lo cual es y debe ser la ultima ratio analizando si sancionar penalmente tiene sentido o implicaría un perjuicio mayor .

En cuanto a los bienes jurídicos que los delitos informáticos protegen se puede indicar que ello dependerá de la postura que se adopte en cuanto a su tratamiento penal, así en aquellos casos en que se estime que los delitos informáticos no están regulados en forma diferente o especial sino que deben irse ajustando a las figuras penales clásicas, el bien jurídico protegido estará dado por aquel bien jurídico asociado al delito común base, por el contrario, en aquellos casos en que exista legislación especial que aborde el delito informático deberá considerarse aquel bien que conforme a la norma misma o la historia de su establecimiento dicha norma tiende a proteger, tal es el caso por ejemplo de nuestra Ley N º 19223 que establece diversas figuras penales de delitos informáticos, y en que se establece un bien jurídico novedoso, cual es la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un

[13] Juan Bustos Ramírez, Obras Completas Tomo I Derecho Penal Parte General, Ara Editores, año 2005, Pág.132.

sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan[14].

Para los autores Magliona y Lopez, doctrinariamente la delincuencia informática se caracteriza por estar constituida por delitos pluriofensivos, en que se afectan bienes jurídicos diversos, entre ellos, no solo la calidad, idoneidad y pureza de la información conforme se señala en la historia de la Ley N º 19223 sino que también se afecta el derecho de propiedad de la información de los sistemas de tratamiento de ella, el patrimonio, el orden socioeconómico, la confianza pública, etc., haciendo presente que dichos bienes jurídicos implican en general una tendencia a dar protección a intereses macro sociales y que afectan a la colectividad en su conjunto como por ejemplo, " la confianza en el funcionamiento de los sistemas informáticos" sin perjuicio de la afectación a los bienes jurídicos clásicos ya señalados [15].

Clasificación de la delincuencia informática y conductas más comunes

En cuanto a las clasificaciones de los delitos informáticos, y siguiendo en este punto a los autores Marcelo Huerta y Claudio Líbano, podemos indicar los siguientes grupos de delitos informáticos, reiterando que sus posibilidades de comisión son infinitas e irán en evolución conforme avanza la tecnología, en primer lugar el llamado fraude informático, los delitos de espionaje informático, de sabotaje informático, delitos de piratería de programas, delitos de hacking, entre otros[16] .

Sin perjuicio de lo cual y por un tema de análisis podemos mencionar la clasificación que da al respecto la Convención de Delitos Informáticos del Consejo de Europa del año 2001 en la cual atiende a la naturaleza del atentado u objetivo, así agrupa en cuatro grandes categorías este tipo de delincuencia a saber, aquellos

[14] Historia de la Ley N º 19.233 Boletín Oficial N º 412-07 de la Honorable Cámara de Diputados y Senado de Chile.

[15] Magliona Markovich, Claudio Paul. López Medel, Macarena Ob. Cit. Pág. 65.

[16] Marcelo Huerta Mirada, Claudio Líbano Manssur. Ob cit. Pág123.

delitos contra la confiabilidad, la integridad y la disponibilidad de los datos y sistemas informáticos, dentro de los cuales encontramos el espionaje, sabotaje, las bombas lógicas, los virus, etc; delitos de Fraude informático, delitos por su contenido, como lo serían los delitos en que se difunde material pornográfico infantil y delitos relacionados con la infracción a la ley de propiedad intelectual y sus derechos.

Fraude Informático

Surge esta figura por la ineficiencia de los tipos clásicos principalmente la estafa para cubrir con sus elementos aquellas defraudaciones en que se utilizaban medios tecnológicos y en especial, si bien en un comienzo se le trataba como una simple estafa se dieron cuenta los tratadistas que de la aplicación de esta figura básica surgían interrogantes muy complejas de subsanar como lo eran principalmente el cuestionamiento en materia de los elementos básicos de este tipo penal, sin que se pudiese dar una respuesta totalmente satisfactoria a la imposibilidad de sustentar que una máquina podía realmente entenderse engañada y producto de ello incurrir en un error y la consecuente disposición patrimonial, si el engaño y el error son procesos mas bien del orden sicológicos y exclusivos de las personas naturales, sin los cuales no existe el delito en comento.

Para los autores Claudio Magliona y Macarena López el fraude informático se define " como aquella defraudación que comprende todas las conductas de manipulaciones defraudatorias, abusos o interferencia en el funcionamiento de un sistema de tratamiento automatizado de datos, con la intención maliciosa de obtener un provecho, para producir un perjuicio económico, no necesariamente material, cuantificable" [17], siendo requisito para estos autores que debe existir previamente una defraudación, es decir, el hecho debe ocasionar un perjuicio económico, no necesariamente individual, irrogado mediante un comportamiento astuto o engañoso, esto es, un medio fraudulento que en el caso puntual de estos delitos sería la manipulación informática, siendo precisamente estos elementos los que en un caso determinado nos permitirán distinguir entre este tipo de ilícito y otro figura sea clásica o

[17] Magliona Markovich, Claudio Paul y López Medel, Macarena , ob. Cit., p 189.

bien de otras de las conductas comprendidas dentro del concepto amplio de criminalidad informática.

Se puede indicar que es el delito informático más común o mejor dicho, que se presenta con mayor frecuencia, esta especie de delito informático se caracteriza por cuanto implica una motivación de índole patrimonial, es decir, la finalidad del autor es obtener una ventaja y ocasiona un perjuicio patrimonial en la víctima, al igual que el resto de los delitos informáticos se comete mediante la utilización y/o manipulación de medios informáticos, sea a nivel de entrada de información (input), sea a nivel de manipulaciones de contenidos de programas, o de los resultados de la información (output) etc., pero siempre ocasionando un perjuicio patrimonial, unido a la existencia propia del elemento base en materia de fraude, esto es, el engaño. Dentro de ejemplos de manipulaciones que suelen utilizarse para estos fraudes podemos indicar las siguientes: " Data diddling¨, consistente en introducir datos falsos al sistema informático para obtener una ventaja patrimonial, como podría ser un pago de un beneficio que no correspondía, o indicar datos falsos de cargas familiares para el pago de un seguro social estatal, el pago esta bien calculado pero sobre la base de una información falsa, introducida en forma ilegal y con el ánimo de defraudar, la técnica llamado " caballo de Troya" que consiste en introducir a un sistema computacional instrucciones a objeto de que en base a ellas el sistema computacional ejecute actividades no autorizadas; la " Técnica del salami", es una técnica muy utilizada y que implica manipular los programas para que procesen erradamente datos que han sido ingresados en forma correcta, es decir, se alteran las instrucciones de ejecución de un programa computacional con miras a obtener una ventaja patrimonial, suele usarse para transferencias sistemáticas de pequeñas sumas de dinero, que pueden no descubrirse tan fácilmente cuando ella se dan conforme a la ejecución del programa, siendo una de las razones de su alta eficacia el hecho de que las operaciones digan relación con montos pequeños lo que hace que generalmente pasen desapercibidos, apostando este tipo de técnicas a lucrarse a costa de procesos reiterados y masivos pero de baja entidad si se consideran individualmente; " El Superzapping, es una técnica de manipulación de programas que proviene de un programa diseñado por IBM para cambiar partes de un programa computacional, y como es de fácil

accesibilidad es usado para fines defraudatorios, alterando partes del programa; “Manipulaciones en el output ” es una técnica que implica que se alteran en forma maliciosa los datos de salida, esto es, los resultados del proceso[18] , las bombas lógicas, que son programas que se insertan en un sistema computacional a fin de que en un tiempo determinado o bien cuando se den determinadas circunstancias inicien su actividad, presentan el gran problema que al diferir sus efectos dificulta la investigación y la detección del autor quien generalmente la insertó cuando tenía acceso al sistema, por ejemplo se da mucho en aquellos empleados de una empresa que son despedidos y usan esta técnica a modo de venganza[19].

Para el autor Gustavo Balmaceda Hoyos [20] la estafa o fraude informático protege el mismo bien jurídico que la estafa clásica pero contra conductas diversas, es decir, ambos protegen el “ patrimonio individual microsocial” la diferencia esta en el tipo de conductas, la estafa clásica la protege frente a conductas engañosas y la informática frente a las manipulaciones informáticas, lo cual le sirve de argumento para sustentar su inclusión en la legislación penal ya existente en materia de defraudaciones, y no un delito de los llamados de apropiación ya que indica que existe distinción entre el patrimonio como bien jurídico protegido en los delitos contra el patrimonio, del patrimonio entendido como objeto material de un delito patrimonial, y si hacemos esta diferencia podríamos concluir que esta figura no puede ser sancionada como hurto u otro delito similar.

Phishing

[18] Marcelo Huerta Mirada, Claudio Líbano Manssur. Ob cit., pág. 124-132.

[19] Hernán Silva Silva. Las Estafas. Doctrina y Jurisprudencia y Derecho Comparado. Editorial Jurídica de Chile año 1996, pág.226 y stgs.

[20] Balmaceda Hoyos, Gustavo. “El Delito de Estafa Informática”. Ediciones jurídicas de Santiago año 2009 , p.115-117.

En cuanto a esta modalidad delictual se puede resumir que se conoce como tal al robo de datos personales, el lograr obtener datos de terceros sin derecho para ello usando diversas modalidades tecnológicas, siendo generalmente el envío de correos electrónicos, el envió de páginas Web falsas que hacen creer al destinatario que están operando en páginas legítimas y por ende entrega información que en otro caso no entregaría, información que es usada con fines o intereses económicos, ya que generalmente es para fraudes, esto es, lograr usar dichas claves para obtener un enriquecimiento patrimonial ilegítimo[21]. Dentro de este concepto amplio de robo de datos podemos incluir dos nuevas modalidades que han surgido con el avance de la tecnología y análisis de los casos más frecuentes, a saber, el llamado Pharming, esto es, la modificación fraudulenta que se efectúa en el sistema computacional de "resolución de nombres", es decir, la manipulación al proceso de conversión de un nombre a una dirección IP lo que permite el desvío del usuario a una página Web falsa y obtener así sus datos e información necesaria para efectuar fraude, y la otra técnica es la conocida como Vishing, en que la obtención fraudulenta de datos personales se efectúa mediante una combinación de técnicas de envío de mail fraudulentos con llamados telefónicos o mensajes de texto a fin de hacerle creer al usuario que es estrictamente necesaria la modificación o revisión de sus datos para evitarse un perjuicio patrimonial y lograr que ingresen a páginas falsas y obtener ilícitamente la información necesaria.

Espionaje Informático

El espionaje informático es una especie de delito informático que consiste básicamente en la obtención de información de forma ilegítima, no autorizada, independiente de la finalidad perseguida, desde un sistema de tratamiento de la información[22]. En la doctrina se indica que este delito no requiere un animo especial

[21] Veronica Rosenblut Gorodinsky. Punibilidad y Tratamiento Jurisprudencial de las Conductas de Phishing y Fraude Informático. Artículo publicado en la Revista Jurídica del Ministerio Público N º 35, pág. 254.

[22] Marcelo Huerta Mirada; Claudio Líbano Manssur. Ob cit Pág. 132-133.

diverso al ánimo real de obtener información no autorizada, cuestión que como se indicó, implica una de las grandes diferencias con el fraude informático, en el cual si se requiere ánimo de lucro y perjuicio patrimonial, en contrario podemos mencionar al autor Español Romeo Casabono para quien es esencial que se tenga un ánimo especial en materia de espionaje, cual es el de obtener una ventaja de naturaleza económica [23].

Dentro de las modalidades más frecuentes que se han conocido en materia de espionaje informático podemos indicar el "wiretapping" esto es, la obtención no autorizada de información mediante la interceptación de las redes de comunicación, "el piggybacking", consiste en mediante engaños hacerse pasar por una persona autorizada y obtener la información necesaria para la comisión del delito informático.

Sabotaje Informático

El sabotaje informático para los autores Marcelo Huerta y Claudio Líbano esta constituido por aquellas conductas que "atentan contra la integridad de un sistema de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en el [24]". Este delito afecta el soporte lógico del sistema, caso contrario, si se afecta el soporte material no estamos hablando de un delito informático sino simplemente de un delito común de daño.

El principal problema que presente este delito, y en general los delitos informáticos, es que estas conductas ilícitas no dejan huellas, son de muy difícil detección e incluso pueden cometerse a distancia, lo que trae aparejada la gran dificultad para determinar su autor y el lugar físico de ejecución que determina la competencia de los tribunales llamados a conocer de ellos.

Dentro de las modalidades usadas para el sabotaje informático se pueden indicar - entre otras- las de " crash programs", que son programas que afectan los soportes

[23] Romeo Casabona, Carlos María, Poder Informático y Seguridad Jurídica, pág. 141 citado por Claudio Magliona y Macarena Lopez, ob. Cit. Pág 58.

[24] Marcelo Huerta Mirada; Claudio Líbano Manssur, ob.cit., pág.139.

lógicos de un sistema de información generalmente en forma reiterada en el tiempo y con distancia espacio-temporal, " bombas lógicas", son programas que se insertan a los sistemas de tratamientos de la información para que bajo una condición o en un tiempo determinados se activen y produzcan la destrucción del mismo, surgió esta técnica generalmente por los mismos fabricantes de los programas computacionales como una forma de asegurar el pago de sus derechos y la no utilización en caso de incumplimiento, pero a nivel doctrinario en el mundo se ha discutido la validéz de esta técnica cuando es usada por el propietario ya que implica el hacerse justicia por propia mano y vulnerar los sistemas de protección de derechos civiles especialmente, los "programas virus", son programas creados para la destrucción y alteración de sistemas de información, tienen la capacidad de copiarse, reproducirse e instalarse en sistemas muy variados y a gran velocidad, con un alto nivel de daño, siendo detectables ya cuando el daño está ocasionado por lo que reviste vital importancia el fortalecimiento de los sistemas de protección y seguridad para evitar sus efectos más que una represión ex post[25] .

En los delitos de sabotaje informático es el sistema de tratamiento de la información el objeto del delito, sus conductas como se dijo tienden a la destrucción o inutilización sea del programa que contiene la información, sea de la información misma.

Alteración de datos

La "Alteración de datos" como tal generalmente es comprendida por algunas legislaciones como parte integrante del llamado sabotaje informático como en Alemania y otros en cambio como Francia y ahora luego de la Ley N º 19223 en nuestro país se consideran como figuras diversas incluso a veces agravadas y como su nombre lo indica implica alterar o modificar los datos contenidos en un sistema de tratamiento de la información.

[25] Marcelo Huerta Mirada; Claudio Líbano Manssur. Ob. Cit., pág. 138-150.

Otro de los ejemplos clásicos de la delincuencia informática es la llamada piratería informática, consistente en la copia ilegal de los programas con la intención de obtener un enriquecimiento económico.

Hacking

En materias de delitos de hacking podemos señalar que se les conoce como tal en general a los accesos no autorizados a sistemas de tratamiento de la información por jóvenes fanáticos en la computación y sin mayor tecnología, el hacking propiamente tal sería este simple acceso no autorizado para satisfacción personal, una especie de logro del hackers, pero hay que tener presente que puede darse que este acceso sea con la finalidad de cometer otro delito y se reconduciría conforme a la intención del agente a las otras figuras delictuales ya vistas o bien al fraude.

Para los autores Magliona y Lopez el simple hacking por muy sencillo e inofensivo que parezca si constituye delito, un delito informático cuando logran descifrar las claves que le permitan el acceso aun en el evento de que por cualquier razón no lleguen efectivamente a conocer el contenido de la información almacenada en ese sistema de tratamiento de la información, aunque reconocen que nuestra Ley Nº 19223 no sanciona este simple acceso sin consecuencias.

Objeto Material

Punto aparte en materia de aspectos relevantes de la delincuencia informática lo encontramos en la determinación para cada caso de cuál es el objeto material del delito y cuál es el objeto jurídico. Al respecto es importante recordar estas diferencias básicas, así el " objeto material de la conducta u objeto de la acción es la cosa o persona sobre la que recae la acción" en tanto el objeto jurídico del delito ... " es el objeto de tutela o bien jurídico", este nunca puede faltar aunque en concepto de Politoff si podría faltar el objeto material como lo sería en el caso de la omisión de denuncia, en los delitos contra la seguridad del Estado, en que se sanciona por envío de noticias

las que no son lógicamente objetos en el sentido de una cosa corporal, por su parte el bien jurídico es el fundamento de la incriminación, es la sustancia de sancionar una conducta determinada y no va expresamente establecido o descrito en el tipo penal [26]. Por lo tanto el objeto material dependerá en cada caso del tipo de delito de que se trata y de su modalidad de comisión, pudiendo ser un programa computacional determinado, una base de datos, un ordenador, etc

II.2.- Aspectos generales en materia de investigación de los hechos constitutivos de la delincuencia informática

La investigación y consecuente acreditación de los delitos en general no es una tarea tan sencilla, surgen problemas cuando el hecho descrito como delito es cometido por diversas personas en tiempos y lugares distintos principalmente en la delincuencia de cuello y corbata lo que se ve reflejado en la tendencia legislativa moderna de simplificar frente a nuevas figuras complejas las exigencias de prueba y reducir los elementos subjetivos, dentro de ello, los delitos económicos, dentro de los cuales podemos comprender los delitos informáticos materia de este estudio. Son por regla general delitos de peligro, como así lo reconoce el profesor Juan Bustos [27] en que el sujeto activo ya adopta por su especial ubicación en el sistema una posición de garante evitando así entrar en distinciones entre delitos de acción u omisión, generalmente es suficiente en ellos una puesta en peligro del bien jurídico que protegen, pero según don Juan Bustos se trata de delitos de simple peligro concreto, no abstracto, ya que de estimar lo contrario implicaría presumir de derecho la puesta en peligro del bien jurídico y con ello la responsabilidad penal lo que en nuestro derecho es inaceptable a la luz de lo previsto en el artículo 19 Nº 3 de nuestra Carta Fundamental .

[26] Sergio Politoff, Jean Pierre Matus, Maria Cecilia Ramirez, obra citada página 190.

[27] Juan Bustos Ramírez, Obras Completas Tomo II, año 2005 Ara Editores, Derecho Penal Parte General. Pág. 599 -600 .

En estos delitos lo normal es que se utilicen para su comisión los correos electrónicos y las páginas Web y representan el aspecto negativo de las innumerables ventajas del avance de la informática. Generalmente el nivel de denuncias es bajo dado que son delitos que no dejan huellas visibles a una persona común, permiten la utilización por parte del delincuente de los mismos medios tecnológicos para eliminar registros y con ellos elementos de prueba suficientes para su persecución, se descubren generalmente al azar y cuando sus efectos ya se han desplegado, ello principalmente debido a la falta de mecanismos preventivos suficientes, dado su alto costo, y por la falta de conocimientos específicos y experticia en materias tecnológicas de las personas que tienen acceso a esta información y a cuyos ojos se desarrollan estas conductas fraudulentas como asimismo del investigador y juzgador llamado a conocer de ellas.

Otro punto en contra es que estos delitos generalmente afectan o involucran a personas jurídicas a quienes les generan en sí grandes pérdidas económicas y quienes se abstienen de denunciar, por cuanto evalúan como un aspecto altamente negativo para su imagen comercial el que públicamente se vean como sujetos vulnerables de este tipo de criminalidad, lo cual implica reconocer ante la comunidad que sus sistemas no son confiables y con ello es mejor soportar la pérdida ocasionada por el delito pero prevenir nuevos hechos reforzando específicamente sus sistemas, lo cual resulta inoperante dado como se indicó el avance cada día mayor y rápido de las tecnologías y la habilidad e imaginación del delincuente para burlar estos sistemas de seguridad, unido al hecho de que generalmente se cometen en una serie de actos, hay separación espacio-temporal entre el hecho y el efecto y entre el sujeto y el lugar en que se produce el efecto del delito.

Ante esta problemática notoria se han planteado por parte de la doctrina posibles soluciones, así se ha indicado por algunos, como Claudio Magliona y Macarena López Medel que para hacer frente a este problema los sistema penales pueden tener dos líneas gruesas de solución, en primer lugar, estimar que los tipos penales tradicionales son suficientes para abarcar estas nuevas formas de criminalidad en que se considera que el computador es un instrumento más de comisión delictual y

sancionarlos conforme a dichos tipos penales o bien considerar que lo informático requiere de una especificidad propia y por lo tanto deben crear leyes especificas que sancionen estas nuevas formas delictuales o bien complementen las ya existentes, dando esto autores como ejemplo el caso Chileno cuando se dictó en el año 1993 la Ley N º 19223 sobre Delitos Informáticos, como un intento de regular estas materias, la cual a su vez critican de ser una ley incompleta, y atentatoria de la seguridad jurídica por tratarse de una Ley extra código[28].

En materia de iter críminis o fases de desarrollo del delito también es importante tener en cuenta las particularidades de este tipo de delincuencia y la forma en cómo se pueden concretar, como asimismo la postura que se adopte en cuanto a los tipos penales aplicables a cada caso, a fin de determinar si es posible o no sancionar estas conductas en aquellas etapas llamadas imperfectas, así las cosas, si se entiende que en el caso puntual de un delito informático se estima que se trata de un delito material o de resultado o un delito formal, si estimamos que se trata de un delito de resultado, esto es, de aquellos que requieren para su consumación que exista un efecto, una consecuencia asociada a la acción del agente surgen problemas de causalidad consistentes en definir las bases o presupuestos por medio de los cuales se va a entender en dicho caso que el resultado es la consecuencia directa del actuar del agente, problema de suma importancia en estos delitos en que por sus modalidades tecnológicas de ejecución generalmente no hay claridad en la intervención directa y simple de un agente, sino que más bien son varios los que intervienen en el resultado final y varias las acciones desplegadas para su ejecución, lo que asimismo complica la investigación penal, problemática que se reduce en el caso de estimarse que se trata de un delito formal, esto es, que se consuma sin necesidad o exigencia de un resultado determinado siendo suficiente la ejecución de la acción descrita en el tipo constituyendo el resultado más bien fases de agotamiento.

Por lo general y como se explicará más en detalle más adelante estimo que los delitos informáticos por regla general pueden encuadrarse dentro de la clasificación de

[28] Magliona Markovich, Claudio Paul. López Medel, Macarena. “Delincuencia y Fraude Informático” Derecho Comparado y Ley N º 19223. Editorial Jurídica de Chile año 1999, p 81.

delitos de resultado, surgiendo con ello la gran problemática de causalidad, imaginemos por ejemplo, un delito cometido en el ciberespacio en que para su consumación intervienen en forma virtual diversas personas o bien se ejecuta en diversas acciones que en conjunto logran el resultado final, en tal evento debemos investigar y tender a analizar la existencia o no de los presupuestos de las teorías que solucionan esta problemática, dentro de las cuáles podemos indicar como las reconocidas las siguientes: La teoría de la equivalencia de las condiciones o de la condictio sine qua non, para cuyos partidarios todas las causas que contribuyen al resultado son equivalentes y para poder determinar si contribuyen o no debe hacerse un ejercicio mental de supresión de forma tal que si la elimino y a causa de ello se modifica el resultado era efectivamente una causa, de lo contrario no, teoría introducida por el jurista Alemán Maximilian Von Buri[29].

Esta teoría de la equivalencia de las condiciones es duramente criticada por Politof, crítica que se basa principalmente en la imposibilidad de con cierto grado de certeza jurídica poner un límite a la cadena causal, produciéndose a su juicio el peligro y la situación anómala de que de seguirla estrictamente se podría sancionar bajo sus supuestos a gente inocente, y que no define ni logra diferenciar aquella causa jurídicamente relevante de aquella que no lo es[30].

Actualmente para solucionar estos conflictos en nuestro sistema penal se privilegia la teoría de la imputación objetiva de Clauss Roxin[31]. Teoría que en complemento de la ya vista de la equivalencia de las condiciones, viene a objetibisar y a establecer diferencias jurídicas de las causas, haciendo en definitiva exigible para imputar un resultado a una conducta que esta conducta objetivamente analizada se enmarque dentro del ámbito de riesgo de atentado al bien jurídico creado por el autor,

---

[29] Von Buri, Maximilian, Uber causalitat und diren veran twortung, 1873, citado por Van Hattum, W.F.C. en Van Bemmelen, J.M citado por Politoff obra citada pág. 176.

[30] Politoff Sergio, Jean Pierre Matus, Maria Cecilia Ramírez, obra citada, página 178.

[31] Roxin, Claus, Strafrecht.allgemeiner teil. Banel I Grundlagen der Aufban Der Vebrechen slhre, 3º edición Munich 1997 citado en Politoff, Sergio, Jean Pierre Matus, María Cecilia Ramírez, obra citada página 178.

esto es, el autor con su conducta objetivamente pone en peligro el bien jurídico y el resultado es objetivamente encuadrable dentro del riesgo creado con ello, en límites objetivos, y que ese tipo de riesgos es precisamente desaprobado por el ordenamiento jurídico, por la norma.

Por último un aspecto también que se presenta con cierta relevancia en este tipo de delincuencia por su especial forma de ejecución es la existencia de problemas concursales principalmente cuando existen reiteraciones de conductas que aisladamente pueden ser vistas o consideradas como un delito único o bien cuando la conducta puede encuadrarse en más de un tipo penal. Como indican los autores Politof, Matus y Ramírez citando a Jescheck [32]se presenta esta problemática de que un hecho es susceptible de ser abarcado por distintos tipos penales precisamente cuando estamos en un sistema penal basado en el principio de legalidad como el nuestro, que de no ser de esta forma no habrían problemas por cuanto existiría una única norma infringida y por ende aplicable, a saber, la llamada infracción al derecho.

En este punto y más que analizar las normas del artículo 74 del Código Penal es importante tener claridad en lo que debemos entender del concepto "un mismo hecho" en tal punto para los autores Politoff, Matus y Ramírez, citando a Etcheberry"[33] "un único hecho es la unidad espacio temporal dentro de la cual se realiza al menos un tipo penal. Si, además, en esa misma unidad espacio temporal se realizan los presupuestos de otro u otros tipos penales entonces decimos que ese hecho constituye dos o más delitos, salvo las excepciones". Esto básicamente recogiendo la normativa de los artículos 74 y 75 del Código Penal, excluyéndose de tales reglas los casos de delito continuado, de la llamada unidad natural de acción, y de los delitos permanentes, habituales o de emprendimiento.

[32] Politoff Sergio, Jean Pierre Matus, Maria Cecilia Ramírez, obra citada, página 445.

[33] Politoff Sergio, Jean Pierre Matus, Maria Cecilia Ramirez, obra citada, página 449.

III PUNIBILIDAD DE DE LOS DELITOS COMETIDOS POR MEDIOS INFORMATICOS

II.1.- ¿Son punibles en Chile los delitos cometidos por medios informáticos y en especial el fraude informático?

Como punto de partida, es importante recoger la idea ya sustentada en el Mensaje con que el Gobierno presento el proyecto de Código Penal al Parlamento, en el que ya en esa época se reconoce como una necesidad básica el adecuar el sistema penal al avance social, al desarrollo social, tendiendo a llenar vacíos legales frente a conductas hasta ese entonces desconocidas, a fin de asegurar el ejercicio de las libertades individuales y los derechos garantizados por la constitución, es decir, ya desde el mensaje de nuestro Código Penal se vislumbraba esta necesidad de adaptar el derecho penal al cambio, necesidad que claramente se ve reflejada frente al surgimiento de la delincuencia informática y sus innumerables y novedosas formas de comisión.

Asimismo, es importante tener presente que la Ley en nuestro Derecho Penal es la única fuente inmediata y directa, conforme se reconocen en los artículos 19 N º 3 inciso 7 y 8 de la Carta Fundamental y artículos 1º inciso 1º y 18 del Código Penal, lo cual implica que solo la ley establece delitos, por lo tanto, si la conducta no esta descrita en la ley es impune en nuestro derecho, por muy reprochable que sea, y ello es corolario del principio de seguridad jurídica que nos gobierna[34].

Por último y como cuestión previa al análisis mismo de la punibilidad de estos hechos en nuestro derecho cabe recordar el principio básico en materia penal de prohibición del uso de la analogía *in malan partem*… "la leyes penales son de derecho estricto y su aplicación no puede ser extendida a otros casos diversos de aquellos

[34] Sergio Politoff , Jean Pierre Matus A.; María Alicia Ramírez G. " Lecciones de Derecho Penal Chileno, Parte General. Editorial Jurídica de Chile año 2004 página 94.

expresamente contemplados por el legislador[35]". Así por muy semejante que sea la conducta no es posible aplicar analogía en materia penal para sancionar conductas similares a la descrita en una norma, no obstante lo cual si es posible la analogía cuando ello beneficia al imputado como por ejemplo en materia de excusas legales absolutorias, ello según opinión de los autores citados Politos, Matus y Ramírez aunque reconocen oposición a esta postura en Etcheberry, para quien incluso la analogía favorable esta prohibida[36]. Por lo tanto viene a ser una herramienta de mucha utilidad para estos casos complejos y novedosos la aplicación de las reglas de interpretación de la ley penal para ver si un tipo penal comprende o no estas nuevas modalidades delictuales, teniendo siempre presente la posibilidad de recurrir en esta tarea al espíritu de la ley reflejada en la historia fidedigna de su establecimiento y bajo un método sistemático para armonizar una norma con el conjunto de preceptos que se relacionan a ella, teniendo siempre como referencia al bien jurídico protegido.

Teniendo claros estos puntos de partida, nos corresponde analizar si esta criminalidad se encuentra o no regulada en nuestra ley penal, es decir, si son ante nuestro derecho delitos propiamente tales, y en tal caso dilucidar cuáles son precisamente los tipos penales comprensivos de estas conductas modernas.

En relación a la punibilidad o no de los delitos cometidos por medios informáticos y teniendo presente la diferenciación ya expresada en los capítulos anteriores en orden a establecer que la delincuencia informática es el género y el fraude informático es la especie, conforme posición mayoritaria, encontramos a nivel doctrinal la postura del profesor Gustavo Balmaceda Hoyos, para quien y sin perjuicio del caso especial de la Ley sobre el Uso Fraudulento de Tarjetas Magnéticas del año 2005 y la Ley N º 19223 sobre " Delitos Informáticos del año 1993 en Chile no existe legislación que regule la delincuencia informática y en particular no hay texto expreso

---

[35] Sentencia de la Excelentísima Corte Suprema de 27 de Mayo del año 1952 en RDJXLIX, 2º parte , sec.4º, p. 135 citada en Sergio Politoff , Jean Pierre Matus A.; María Alicia Ramírez G. " Lecciones de Derecho Penal Chileno, Parte General. Editorial Jurídica de Chile año 2004 página 99.

[36] Sergio Politoff , Jean Pierre Matus A.; María Alicia Ramírez G. " Lecciones de Derecho Penal Chileno, Parte General. Editorial Jurídica de Chile año 2004 página 100.

en materia de “estafa informática”, delito que para este autor reviste especial relevancia dado el avance y masividad de los medios tecnológicos informáticos en la actualidad y a su especial naturaleza de constituir delitos “ transnacionales”, es decir, cuya ejecución y efectos trascienden las fronteras físicas de un país[37]. Por lo tanto a falta de texto expreso que regule la materia y abordando en particular el caso de la estafa informática, para él el problema se debe centrar en determinar si la figura clásica del delito de estafa es una figura penalmente suficiente para sancionar las defraudaciones por medios informáticos o caso contrario, es necesario una legislación complementaria y tales conductas resultarían impunes.

Este autor sostiene que no es necesaria nueva legislación para sancionar las estafas informáticas por cuanto a su juicio la figura de la estafa clásica es una figura comprensiva de este tipo de conductas, aunque su parecer es minoritario. Parte de la base de que la razón de que la postura mayoritaria en la doctrina niegue la suficiencia de la estafa clásica para sancionar por dicha vía la estafa informática es que se basan en una concepción errada de los elementos tradicionales de este delito, indicando que dado el avance de los medios informáticos y de las relaciones sociales deben readecuarse las interpretaciones que se dan para hacer inclusivos en la estafa clásica este tipo de conductas que utilizan para defraudar los medios informáticos y propender más que a una legislación nueva en la materia a una colaboración internacional que facilite la investigación y persecución de tales conductas, citando como un buen ejemplo en la materia la Convención de Budapest del Cibercrímen de fecha 23 de Noviembre del año 2001 establecida en el seno de la Unión Europea, sin perjuicio de reconocer que es una realidad ajena a nuestro sistema dado que Chile al menos hasta abril del año 2008 no habría suscrito dicha convención por nuestro país, la cual entró en vigencia en julio del año 2004[38].

Así para este autor y partiendo del supuesto que la estafa informática es punible bajo la figura clásica hace presente una segunda problemática a abordar al respecto y que viene dada por la especial naturaleza de estos delitos, en que, por regla

[37] Balmaceda Hoyos, Gustavo. “ El Delito de Estafa Informática”. Ediciones jurídicas de Santiago año 2009 , p. 32.

[38] Balmaceda Hoyos, Gustavo, Ob. Cit., pp 38-39.

general, los hechos que la constituyen permiten su repetición y su ejecución reiterada en forma automatizada y que por ende, siguiendo las clasificaciones tradicionales de los delitos se podría decir que se tratarían en general de delitos de los llamados "delitos continuados" o bien "delitos de comisión instantánea y de efectos permanentes".

Frente a esta repetición de conductas plantea como solución el distinguir si en el caso puntual existe una única intervención del sujeto que activa un proceso posterior de repetición automático, o existen varias intervenciones que generan la repetición de procesos, en el primer caso sostiene que la solución es considerar la conducta como un hecho único y negar la existencia de delito continuado y para el segundo caso plantea el reconocimiento de la aplicación de las reglas del delito continuado aún en el evento de que se afecten a diversas personas siempre y cuando se den los otros requisitos clásicos de este tipo de categoría delictual, a saber, que la reiteración de conductas se de en un contexto determinado y que subjetivamente exista unidad de propósito criminal[39].

Por su parte para los autores Claudio Paul Magliona Markovich y Macarena Lopez Medel, efectivamente hubo un cambio grande en la sociedad a través de la masificación del uso de medios computacionales que implicó en definitiva el aumento del riesgo en materia de criminalidad, dentro de las cuales el género es la delincuencia informática y una especie de este es el "fraude informático", reconociendo que la solución chilena inicial de subsumir este fraude en la figura clásica de estafa fue cada día mayor, pero que ello se esta descartando en el derecho comparado por ser considerado insuficiente, llegando incluso ellos a la conclusión y dada la fecha de su trabajo, esto es al año 1999 que en Chile y motivado por las omisiones de la ley Nº 19223 el fraude informático no puede ser castigado penalmente, dado que las figuras

[39] Balmaceda Hoyo, Gustavo, Ob. Cit. , p 74 y ss.

de dicha ley no lo comprenden en forma expresa y no es posible aplicación supletoria de la figura de estafa clásica[40].

Para esos autores el simple hacking por muy sencillo e inofensivo que parezca si constituye delito, un delito informático cuando logran descifrar las claves que le permitan el acceso aun en el evento de que por cualquier razón no lleguen efectivamente a conocer el contenido de la información almacenada en ese sistema de tratamiento de la información, aunque reconocen que la Ley N º 19223 no sanciona este simple acceso sin consecuencias[41].

Ellos sostienen que el engaño y su consiguiente error, ambos elementos característicos de toda estafa, están limitadas al ámbito de las personas naturales por ser considerado el error estrictamente como un elemento psicológico y por lo mismo estiman que por regla general no se podrá dar este elemento en los fraudes informáticos en los que en general no es una persona la que es engañada, salvo en aquellos casos en que el computador no es mas que un medio auxiliar en la toma de decisiones, caso en el cual el engañado sería la persona que utiliza este medio auxiliar para decidir la posterior disposición patrimonial y por ende se podría aplicar el tipo penal de la estafa clásica, es decir, estos autores apoyan la concepción sicológica del error y niegan con ello la posibilidad de engañar a una máquina, incluyendo en esta imposibilidad también aquellos casos en que en el proceso intervienen personas pero sin que dichas personas tengan poder real de decisión sino que más bien con una intervención mecanizada por los procesos de trabajo y sin conocimiento de lo que implican los datos manipulados, esto es, sin influencia en su comportamiento.

Concluyen entonces que nuestra estafa no abarca el fraude informático y tampoco lo hace la Ley N º 19223, en este último caso basan su opinión en la historia de la Ley en que del análisis de las discusiones planteadas durante su tramitación, las

[40] Magliona Markovich, Claudio Paul. López Medel, Macarena, “Delincuencia y Fraude Informático” Derecho Comparado y Ley N º 19223. Editorial Jurídica de Chile año 1999, pp. 13 y ss.

[41] Magliona Markovich, Claudio Paul. López Medel, Macarena, ob. cit., pág. 63.

indicaciones del entonces Ministro de Justicia don Francisco Cumplido de pretender abarcar con esta legislación el fraude informático no fueron acogidas por los informes de la comisión de Constitución, Legislación y Justicia[42], como segundo argumento para dicha conclusión es que la Ley N º 19223 tiene su fuente inspiradora en la Ley Francesa del año 1988 que no contempla el fraude informático y como tercer argumento indican el texto mismo de la ley en que no se contemplan los elementos propios del fraude en general y menos el informático en particular[43]. Es más niegan posibilidad a la tesis de aplicar a estos casos las figuras del hurto y de la apropiación indebida, señalando en resumen que a su juicio la solución pasa por que tales conductas constitutivas de delincuencia informática, mas bien de fraude informático sean expresamente reguladas mediante una reforma legal a nuestro Código Penal y con un articulado propio e inclusivo de la estafa pero especifica en sus elementos característicos.

En posición contraria a esta postura rígida de que la Ley N º 19223 no regula el fraude informático la encontramos en la posición de Alejandro Vera Quilodrán, quien señala que si se encontraría tipificado el fraude informático , específicamente en el artículo 3º de la citada Ley aunque sin ahondar en mayores argumentaciones que sustenten dicha postura[44] .

Por su parte y en una posición mixta encontramos la postura de don Eduardo Abedrapo Bustos, quien sostiene que eventualmente podrían reconducirse los casos de fraude informático a las figuras descritas en los artículos 2º y 3º de la Ley N º 19223 cuando además de los elementos de dichas figuras se persiga otra finalidad que

[42] Boletín Oficial N º 412-07 de la Honorable Cámara de Diputados y Senado de Chile, Primer Informe de la Comisión de Constitución, Legislación , Justicia y Reglamento, p. 3906, citado por los autores Magliona Markovich, Claudio Paul. López Medel, Macarena, ob. cit. , pág 230.

[43] Magliona Markovich, Claudio Paul. López Medel, Macarena, ob. cit., pág. 227 y ss.

[44] Vera Quilodrán, Alejandro A. Delito e Informática. La informática como Fuente del Delito. Ediciones Jurídicas La Ley, Santiago, Chile 1996, p.108.

abarque los elementos de la defraudación, para lo cual invita a realizar una aplicación extensiva de dichas normas [45].

En relación a los casos especiales, podemos ir mencionando los más relevantes para ver su tratamiento penal, así por ejemplo en materia de transferencias electrónicas de fondos fraudulentas para la mayoría de la doctrina constituyen una modalidad de fraude informático y entrarían dentro de la discusión ya vista de si es posible o no comprenderlo dentro de las figuras clásicas.

Tratándose de las conductas efectuadas por medios de cajeros automáticos, por ejemplo, por el uso de tarjetas falsas o sustraídas se señala por la mayoría de la doctrina que no siempre constituyen un fraude informático aunque si se encuentran dentro de la llamada delincuencia informática, existiendo hasta el año 2005 toda una discusión doctrinaria en la materia en cuanto al tipo penal aplicable, dado que a falta de regulación especial se trataba de subsumir el uso de cajeros automáticos con tarjetas falsas por ejemplo en la figura clásica de la estafa con toda la problemática que de ello deriva y que vimos con antelación y que incluso se discutía que se trataba de conductas atípicas, asimismo surgían problemas en cuestionarse si de aceptarse la aplicación de la figura penal de la estafa debería también aceptarse la existencia de concurso con las figuras de las falsificaciones, principalmente en el caso de retiro de fondos de un cajero por uso de una tarjeta falsificada, o los casos de clonación.

Siguiendo este orden de ideas se discutía además qué tratamiento debía darse a aquellas situaciones accidentales en que hay aprovechamientos de sucesos ajenos a la voluntad inicial del hechor, como por ejemplo un error bancario o un desperfecto del cajero, para los autores Magliona y Lopez dichas conductas no constituyen fraude informático sino mas bien se trata de una problemática propia del ámbito civil y en aquellos casos en que se trataba de uso abusivo de tarjetas y para evitar la impunidad de tales conductas reprochables y salvar la problemática que trae

[45] Abedrapo Bustos, Eduardo, Ley N º 19223 sobre Delito Informático, Memoria Elaborada en 1996 para optar al grado de Licenciado en Ciencias Jurídicas y Sociales de la Universidad de Chile, p-70 .

aparejada el subsumirlas dentro del tipo penal clásico de la estafa, se sancionaban en algunos casos como un caso de robo con fuerza en las cosas, siguiendo para ello el modelo Español y nuestra legislación asimilando la ficción existente en materia de llaves fictas con la fuerza y éstos con el uso de tarjetas falsificadas o hurtadas, asimilar tales circunstancias[46], no obstante lo cual hoy podemos decir que gran parte de estas discusiones tendrían solución con la entrada en vigencia de la Ley N º 20009 de marzo del año 2005, que establece en forma expresa conductas constitutivas de delito informático asociado al uso fraudulento de tarjetas bancarias.

Por último y dado que el phishing es uno de los delitos que se presentan con mayor frecuencia veremos en este punto y en forma general si es posible o no sancionar en nuestro derecho este tipo de conductas, para ello se ha sostenido que es primordial antes de delimitar si es o no punible el phishing en si mismo ver y analizar en particular cuál fue precisamente la modalidad empleada para la obtención fraudulenta de datos y en su caso el objetivo de la misma, así las cosas y como se verá en detalle más adelante al analizar la ley respectiva, en aquellos casos en que la modalidad de ejecución ha implicado alteración o modificación de programas o más bien de sistemas de tratamiento de la información sería sancionable en las figuras penales del sabotaje informático del artículo 1º de la Ley N º 19223 caso contrario debe analizarse si es posible configurar o no un fraude, un delito de estafa y entra en juego la discusión ya planteada en cuanto a esta figura penal, en relación a este punto encontramos la opinión de la abogada Veronica Rosenblut Gorodinsky, para quien es perfectamente sostenible la existencia del engaño y del error característicos de las estafas clásicas en una conducta de phishing, salvando ya dos de los grandes cuestionamientos que se plantean a la penalización del fraude informático mediante el uso de la figura clásica de estafa, pero cuestiona o más bien reconoce que existe duda en cuanto a la posibilidad de determinar como efectiva disposición patrimonial por parte del sujeto engañado el mero hecho de entregar sus datos personales y con ello relacionarlo con el perjuicio, dado que estos, es decir, los datos personales, las claves, en si mismos y que son la conducta de disposición efectiva realizada por el engañado, no tienen valor económico en si, lo mismo se cuestiona la posible solución

[46] Magliona Markovich, Claudio Paul. López Medel, Macarena, ob. cit., pág 202.

que se daría al caso en que salvado lo anterior, el que obtiene en forma fraudulenta la información o phisher no usa la misma para defraudar sino que la vende a un tercero para que éste otro cometa delito[47]. Incluso podría darse el caso de que se cuestione la existencia de concursos sea de leyes penales o bien concurso de delitos, real o medial, lo cual deberá ser resuelto judicialmente analizando caso a caso.

No obstante lo ya dicho, es importante recalcar como se verá en los ejemplos de sentencias que se exponen en este trabajo, que independiente de las discusiones doctrinarias en la materia nuestros tribunales de justicia en el último tiempo se han inclinado por hacer aplicable al fraude informático la figura de la estafa calificada por el medio engañoso, esto es , la estafa del artículo 468 del Código Penal, e incluso, en aquellos casos en que la modalidad de comisión es precisamente una conducta informática de espionaje o sabotaje han aplicado las reglas relativas al concurso material y a veces medial entre la estafa y el delito especial de espionaje o sabotaje contemplado en la Ley N º 19223[48].

III.2.- Legislación existente en la materia

En materia de legislación aplicable a la delincuencia informática mencionaremos en este trabajo en primer lugar cuál es la realidad general o sistema de regulación existente en los países cuyas legislaciones han servido de sustento a nuestra legislación penal, a saber España, Francia, Alemania e Italia, en lo que a sus aspectos generales se refieren para luego ver cuál es precisamente nuestra realidad nacional y analizar las leyes que rigen actualmente en nuestro país, sean de índole internacional, sean de carácter nacional .

---

[47] Veronica Rosenblut Gorodinsky. Punibilidad y Tratamiento Jurisprudencial de las Conductas de Phishing y Fraude Informático. Artículo publicado en la Revista Jurídica del Ministerio Público N º 35, pág. 258.

[48] Veronica Rosenblut Gorodinsky. Punibilidad y Tratamiento Jurisprudencial de las Conductas de Phishing y Fraude Informático. Artículo publicado en la Revista Jurídica del Ministerio Público Nº35, pág. 260.

En cuanto a la forma de abordar penalmente la delincuencia informática no existe un sistema único al respecto, hay países que simplemente han trabajado sobre la base de complementar sus figuras clásicas, otros han creado figuras especiales y otros han utilizado sistemas mixtos de complemento y legislación especial, haciendo presente que en materia internacional se han realizado esfuerzos para atacar este tipo de criminalidad, un buen ejemplo a mencionar es el Convenio sobre Cibercriminalidad del Consejo de Europa del 23 de Noviembre del año 2001 el cual esta abierto a países no miembros de la Comunidad Europea y que en nuestro caso aún no hemos adherido estando en etapa de estudio, normativa internacional que contempla una serie de medidas a los miembros para que adecuen sus legislaciones a la represión de esta moderna forma de criminalidad.

En el caso de España, este país se ha preocupado del tema de la delincuencia informática y ha optado por la técnica legislativa de complementar sus figuras básicas clásicas y adaptarlas a estas nuevas realidades, así en el Código Penal se contemplan figuras especiales que regulan este tipo de ilícitos, ello cuando se refieren a ataques al sistema de tratamiento de la información, dado que los atentados a los soportes físicos que contienen dicha información se rigen por las figuras clásicas, como el delito de daños. En cuanto a la figuras constitutivas de delincuencia informática que contempla el Código Penal Español podemos indicar entre otros, el sabotaje informático, la protección de datos sensibles de una empresa como una especie de espionaje informático, protección asociada a ordenadores, la desprotección de programas computacionales mediante dispositivos especiales, la piratería asociada a ordenadores, la estafa cometida por medio informático, en este caso haciendo mención a que el uso de medios informáticos en el Derecho Penal Español se encuentra inserto en el concepto de "uso de manipulación informática o artificio semejante " y que se comprende en ello el engaño y el error, es decir, no exige elementos subjetivos independientes por la especial características del delito , debiendo tratarse de una transacción no consentida, que en el caso de las manipulaciones informáticas dicen relación con órdenes de traspaso patrimonial sin derecho legítimo para ello, aunque se limitan estas figuras a las transferencias electrónicas de fondos, regula además el uso de tarjetas de créditos en forma fraudulenta y de cajeros automáticos, en el caso de

las tarjetas bancarias con la particularidad esta legislación de contar con norma expresa, esto es, el artículo 239.5 del Código Penal Español que hace equiparable el uso fraudulento de tarjetas bancarias al uso de llaves falsas y lo sanciona expresamente como robo con fuerza en las cosas, solución que como hemos visto en este trabajo, ya estaban dando nuestro tribunales de justicia para estos casos antes de la dictación de nuestra ley especial al efecto [49].

En Francia se regula la delincuencia informática en el Código Penal pero con un capítulo especial con figuras especiales de esta delincuencia, sin perjuicio de estimar como comprensivo de la figura clásica de estafa el fraude informático, para lo cual se estima comprensivo del termino " maniobras fraudulentas" al uso de técnicas informáticas para defraudar, no exigiendo por ello elementos subjetivos adicionales y evitando así las controversias que en nuestro sistema existen en materia de posibilidad de engañar a una máquina por ser el engaño y en consecuente error elementos meramente subjetivos y relativos a la persona humana[50].

Por su parte el derecho Alemán ha avanzado bastante en la regulación de la delincuencia informática creando legislación especial y mediante variadas reformas legales complementando y/o modificando su Código Penal, en la actualidad por ejemplo contempla normativa especial, figuras especiales de espionaje de datos, estafa informática, engaño en el tráfico jurídico mediante sistemas de procesamientos de datos, sabotaje informático.

Similar situación a la anterior se contempla en Italia, país en el cual su Código Penal contempla expresamente figuras de delincuencia informática como lo es el acceso abusivo a un sistema informático, la difusión de programas dirigidos a producir daños o interrumpir un sistema informático, falsificación informática, espionaje

[49] Informe " Delitos informáticos en la Legislación de España, Francia, Alemania e Italia" Patricia Canales. Sección de estudios Biblioteca del Congreso Nacional . Santiago de Chile , Julio del año 2004. Depesec /bcn/serie informe años XIV. Pág. 2 y ss.

[50] Informe " Delitos informáticos en la Legislación de España, Francia, Alemania e Italia" Patricia Canales. Sección de estudios Biblioteca del Congreso Nacional . Santiago de Chile , Julio del año 2004 . Depesec /bcn/serie informe años XIV. Página 31 y ss.

informático, fraude informático con un sistema de pena conforme la calidad del agente en relación al medio empleado, esto es, a diferencia de otros países que como se indicó regulan figuras especiales de delincuencia informática pero mantienen el fraude como comprensivo en el tipo penal clásico de estafa, Italia establece un tipo penal especialmente regulado al efecto, una figura bastante novedosa a mi juicio es el artículo 392 del Código Penal Italiano, norma que regula la figura de ejercicio arbitrario del derecho, o llamado ejercicio arbitrario de la propia razón con violencia sobre programas informáticos, esto mas bien referido a aquellos casos en que se utiliza técnicas violentas de destrucción de sistema más allá de lo legítimamente permitido, dándose el ejemplo del titular de un software que coloca una bomba de auto destrucción en caso de querer ser copiado pero que se extienda sus efectos más allá de dicha protección, ese daño adicional estaría cubierto por esta figura a fin de evitar un abuso del derecho.

Leyes Chilenas que penalizan la delincuencia informática

En Chile y más allá de las discusiones ya vistas en orden al alcance o no de las figuras clásicas para abarcar la penalidad de la delincuencia informática, lo cierto es que se han dictado dos grandes leyes que tratan directamente o indirectamente este tipo de delincuencia, sin perjuicio de la aplicación a casos constitutivos de dichos ilícitos de normas del Código Penal y de otras leyes especiales como en materia de derechos marcarios y que serán analizadas en tales aspectos, dichas leyes por orden cronológico la encontramos en la Ley Nº 19223 sobre Delitos Informáticos y la Ley N º 20009 sobre tarjetas de crédito bancarias, esta última de una forma indirecta, por cuanto como se dirá, dentro de las modalidades de comisión que se establece en su articulado es perfectamente posible que se utilicen medios informáticos y por ende se pueda calificar de delincuencia informática directa o bien que concurra en concurso con figuras propias de la Ley N º 19223.

Análisis de la Ley N º 19223

La primera Ley dictada en Chile y que aborda en forma expresa la criminalidad informática es la Ley N º 19223 sobre Delitos Informáticos, ley promulgada el 28 de Mayo del año 1993 y que entró en vigencia el 07 de Junio del mismo año, fecha de su publicación en el Diario Oficial, legislación que se origina de una moción parlamentaria del Diputado Jose Antonio Viera-Gallo quien reconociendo la realidad social de la época en orden a la masificación de los sistemas computacionales de tratamiento de la información y la necesidad de legislar frente a este avance con el objeto de asegurar el nuevo bien jurídico que surge como digno de protección, esto es, la …" calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan [51]". No obstante lo anterior y ser el primer intento de una legislación especial aplicable a la delincuencia informática, entendida en general como aquellas conductas ilícitas que se ejecutan por medios informáticos, principalmente computadores, es una ley que ha resultado ser insuficiente por sus limitados alcances, ello a juicio del profesor Luis Ortega Quiroga[52], en especial por entender que dicha ley no incluye figuras de bastante ocurrencia como lo es el fraude informático propiamente tal, sin que este totalmente claro si se trato de una simple omisión del legislador o bien si fue una acción adrede por estimar nuestro legislador penal que si estaría incluido en su articulado este tipo de figuras o por ultimo si fue una omisión intencionada por estimar nuestro legislador que para el fraude informático no se requería a la fecha ley nueva siendo susceptible de encuadrar tal figura en los tipos penales comunes, en especial, en la figura de estafa.

Esta Ley a juicio de los autores Magliona Claudio y Macarena López, protege un bien jurídico tanto personal como social, en este último caso, se traduce en la confianza que la comunidad tiene en los sistemas informáticos, y sus tipos penales

[51] Boletín oficial N º 412-07 de la Honorable Cámara de Diputados y Senado de Chile, pp 1903-1904.

[52] Prólogo a la obra de Magliona Markovich, Claudio Paul. López Medel, Macarena , "Delincuencia y Fraude Informático" Derecho Comparado y Ley N º 19223. Editorial Jurídica de Chile año 1999

son pluriofensivos, afectando además de los bines jurídicos novedosos ya indicados bienes jurídicos clásicos como la propiedad de la información, la privacidad de las personas, la fidelidad en la custodia de un sistema informático, entre otros [53].

En cuanto a los fundamentos tenidos en vista para la dictación de esta ley se pueden indicar principalmente tres, a saber, primero que se quiera o no era un hecho cierto que a esa época ninguna organización social podía estar ajena a los avances en materia de informática y prescindir de ella , más bien, se podía apreciar que cada día existía mayor dependencia a su utilización, segundo, que el avance de estos modernos medios tecnológicos no solo estaba trayendo beneficios a la sociedad sino además que estaba haciendo surgir delitos nuevos, desconocidos hasta entonces en sus modalidades de comisión, surgiendo como estrictamente necesario el ajustar nuestra legislación para reprimir este tipo de conductas, todo ello tendiendo a proteger nuevos bienes jurídicos que con tales avances se fueron presentando, por último se basa en el reconocimiento general de que para la mayoría de nuestra doctrina y jurisprudencia para abordar estas nuevas formas de criminalidad la figuras clásicas no era suficientes y su aplicación no estaba exenta de cuestionamientos de peso, por todo lo cual se hacía necesario legislar.

Esta ley contempla dos grandes tipos penales que a su vez se subdividen en subtipos según sea el objeto de protección, así tenemos la figura del sabotaje informático, sea contra el sistema de tratamiento de la información o sus partes integrantes, contra el funcionamiento del sistema y contra los datos contenidos en él; el delito de espionaje informático con una arista de obtener y conocer la información y otra de difundirla, con figuras agravadas en relación a la calidad del agente.

[53] Magliona Markovich, Claudio Paul. López Medel, Macarena , “Delincuencia y Fraude Informático” Derecho Comparado y Ley N º 19223. Editorial Jurídica de Chile año 1999, pp 135 y ss

Sabotaje Informático de la Ley N º 19223

Se encuentra regulada esta figura en los artículos 1º y 3º de la Ley N º 19223 cuyo texto indica lo siguiente:

"Artículo 1º: 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 3º: 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.

Sujeto activo

En cuanto a sujeto activo, este delito no requiere una calidad especial en el sujeto activo, puede ser cualquiera, aunque se reconoce que generalmente se trata de personas con alto nivel de conocimiento en materia informática.

Conductas punibles

En relación a las conductas que constituyen este tipo penal se puede indicar la destrucción de un sistema de tratamiento de la información o sus partes integrantes, esto abarca el soporte lógico o software, y en cuanto al soporte físico o hardware es discutido si se incluye o no en este delito, o bien si su penalidad queda reservada para las figuras clásicas como la del delito de daños, versus quienes sostienes que en base a la historia de la ley y a la definición del término " componentes" que da la RAE se

podrían incluir, no obstante lo cual la opinión prevalente es que se regule el soporte físico conforme las figuras clásicas y en tal caso surgirían problemas de concurso aparente de leyes penales que deben ser solucionados judicialmente conforme los principios generales del derecho como lo sería el de especialidad; Inutilización de un sistema de tratamiento de la información o de sus partes o componentes, es decir, hacer que ya no funcionen o no presten la utilidad propia que tenían, sea total o parcialmente a consecuencia de la conducta del sujeto; Atentar contra el funcionamiento del sistema de tratamiento de la información, sea impidiendo o imposibilitando que funcione, que lo haga en forma inadecuada o bien mediante su modificación, este término usado en sentido amplio comprensivo de toda alteración a éste.

Existe en materia de sabotaje informático como se dijo una figura agravada contemplada en el inciso 2º del artículo 2º de la Ley N º 19223 que consiste en aumentar la penalidad cuando a raíz de la conducta constitutiva de sabotaje se ocasiona daño a los datos contenidos en el sistema de tratamiento de la información, sin que se delimite expresamente la entidad de este daño para la determinación de la sanción, cuestión que debe ser resuelta judicialmente conforme las normas generales como lo sería el artículo 69 del Código Penal.

Las figuras antes vistas, sean normales o en su modalidad agravada afectan al sistema mismo de tratamiento de la información, pero el artículo 3º de la Ley N º 19223 contempla una modalidad de comisión que guarda relación directa a la información misma contenida en el sistema de tratamiento de la información, es decir, el objetivo perseguido por el sujeto en su actuar es precisamente producir daños en la información y no sólo sería una consecuencia de las demás conductas de sabotaje como se establece en las figuras del artículo primero ya vistas, siendo en este caso las conductas punibles el alterar, destruir o dañar la información, abarcando cualquier cambio en la información, la pérdida definitiva de datos, y cualquier atentado contra la integridad de la información. Para entender esto es importante aceptar que existen diferencias entre la información contenida en un sistema con el soporte lógico que la

contiene, que sería el programa computacional, y de éstos con el soporte físico o CD en que se materializan[54].

Espionaje informático contemplado en la Ley N º 19223

Las figuras de espionaje informático se encuentran reguladas en los artículos 2º y 4º de la Ley N º 19223, cuyo texto indica:

"Artículo 2º : 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 4º: 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[55]".

Sujeto activo

Al igual que en el caso del sabotaje en principio sujeto activo de este delito puede ser cualquiera siempre eso si que no tenga autorización para acceder al sistema de tratamiento de la información.

[54] Oficio N º 422 de fecha 27 de Septiembre del año 2001 del entonces Fiscal Nacional del Ministerio Público Guillermo Piedrabuena Richard. Página 7

[55] Ley Nº 19223 del Ministerio de Justicia sobre Delito Informáticos publicada en el Diario Oficial de Chile el 07 de Junio del año 1993

Conductas Punibles

Este tipo penal es especial por cuanto se requiere que sea ajustado en la forma de comisión a las modalidades que expresamente contempla el legislador, esto es mediante la interceptación, interferencia o acceso indebido, y no cualquier modalidad por medio de la cual se pueda obtener información no autorizada de un sistema de tratamiento de la misma.

Interceptar implica apoderarse de la información mientras se transmite pero sin impedir que llegue a destino, interferir significa cruzarse en el camino de la información con tecnología que le permita obtener esta información en forma ilegítima, información que al igual que en el caso anterior seguirá su destino normal, pero con la diferencia que la información llega al destinatario final en forma distinta, con alteraciones.

Por su parte el acceso comprende el ingreso a un sistema de tratamiento de la información para obtener la información en él contenida, por medio de este acceso puede conocerse toda la información que dicho sistema tenga, lo cual no sucede en las modalidades de interceptación e interferencia, en las cuales sólo se tendrá acceso a la información que en ese momento esta siendo transmitida y no al conjunto. Aspecto común a estas modalidades de espionaje informático es que son conductas cometidas con utilización de medios tecnológicos adecuados para ello y no simple conocimiento al azar de información reservada.

Elemento subjetivo especial

El artículo 2º de la Ley Nº 19223 requiere la concurrencia de un elemento subjetivo especial, esto es, la existencia de ánimo de apoderarse, usar o conocer indebidamente la información, aunque no es necesario que se logre este objetivo para su consumación[56].

[56] Oficio N º 422 de fecha 27 de Septiembre del año 2001 del entonces Fiscal Nacional del Ministerio Público Guillermo Piedrabuena Richard. Página 9.

Este apoderamiento implica obtener la información y comportase en relación a ésta como si fuera su dueño, el usar implica la utilización de la misma, esto es con fines especiales y el conocer es poder interiorizarse del contenido de la información, todo lo cual se requiere sea ejecutado sin derecho, esto entendido en sentido amplio de falta de autorización o requisitos para ello.

Este articulado regula lo que se conoce en doctrina como hacking indirecto, ya que se requiere el acceso con fines determinados siendo impune a la luz de esta ley el hacking directo o el simple acceso sin motivación especial[57].

Delito de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información

Este tipo penal esta contemplado expresamente en el artículo 4º de la Ley N º 19223 cuyo texto ya fue señalado, tiene la limitación especial en cuanto al sujeto activo, ya que por su descripción se requiere que aquel que revela o difunde la información debe haber accedido a ella en forma legítima, es decir, con derecho, y dentro de ello establece una figura agravada en su inciso segundo para aquellas personas que tienen un cargo además de responsabilidad de la seguridad del sistema de tratamiento de la información, ello se justifica por los principios de rigen las normas de reserva de información y que de lógica nos orientan a pensar que no es posible exigirle el mismo nivel de reserva a todas las personas o con relación a toda información. Este delito protege en especial la fidelidad de la custodia de la información.

[57] Oficio N º 422 de fecha 27 de Septiembre del año 2001 del entonces Fiscal Nacional del Ministerio Público Guillermo Piedrabuena Richard. Página 11.

Alcance del término maliciosamente empleado en esta Ley

Las figuras penales que contempla esta ley son tipos dolosos y que además tienen la particularidad de exigir elementos subjetivos adicionales, así los artículos 1,3 y 4 utilizan el término " maliciosamente", exigencia que doctrinariamente ha sido interpretada en forma diversa, así para el profesor Eduardo Abedrapo Bustos citado por los autores Magliona y López, la inclusión de este término en forma expresa por el legislador indica que para éste sólo pueden sancionare las conductas cuando en ello concurre dolo directo, otros autores también citados como Marcelo Huerta Miranda y Claudio Líbano Manzur manifiestan que esta palabra implica sanción a título de dolo directo pero que a diferencia de Abedrapo abarcaría además el llamado " dolo de las consecuencias necesarias", pero ambos coinciden en que en ningún caso pueden aplicarse para estas figuras ni la culpa ni el dolo eventual [58] . En igual sentido se puede mencionar a Jose Rodrigo López Pinto, Ricardo Alberto Coronado Donoso y Pedro Varela Corvalán[59].

En sentido disidente encontramos la postura de don Alejandro Vera Quilodrán, para quien esta inclusión de la palabra " maliciosamente" efectuada por el legislador de la Ley N º 19223 es como en general lo ha resuelto la jurisprudencia un tema netamente de alteración del peso de la prueba, que implica que no se aplica la presunción genérica de dolo del artículo 1º del Código Penal y por lo tanto éste en esos tipos penales deberá ser acreditado[60], posición a su vez compartida por los autores Magliona y López ya citados[61]. Un segundo elemento subjetivo que puede desprenderse de esta ley es la exigencia de un ánimo especial que establece la figura

---

[58] Magliona Markovich, Claudio Paul. López Medel, Macarena, ob. citada, p 147.

[59] López Pinto, Jose Rodrigo; Coronado Donoso, Ricardo Alberto, Varela Corvalán, Pedro Alejandro, " Delitos Informáticos , nuevas figuras penales" Memoria elaborada en 1994 para optar al grado de Licenciado en Ciencias Jurídicas y Sociales de la Universidad Central, p. 80, citado por Magliona Claudio y López Macarena en ob. cit. , p 148.

[60] Vera Quilodrán, Alejandro A., Delito e Informática. La Informática como fuente del Delito. Ediciones Jurídicas La Ley, Santiago, Chile, año 1996, pp 215-216 .

[61] Magliona Markovich, Claudio Paul. López Medel, Macarena , ob. cit., p 156.

del artículo 2º de la Ley N º 19223, esto es, el animo de apoderarse, usar o conocer indebidamente de la información.

Los autores Magliona y Lopez critican esta Ley en diversos aspectos, en primer lugar y como ya se indico se le critica el ser una Ley extra código lo cual afectaría la seguridad jurídica y el fácil acceso a su conocimiento, el hecho de que a su juicio no era necesario crear nuevos tipos penales para abarcar las figuras en ella contempladas sino más bien hubiera sido aconsejable adaptar mediante complementaciones legislativas las figuras clásicas para comprender esta moderna criminalidad, que no se ocupa del problema efectivo que estos delitos presentan en materia probatoria, debiendo a juicio de los referidos autores ser necesario un procedimiento especial que trate la acreditación de este tipo de delincuencia no siendo suficiente el sistema procesal penal vigente a dicha época y que el hecho de que su redacción final abarque conceptos ambiguos confundiendo el sistema informático con el soporte material que lo contiene da lugar a la existencia de concurso aparente de leyes penales con las figuras clásicas que si abarcarían el atentado al soporte material, agregando por último que resulta una ley insuficiente por cuanto a su juicio no regularía el "fraude informático"ni el "simple delito informático" de acceso indebido ajeno a intencionalidad, como son los casos de hacking directo [62].

Para el autor Hernán Silva Silva, esta Ley cuya fuente o antecedente directo es la legislación Francesa del año 1938, efectivamente sería el primer intento nacional por abordar esta delincuencia, estableciendo figuras dolosas y a su juicio de dolo directo excluyendo la posibilidad de sancionar el cuasidelito[63].

[62] Magliona Markovich, Claudio Paul. López Medel, Macarena , ob. Cit., p 174-178

[63] Hernán Silva Silva. Las Estafas. Doctrina, Jurisprudencia y Derecho Comparado. Editorial Jurídica de Chile año 1996. Pág. 232.

Ley Nº 20009

En este acápite del trabajo es interesante mencionar como legislación aplicable en materia de delincuencia informática en nuestro país a la Ley N º 20009 promulgada con fecha 18 de marzo del año 2005 y publicada en el Diario Oficial el 01 de Abril del año 2005, norma que regula o limita la responsabilidad de los usuarios de tarjetas de crédito y débito por el mal uso que hagan terceros frente a tarjetas extraviadas, hurtadas o robadas y establece un tipo penal especial de uso fraudulento de dichas tarjetas, ello en el artículo 5º de la referida Ley cuyo texto indica lo siguiente:

"Artículo 5º: Las siguientes conductas constituyen delito de uso fraudulento de tarjeta de crédito o débito:

a) Falsificar tarjetas de crédito o débito.
b) Usar, vender, exportar, importar o distribuir tarjetas de crédito o débito falsificadas o sustraídas.
c) Negociar, en cualquier forma, con tarjetas de crédito o débitos falsificadas o sustraídas.
d) Usar, vender, exportar, importar o distribuir los datos o el número de una tarjeta de crédito o débito, haciendo posible que terceros realicen operaciones de compra o de acceso al crédito o al débito que corresponden exclusivamente al titular.
e) Negociar en cualquier forma, con los datos o el número de tarjeta de crédito o débito, para las operaciones señaladas en la letra anterior.
f) Usar maliciosamente una tarjeta bloqueada, en cualquiera de las formas señaladas en las letras precedentes.

La pena por este delito será de presidio menor en cualquiera de sus grados.

Esta pena se aplicará en su grado máximo, si la acción realizada produce perjuicio a terceros."

Este tipo penal es un tipo penal abierto en cuanto a las posibilidades de ejecución, dentro de las cuáles perfectamente es posible se ejecuten técnicas propias

de la delincuencia informática y por ende serían casos de sanción directa a la delincuencia informática o bien indirecta cuando se estima la existencia de reglas concursales con figuras expresamente tipificadas como lo serían las del artículo 2º de la Ley N º 19223, por ejemplo en casos de los llamados skimming, en los cuales se copian los datos de bandas magnéticas mediante un acceso no autorizado con el fin de usarlo para efectuar transferencias de fondos fraudulentas, haciendo presente que en el caso de las figuras del artículo 5º de la Ley N º 20009 son delios de mera actividad, esto es, en que no se requiere para su consumación la existencia de perjuicio, no siendo este elemento parte del tipo sino una regla de penalidad ya que se establece en forma expresa que en caso de existir perjuicio a terceros la pena se aplica en su tramo máximo.

III.- 3.- Tipos penales posibles de aplicar en cada caso a la luz de la jurisprudencia

Para abordar el análisis de las respuestas que nuestros tribunales de justicia han dado a los casos de delincuencia informática, recordaremos en primer término los aspectos generales en materia de tipicidad.

En primer lugar debemos decir que el "tipo penal" comprende el conjunto de elementos que integran la descripción legal de un delito. Por su parte la "tipicidad" es la adecuación de una conducta del mundo real a esa descripción legal[64]. Y que en resumen la labor de los tribunales se centra entre otros aspectos, en realizar esta adecuación, para lo cual se basan en las normas legales existentes, en principios generales del derecho, en la doctrina , entre otros elementos.

En esta labor judicial, y del análisis de los fundamentos de las sentencias de nuestros tribunales podemos indicar que para elegir o determinar el tipo penal aplicable

[64] Sergio Politoff L.; Jean Pierre Matus A.; María Cecilia Ramírez G. Lecciones de Derecho Penal Chileno. Parte General. Editorial Jurídica de Chile 2004, p 183.

al caso, y también para defender su competencia, muchas veces los tribunales recurren a las definiciones y clasificaciones que la doctrina ha realizado de los delitos, basadas estas clasificaciones en la forma en que las conductas están descritas en los respectivos tipos penales.

Dentro de estas clasificaciones nos encontramos principalmente con los llamados " delitos simples", esto es, aquellos tipos penales en que el hecho se perfecciona con una acción y en su caso, un resultado, es decir, cuya entera realización es inmediata; " delitos habituales", aquellos en que la conducta descrita sólo se torna punible cuando es reiterada; " delitos continuados", aquellos en que el tipo penal describe conductas individualmente punibles pero que en el caso puntual, por determinadas conexiones la ley permite sancionarlo como un solo hecho; "delitos permanentes", aquellos que crean un estado delictivo, una consumación permanente; "delitos instantáneos de efectos permanentes", esto es, aquellos en que el delito se consuma en un solo acto pero que genera efectos más menos permanentes en el tiempo [65].

Asimismo es importante recordar lo ya expuesto en capítulos anteriores, en orden a tener claridad que los delitos informáticos son delitos especiales que pueden coexistir con delitos comunes, es más muchas veces se confunden, como por ejemplo cuando un delito común, se facilita su ejecución por la utilización de un medio informático, y que para su tratamiento muchas veces será necesario utilizar las reglas aplicables en materia de concursos y en materia de principios básicos como la preeminencia del delito especial por sobre el común.

A continuación se analizarán algunas sentencias de nuestros tribunales de justicia sobre hechos que configuran conductas propias de delincuencia informática a fin de poder determinar cuál ha sido la solución que se le está dando a estos casos y el fundamento de las mismas.

En primer lugar y dentro de la exposición de las soluciones jurisprudenciales a la materia se puede mencionar una sentencia del Tribunal de Garantía de Viña del Mar

[65] Sergio Politoff L.; Jean Pierre Matus A.; María Cecilia Ramírez G. Ob. Cit., pp 188 y sgts.

del año 2005 en que sancionó la alteración de los datos de una tarjeta bancaria y su uso conforme el tipo penal del artículo 5 de la Ley N º 20009 [66].

En el mismo año el Tribunal de garantía de Temuco sentenció un caso de clonación de tarjetas que se suscitó antes de la entrada en vigencia de la Ley N º 20009 como un caso de falsificación documental , considerando la tarjeta en si misma como un instrumento privado mercantil del artículo 197 inciso segundo en relación al artículo 193 del Código Penal y por delito reiterado de espionaje informático del artículo 2 de la Ley N º 19223 [67].

---

[66] **Causa RUC Nº 0500548885-2 RIT 6237-2005**, Sentencia de Fecha 08 de Noviembre del año 2005 dictada por el Tribunal de Garantía de Viña del Mar en Procedimiento Abreviado. Los hechos de la causa dicen relación con la utilización por parte del acusado de una tarjeta de crédito bancaria falsificada, consistiendo la falsificación en la alteración de los datos visibles de dicho plástico, esto es los datos del titular, haciendo aparentar como titular al acusado, datos que diferían a los contenidos en la banda magnética y que eran los legalmente válidos, alteración que permitió fuera usada en el Casino de Viña para adquirir fichas de juego. En esta sentencia se encuadra estos hechos en la figura especial de la letra b del artículo 5 de la Ley Nº 20009 sobre Tarjetas Bancarias, esto es, uso malicioso de tarjeta de crédito falsificada en grado de consumado y en calidad de autor, no existiendo cuestionamiento en cuanto al lugar de comisión de este delito, por cuanto toda la conducta fue desarrollada materialmente en un mismo territorio físico, a saber, el Casino de Viña del Mar.

[67] **Sentencia dictada en procedimiento abreviado en causa RUC Nº 0400172957-3 RIT 1835-2004** por el Tribunal de Garantía de Temuco de fecha 02 de Marzo del año 2005. Esta sentencia tiene la particularidad de referirse al tratamiento jurisprudencial a un caso de clonación de tarjetas bancarias antes de la entrada en vigencia de la Ley N º 20009 que regula expresamente la materia. En cuanto a los hechos que se dan por establecidos dice relación con que el día 15 de Mayo del año 2004 en horas de la tarde los acusados fueron detenidos por ser sorprendidos accediendo subrepticiamente a información codificada de las bandas magnéticas de las tarjetas de débito y crédito de clientes del Banco Estado de una sucursal de la ciudad de Temuco, acciones de acceso a la información que efectuaban con el propósito de poder copiar en otros plásticos y con el uso de las claves de seguridad que ellos obtenían espiando a las víctimas poder generar nuevas tarjetas y sustraerles el dinero de sus cuentas, encontrándoles en su poder diversas tarjetas clonadas entre otros objetos. En este caso el tribunal , haciendo suyas las alegaciones del Ministerio Público y de la parte querellante, estimó que las tarjetas bancarias si debían considerarse instrumentos privados de carácter mercantil, siendo argumento para ello entre otros, la naturaleza de las operaciones que en ella se involucran y las relaciones bancarias, conforme lo ha considerado además el mismo Banco Central , y por ende estimó condenar en este caso por delitos reiterados de Falsificación de instrumento privado mercantil del artículo 197 inciso segundo en relación al 193 N º 1 del Código Penal en grado de frustrado por cuanto no se alcanzó a causar perjuicio efectivo a las víctimas y por delito reiterado de espionaje informático del artículo 2 de la Ley Nº º 19223 en grado de consumado.

Por su parte y en meses cercanos a los aludidos el Tribunal Oral en lo Penal de Rancagua conociendo también de un caso de clonación y uso de tarjetas bancarias previos a la Ley Nº 20009 dio una solución jurídica diversa, esto es, el considerar las tarjetas como asimilables al uso de llaves falsas o sustraídas condenando en definitiva por el delito del artículo 443 N º 2 del Código Penal, y negando en forma expresa la posibilidad de aplicar delito informático de la Ley N º 19223 como fue el caso del tribunal de Temuco, basado en la intencionalidad del autor [68]

En materia de transferencias bancarias fraudulentas, esto es, phishing, se puede mencionar el planteamiento del Octavo Juzgado de Garantía de Santiago de

[68] **Sentencia dictada en Juicio Oral en causa RIT Nº 69-2005 del Tribunal Oral en Lo Penal de Rancagua** de fecha 23 de Julio del año 2005 sobre uso de tarjetas bancarias, referida a hechos cometidos con antelación a la Ley N º 20009 y en la cual se le da una solución jurídica distinta a la ya analizada. El juicio en resumen se refería a cinco hechos, cinco víctimas distintas pero un mismo acusado en la cual se repetía básicamente la conducta de que el acusado se acercaba a personas que estaban efectuando operaciones en un cajero automático con sus tarjetas y aprovechándose de un momento de descuido les cambiaba las tarjetas bancarias por otras falsas que él tenía o bien en uno de los casos la arrebato y se fue del lugar habiendo previamente espiado a las personas y memorizado las claves de acceso al cajero, para posteriormente con dichas tarjetas y claves sustraer dinero desde las cuentas de los afectados ocasionando perjuicio efectivo a las víctimas. Se discutió en este caso la calificación jurídica que debía darse , así por parte del ente acusador se estimó que debía considerarse que la tarjeta bancaria es asimilable al uso de llaves sustraídas y por ende se estaría en presencia de un caso de Robo con Fuerza en lugar no habitado , reiterado y en grado de consumado, por su parte la defensa alegaba la imposibilidad de aplicar esta figura por no haber mediado fuerza en el actuar de su cliente y por la imposibilidad de aplicar en forma analógica las normas legales, que si el legislador hubiere querido incorporar en el concepto de llaves a las tarjetas bancarias lo hubiera efectuado como si lo hizo el Código Penal Español y que la figura legalmente aplicable al caso es el artículo 2 de la Ley N º 19223 y en su defecto el tipo penal de hurto simple , resolviendo en definitiva el tribunal que tales hechos efectivamente eran encuadrables en la figura penal del artículo 443 Nº 2 del Código Penal estimando que las tarjetas bancarias debían ser consideradas dentro del concepto de llaves verdaderas sustraídas u otro instrumento semejante, que dicho tipo penal al respecto en cuanto a instrumento es un tipo penal abierto y que fue precisamente el uso de la tarjeta y de las claves lo que permitió abrir un mueble cerrado y sustraer dinero, en estos casos abrir y/o acceder al cajero automático y sacar el dinero de las cuentas de los titulares, negando posibilidad a la aplicación del tipo penal del artículo 2 de la Ley N º 19223 por cuanto la finalidad del acusado al ejecutar sus conductas y acceder a la información del cajero, que bien podría estimarse éste como un sistema de tratamiento de la información , lo fue con el claro objeto de sustraer dinero de las víctimas y por lo tanto era el medio necesario para su objetivo final.

diciembre del año 2007 en el cual se optó por el tipo penal de Estafa del artículo 468 del Código Penal , no aplicando las figuras especiales de la Ley N º 19223 no por un tema de fondo sino más bien por falta de prueba tendiente a acreditar vinculación de los sujetos con los verbos rectores de los tipos penales especiales, que habría sido la respuesta adecuada al caso [69] .

Por su parte, el Cuarto Juzgado de Garantía de Santiago , en sentencia de Septiembre del año 2010 y conociendo de un caso de phishing compartió el criterio del tribunal anterior condenando como delito de Estafa reiterada del artículo 468 del Código Penal, sin que hubiese mención alguna eso si a la procedencia o no de la aplicación de la Ley N º 19223 como se ha efectuado en otros casos [70].

---

[69] **Sentencia dictada en procedimiento abreviado por el Octavo Juzgado de Garantía de Santiago en causa RUC Nº 0700157424-2 RIT 1745-2007 de fecha 27 de Diciembre del año 2007 :** Los hechos de esta causa dicen relación con que entre fines del año 2006 y mayo del año 2007 diversos clientes de un banco sufrieron transferencias fraudulentas desde sus cuentas a las de terceros o defraudaciones mediante órdenes falsas que se dieron para generar vales vistas a favor de terceros, todo ello a través del mecanismo conocido como phishing esto es, que se capturaba la información sobre claves secretas de los clientes del banco por medio de correos electrónicos falsos con clonación de páginas del Banco y así los clientes entregaban sus datos de claves, datos que luego eran usados por los imputados para girar y hacer transferencias de fondos a su favor y poder retirar dineros, estos hechos fueron calificados por el ente persecutor como estafa del artículo 468 del Código Penal en concurso medial con el delito del artículo 2 de la Ley N º 19223, no obstante lo cual el tribunal, y sin perjuicio de que la defensa no cuestionó la calificación jurídica sostuvo que en el caso de marras sólo se daban los presupuestos del delito de estafa del artículo 468 del Código Penal desestimando la concurrencia del tipo penal especial de la Ley N º 19223 al estimar que faltaron antecedentes para vincular a los sujetos a las actividades precisar de interceptar, interferir o acceder en los términos de dicho tipo penal más allá de la aceptación de los hechos dentro del contexto del procedimiento abreviado.

[70] **Sentencia dictada en causa RUC Nº 0900880251-0 RIT 13685-2009 del Cuarto Juzgado de Garantía de Santiago en procedimiento abreviado, de fecha 08 de Septiembre del año 2010** : Los hechos que se dieron por acreditados en este caso dicen relación con un caso de phishing, y con conductas desplegadas tanto en Chile como en el extranjero, siendo la modalidad de operación que terceros generalmente desde México enviaban mensajes y correos electrónicas engañosos a clientes de cuentas corrientes bancarias en Chile en las cuales al ingresar eran derivados a otra página que simulaba ser del respectivo Banco, logrando mediante engaño que los titulares ingresaran sus datos de claves y cuentas para así efectuar transferencias a cuentas de ahorros de personas que habían sido contactadas con tal objeto en Chile por el acusado y a cambio de una comisión o porcentaje pasaban sus cuentas para el traspaso de dinero fraudulentos cuyo mayor importe era remitido al extranjero, logrando con estas operaciones en el año 2009 y parte del 2010 defraudar a lo menos a 62 victimas

Ejemplo de aplicación conjunta de las figuras de la Estafa del artículo 468 del Código Penal y del delito de Espionaje Informático de la Ley N º 19223 para los casos de pharming lo encontramos en la sentencia dictada en abril del año 2011 por el Juzgado de Garantía de Concepción, al resolver un caso de creación de una página web falsa con intención de acceder a los datos de clientes que permitan lucrarse [71].

Analizando jurisprudencia de casos de lo que se podría llamar estafa informática se puede indicar la sentencia de la Segunda Sala del Tribunal de Juicio Oral en lo Penal de Curicó, la cual en sentencia de Marzo del año 2010 sancionó un caso de engaño para obtener recursos mediante alteración de sistema informático como delito de Estafa en concurso medial con el delito Informático del artículo 1º de la Ley Nº 19223, aunque corresponde hacer presente que se trata de un caso de voto de mayoría [72].

---

distintas. En este caso el ente persecutor calificó los hechos como delito de estafa del artículo 468 en relación al 467 del Código Penal en carácter de reiterado, calificación que fue compartida por el tribunal condenado a dicha persona por el delito de estafa reiterada y en calidad de autor, entendiendo cometido el delito en esta jurisdicción sin indicar mayormente el razonamiento de ello y sin hacerse en este caso discusión en cuanto al principio de ejecución del delito dado que las conductas engañosas que permitieron acceder a la cuentas de los afectados fueron desplegadas desde el extranjero, lo cual de seguirse las normas generales aplicables a la materia se podría decir que el tribunal en relación al principio de ejecución era incompetente, no obstante lo cual se siguió en este caso la teoría de la ubicuidad, esto es, determinar competencia por el lugar en el cual se producen los resultados, en este caso, el lugar en los cuales se efectuaron las transferencias de fondos .

[71] **Sentencia dictada en causa RUC Nº 1010008200-K RIT 2294-2010 del Juzgado de Garantía de Concepción en procedimiento especial abreviado de fecha 13 de Abril del año 2011**: Los hechos de este caso consistieron en que el acusado con ánimo de apoderarse y usar la información contenida en un sistema de tratamiento de información, esto es, datos de cédulas de identidad, claves y cuentas bancarias accedió a dicho sistema , para lo cual creo una página Web falsa que simulaba ser del Banco Santander, la envió mediante correos a varios cuentacorrentistas y estos bajo engaño ingresaron sus claves y datos, datos que por programación previa efectuada a la página por el acusado le eran enviados a su correo y con los cuales pudo efectuar transferencias de fondos a otras cuentas perjudicando a las víctimas . Se estimó por parte del ente acusador que en este caso se configuraban dos delitos informáticos del artículo 2 de la Ley N º 19223 y dos delitos de estafa del artículo 468 en relación al 467 N º 2 del Código Penal, ambos consumados y atribuyendo al acusado participación de autor, calificación que fue compartida por el tribunal estableciendo al efecto relación concursal medial entre los delitos informáticos y las estafas.

[72] **Sentencia dictada con fecha siete de marzo del año 2010 en causa RUC Nº 0910014546-1 RIT 81-2010 por la Segunda Sala del Tribunal de Juicio Oral en lo Penal de**

Por último mencionaré la sentencia dictada en Marzo del año 2008 por el Octavo Juzgado de Garantía de Santiago en el cual se conoció un caso de fraude informático y se calificó como delito de estafa del artículo 468 del Código Penal en concurso con los delitos de usurpación de nombre del artículo 214 del Código Penal y delito especial del artículo 2º de la Ley Nº 19223 [73].

Curico: El caso se refiere a cajeras de un supermercado que idearon un sistema que les permitía impedir u obstaculizar el funcionamiento del sistema informático instalado por la empresa en las cajas y que permitía generar códigos telefónicos de prepago, para eso al efectuar una venta normal ellss ingresaban códigos erróneos que bloqueaban el sistema y mientras se producía el desbloqueo mediante anulación de la operación se producía un tiempo de receso o descontrol computacional de las cajas, tiempo suficiente que permitía generar códigos de PIN telefónicos sin que esto quedara registrado de alguna forma para la empresa y así evitar ser sorprendidas, generando diversos códigos gratuitos para ellas y que la empresa debió pagar a las compañía de telefonía generándose perjuicio por diversos montos . Lo anterior el acusador lo calificó como estafa del artículo 468 del Código Penal en concurso con el delito informático del artículo 1º de la Ley N º 19223 , ambos en grado de consumados, por su parte la defensa alegó falta de pruebas en materia de participación y en lo que respecta a los tipos penales que es lo que nos interesa en este trabajo, señaló la negativa a aplicar el delito de estafa por la imposibilidad de engañar a una máquina como habría sucedido en este caso y en cuanto a la existencia de delito informático que ello tampoco se daría dado que nunca hubo a su juicio alteración efectiva del software el cual siguió funcionamiento como debía . Los sentenciadores de mayoría optaron por condenar por los delitos de Estafa en concurso medial con el delito informático del artículo 1º de la Ley N º 19223, ambos consumados y como autoras , aceptando la existencia de engaño óptimo en el caso de marras, señalado que el engaño estaba dado principalmente en simular ventas falsas mediante estas alteraciones de programas induciendo a error al dueño al creer efectivamente en la legitimidad de las mismas y por ende incurriendo en disposición patrimonial al pagar al tercero por ellas, siendo las cajas registradores el medio empleado para gestionar el engaño doloso de las acusadas ; reconociendo este fallo además los elementos del delito informático, haciendo alusión al bien jurídico protegido y a la amplitud en cuanto al sujeto activo, es decir, que no requiere una calidad especial como trató de hacer entender la defensa , y que frente a la alegación de que el sistema siguió operando y por ende no fue alterado indicaron que si hubo obstaculización lo que implica modificación de su funcionamiento suficiente para configurar el ilícito en cuestión, sin que el tipo penal exija perentoriamente que el sistema deje de funcionar por completo, ya que abarca la figura su modificación en el sentido de alteración que da la RAE. No obstante lo cual hubo voto de minoría en el cual se indicó que se estaba por absolver de la estafa por cuanto no se daban los presupuestos del engaño y del error consecuente propio de este ilícito, dado que se trataba de disposición patrimonial motivada por alteración de un sistema computacional y que en ello no podía entenderse engaño y error, sino solo la figura especial de la Ley N º 19223 ya referida.

[73] **Sentencia dictada en causa RUC Nº 0700444765-9 RIT 3665-2007 del Octavo Juzgado de Garantía de Santiago en procedimiento abreviado de fecha 14 de Marzo del año 2008** : Se refiere este caso a que el acusado haciéndose pasar por otra persona contactó mediante correos electrónicos a una empresa con la cual acordó la compra de un celular y un notebook

IV COMPETENCIA DE LOS TRIBUNALES CHILENOS PARA CONOCER DE LOS HECHOS CONSTITUTIVOS DE DELINCUENCIA INFORMÁTICA Y EN PARTICULAR DEL FRAUDE INFORMÁTICO

IV.1.- Aspectos generales de la competencia de nuestros tribunales

La base para determinar los casos en que la Ley Penal Chilena es aplicable a hechos que revisten carácter transnacional se resumen en texto expreso a los artículos 5º y 6º del Código Penal Chileno en que se reconoce como principio básico la territorialidad, sancionando las conductas cometidas en territorio chileno independiente de la nacionalidad del agente y sólo por excepción los hechos cometidos fuera de su territorio, a saber, los casos contemplados en los artículos 13, 431 y siguientes del Código Orgánico de Tribunales y en leyes especiales, lo cual a su vez determina la jurisdicción de nuestros tribunales de justicia. Para este trabajo, lo central es analizar las complicaciones que este principio tiene en materia del concepto de territorio, concepto que clásicamente es tomado más bien como de orden físico-material, salvo casos especiales en que por una ficción legal se entiende por "territorio"

---

por la suma de 800 mil pesos, debiendo el acusado efectuar para ello transferencia de fondos al dueño de la empresa, acto seguido y con el objeto de obtener dinero el acusado ingreso al sitio Web del Banco de Chile usando fraudulentamente los datos y claves de una titular de cuenta corriente y efectuó transferencia de fondos para pagar el trato con el dueño de la empresa por el computador pasando posteriormente al retiro de las especies, logrando solo retirar el computador ya que el celular no estaba en esos momentos en stock siendo perjudicada la titular de la cuenta bancaria en la suma de 800 mil pesos . Estos hechos el ente persecutor los calificó como estafa calificada por el tipo de engaño, esto es la estafa del artículo 468 en relación al 467, ambos del Código Penal , y de los delitos de " fraude informático" a su juicio previsto y sancionado en el artículo 2 de la Ley Nº 19223 consumado y el delito de usurpación de nombre previsto en el artículo 214 del Código Penal Consumado, en relación a estas calificaciones la defensa sólo se opuso a la existencia de delito informático y a la estafa, en cuanto a la estafa alega que no hay disposición patrimonial ni engaño sin dar mayores argumentaciones y en cuanto al llamado fraude informático no alega cuestiones de tipicidad sino más bien de falta de prueba en cuanto a la intervención de su representado en los hechos, resolviendo en definitiva el tribunal acoger íntegramente la calificación del ente persecutor .

a un lugar que realmente, o más bien físicamente no lo es, como por ejemplo el caso de los buques mercantes chilenos en alta mar para determinados aspectos[74].

Según los profesores Politoff, Matus y Ramírez[75], no existe en nuestra legislación texto expreso que determine en forma precisa cuando un delito se debe entender cometido en nuestro territorio, siendo principalmente tres teorías las aplicables para la solución de esta problemática, a saber, la " teoría de la actividad" por medio de la cual básicamente se sostiene que se debe tener en consideración el lugar del principio de ejecución de la conducta, " teoría del resultado", que sostiene que se debe considerar el lugar en que la conducta desplegó sus efectos propios, y la " teoría de la ubicuidad", la cual sostiene que ante un delito consumado somos competentes tanto si en Chile se dio principio de ejecución o si sólo se produce el resultado punible, esta última teoría recogida por la mayoría de la doctrina y jurisprudencia Chilena como se verá más adelante.

Todo lo anterior debe tenerse presente sin perjuicio de lo establecido en el artículo 302 del Código de Bustamante, del cual somos parte vinculante, norma que establece " cuando los actos de que se componga un delito se realicen en Estados contratantes diversos, cada Estado puede castigar el acto realizado en su país, si constituye por sí solo un hecho punible. De lo contrario, se dará preferencia al derecho de la soberanía local en que el delito de haya consumado" .

No obstante lo anterior, hay casos de excepción en que se aplica la extraterritorialidad de la ley penal chilena, y con ello se amplía la competencia de nuestros tribunales para conocer de ellos, como los descritos en el artículo 6º del Código Orgánico de Tribunales y en leyes especiales como lo es el artículo 3 N º 2,3 y 4 del Código de Justicia Militar pero que no se refieren en forma expresa a los tipos de delito que abarca este trabajo, esto es, a los casos de delincuencia informática.

---

[74] Sergio Politoff L.; Jean Pierre Matus A.; María Cecilia Ramírez G. Lecciones de Derecho Penal Chileno. Parte General. Editorial Jurídica de Chile 2004 pp 19-53.

[75] Sergio Politoff, Jean Pierre Matus, María Cecilia Ramírez, ob cit. , pp 118 y sgts.

IV.2.- Problemas para la determinación del lugar de comisión y ley aplicable a la criminalidad informática, principalmente al fraude informático

Uno de los principales problemas es el carácter de delitos transnacionales, cuyas conductas o efectos se extrapolan al ámbito territorial de un país determinado, surgiendo un concepto nuevo de espacio delictual, el llamado " ciberespacio", definiéndose éste como " un espacio virtual de interacción, un espacio relacional que se constituye a través del intercambio de información, es decir, es espacio y es medio[76]".

El espacio en el cual se desarrollan estos delitos en principio entra en pugna con los principios básicos en materia de aplicación de la ley penal de los países, que por lo general, y como es en nuestro derecho es el de la territorialidad, con una concepción física del territorio. Don Gustavo Balmaceda Hoyos plantea como solución a esta problemática la necesidad de flexibilizar estos principios y conceptos rígidos para permitir el ejercicio jurisdiccional de un país en estos espacios no físicos llamados cíberespacios, siendo la tendencia observada por dicho autor el pasar de este principio rígido a uno comprensivo de este espacio no físico bajo el amparo de los principios de "protección" y de " justicia universal" ello por cuanto la simple colaboración internacional no ha sido ni será suficiente[77].

En el caso de los catedráticos Politoff, Matus y Ramírez, ellos plantean como solución el poder aplicar el principio de " Universalidad", esto es, aquellos casos en que se permite aplicar la ley chilena y se le da competencia a nuestros tribunales a casos cometidos fuera de nuestro territorio por afectar bienes jurídicos de relevancia universal, bienes que deben tener, eso si, a lo menos consagración a nivel de tratados internacionales que sean vinculantes para nuestro país, tratado que debe implicar la

[76] Balmaceda Hoyos, Gustavo. Ob. cit., pág. 60.

[77] Balmaceda Hoyos, Gustavo. Ob. cit., pág. 84.

obligación al Estado de perseguir e idealmente tipificar el delito asociado a ese bien jurídico[78].

El lugar del hecho delictivo determina en principio la ley aplicable y la competencia de los tribunales de un Estado. Para Juan Bustos Ramírez [79] en los llamados "delitos a distancia" la teoría más aplicable y que satisface las exigencias prácticas es la de la ubicuidad.

Por lo ya dicho en materia de determinación de legislación aplicable y competencias debe "jurídicamente" y no "físicamente" ubicarse espacialmente al hecho constitutivo de estafa o de criminalidad informática para solucionar estas problemáticas. Si toda la conducta se ejecuta en un país rige el principio de territorialidad y se aplica la ley de ese país y hay que analizar entonces el tribunal competente sobre las normas generales de competencia, en nuestro caso, sobre la base de la aplicación como se señaló del artículo 157 del Código Orgánico de Tribunales que no es otro que el del lugar en que se inició la ejecución del hecho, esto es lo básico pero no es lo que pasa normalmente, los problemas surgen cuando se ejecutan las conductas que conforman el tipo penal en diversos lugares, o bien los resultados ocurren en un lugar distinto incluso en el extranjero.

En estas materias es importante la postura que refleja la doctora en derecho Claudia Cárdenas Aravena, quien aborda esta problemática en relación específicamente a los llamados ciberdelitos, esto es aquellos delitos cometidos a través de Internet, que ciertamente y como se vio constituyen gran parte de la delincuencia informática, quien sostiene que si bien este tipo de delincuencia no escapa en materia de determinación de lugar de comisión a las reglas generales y teorías generales aplicables al respecto, como lo es la del principio de territorialidad, por sus características requiere una interpretación más abierta de los conceptos tradicionales en materia de lo que debe entenderse por lugar de comisión y/o lugar de

[78] Sergio Politoff, Jean Pierre Matus, María Cecilia Ramírez, ob cit., pp 123-125.

[79] Juan Bustos Ramírez, Obras Completas Tomo I Derecho Penal Parte General, Ara Editores, año 2005, pág 606-607.

la ejecución de un delito, es decir, con mayor amplitud a aquellos delitos cometidos simplemente en lugares territoriales definidos, esto por cuanto son cometidos en un lugar indeterminado conforme los parámetros tradicionales de lo que es el territorio, esta amplitud jamás debe llegar al extremo de hacer que estos delitos tengan una persecución sin límites y de carácter universal, ello por la inseguridad jurídica que implica esta situación, por la vulneración de derechos de los inculpados y particularmente por cuanto si bien son conductas reprochables penalmente no revisten la gravedad y los presupuestos que se han definido tradicionalmente para sustentar las normas que en materia de persecución extraterritorial y más bien dicho universal existen en la materia, lo cual esta claramente reservado para casos extremos como lo es por ejemplo el genocidio[80] .

Para Balmaceda Hoyos debe tenerse en consideración los elementos del derecho internacional público y los principios universales que sustentan incluso la aplicación extraterritorial de la ley por razones de interés superior como lo serían los principios de personalidad, protección y de justicia universal, e indica como una solución básica la distinción del tipo de delito, así, tratándose de un delito de resultado se puede aplicar la teoría de la ubicuidad siendo entonces competente y se aplica la ley del lugar en que efectivamente ese resultado se produce, pero en los llamados delitos " de contenido" hay soluciones diversas, unos abogan por el lugar en que el autor ejecuta un acto tendiente a la realización del tipo y otros por los efectos o ubicación de la víctima.

Para Balmaceda y basado en su planteamiento de que la estafa informática es de igual naturaleza que la estafa tradicional y por ende puede clasificarse en un delito de resultado en que generalmente éste estará dado por la transferencia de fondos no consentida será el lugar en que éste se produce el que rija la competencia y la ley aplicable[81], para lo cual sostiene que no puede estarse al concepto clásico de disposición patrimonial dado que en la estafa informática es diverso por su propia

[80] Cárdenas Aravena, Claudia. "El lugar de comisión de los denominados ciberdelitos" . Política criminal N º 6 año 2008 (www.políticacriminal.cl)
[81] Balmaceda Hoyos, Gustavo. Ob. cit, pág 99-100.

naturaleza e implica como se indicó para este autor toda transferencia no consentida de activos patrimoniales, o en su caso, tratándose del resto de la criminalidad informática por el lugar donde se produce la alteración del funcionamiento del sistema informático, aplicando la teoría de la ubicuidad pero con modificaciones en orden a exigir una vinculación de relación territorial con el lugar físico del resultado objetivo dando como ejemplo que se use un sitio de ese lugar, su idioma, y así salvar los cuestionamientos en materia de seguridad jurídica.

Al respecto es importante señalar la declaración efectuada en el Convenio sobre Cibercriminalidad del Consejo de Europa celebrado en Budapest el 23 de Noviembre del año 2001, del cual aún no somos parte, pero en el que se establece como principio básico que todo país en cuyo territorio se produzcan los efectos causados por el delito informático tendrá competencia para investigarlo y perseguirlo, asimismo establece una serie de disposiciones para facilitar la cooperación internacional importante en estas materias.

V. CONCLUSIONES

En esta etapa del trabajo y conforme a lo expuesto precedentemente se puede indicar a modo de conclusión como un hecho claro y fuera de discusión que en las últimas décadas ha existido una gran proliferación a nivel de desarrollo informático en todo el mundo, de lo cual nuestro país no escapa , desarrollo que en lo concreto ha implicado el surgimiento de nuevas conductas reprochables y que deben ser sancionadas penalmente, por cuanto afectan el normal desarrollo de la comunidad e involucran atentados a bienes no solo individuales sino que supraindividuales, cuyos efectos por lo general trascienden las fronteras de los estados.

Que uno de los grandes problemas de esta delincuencia moderna es precisamente el uso de elementos técnicos e informáticos cuyos avances son

difícilmente predecibles, cuya evolución es más rápida que la modernización o actualización del derecho llamado a reprimirlo, con la consecuente dificultad de que existe una deficiencia en el conocimiento técnico de estas nuevas tecnologías y de las características de esta nueva delincuencia por parte de quienes están precisamente llamados a investigarlas y a sancionarlas, como de quienes a su vez están encargados de regularlas legalmente, versus el surgimiento de delincuentes cuyo perfil es ser por regla general sujetos con bastos conocimientos en materia informática y económica, lo que crea claramente un gran espacio de desigualdad en su enfrentamiento, todo lo anterior encuadrado en sistemas altamente vulnerables por deficiencia de mecanismos efectivos de protección que puedan evitar la concreción de estas conductas, sistemas que suelen ser de alto costo para su implementación y de una corta vida en cuanto a su efectiva utilidad, por cuanto cada vez que surge un mecanismo para evitar que sea vulnerado dicho sistema, los delincuentes inventan otro que lo haga vulnerable con igual y muchas veces mayor rapidez que su implementación masiva, a modo de ejemplo basta solo pensar en los virus y antivirus lanzados al mercado en los últimos tiempos que ya al año siguiente quedan obsoletos.

Asimismo se puede concluir que independiente de la postura o sistema que se adopte en cuanto a incluir o no esta nueva criminalidad en los tipos penales clásicos, lo cierto es que claramente las figuras clásicas entendidas en sus interpretaciones tradicionales a la luz de estos avances se presentan como insuficientes para abarcar esta delincuencia tan especial, siendo necesario adecuar sea la interpretación de sus elementos, complementar sus estructuras para hacerlas compresivas de estas modalidades modernas de criminalidad en términos amplios a fin de no quedar atrás con el avance de nuevas tecnologías pero manteniendo los elementos básicos que permitan respetar los principios generales en materia de seguridad jurídica, sea creando leyes especiales, adecuación que no solo debe comprender los textos legales sino que debe necesariamente incluir capacitación permanente a los llamados a aplicar las normas y a quienes tienen como función la creación del derecho, todo ello dentro de un marco de constantes esfuerzos por potenciar la cooperación internacional, tanto para la investigación criminal como para la represión de tales conductas, que como se indicó en este estudio son generalmente transnacionales.

Por último y en cuanto a la pregunta indicada al inicio de este trabajo en orden a sostener si en Chile son o no punibles las conductas constitutivas de delincuencia informática y en especial el fraude informático, me sumo a la postura de que actualmente si existe legislación que sanciona estas conductas, una especial a saber la Ley N º 19223 que abarca expresamente las principales figuras informáticas como lo son el sabotaje y espionaje en sus diversas formas aunque con la limitación de no sancionar aquellas figuras culpables y que son de bastante ocurrencia en términos prácticos y con grandes efectos dañinos a la comunidad, y en cuanto al fraude estimo que si es sancionable bajo la figura clásica de la estafa, en especial y como lo ha indicado la jurisprudencia analizada, en aquella estafa calificada por el engaño, pudiendo perfectamente encuadrarse el uso de medios tecnológicos que no estén expresamente reglados en el concepto de “otros medios semejantes” que utilizada dicho tipo penal, es más, aún de no estimarse dicho término compresivo de estas herramientas no debemos olvidar la figura de la llamada estafa residual del artículo 473 de nuestro Código Penal que perfectamente estimo podría ser aplicada, teniendo eso si, una interpretación amplia y actualizada de los elemento típicos acorde a la evolución de la sociedad, sin dudas temas no exentos de polémica y que seguirán siendo de actualidad prácticamente en forma permanente, y un buen desafío para los estudiosos del derecho .

VI BIBLIOGRAFIA

BALMACEDA HOYOS, GUSTAVO “El delito de Estafa Informática”. Ediciones Jurídicas de Santiago año 2009

BUSTOS RAMIREZ, JUAN “Obras Completas Tomo I “Derecho Penal Parte General. ARA Editores, año 2005

BUSTOS RAMIREZ, JUAN “Obras Completas Tomo II “Derecho Penal Parte General. ARA Editores, año 2005

HUERTA MIRANDA ,MARCELO- LIBANO MANZUR , CLAUDIO “Delitos Informáticos” Segunda Edición complementada y actualizada a 1998. Editorial Jurídica Conos Sur Ltda.

MAGLIONA MARKOVICTH, CLAUDIO PAUL- LOPEZ MEDEL, MACARENA “ Delincuencia y Fraude Informático” Derecho Comparado y Ley N º 19223. Editorial Jurídica de Chile año 1999.-

POLITOFF L. , SERGIO- MATUS A. JEAN PIERRE- RAMIREZ G. .MARIA ALICIA “ Lecciones de Derecho Penal Chileno. Parte General. Editorial Jurídica de Chile año 2004

SILVA HERNAN. Las Estafas. Doctrina, Jurisprudencia y Derecho Comparado. Editorial Jurídica de Chile año 1996

VERA QUILODRÁN, ALEJANDRO A., Delito e Informática . La informática como fuente del delito. Ediciones Jurídicas La Ley, Santiago , Chile, 1996

Articulo denominado “ Punibilidad y tratamiento jurisprudencial de las conductas de phishing y fraude informático” escrito por doña Veronica Rosenblut Gorodinsky, Abogada de la Unidad Especializada en Lavado de Dinero, Delitos Económicos y

Crimen Organizado de la Fiscalía Nacional, Ministerio Público, publicado en las páginas 254 y siguientes de la Revista Jurídica del Ministerio Público N º 35.

Artículo denominado " El lugar de comisión de los denominados ciberdelitos" escrito por doña Claudia Cárdenas Aravena, Doctora iuris Universidad de Chile aprobado en Octubre del año 2008 . Polit. Crim., N º 6, 2008, A2-6,pp 1-14 . (http://www.politicacriminal.cl)

Boletín Oficial N º 412-07 de la Honorable Cámara de Diputados y Senado de Chile . (Relativo a la Ley N º 19223)

Informe Titulado " Delitos Informáticos en la Legislación de España , Francia . Alemania e Italia" elaborado por Patricia Canales con la colaboración de Virginia Loiseau , Sección de Estudios de la Biblioteca del Congreso Nacional, Santiago de Chile, Julio del año 2004. DEPESEX/BCN/Serie de informes año XIV

Oficio N º 422 de fecha 27 de Septiembre del año 2001 del Fiscal Nacional del Ministerio Público Guillermo Piedrabuena Richard que adjunta informe de la unidad de Asearía Jurídica del Ministerio Público en materia de diligencias e investigación de Delitos Informáticos contemplados en la Ley N º 19223 y el fraude informático.

Texto de la Ley N º 19223 sobre Delitos Informáticos, promulgada el 08-05-1993 y Publicada el 07-06-1993. Ministerio de Justicia . Gobierno de Chile .

Texto de la Ley N º 20009 publicada en el Diario Oficial el 01 de Abril del año 2005 " Limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas"