UNIVERSIDAD DE CHILE

Facultad de Derecho

Departamento de Ciencias Penales

Análisis de la aplicación judicial de las normas penales contenidas en la Ley 19.223, que tipifica figuras penales relativas a la informática en general, y la aplicación del artículo 3°, que tipifica el delito de alteración de datos en particular

Memoria de Prueba para optar al grado de Licenciado en Ciencias Jurídicas y Sociales de la Universidad de Chile

Autor: Franco Lobiano Barría

Profesor guía: Antonio Bascuñán Rodríguez

Santiago, Chile

2020

Agradezco a quienes formaron parte de este largo proceso, en el que la redacción de una memoria es solo un punto al final. En especial a mi familia por su paciencia de oro y a mi profesor guía por el apoyo, sin distinción del tema a tratar.

Índice

Resumen

El presente trabajo de investigación se enmarca dentro de la aplicación de la normativa penal contenida en la ley 19.223, que tipifica figuras relativas a la informática y específicamente su artículo 3°, que establece el delito de alteración de datos. Dicha ley, desde su discusión y posterior dictación fue criticada, tanto por su insuficiencia como por sus excesos, situación que se ha hecho cada vez más urgente y que exige una modernización en la materia. Este trabajo recopila un total de 174 sentencias relativas a la aplicación de la ley 19.223 dictadas entre los años 2010 y 2018, ambos inclusive. Dichas sentencias fueron utilizadas para exponer las distintas visiones y conceptos generales discutidos durante su vigencia. De las sentencias recolectadas, se hace uso de 45 de ellas, para analizar y exponer de forma lata y ordenada, en que se han entendido los elementos del delito contenido en el artículo 3° relativo al delito de alteración de datos, a saber: bien jurídico protegido, autoría, tipo objetivo incluyendo este: verbo rector, objeto de ataque, medios y circunstancias comisivas, tipo subjetivo, causas de justificación y causas de exculpación. De esta forma, se pretende poner en conocimiento del lector especializado tanto las sentencias recopiladas, como su análisis posterior.

Así, cada capítulo que conforma la obra, concluye con una idea de cómo han sido entendidos en su aplicación los conceptos típicos del artículo 3°, los que a veces coinciden con la aplicación de las doctrinas penales generales, y en otras se inclinan por una especificación de los elementos que conforman las modernas tecnologías y su adaptación dentro del sistema jurídico-penal.

Introducción

La ley 19.223 que tipifica figuras penales relativas a la informática es el instrumento legal mediante el cual se intentó hacer frente a las eventuales conductas constitutivas de delito que habían surgido con el avance tecnológico y de las ciencias de información. A la fecha de dictación de la ley –año 1993–, nos encontrábamos como país en un momento de incertidumbre en cuanto a la evolución y utilización de las llamadas Tecnologías de la Información y Comunicación o TICs. Y se puede afirmar, que a partir de este desconocimiento es que se redactó la tan criticada ley 19.223, que tuvo la intención de llenar los vacíos jurídico-penales causados por el desarrollo de las nuevas tecnologías, las que influyeron de diferentes formas en la afectación de bienes jurídicos, e incluso la creación de uno nuevo: el de calidad, pureza e idoneidad de la información. Lo cierto es que los años han pasado y tanto los conceptos relativos al llamado derecho informático, la criminalidad informática y los delitos informáticos, como también los conceptos técnicos tratados específicamente por la ley 19.223 han sido objeto de distintos trabajos de investigación por parte de la doctrina nacional y de esfuerzos jurisprudenciales para lograr su adecuada aplicación, teniendo en cuenta los fines de la norma y enfrentando con ello los defectos de la misma. Dicha ley ha sido criticada de manera generalizada tanto por la doctrina como por la jurisprudencia nacional, tanto por los vacíos como por los excesos a la hora de tipificar los delitos que en ella se contemplan.

Para tratar de salvar dicha situación, y ante la indiscutible debilidad de la ley, se han presentado ante el Congreso Nacional distintos proyectos de reforma que intentan adecuar la situación vigente en nuestro país a una regulación penal que diga relación con los fenómenos informáticos contemporáneos, en algunas ocasiones modificando la actual legislación[1], en otras derogando definitivamente la legislación actual en la materia[2]. Por otro lado, es posible mencionar el trabajo que ha realizado en los distintos proyectos de reforma de Código Penal en los que también se trata esta materia. Por su parte a nivel internacional es posible mencionar el Convenio sobre la

[1] Boletín 9998-07 que Modifica la ley N° 19.223, que Tipifica Figuras Penales Relativas a la Informática, sancionando la distribución, exhibición o reproducción de material pornográfico infantil.
[2] Boletín 10145-07 que Tipifica y sanciona los delitos informáticos y deroga la ley N° 19.223 y Boletín 12192-25 que Establece nomas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.

Ciberdelincuencia o Convenio de Budapest, que constituye el principal esfuerzo por regular la criminalidad informática. El convenio de Budapest, fue suscrito por Chile en el año 2001 y promulgado con declaraciones y reservas en el año 2017. Actualmente, se encuentra en tramitación un proyecto de ley que incorporaría la normativa internacional de Budapest al derecho interno, adecuándolo definitivamente a las particularidades de nuestro sistema jurídico, y derogando necesariamente para ello la Ley 19.223[3]. Lo que se ha tenido presente a la hora de realizar la presente investigación.

Si bien la derogación de la normativa vigente en materia de delitos informáticos es inminente, es innegable que quedará un precedente valioso en lo relativo a la vigencia de la actual ley informática, constituido tanto por la doctrina generada a partir de la misma, como por la jurisprudencia pronunciada en su aplicación. Ello, toda vez que las conductas que pueden revestir las características de delitos derivadas del uso de las nuevas (y ya no tan nuevas) tecnologías que aumentan día a día, al igual que el avance en la complejidad de los equipos tecnológicos utilizados, tanto como medio de comisión de delitos, como también objeto de ataque de los mismos. Esta característica de velocidad en la evolución de la tecnología, choca con la velocidad de legislar sobre esta materia, sea en área penal como es el caso de la cibercriminalidad, como también en el área civil en relación a la protección de datos o incluso en el área constitucional con la generación de nuevos derechos constitucionales como el acceso a internet, haciendo necesario contar con conceptos jurídicos que sean precisos y técnicamente correctos, pero que a la vez que permitan cierta flexibilidad en la aplicación de los mismos: como sería el caso de: sistema de tratamiento de información, datos o información, todos ellos contenidos en la actual ley 19.223.

En el presente trabajo de investigación se tuvo por objetivo principal la recopilación de jurisprudencia relativa a la aplicación de ley 19.223 en general y de su artículo 3° en particular, el que contiene el llamado delito de alteración de datos. Para poder contar con el material sobre el cual se trabajará, se enviaron solicitudes a través de la ley de transparencia al Poder Judicial y al Ministerio Público, bajo los siguientes términos: los Roles Únicos de Causa (R.U.C.) de las

[3] Boletín 12192-25.

causas relativas a la ley 19.223, cuya forma de término haya sido sentencia definitiva, ya sea absolutoria o condenatoria, dictadas entre los años 2010 y 2018 (ambos años incluidos). Una vez recibida la información[4] de ambas instituciones, se procedió a unificar ambos listados y descargar cada una de las sentencias desde la página web del Poder Judicial[5]. En esta fase también se procedió a descargar aquellas sentencias que provinieran de los tribunales superiores de justicia en las causas penales tratadas. Además, se filtró aquellas que por algún motivo no tuviesen pertinencia alguna con el presente trabajo, estos fueron: que no se tratara en la sentencia alguno de los delitos contemplados por la ley informática; que no se encontrará la causa individualizada en página web del Poder Judicial; o, que no correspondiera la fecha de la sentencia a los márgenes establecidos para la investigación. El listado total de sentencias contuvo 187 sentencias, las que luego de ser filtradas alcanzan un total de 174[6], incluyendo sentencias que recorren toda la jerarquía judicial en materia penal[7]. Posteriormente, se procedió a darle correspondiente análisis a cada una de las sentencias recolectadas y a clasificarla según la materia pertinente a este trabajo de investigación, elaborando una ficha jurisprudencial para aquellas sentencias relevantes para el presente estudio[8].

En cuanto a la presentación de la investigación, esta se estructura en tres capítulos. El primero de ellos, relativo al marco conceptual, introduce un primer apartado sobre los conceptos de cibercrimen, delitos computacionales y delitos informáticos, dejando de relieve la importancia de distinguirlos y las repercusiones que esto trae aparejado. Posteriormente, se contempla un acápite para analizar la historia fidedigna de la norma en comento, la que ha sido objeto de diversas críticas por parte de la doctrina nacional. A continuación, se analizan los fines de protección de la norma que tuvo en cuenta el legislador al momento de la dictación de la ley y su posterior desarrollo por parte de la doctrina y jurisprudencia nacional. Para finalizar, en el cuarto apartado se ubica a la Ley 19.223 dentro del contexto jurídico-penal chileno.

[4] La que conforma el grueso de la muestra analizada, mas no su totalidad. Aunque la incorporación se sentencias ajenas a esta es excepcionalísima y se expresará su incorporación, de ser necesaria.
[5] https://oficinajudicialvirtual.pjud.cl
[6] Anexo I
[7] Esto es Juzgados de Garantía; Tribunales de Juicio Oral en lo Penal; Corte de Apelaciones; y Corte Suprema. En cuanto a las sentencias relativas a primera instancia en los Juzgados del Crimen del antiguo sistema de procedimiento penal, no fue posible su obtención, aunque en ocasiones, se cuenta con las sentencias que, en dicho contexto, se dictaron por los tribunales superiores de justicia.
[8] Anexo II

En el segundo capítulo, se aborda en concreto el análisis del tipo penal contenido en el artículo 3° de la referida ley, usando para ello las sentencias recopiladas. El art. 3°, contempla el delito de alteración de datos contenido en un sistema de tratamiento de información. Para exponer la información de forma ordenada, se utilizará la exposición del género comentario de Código Penal donde la información será sistematizada conforme al orden conceptual de la teoría general del delito, esto es: bien jurídico, autoría, elementos del tipo objetivo [verbo rector, objeto de ataque, medios y circunstancias comisivos], tipo subjetivo y eventuales elementos subjetivos del tipo, causas de justificación, causas de ausencia de culpabilidad y de exculpación. Donde, cada uno de los elementos de la teoría general del delito constituirá un apartado dentro de dicho capítulo.

El tercer capítulo corresponde a las conclusiones que se pueden adoptar al analizar la aplicación de las normas de la Ley 19.223 en general y en particular de su artículo 3° sobre el delito de alteración de datos.

Finalmente, se incluye en un primer anexo, el listado de 174 sentencias recopiladas, dictadas entre los años 2010 y 2018, con la debida individualización mediante su Rol o Ruc, y en un segundo anexo las fichas de análisis jurisprudencial elaboradas para el estudio de los diferentes elementos usados para la exposición de los capítulos del trabajo de investigación.

I. Marco conceptual

i. Conceptos relativos a la criminalidad informática: delitos computacionales, delitos informáticos y cibercrimen

La importancia de la tecnología aplicada a las comunicaciones y sistemas de almacenamiento de datos, como forma de entendimiento y relación entre humanos, hoy no solamente es indiscutida, sino que también impredecible en su futuro. El involucramiento de los conceptos de digitalización, informatización, y de las formas u objetos que los hacen palpables –como computadores o celulares– ya no son ajenos a nadie, por sus efectos en nuestra sociedad, la llamada sociedad de la información, y en el futuro de esta misma. Estos efectos, son asimismo objeto de debate, tratados de distintas formas y en distintas disciplinas como obras de arte, premoniciones tecnofóbicas o utópicas. Es decir, la informatización de la vida, se ha colado hasta los más recónditos lugares de la cotidianeidad humana. Estas tecnologías, adopten la forma que adopten, forman parte de la normalidad de la humanidad, de la manera en que cada individuo percibe su entorno y se relaciona con él, y al hacerlo se producen también conflictos entre los individuos, caracterizados esta vez por el entorno informatizado o digitalizado. Cuando comienzan los conflictos, se crea a su vez el Derecho, que en su afán regulatorio de conflictos, pretende reglamentar el fenómeno informático, por ejemplo, en el área civil regulando los contratos informáticos, licencias sobre *softwares*, derechos de propiedad intelectual sobre los mismos, etc. Por otro lado, en el área constitucional, ésta ha significado un desafío para establecer una nueva gama de derechos, vinculados con derechos constitucionales ya existentes como la intimidad ligada a los datos personales, o incluso generar derechos constitucionales de un nuevo orden específicamente informáticos, como por ejemplo el derecho a acceso a las tecnologías de información o el derecho de acceso a internet. Ahora bien, es predecible que con el incremento del uso que se da a las nuevas tecnologías, aumente también los abusos de ellas, vulnerando muchas veces derechos de terceros o bienes jurídicos de interés para el ordenamiento jurídico. Esto, llevado al plano del derecho penal, significa que es predecible que a medida que aumenta el uso de las nuevas tecnologías, tanto en cantidad como en calidad de las mismas,

aumentará también la cantidad de conductas potencialmente delictivas, las que a su vez asumen mayor diversidad según el avance tecnológico, haciéndose cada vez más complejas. Dichas conductas, al superar cierto margen de vulneración o puesta en peligro de un determinado bien jurídico, se dirá que tienen la aptitud para ser tipificadas como delitos por parte del legislador penal. Ello, toda vez que en materia penal, la tipificación de una conducta como delito, y la intervención de del sistema penal debe operar en *ultima ratio,* o dicho de otra forma, cuando los demás mecanismos de protección que posee el Derecho no sean vistos como suficientes para la protección de determinados bienes jurídicos.

Al tipificarse una determinada conducta como delito en este nuevo medio informatizado, la doctrina penal, tanto nacional como extranjera comenzó a debatir si es que este grupo de "nuevos delitos", formaban o no una categoría diferente de delitos –delitos informáticos–, y dichas posturas, a su vez argumentaron de diversa manera para responder a la pregunta sobre la finalidad de protección de estas figuras penales. Desde el año 1978[9], hasta la fecha de publicación de este trabajo, los esfuerzos por conceptualizar y definir los márgenes del fenómeno informático aplicado al campo del derecho penal, se ha caracterizado por la falta de consenso, tanto en la doctrina nacional como en la doctrina comparada. Así como también, en las diferentes formas de tratamiento legislativo que se han usado para hacer frente a la criminalidad informática en las diferentes legislaciones del globo, lo que repercute especialmente en delitos en los que el medio de comisión es una red de computadores interconectados en una red, como lo es internet.

Como se ha señalado, nuestro país, trata el tema de la criminalidad informática en la ley 19.223 tipifica figuras penales relativas a la informática, y aunque no es la única norma vinculada con la ciencia informática[10], es la más relevante en cuanto a la regulación de los delitos vinculados a la ciencia informática. De esta forma, para analizar la aplicación de la norma contenida en el

[9] Año de dictación de La *Florida Computers Crime Act*, del Estado de Florida, EE.UU. La que corresponde a la primera normativa relativa a delitos en el nuevo contexto informatizado. En Huerta, M. y Líbano, C. (1998). Los delitos informáticos. p. 106.

[10] A modo de ejemplo, en materia civil la ley 19.628, sobre protección de datos de carácter personal; y en materia penal el art. 36 B de la ley general de telecomunicaciones, sobre interceptación de servicios de telecomunicaciones y otros; o, la ley Nº 20.526 que modifica artículo 366 quáter y quinquies del Código Penal, con objeto de incluir el delito de acoso cibernético infantil o *child grooming*; entre otros.

artículo 3° de la ley 19.223, que forma el punto central de este trabajo, es necesario revisar cómo han sido entendidos los conceptos que vinculan la ciencia informática con el derecho penal en nuestro país[11], y como estos han sido recogidos por la jurisprudencia. Lo que por cierto, está lejos de ser pacífico.

En materia de criminalidad informática, lo primero que hay que recalcar es la inexistencia en la legislación nacional de la definición de los conceptos que conforman el presente acápite –delito informático, delito computacional, cibercrimen–, ni siquiera la ley 19.223, aunque en su título indica que "tipifica figuras penales relativas a la informática"[12] define los conceptos mencionados. No obstante, en la doctrina nacional, tanto la definición de los delitos informáticos, delitos computacionales como la de cibercrimen, han sido objeto de diversos esfuerzos de conceptualización, los que sin embargo y como ya se señaló, están lejos de llegar a un consenso. En este primer apartado, se pretende poner de relieve dicha falta de consenso en la doctrina chilena, ejemplificando su uso eventual con aquellas sentencias de los tribunales penales y superiores de justicia que los recojan. Por ello, a modo de establecer alguna certeza en su uso, se expondrá la forma en la que han entendido algunos juristas de nuestro país los principales conceptos jurídicos relativos a la criminalidad informática[13], para luego exponer las concepciones que de los mismos han tenido nuestros tribunales. Así, este primer acápite refiere a los esfuerzos de conceptualización de: delitos computacionales, delitos informáticos y cibercrimen.

En primer lugar, en la doctrina se distingue entre delitos computacionales o delitos informáticos en sentido amplio; y delitos informáticos, también llamados delitos informáticos propiamente

[11] Previamente, conviene diferenciar entre el llamado "derecho informático" y la "informática jurídica". Siendo el primero una rama de estudio del Derecho, permeado por el fenómeno informático. Mientras que el segundo hace referencia a la aplicación y utilidad que la ciencia informática tiene para el desarrollo de la labor jurídica en todas sus esferas, y que por cierto, son de la más variada índole. Como por ejemplo los programas de tratamiento de información, y bases de datos de contenido jurídico.

[12] No obstante ello, en el Derecho Internacional, ver el Convenio sobre Cibercrimen del Consejo de Europa o Convenio de Budapest, al cual adhirió Chile en el año 2017, y que estaría próxima a su incorporación a nuestro ordenamiento, derogando la ley 19.223. Este instrumento, si hace definición de los conceptos, e incluso se hace referencia a la preferencia en la utilización de algunos de estos por sobre otros.

[13] En oposición a los conceptos técnicos derivados de la ciencia informática, cuya importancia es obvia, pero no corresponde hacer en este estudio referencia a las categorías y conceptos derivadas de esta sino que más bien, se tomarán de la siguiente fuente bibliográfica: Huerta, M., y Líbano, C. (1998). Delitos informáticos.

tales. Se puede afirmar que mayoritariamente se ha entendido en la doctrina nacional como pertenecientes al grupo de los delitos computacionales, a aquellos delitos "que tienen por única particularidad que el computador sirve de instrumento para cometer delitos que tradicionalmente se cometían por otros medios"[14]. Ejemplo de ello serían las injurias o amenazas realizadas por un usuario a otro en la plataforma de alguna red social, entiéndase por ejemplo Facebook, Instagram u otra. Luego, al referirse la gran mayoría de la doctrina al segundo grupo, esto es, los delitos informáticos propiamente tales, lo hace en el sentido de considerarlos como aquellos delitos que contando con la particularidad recién mencionada, "no [son] reconducibles a delitos tradicionales ya sea porque se protege un bien jurídico enteramente distinto o porque se está protegiendo un bien jurídico tradicional, pero algún elemento del delito no es posible encuadrarlo en alguna figura típica tradicional"[15]. Estas definiciones pertenecen a Juan Pablo Hermosilla y Rodrigo Aldoney, quienes en su trabajo "Delitos Informáticos", señalan los diferentes matices en los que se han fijado los autores nacionales para explicar la imposibilidad de reconducir a tipos tradicionales los mentados delitos informáticos. Los criterios diferenciadores en los que enfatizan los autores son: la protección de un bien jurídico diferente a los tradicionales, el que estaría constituido según la historia fidedigna de la ley 19.223 por "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"[16]; o bien, porque los elementos del delito, dadas las particularidades de ellos, constituida principalmente por la cualidad de ser conductas "informatizadas", no permiten configurar las figuras típicas tradicionales, haciendo necesaria la creación de nuevas figuras penales, como por ejemplo el fraude informático o el hacking blanco, ambas sin tipificación en nuestro país. O a lo menos, la adaptación de delitos tradicionales, en lo relativo a sus modos de comisión informatizados, como es el caso del delito del artículo 161 A del Código Penal, sobre captación, reproducción y difusión "por cualquier medio" de comunicaciones privadas.

[14] Hermosilla, J.P. y Aldoney, R. (2002). Delitos informáticos. p. 418.
[15] *Ibídem*. p. 418.
[16] Historia fidedigna de la ley Boletín 412-07. Primer Trámite Constitucional: Cámara de Diputados. Moción Parlamentaria en Sesión 19. 16 de julio, 1991.

De esta forma, se pueden mencionar diversos autores que han señalado que tanto la comisión, contra o mediante un sistema de tratamiento de la información, sumada a la imposibilidad de reconducción hacia tipos tradicionales, forman el criterio que caracterizaría a los delitos informáticos. Sin perjuicio de los matices, que entre estos autores existan, coinciden mayoritariamente en que el objeto de ataque descrito en los delitos informáticos es el soporte lógico del sistema de tratamiento de información[17]. Entre estos autores, se pueden señalar a Marcelo Huerta y Claudio Líbano, quienes definen el concepto de delitos informáticos con afanes omnicomprensivos, entendiéndolo como: "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual generalmente producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro".[18]

Por su parte, los autores Rodolfo Herrera y Alejandra Núñez formulan la siguiente definición de delito informático: "toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable (preferentemente dolosa), y que atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del uso de natural de las tecnologías de la información, y el cual se distingue de los delitos computacionales o tradicionales informatizados".[19]

En el mismo sentido Renato Jijena, formula el concepto de delito informático de la siguiente forma: "aquella conducta típica – tipificada o establecida como ilícito por la ley–, antijurídica – contraria a derecho– y culpable – con intención dolosa o por negligencia–, cometida contra el soporte lógico de un sistema informático o de tratamiento automatizado de información

[17] Moscoso, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. p. 15.
[18] Huerta, M., y Líbano, C. (1998). Delitos informáticos. p. 116.
[19] Herrera Bravo, R. y Núñez Romero, A. (1999). Derecho informático. p. 218.

("programas o instrucciones" y "datos de cierta naturaleza o importancia"), generalmente mediante elementos computacionales".[20]

Esta informatización de las conductas, está representada en la idea de que el objeto material del delito informático, deba ser el soporte lógico del sistema automatizado de procesamiento de la información o *software* de este. Lo que en palabras de Romina Moscoso, se leerá de la siguiente forma: "La especialidad de los delitos informáticos radica en el objeto material, supuesto básico bajo el cual se desenvuelven. El soporte lógico de un sistema automatizado de información es el objeto de ataque de un sujeto activo informático, ya sea para introducir un elemento nocivo, obtener datos o programas ajenos ilícitamente o alterar su funcionamiento, entre otras figuras comisivas".[21]

Finalmente, se puede mencionar la opinión de Hernando Morales, quien si bien es de la misma línea de pensamiento que los autores antes tratados, los matices que presenta su postura se refieren a considerar como delitos informáticos propiamente tales, a aquellos cuyo bien jurídico protegido es la información, mientras que los delitos computacionales serían aquellos cuyo bien jurídico resulta amparado por otras nomas penales[22].

[20] Jijena Leiva, R. (2008). Delitos informáticos, Internet y derecho. p. 148. En el mismo sentido Moscoso Escobar, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. pp. 13 y ss.; González Marín, P. (2013). Desde el delito computacional al delito de alta tecnología: Notas para una evolución hacia el concepto y estructura del delito informático. p. 1085, quien lo entiende de la siguiente manera: "una conducta típica, antijurídica y culpable cometida mediante el uso de la informática, contra el soporte lógico (*software* de un sistema de tratamiento de la información, los datos contenidos digitalizaos contenido en el o los programas computacionales empleados en el mismo)". También, Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. pp. 160 y ss., en los siguientes términos: "delitos informáticos en sentido estricto (en adelante "delitos informáticos"), entendiendo por tales aquellas conductas (delictivas) que afectan el *software* o soporte lógico de un sistema de tratamiento automatizado de la información". En el mismo sentido, lo entienden Lara Gálvez, J.C., Martínez Maraboli M., y Viollier Bonvin, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. pp. 108 y ss., haciendo extensible este entendido a la misma legislación chilena, toda vez que "En consecuencia, cuando la legislación chilena habla de delitos informáticos lo hace en referencia a la protección mediante el derecho penal de los datos y sistemas informáticos, mas no de los cibernéticos en general, siguiendo así la al concepto restringido de delito informático sostenido también en la ONU como todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos".

[21] *Óp. cit.*, Moscoso, R. (2014). p. 15.

[22] Citado por Jijena Leiva, R. (1992). Chile, la protección penal de la intimidad y el delito informático. pp. 85 y ss.

No se tiene dentro de este estudio algún registro de la distinción expresa entre los conceptos de delitos computacionales y delitos informáticos por parte de la jurisprudencia nacional, pero sí de sentencias que acogen las definiciones que los autores nacionales han propuesto sobre el concepto de delito informático propiamente tal:

Así, la sentencia de la Corte de Apelaciones de Concepción en causa Rol 844-2014 (30.01.2015) en su considerando 5° acoge la definición de los autores Líbano y Huerta, la que como se dijo es a su vez compartida por la mayoría de la doctrina nacional, refiriéndose además a la tradicional clasificación de los delitos contenidos en la ley 19.223 en delitos de sabotaje informático y delitos de espionaje informático, y dentro de la cual cabría incluir el delito de alteración de datos dentro el grupo de sabotajes informáticos:

> Que, son delitos informáticos 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 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. (Marcelo Huerta y Claudio Líbano, Delitos Informáticos)
>
> Siguiendo la clasificación efectuada por los autores antes citados, la Ley 19.923 contempla dos figuras delictivas: I Sabotaje informático y II Espionaje Informático, las cuales se subdividen en categorías distintas atendiendo al objeto contra el cual se atenta y/o el modus operandi.
> El sabotaje informático tiene tras manifestaciones que se consagran atendiendo el objeto que se afecta con la acción punible:
>
> a) atentados contra un sistema de tratamiento de la información o de sus partes componentes; (art.1, primera parte)

b) atentados en contra del funcionamiento de un sistema de tratamiento de la información; (art.1 segunda parte)

c) atentado contra los datos contenidos en un sistema automatizado de tratamiento de la información. (art.3).[23]

La prevención del Juez don Edmundo Devia, contenida en la sentencia del Tribunal Oral en lo Penal de Coyhaique Ruc 1610036482-9 (24.07.2018), se refiere a que la diferenciación de elementos que constituyen un sistema de tratamiento de información, poniendo el énfasis en que lo que caracteriza a delitos informáticos, es que el objeto de ataque de estos es el soporte lógico del sistema. Más adelante, clasifica los delitos informáticos en tres grupos, agregando a la clasificación tradicional antes mencionada, el grupo de fraude informático, incluyendo los delitos de alteración de datos dentro de esta, lo que no es compartido por la doctrina ni jurisprudencia nacional. Señala en su prevención:

> Los delitos informáticos se caracterizan porque sancionan conductas dirigidas en contra **soporte lógico** de un sistema tratamiento información, como sería por ejemplo un computador, que se compone de dos partes el soporte lógico, a saber los datos, la información contenía el sistema, es decir el software y el **soporte físico** los cables, chips, carcasa el equipo, decir el hardware, por ello una conducta dirigida contra los datos es un delito informático, mientras que una dirigida contra soporte físico, sólo es un delito de daños. De esta forma las conductas tipificadas en la Ley N° 19.223, tratándose de delitos con carácter informático, el objeto sobre el cual recaen dichas conductas es inmaterial, distinguiéndose tres modalidades de criminalidad informática, esto es fraude informático, el sabotaje informático y el espionaje informático. Los primeros, se

[23] En términos más amplios TOP Temuco RUC 1700268031-9 (22.07.2018), en su considerando 17° literal B señala:

> El delito informático puede definirse como cualquier conducta ilegal, no ética o no autorizada, que involucra el procesamiento automático de datos o la trasmisión de los mismos (según la Organización para la Cooperación Económica y el Desarrollo), o como toda acción típica, antijurídica y culpable, para cuya consumación se utiliza o afecta una computadora o sus accesorios (según el criterio de la Comisión que redactara uno de los anteproyectos sobre informática)

> encuentran las alteraciones o manipulaciones, de los datos, ya sea al recopilarlos, procesarlos, estando almacenados o al transmitirlos telepáticamente, como de los programas del sistema computacional; los espionajes informáticos se encuentran las figuras de obtención ilícita, dolosa y sin autorización de datos o información relevante y de programas computacionales; y el sabotaje informático el cual se configuran las conductas de atentados que causan daños, destruyen o inutilizan un sistema computacional.

En cuanto al concepto de Cibercrimen o Ciberdelitos, se puede afirmar que tampoco existe un entendimiento unívoco en la doctrina nacional. La mayoría de la doctrina –la que ha hecho referencia a este concepto–, la ha conceptualizado poniendo de relieve que al hacer uso del mismo se referirán a: "aquellos delitos que para su comisión requieren necesariamente de una red de computadores (internet). Esto abarca un concepto delictivo bastante amplio, pues internet se presenta como medio para cometer delitos que importan emisión, transferencia o intercambio de información, atentados contra datos protegidos y otros"[24]. Así, a diferencia de lo que ocurre con la distinción entre delitos computacionales y delitos informáticos, donde la referencia a los primeros es por el solo hecho de que el ataque sea realizado por medio, o contra un sistema automatizado de procesamiento de información. Y, en cuanto a los segundos, en que dicho ataque en contexto informatizado no sea además posible su reconducción a un tipo tradicional. Lo que caracteriza al concepto de ciberdelitos es en cambio, en que para la realización de determinadas conductas, sea necesaria para su comisión el uso de una red de computadoras, siendo la más común para ello internet. Este concepto amplio es usado, según su contenido y características por el autor Patricio González Marín, incluyendo dentro del mismo cinco áreas de protección contra conductas potencialmente configuradoras de un cibercrimen, comprendiendo: "los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos abarcando los delitos de acceso ilícito, piratería, hacking, cracking, espionaje de datos, interceptación ilegal e interferencia o manipulación de los datos e interferencia con el sistema, entre otros ataques contra la integridad del sistema, incluyéndose el sabotaje y los ataques de denegación de servicios (DoS).

[24] Cárdenas Aravena, C. (2008). El lugar de comisión de los denominados ciberdelitos. pp. 2 y ss. En el mismo sentido, Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. p. 237.

Abarca también los delitos relacionados con el contenido, entre los que se encuentran la incitación al odio y racismo; la producción, distribución y consumo de material erótico y pornográfico, principalmente el de naturaleza infanto-juvenil; el juego ilegal; la difamación e información falsa; el correo basura y amenazas conexas.

Incluye, además, el Ciberdelito los llamados Delitos Informáticos que esta vez comprenden como ya se indicó, el abuso de dispositivos, la falsificación informática, el robo y usurpación de identidad, y el fraude informático. A todo esto cabe agregar, los delitos relacionados con la propiedad intelectual, derechos de autor y marcas y, por último los delitos referidos a los daños y destrucción contra el *hardware*, *firmware* y *software*.

Por último la legislación comparada se ha ido abriendo a la posibilidad jurídica de combinación de estos delitos como ocurre con el Ciberterrorismo, la guerra informática o el blanqueo de dinero y el lavado de activos".[25]

Esto, no quiere decir que los conceptos de delitos informáticos, delitos computacionales, y ciberdelitos sean excluyentes entre sí, pudiendo un delito informático o computacional, ser a su vez considerado como un ciberdelito. Toda vez que el criterio diferenciador de este concepto radica en el uso una red de computadoras o internet, los que pueden ser usados también en algunos delitos informáticos o computacionales.

Por otro lado, algunos autores nacionales han propuesto nuevas formas de diferenciación conceptual dentro de la criminalidad informática, principalmente a raíz de la crítica al concepto de delito informático, considerándolo un concepto errático, dado que adolecería de un alta cuantía de ambición y artificialidad: "ambiciosa, porque no es tarea fácil delimitar nítidamente los contornos de lo informático frente al fenómeno delictivo y, creemos que resulta artificial, porque en estricto rigor el ´delito informático` no existe. Por esta razón parece mejor entonces utilizar un concepto funcional y criminológico del mismo, que sea lo suficientemente amplio para poder abarcar a todos estos conflictos"[26]. Esta crítica, está basada en los siguientes argumentos: en primer lugar, en cuanto al sustantivo delito, que al pertenecer a la ciencia del

[25] *Óp. cit.*, González Marín, P. (2013). pp. 1087 y ss. En este sentido también, el ya citado Jijena Leiva, R. (2008). p. 155.

[26] Balmaceda Hoyos, G. (2009). El delito de estafa informática. pp. 67 y ss.

Derecho, debe naturalmente ser entendido en este sentido, cual es dentro de la teoría jurídica del delito, lo que implica que para hablar de estos, necesariamente la conducta deba coincidir con el tipo que la legislación prevé, esto es, estar tipificado. Considerando el constante avance de las conductas que pueden ser tipificadas como delito en el ámbito informático, esto trae como infortunio la rigidez del concepto. En segundo lugar, se le critica por englobar dentro del mismo término conductas de la más variada índole, que solamente tienen en común la vinculación con un aparato computacional. Por último, si bien el concepto de delito informático presentaría un aspecto de plasticidad, en el sentido de poder englobar conductas que se ejerzan sobre la tecnología o por medio de ella, no podría hablarse de "un" delito informático, sino que de las más variadas conductas, las que además vulnerarían bienes jurídicos diferentes y cuyos medios comisivos tampoco presentarían siempre características similares[27].

Resultan aclaratorias las palabras de Laura Mayer, quien aborda el problema manifestando también su disconformidad con el concepto, indicando lo siguiente:

"En comparación con el bien jurídico, el concepto de ´delito informático` ha sido abordado por un número mucho menor de autores, fundamentalmente porque constituye un término relativamente reciente, cuyo surgimiento no es imaginable sin la existencia de computadoras. Se trata, no obstante, de una expresión equívoca, ya que se la emplea para aludir a realidades que no son coincidentes entre sí.

El término criminalidad informática en sentido amplio o criminalidad cometida ´mediante` sistemas informáticos, suele utilizarse para referir la comisión de delitos tradicionales a través de computadoras o de internet (v.gr. extorsión o difusión de pornografía infantil). En cambio, la expresión criminalidad informática en sentido estricto, criminalidad cometida ´respecto de` o ´contra` sistemas informáticos o, simplemente, criminalidad informática, suele emplearse para aludir a comportamientos delictivos que inciden, directamente, en un sistema informático (v.gr. sabotaje o espionaje informático). Por su parte, el concepto de ´cibercrimen` suele utilizarse para aludir a la criminalidad informática (en sentido amplio o estricto) llevada a cabo a través de internet. Ahora bien, de acuerdo con la doctrina, no toda conducta (delictiva) que recae en

[27] *Ibídem*. En el mismo sentido, Magliona Markovicth, C., & López Medel, M. (1999). Delincuencia y fraude informático: Derecho comparado y ley n° 19.223. pp. 34 y ss.; Álvarez Fortte, H. (2009). Los delitos informáticos. pp. 105 y ss.

un sistema de tratamiento automatizado de información constituye un delito informático en estricto sentido. Por el contrario, ha de tratarse de comportamientos que incidan en el *software* o soporte lógico, esto es, en los programas, instrucciones y reglas informáticas que permiten el procesamiento de datos en una computadora. A diferencia de ellos, las conductas que solo afectan el *hardware* o soporte físico de un sistema informático, o sea, los componentes que integran la parte material o tangible de una computadora, pueden ser subsumidas, en términos generales, en los delitos (patrimoniales) clásicos y, muy especialmente, en el tipo penal de daños".[28]

A modo de conclusión, y para establecer alguna base en el uso de los conceptos anteriormente referidos, se entenderá en adelante por delito informático, aquella conducta, típica, antijurídica y culpable, cometida contra el soporte lógico de un sistema automatizado de tratamiento de la información. Por delito computacional, se entenderán aquellas conductas, típicas, antijurídicas y culpables, dirigidas contra un sistema automatizado de tratamiento de información, o por medio de este, y que admiten una reconducción a delitos tradicionales. Por otra parte, se entenderá por cibercrimen aquellas conductas que, pudiendo o no estar tipificadas como delito, son cometidas contra o por medio de un sistema de procesamiento automatizado de información, y tiene como característica principal que se ejecuta en el contexto de una red de dispositivos de procesamientos de datos, siendo la más común de estas redes internet.[29]

Los delitos informáticos, en un sentido amplio, admiten múltiples clasificaciones en la doctrina, tanto nacional como extranjera, pero el tema escapa al objeto de este trabajo de investigación, por lo que se tomará como base la clasificación que propone Gustavo Balmaceda Hoyos[30] en su texto "El delito de estafa informática", una clasificación que de acuerdo con los autores es de una amplitud tal, que hace posible englobar dentro del concepto de delito informático múltiples

[28] *Óp. cit.*, Mayer Lux, L. (2017). p. 237.
[29] La importancia de su distinción radica tanto en lo académico, como en la adecuada clasificación de los tipos penales y la precisión conceptual de los mismos lo que influye, a su vez en una adecuada y más sana legislación venidera, toda vez que los legisladores tendrán claridad al discutir sobre las conductas merecedoras de reproche penal.
[30] Este autor tiene una postura crítica del concepto de delito informático, por lo que hace que se incline por definiciones amplias y funcionales, para facilitar el análisis del posible encaje de las nuevas conductas en los tipos tradicionales, pero sin cerrar la puerta a soluciones también nuevas y específicas a estos comportamientos. Balmaceda Hoyos, G. (2009). pp. 68 y ss.

conductas[31]. Así es, que estos delitos pueden encasillarse dentro de los siguientes tópicos, ejemplificando lo variado de las modalidades y dimensiones que pueden adoptar los delitos informáticos:

a) Delitos que atentan contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos: el *hacking* informático el que es entendido como la penetración de sistemas informáticos a través de manipulaciones técnicas perpetradas únicamente para superar medidas de seguridad técnicas, o con el objetivo de sabotear, espiar o manipular; otras formas de acceso ilegal como lo son evitar la protección de contraseñas; el uso de ejecuciones de *hardware* y *software* defectuosos; el *spoofing* de IP (*internet protocol*) y DNS (*domain name service*), referidos ambos a ganar el acceso no autorizado para computadores o redes desde afuera fingiendo ser un dispositivo autorizado y de confianza dentro de la red traspasada; y el *phishing*. Dentro de este tópico referido a la confidencialidad, integridad y disponibilidad de los datos, también caben las siguientes conductas: el uso de computadores engañosos; la interceptación de datos (envolviendo tecnología de telecomunicaciones y/o telefónica vía *bluetooth*); el daño; el espionaje; el sabotaje, cuyo método más común es causar un daño lógico mediante la introducción de un Virus o un *Worm*; y la extorsión informática.

b) Delitos tradicionales relacionados con computadores: El fraude informático (a través de las siguientes formas como ejemplo: manipulaciones informáticas, subastas fraudulentas y otros servicios de órdenes en línea fraudulentos, uso ilegal de tarjetas de ATM o *smartcards*, y formas similares de pago, abuso de tarjetas de crédito, robo de identidad, mal uso de las redes telefónicas tradicionales, abuso de marcadores de internet, etc.); falsificación informática; incentivos a niños en línea y otras formas de búsqueda de víctimas; y ataques amenazadores contra la vida.

c) Delitos referidos al contenido: la pornografía infantil; el racismo, el discurso aversivo y la glorificación de la violencia; solicitar, incitar, suministrar instrucciones y ofrecer cometer delitos; el *cyberstalking* o acecho a una persona mediante el uso de algún dispositivo

[31] Esta clasificación amplia es tomada por el autor del desarrollo en el derecho comparado, en específico la clasificación propuesta por Ulrich Sieber.

tecnológico; la difamación y diseminación de información falsa vía internet; la destrucción maliciosa de un sitio web; y el juego en internet.

d) Delitos que infringen el *copyright* y en contra de derechos relacionados: la reproducción no autorizada y uso de programas de computador; la reproducción no autorizada y uso de música y películas; la reproducción no autorizada de bases de datos; la reproducción no autorizada y uso de libros; el uso no autorizado de sitios web o *framing*; y el uso no autorizado de un dominio de internet.

e) Delitos que infringen la privacidad: el acceso no autorizado a datos personales; y la distribución no autorizada y conexión de los datos personales.

Por otro lado y de forma mucho más acotada, se cuenta también con la clasificación tradicional de los delitos informáticos, que clasifica los delitos contenidos en la ley 19.223 en las categorías de Sabotaje informático y Espionaje informático. Incluyendo en las primera las conductas descritas por los artículos 1° y 3°, referidos al ataque contra el sistema de tratamiento de información y alteración de datos respectivamente; y los artículos 2° y 4°, que contienen los delitos de acceso indebido y difusión de datos, respectivamente[32].

A modo de introducir desde ya la materia a tratar en el Capítulo II, se puede clasificar el delito del artículo 3°, esto es el delito de alterar, dañar o destruir los datos contenidos en un sistema de tratamiento de información como un delito de sabotaje informático, si se adopta la clasificación tradicional de los delitos informáticos en nuestro país; o bien, como un de delito que atenta contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, en caso de seguir la clasificación amplia antes descrita.

[32] Óp. Cit., Huerta, M., y Líbano, C. (1998). p. 285.

ii. La historia fidedigna del establecimiento de la Ley 19.223

La Ley 19.223 ha sido objeto de diversas críticas por parte de la doctrina nacional, tanto a nivel de discusión del proyecto legislativo en las respectivas salas y comisiones, como en las consecuencias de su escasa aplicación. En este apartado, se efectúa un breve resumen de la historia fidedigna de dicha ley, colocando el énfasis en las críticas de las cuales ha sido objeto, desde su dictación hasta la fecha de este trabajo. Aun así, conocer estas críticas tiene la importancia de formar un precedente para ser considerados en el futuro, sea en la discusión de la nueva ley o en la aplicación de sus nomas.

Sabido es, que el proyecto de legislar sobre la materia fue propuesto por moción del diputado José Antonio Viera-Gallo, la que fue presentada ante la cámara baja del Congreso Nacional con fecha 16 de julio de 1991, y la que tras las sucesivas etapas de discusión, fue finalmente publicada en el diario oficial con fecha 7 de junio de 1993. Ahora bien, desde su presentación a la Cámara de Diputados, hasta su fecha de publicación, el proyecto sufrió importantes modificaciones en su cuerpo, las que se vieron plasmadas en el articulado final de la Ley 19.223.

El proyecto original constaba de cinco artículos, y su texto era el siguiente:

> Artículo 1°. El que indebidamente destruya, inutilice, obstaculice, impida o modifique el funcionamiento de un sistema automatizado de tratamiento de información sufrirá la pena de presidio menor en su grado máximo.
> Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, en alguna de las formas señaladas en el artículo cuarto, la pena será la indicada en éste aumentada en un grado.
>
> Artículo 2°. El que sin derecho intercepte, interfiera, o acceda a un sistema automatizado de tratamiento de información será castigado con presidio menor en su grado medio.

> Artículo 3°. El que revele, transmita o se apodere indebidamente de la información contenida en un sistema de tratamiento de la misma, incurrirá en la pena de presidio mayor en su grado mínimo.
> Si quien realiza estas conductas es el responsable del sistema la pena se incrementará en un grado.
>
> Artículo 4°. El que indebidamente introduzca, transforme, desfigure, altere, dañe o destruya los datos contenidos en un sistema automatizado de tratamiento de información será castigado con presidio mayor en su grado medio.[33]
>
> Artículo 5° Si las conductas de los artículos anteriores son efectuadas con ánimo de lucro, la pena aumentará en un grado.

En el primer trámite constitucional, la Comisión de Constitución, Legislación y Justicia optó por legislar en la forma señalada en el proyecto original, esto es, haciéndose cargo de figuras delictivas específicas en una ley extra Código Penal, en vez de legislar abarcando la totalidad de la problemática informática, contemplando para ello la incorporación a las figuras penales tradicionales, ya existentes en el Código Penal, estas nuevas formas de comisión de ilícitos facultadas por las nuevas tecnologías, tipificando así el mínimo posible de delitos en leyes especiales, las que solo serían necesarias en caso de no ser posible la adaptación de tipos tradicionales a estas nuevas formas de comisión. Y evitando de paso, los posibles problemas de repetición y concursos entre figuras penales[34]. Esta idea, fue propuesta en la comisión por parte de Francisco Cumplido, el entonces Ministro de Justicia, no obstante desechada en pos de la protección del nuevo bien jurídico surgido con la tecnología y los sistemas de tratamiento de datos[35]. En la discusión y votación del proyecto en la Cámara de Diputados, fueron finalmente

[33] Subrayado por el autor de la presente investigación, para destacar el delito que finalmente se tipificará como el actual artículo 3° de alteración de datos que corresponde al objeto principal de estudio.
[34] En el presente trabajo de investigación se pudo observar una gran cantidad de casos en que se dio origen a estos problemas, particularmente en materia de concursos, cuyo tratamiento en extenso escapa al objeto principal del mismo.
[35] La discusión entre las formas de legislar sobre la tipificación de los delitos derivados del fenómeno informático será abordada en el apartado iv, denominado "La posición sistemática de la ley 19.223 en el contexto del derecho penal chileno".

aprobadas las siguientes modificaciones: se retiraron los artículos 3° y 5°, y propuesto uno nuevo que pasaría a conformar –provisoriamente– el artículo 4° y rezaba: "Artículo propuesto: El tribunal podrá cambiar las penas establecidas en los artículos anteriores por penas pecuniarias de multa, de cinco a mil unidades tributarias mensuales, cuando las consecuencias del delito no fueren de especial gravedad". Además, en el artículo 1°, se cambió la palabra "indebidamente" por "maliciosamente", y se rebajó la pena asociada al delito a presidio menor en su grado medio a máximo. Por su parte, el artículo 2°, fue modificado en el sentido de bajar su penalidad a presidio menor en su grado mínimo a medio. Además, se agregó en la discusión en la cámara de diputados la frase: "el que sin derecho y con ánimo de apoderarse indebidamente de la información contenida en un sistema automatizado de tratamiento de la misma, lo intercepte, interfiera o acceda a él". En el artículo 4°, también fue sustituida la palabra "indebidamente*"* por "maliciosamente*"*. Y, se suprimieron las expresiones "introduzca, transforme y desfigure*"*, considerándose comprendidas dentro del concepto "altere*"*. Además de pasar a ser el artículo 3°, luego de la eliminación del original.

Previa aprobación en la Cámara de Diputados, en el segundo trámite constitucional el proyecto ingresó al Senado para su discusión, el cual derivó el proyecto a la Comisión de Constitución, Legislación, Justicia y Reglamento. Dicha Comisión, realizó algunas sugerencias y modificaciones a algunas partes del proyecto: La supresión de las palabras "automatizado*"* de los artículos 1°, 2° y 3°[36]. En el artículo 2°, fue quitada la expresión "sin derecho*"* vinculada al verbo apoderarse, toda vez que su sentido se encontraba contenido en la expresión "indebidamente". Además, bajo sugerencia de la Asociación Chilena de Empresas de Informática A.G., fue incorporado un nuevo artículo orientado a penalizar a quien "incurra en revelación o transmisión maliciosa de datos contenida en un sistema de información castigándolo con la pena de presidio menor en su grado medio, aumentando la penalidad en un grado si el autor es el responsable del sistema". Además, la comisión rechazó la propuesta de

[36] Modificación, que a juicio de la mayoría de la doctrina nacional desvirtuó el sentido original del proyecto, el que estuvo previsto para la protección contra ataques en un contexto informatizado, entendido este solo dentro de un contexto de sistemas "automatizados" de tratamiento de la información, y no en contextos de tratamiento manuales de la misma, como sería el caso de carpetas y archivadores con información contenida en papeles u otros documentos. Aunque por otra parte, como se analizará más adelante la jurisprudencia ha aplicado esta norma solo a sistemas automatizados de tratamiento de información entendiéndola dentro de su contexto original.

incorporar la posibilidad judicial de permutar la pena privativa de libertad por una multa en caso de que no se hayan producido daños graves a raíz de los delitos contemplados en la ley.

Luego, en la discusión senatorial, se presentaron indicaciones de legislar sobre el cuasidelito informático, las que fueron rechazadas por la Comisión en su segundo informe, en el cual basó su decisión en consideraciones de orden penales y civiles, las que vale traer a colación: en cuanto al fundamento penal, es que nuestro ordenamiento solo permite el castigo de cuasidelitos cuando ellos son cometidos contra las personas, excluyendo de esta forma la posibilidad del castigo de las conductas culposas cometidas contra la propiedad. Por otro lado, la consideración civil responde a la razón de que las conductas culposas que generan daño económico a otros, se encuentra protegida por el estatuto de responsabilidad extracontractual, la que actúa en favor de la víctima a título de indemnización de perjuicios. Posterior a la emisión del segundo informe por parte de la comisión, el Senado pasó a establecer las siguientes modificaciones: sobre el artículo 2°, se incluyen además de apoderarse como verbo rector del tipo, las voces "usar o conocer" indebidamente. En el artículo 4°, se cambió el verbo "transmita" por el verbo "difunda", el que se entendió más amplio que el primero.

En el tercer trámite constitucional, en mayo de 1993 la Cámara de Diputados aprobó las modificaciones introducidas por el Senado, despachándose el proyecto. Para posteriormente, en el cuarto trámite constitucional en junio del mismo año, dar cuenta en el Senado de la aprobación que hizo la Cámara de Diputados de las modificaciones introducidas por este. Para finalmente, promulgar el proyecto por parte del Presidente de la República el 28 de mayo de 1993, para ser publicado en el Diario Oficial el 7 de Junio de 1993. El texto definitivo de la ley 19.223, que tipifica figuras penales relativas a la informática, es hasta hoy día, el siguiente:

> Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
> Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

> Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.
>
> Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.[37]
>
> Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

En cuanto las críticas al texto de la ley, se toma como referencia el trabajo de Renato Jijena "Delitos informáticos, internet y derecho"[38], las que se sistematizarán sin pretender realizar una exégesis de las mismas.

Lo primero que salta a la vista, es que del texto de la ley se desprende que su protección engloba dentro de los delitos informáticos los daños cometidos contra el soporte físico de un sistema de tratamiento de información, o *hardware* del mismo, siendo que esta conducta no es sino un delito común de daños, constituyendo un error en la tipificación de esta conducta, derivada según el autor de la "ignorancia parlamentaria"[39]. Toda vez que, existía en tiempos de dictación de la ley –e incluso hoy en día–, desacuerdos, confusión y desconocimiento, sobre lo que debe entenderse por delito informático, y por la especificación del objeto material del mismo delito. Esta confusión inicial, derivó en la protección del *hardware* como un delito informático, y no

[37] Subrayado por el autor del presente trabajo de investigación para recalcar el objeto del mismo.
[38] *Óp. cit*., Jijena Leiva, R. (2008).
[39] *Ibídem*. p. 157.

como un delito tradicional de daños ya contemplado por el ordenamiento jurídico, que hubiese sido lo adecuado.

En materia de protección de datos, la ley 19.223 excluye de su ámbito de aplicación, los delitos cometidos contra los datos personales o nominativos, extrayendo el autor, como conclusión de ello, que esta ley no considera la intimidad como un bien jurídico digno de protección jurídica. Esta ley tampoco distingue la naturaleza de los datos objeto de ataques. Ello, porque se tipifica la conducta contra los sistemas de tratamiento de información, sin considerar que la relevancia del daño, en último término está dada por la naturaleza de la información contenida en ellos. Estos datos, a su vez, pueden obedecer a diferentes ámbitos de intereses, representados por bienes jurídicos diversos como el patrimonio, la intimidad o los secretos industriales. Así, en palabras del autor: "la alteración de datos que dan cuenta de una situación patrimonial merecen mayor nivel de protección que los datos que, por ejemplo, dan cuenta de una receta de cocina", toda vez que el bien jurídico es diferente, y uno de mayor importancia que el otro[40].

Se suma a ello, la alta penalidad que consagra el artículo 3° para aquellas personas que incurran en la conducta descrita –presidio menor en sus grados medio a máximo–, sin hacer la distinción entre las calidades de los datos maliciosamente alterados, dañados o destruidos. Esta crítica, relativa a la alta penalidad impuesta por la ley 19.223, es particularmente significativa en el artículo 3°, pero según Rodolfo Herrera Bravo se hace extensiva a todo el articulado de la misma, toda vez que consagrar penas privativas de libertad en este tipo de delitos no pareciera ser la forma más adecuada de enfrentarse a los mismos[41].

[40] *Ibídem*. p. 158.

[41] Así, citando un informe del Instituto de Ciencias Penales enviado al congreso durante la tramitación del proyecto, en el cual, su entonces director Carlos Kunsemüller, se refirió al tema en las siguientes palabras: "…consideramos muy positivo el hecho que se consagre la facultad del tribunal instructor de sustituir la pena… por multa cuando….- Creemos que en este tipo de delitos, de caracteres muy particulares, en cuanto al entorno cultural y socio-económico en que normalmente se habrán de producir y a la tipología criminológica de los delincuentes, la privación de libertad –cuya crisis es por todos reconocida- no parece ser el tipo de sanción más adecuado. desde un punto de vista político criminal. Una pena pecuniaria severa, bien administrada, y ejecutada, a través del sistema de días-multa, por ejemplo, con fracciones que disminuyan en forma sustancial el nivel de la vida del condenado, como así mismo, ciertas formas de trabajo obligatorio, como la prolongación de la jornada laboral, el trabajo de fin de semana, la ejecución controlada de determinadas actividades, destinadas a reparar el daño ocasionado… podrían operar como alternativas que satisfarían las exigencias de retribución, prevención general y especial, sin provocar los males tan conocidos de la pena carcelaria".

En cuanto al bien jurídico protegido, se estableció en la discusión del proyecto, en cuanto a la finalidad de protección de la ley, que esta tenía por objeto "proteger este nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales, la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema de tratamiento de la misma y de los productos que de su operación se obtengan"[42]. Renato Jijena, considera que la actitud del legislador de esta ley, al optar por proteger este "nuevo bien jurídico" fue "errada, simplista, burda y ambigua". Así, explica el autor, "nos pareció inadecuado aludir a ´la información en cuanto tal, sin otorgarle una carga o contenido valorativo, sin reparar en que no todo conjunto de datos reviste igual importancia´"[43]. Este error, se puede afirmar que no fue involuntario sino que más bien intencional, toda vez que "la Comisión de Constitución y Legislación fue sumamente clara en su segundo informe, cuando señaló que ´al legislar no debe importar el tipo de legislación sino las acciones delictuales (métodos de comisión) para obtenerla de forma ilícita´"[44]. Continúa el autor, señalando que en el segundo informe de la Comisión de Constitución de la Cámara de Diputados, el error se agrava, al punto de que solo resta concluir una incomprensión conceptual y de desconocimiento de la razón de ser de la criminalidad informática. Ello, porque textualmente señala la Comisión que "para ella el sistema informático es un nuevo bien jurídico que se quiere proteger, el cual difícilmente puede asimilarse a otros penalmente protegidos"[45]. Esto demuestra que, si bien la confusión de considerar como delitos informáticos a los ataques contra el soporte físico del sistema es una falta grave de conocimientos conceptuales, el considerar el sistema de tratamiento de información, esto es el objeto material de los delitos informáticos como el bien jurídico protegido por el mismo, haciéndolos equivalentes, resulta aún más grave.

Adicionalmente, la ley ha sido duramente criticada por insuficiente, al no llenar los vacíos que existían –y aún existen– en determinadas materias, como en caso del llamado fraude

Citado por Herrera Bravo, R. (1998). Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la ley chilena N° 19.223. pp. 4 y ss.

[42] *Óp. cit.,* Jijena Leiva, R. (2008)

[43] *Ibídem.*

[44] *Ibídem.*

[45] *Ibídem.*

informático, el que puede ser entendido de una forma amplia como "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"[46]. En su trabajo de investigación, Claudio Magliona y Macarena López, destinan el punto central de ella al análisis de este delito, donde una de sus conclusiones es la inexistencia de este delito en las conductas descritas en la ley 19.223[47]. Lo que además, encuentra sustento explícito en la jurisprudencia nacional[48].

Además, por un sector de la doctrina, se le critica a la ley 19.223 que si bien, en su artículo 2°, contempla el acceso indebido a un sistema de tratamiento de información lo hace con la exigencia de un ánimo especial, esto es el "ánimo de apoderarse, usar, o conocer la información contenida en este o ánimo de alterar los datos". Ello quiere decir, que mientras no concurra este ánimo especial, no se incurre en la conducta tipificada por el artículo 2°, lo que apareja como consecuencia, que el mero acceso no se encuentre tipificado como delito en nuestro ordenamiento. Un acceso, acompañado de un *animus iocandi*, por ejemplo, o un acceso con la intención de demostrar conocimientos en el área de la informática, no se encuentra sancionado por el ordenamiento jurídico penal chileno. Esto, según algunos autores, constituye una omisión de la ley que debiese subsanarse, toda vez que constituiría una acción potencialmente delictiva[49], aunque la penalidad asociada, claro está, debiese ser menor. Por otro lado, hay autores que consideran que a pesar de la falta de tipificación de esta conducta, no es adecuado tipificarla

---

[46] *Óp. cit.*, Magliona Markovicth, C., & López Medel, M. (1999). p. 189.

[47] *Ibídem*. pp. 227 y ss. Los autores, hacen uso de motivos de historia legislativa, legislación comparada en la cual se basó la ley 19.223, en particular su regulación en ley francesa de 1988, y razones específicas del texto de la ley 19.223.

[48] En este sentido SCA Valdivia, Rol 312-2018 (22.05.2018) haciendo referencia al concepto de estafa informática; SCA Concepción, Rol 844-2014 (30.01.2015); SJG Curicó, Ruc 1301170732-1 (04.09.2015); y finalmente la sentencia del JG Concepción 1410003541-4 (16.05.2016) que destaco:

> éste y si bien en principio doctrinalmente enfrentamos un fraude informático, no encontrándose éste tipificado en nuestra legislación, se ha dado por establecido el referido delito, descartando cualquier otro no cubierto en todos sus elementos como éste de mayor simpleza, que requiere sólo de alteración de datos, aunque no existiese perjuicio alguno para el administrador del sistema de tratamiento de información, pues lo relevante es que se afecte el soporte lógico del sistema, lo que hizo al ingresar información no fidedigna en el sistema registral mediante una cancelación improcedente, que sólo en el sistema puede producir efecto no así en la boleta de garantía como evidencia de la caución que involucra tal documento.

[49] *Óp. cit.*, Magliona Markovicth, C., & López Medel, M. (1999). p. 178.

como delito, dado que en la conducta se desarrolla en el ámbito de un bien de libre acceso al público, cual es internet, "en que no existen derechos a la intimidad absolutos sobre la información que se contiene en los sitios de dominio electrónico, puesto que estos se exponen al riesgo en forma consciente, con pleno conocimiento de la potencial vulnerabilidad de las restricciones al acceso". Además, al ser considerado como un delito de peligro abstracto, el *hacking*, en su faceta de mero acceso "es ejercicio de la libertad de información, por lo que no puede ser justificación de tipificación a título de delito de peligro, sin que ello importe violar flagrantemente la proscripción de censura previa", derivada del art. 19 n° 26 de la Constitución Política de la República[50].

iii. Las distintas finalidades de protección de la Ley 19.223: sistematización teleológica de su regulación

La exposición de los conceptos e ideas de este capítulo está, en su mayor medida, tomada de la investigación realizada por Laura Mayer Lux[51], la que aborda la cuestión de forma mucho más profunda que en el presente trabajo. Aquí, el único propósito es poner en conocimiento de quien lea, las formas en que se han entendido los fines de protección de la ley 19.223 a lo largo de su vigencia. Así, desde una base doctrinaria, se esbozarán las distintas concepciones que se han tenido del criterio de protección de los delitos informáticos en general, para luego exponer cuáles han sido las formas en la que los tribunales del país han conciliado dichas posturas con la situación fáctica a cual se enfrentan.

En primer lugar, resulta útil aclarar que se dará por establecido que se entenderá por bien jurídico lo que la autora establece como: "aquellas condiciones materiales e inmateriales de las personas cosas o instituciones, que sirven al libre desarrollo del individuo en un Estado democrático de derecho. Además, asumirá que para cumplir adecuadamente las funciones que le son propias, los bienes jurídicos deben identificarse directa o indirectamente con intereses concretos de personas concretas, cuya tutela penal se justifica frente a ataques graves de terceros, a la vez que

[50] Escalona Vásquez, E. (2004). El hacking no es (ni puede ser) delito. pp. 166 y ss.
[51] Laura Mayer Lux. (2017). El bien jurídico protegido en los delitos informáticos.

solo resulta legítima en la medida en que pueda conciliarse con las normas constitucionales vigentes"[52].

Luego, resulta relevante también señalar las funciones que cumple el bien jurídico para la ciencia penal y es que, como indica la autora, su importancia radica en tres grandes ejes. En primer lugar, este concepto "permite fundamentar el castigo punitivo de las conductas que lo lesionan o ponen en peligro y constituye un requisito ineludible para el ejercicio del ius puniendi"[53]. En segundo lugar, indica que tanto "la importancia relativa de un bien jurídico como su grado de afectación sirven de criterio para el establecimiento de penas proporcionales"[54]. En tercer lugar, "permite determinar el injusto específico de cada delito, sistematizar los tipos penales que conforman la parte especial y orientar la interpretación de los comportamientos que ellos reprimen"[55]. En otras palabras, el bien jurídico es útil a la ciencia penal, tanto como fundamento del castigo, así como para evaluar la proporcionalidad del mismo, y además, como criterio sistematizador de la parte especial.

A grandes rasgos, las posturas doctrinales sobre el bien jurídico protegido por la ley sobre figuras penales relativas a la informática en Chile asumen tres posiciones, las que a su vez se vinculan con la forma en que se debiese legislar sobre estos delitos. Es decir, dependiendo del fin de protección de la norma se establecería si la correcta tipificación de estos delitos debiese darse en textos fuera del Código Penal en leyes específicas, o bien, dentro del Código Penal.

En primer lugar, se encuentra la postura de que la ley 19.223 protege "un bien jurídico específico, propiamente informático, diverso del que protegen los delitos tradicionales"[56]. Esta forma de asumir el rol de tutela de los delitos informáticos trae aparejada la propuesta de tipificación de estos delitos en normas especiales, extracódigo, "tendiente a la tutela autónoma de este específico interés que vayan más allá de una mera reformulación de los tipos penales

[52] *Ibídem*. p. 236.
[53] *Ibídem*. p. 235.
[54] *Ibídem*.
[55] *Ibídem*. p. 236.
[56] *Ibídem*. p. 238.

tradicionales"[57]. Es en este sentido, en el que la ley 19.223 fue orientada durante su elaboración. Así se extrae de las sesiones de discusión del proyecto, en que se destinó a proteger un "nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales" y que corresponde según la forma de entender del legislador de esta ley a: "la calidad, la 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" [58]. No obstante ello, la autora propone en su texto una forma de entender el bien jurídico protegido como puramente informático más precisa y acorde al desarrollo de las tecnologías de información y comunicación actuales, toda vez que si recordamos, la ley 19.223 fue discutida y dictada entre los años 1991 y 1993, años en los cuales aún no se podía siquiera dimensionar la evolución que tomarían las TICs. Concluye la autora que: "El reconocimiento de la funcionalidad informática como bien jurídico específico, propiamente informático, se justifica si los delitos informáticos, junto con incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. En ese contexto, la funcionalidad informática constituye, por una parte, un interés cuyo sentido y alcance debe precisarse dinámicamente, así como en atención a la forma en que opera el uso de redes computacionales, en tanto sistemas de interconexión (remota y masiva) entre los individuos. Ella constituye, por otra parte, un bien jurídico instrumental de carácter colectivo, cuya tutela penal debe verificarse en términos particularmente acotados".*[59]*

En segundo lugar, se encuentra la doctrina que, por el contrario de la anterior, sostiene que "los delitos informáticos no tutelan bien jurídico específico y que en ellos ´lo informático´ no es más que un contexto delictivo o un particular medio de afectación de bienes jurídicos tradicionales como la intimidad, o privacidad, el patrimonio o la fe pública"[60]. La consecuencia inevitable, en términos de una buena técnica legislativa será entonces, la tipificación de estas figuras dentro de los tipos tradicionales según el bien jurídico tutelado, sea incluyéndolas directamente en

[57] *Ibídem*.
[58] Historia fidedigna de la ley Boletín 412-07. Primer Trámite Constitucional: Cámara de Diputados. Moción Parlamentaria en Sesión 19. 16 de julio, 1991.
[59] *Óp. cit.*, Mayer Lux, L. (2017). p. 255.
[60] *Ibídem*. p. 239.

estos, o bien modificando la tipificación de los delitos tradicionales para incorporar el factor informático en la configuración de los mismos[61].

En tercer lugar, la doctrina quizás mayoritaria en nuestro país, es aquella que considera los tipos de la ley 19.223 como "figuras pluriofensivas, esto es, delitos que afectan a más de un bien jurídico"[62]. Una parte de esta doctrina sostiene que los "delitos informáticos protegen un bien jurídico específico, propiamente informático, y común a todos los delitos de la ley 19.223; a la vez que lesionan o ponen en peligro otros bienes jurídicos, como la intimidad o privacidad, el patrimonio o la fe pública", compatibilizando, de esta manera las dos posturas anteriormente mencionadas[63].

La jurisprudencia mayoritaria, en cuanto al alcance de protección de la ley 19.223, se pronuncia en el sentido de la postura que considera a los delitos informáticos contenidos en dicha ley como pluriofensivos. Esto es que, además de proteger un bien jurídico nuevo, puramente informático como quedó establecido en la discusión legislativa, protegería además distintos bienes jurídicos tradicionales según sea el caso.

En cuanto a la jurisprudencia en esta materia, resulta relevante mencionar la sentencia de la Corte Suprema causa Rol 3951-2012 (20.03.2013), que rechazó los recursos de casación en el fondo interpuestos en el marco de un procedimiento judicial militar, donde se condenó a tres personas por los delitos de los artículos 2° y 4° de la ley informática, referidos al delito de acceso indebido y difusión de datos respectivamente. Los hechos de esta causa se refieren a que en un regimiento militar ubicado en Limache, un Oficial solicitó un *pendrive* a otro, con la excusa de respaldo de documentos. Dicho individuo, se dirigió a su oficina y accedió sin autorización al computador personal de su vecina de oficina, que ostentaba el grado de Subteniente. Habiendo

[61] En este sentido, se pronuncian en la doctrina nacional Medina Schulz, G. (2014). Estructura típica del delito de intromisión informática. p. 96; Londoño Martínez, F. (2004). Los delitos informáticos en el proyecto de reforma en actual trámite parlamentario. p.173; Hernández Basualto, H. (2008). Uso indebido de tarjetas falsificadas o sustraídas y de sus claves. p. 23. Todos ellos citados en Mayer Lux, L. (2017). p. 239.

[62] *Óp. cit.*, Mayer Lux, L. (2017). p. 239.

[63] Adhieren a este planteamiento Magliona Markovicth, C. (2002): Análisis de la normativa sobre delincuencia informática en Chile. p. 238; Magliona Markovicth, C., & López Medel, M. (1999). p. 64; Moscoso Escobar, R. (2014). p. 17, p. 35; Donoso, Matías (2002). Bien jurídico protegido y delincuencia informática. pp. 144 y ss. Todos ellos citados en Mayer Lux, L. (2017). p. 239.

accedido a este, copió en el *pendrive* prestado una serie de archivos contenidos en carpetas, dentro de los cuales se contenían algunas fotografías y videos de contenido sexual de la referida Subteniente, archivos que fueron exhibidos dentro de un grupo de Oficiales del Regimiento de Limache durante los días sucesivos. Fueron presentados respectivamente dos recursos de casación en el fondo ante la Corte Suprema, en cuyo conocimiento, se pronuncia en su considerando 6° acerca de cómo la ley 19.223, además de proteger los sistemas de tratamiento y almacenamiento de datos, en el artículo 4° se protegería el bien jurídico referido a la intimidad, referido en el caso de autos al núcleo duro de la intimidad personal, como lo es la vida sexual de las personas, y utilizándolo como argumento para en definitiva rechazar los recursos interpuestos, reafirmando la condena de los imputados. Asumiendo de esta forma, una postura en la que la ley de delitos informáticos tipifica delitos de carácter pluriofensivos[64]. Así, la Corte:

> Lo que se sanciona es el empleo de procedimientos dolosos destinados a afectar no sólo el sistema de tratamiento y almacenamiento de datos como erróneamente postulan las defensas, sino también difundir la información ilícitamente obtenida, de manera que sea conocida por terceras personas, lo que a su turno incrementa las posibilidades de que nuevamente sean utilizados y difundidos, como en la especie ocurrió. En el caso de autos quedó establecido que los sentenciados de un modo subrepticio o con un conocimiento no autorizado de la clave de acceso a un computador, vulneraron un *software* e información confidencial allí almacenada, la que se extrajo a través de un dispositivo externo de almacenamiento para efectos de exhibirse y difundirse a terceros.

[64] En el sentido de considerar los delitos como pluriofensivos, y en específico referidas a la protección de la privacidad, también se pronuncia la SCA de Valparaíso Rol 837-2012. (08.08.2012) que rechazó el recurso de nulidad presentado y confirmó, por ende, los argumentos de la STOP de Viña Ruc 0910023307-7 (23.04.2012). Entre sus motivos para absolver, se señala que "*Tampoco resultó probado que los acusados hubieren vulnerado el derecho a la privacidad de ambas funcionarias"*, a las que se los acusaba de cometer el delito contenido en el artículo 4° de la ley; También, la sentencia del TOP de Coyhaique en causa Ruc 1610036482-9.(24.07.2018) Que, en la prevención hecha por el Juez Sr. Edmundo Devia refiriéndose al artículo 2° y 4° de la ley, asevera *"que ambos artículos protegen la privacidad del titular de la información, entendiéndose como la eventual posibilidad de excluir a terceros del acceso a esferas de dominio de ese titular, es decir se puede concordar esa noción de privacidad como concepto formal, pero se debe tener en cuenta el rasgo distintivo especial de excluir a terceros".*

> En lo que respecta al bien jurídico, el legislador dispensa en este caso una protección penal especial entre otros, a los denominados datos sensibles o el llamado "núcleo duro" de la intimidad personal, entre los que se encuentran aquellos que recaen en la vida sexual de las personas, carácter que tenía la información a la que los sentenciados accedieron y compartieron con otros sujetos.
>
> Así las cosas, en el caso de autos debe concluirse que al hacerse aplicación de la norma sancionatoria que se estima conculcada no se ha incurrido en infracción de ley, pues en la sentencia atacada han sido declarados aquellos hechos señalados en la disposición y que constituyen el acto típico, lo que hace que los recursos no puedan ser acogidos.

No obstante, esta sentencia fue obtenida con un voto en contra, correspondiente al Sr. Haroldo Brito, quien se opuso a este argumento, y por ende estuvo por acoger los recursos de casación en virtud que la conducta de los imputados no afecta el bien jurídico protegido por esta ley, el que estaría constituido por uno puramente informático:

> el hecho de haberse copiado una información contenida en un registro computacional para, luego, mostrarla a terceros, no importa el ilícito del artículo 4° de la Ley N° 19.223, por cuanto del examen de su artículo 1° deriva que el bien jurídico protegido dice relación con la seguridad de los sistemas de información o sus partes, su funcionamiento, su indemnidad o el uso indebido de la información, lo cual no ha sido lesionado en modo alguno, en su entendimiento, el fallo impugnado incurre en la infracción de ley denunciada.

Se puede afirmar, según las sentencias analizadas, que cuando los tribunales hacen referencia al bien jurídico protegido por la ley 19.223, parten de la base de que en la historia legislativa de la misma se estableció expresamente la existencia de un bien jurídico nuevo, por lo que difícilmente podrían obviar esta consideración. Ahora bien, algunas de las sentencias al hacerlo reconocen la existencia de otros intereses protegidos por los delitos informáticos, acercándose

por ello a la postura que considera estos ilícitos como pluriofensivos, tal como en caso recién expuesto. Aunque no por ello, puede afirmarse que sea conteste. Mayor abundamiento sobre las posturas adoptadas por los tribunales de justicia, serán abordadas en el Capítulo II.

iv. La posición sistemática de la Ley 19.223 en el contexto del derecho penal chileno

Para finalizar el marco histórico y conceptual, por el cual se regirá este trabajo de investigación, corresponde hacerse cargo de la posición sistemática que ocupa la ley 19.223 en nuestro Derecho. Luego de las consideraciones, tanto de política legislativa, como teóricas que se sostuvieron en la discusión del proyecto en el Congreso Nacional expuestas en los apartados anteriores, el resultado fue la consagración de algunas figuras penales relativas a delitos informáticos contenidas en cuatro artículos de una ley especial, esto es, fuera del Código Penal. Estas figuras, muchas veces presentan problemas de aplicación, como se da en caso de ser el artículo 1° de la ley 19.223 una repetición del tipo tradicional de daños, consagrados en el Código Penal, pero enfocado a los daños a un sistema de procesamiento de datos en su parte física o *hardware*. O bien, la no inclusión oportuna de otros tipos penales, como el fraude informático, cuya falta de tipificación ha llevado a los actores del sistema penal a hacer malabares para adecuar la concepción del mismo a los delitos actualmente vigentes.

La idea de tipificar estos delitos fuera del sistema penal general, no fue –ni es– compartida por todos los actores del derecho informático, y sin ir más lejos dentro de la discusión parlamentaria de la ley 19.223, incluso se sostuvo por parte del gobierno de turno, la idea de incorporar los delitos contenidos en la moción del diputado Viera-Gallo al Código Penal, idea que finalmente fue desechada[65]. Posteriormente, en diferentes propuestas de reforma legislativa esta idea ha persistido, con el afán de que los delitos computacionales e informáticos contenidos en la ley 19.223, y otros no contenidos oportunamente en esta, pasen a integrar el Código Penal. Esta forma de incluir los delitos informáticos dentro del sistema criminal general, puede darse mediante la complementación de delitos tradicionales, incorporando las nuevas modalidades de

[65] Contenido en el Segundo informe de la Comisión de Constitución Legislación, y Justicia sobre el proyecto de ley sobre delito informático, Boletín Oficial número 412-07.

comisión derivadas de las nuevas tecnologías, o bien, mediante la creación de nuevos tipos penales creados para hacer frente a nuevas conductas que ponen en peligro o vulneran bienes jurídicos protegidos por el Derecho, los que en concordancia con la lógica de los bienes jurídicos protegidos, serían incluidos y clasificados bajo los capítulos y títulos respectivos. Ello, toda vez que dicha figura no sea reconducible, sin más, a algún tipo tradicional prexistente, como ocurre actualmente con el artículo 1° de la ley, en relación a los ataques al *hardware*, que bien puede incluirse dentro de las formas de comisión del delito tradicional de daños.

Así, es posible dividir las posturas que la doctrina nacional ha adoptado a este respecto, en dos grupos. Por un lado, se encuentra aquella llamada postura fenomenológica, caracterizada por considerar el fenómeno informático como una nueva y especial área del Derecho, a la que correspondería darle un tratamiento separado de las tradicionales. Por otro lado, aquella doctrina basada y orientada según el bien jurídico protegido, la que postula que estos nuevos tipos penales surgidos con la informática, si bien modifican la forma de comisión de los atentados contra bienes jurídicos, son solamente esto: formas nuevas de comisión de conductas atentatorias contra bienes jurídicos prexistentes. Razón por la cual, convendría su regulación de acuerdo al sistema penal general, esto es dentro del Código Penal.

Resulta pertinente citar a Héctor Álvarez Fortte, en cuanto al análisis de la forma de legislar por la que optó el legislador de la ley 19.223, al exponer que "En la época en que se dictó la ley 19.223 (y al día de hoy también) existían dos corrientes de respecto del tratamiento de este tipo de delitos: por un lado una corriente postulaba en tratar los delitos informáticos como una nueva pequeña rama del Derecho penal, este es el modelo fenomenológico[66]. La segunda corriente intenta integrar el tema de los delitos informáticos en el campo ya regulado por el Derecho penal, introduciendo solo las modificaciones o ampliaciones necesarias en los tipos penales tradicionales, de manera tal de poder comprender en ellos la ejecución de los tipos por medio

[66] La expresión fenomenología aplicado a este disciplina, está originalmente tomada del informe del profesor Héctor Hernández, y "se usa para significar la apuesta por una incriminación directamente en función de las modalidades comisivas (el fenómeno, desde un punto de vista criminológico), antes que en atención a la valoración jurídica de dichas modalidades o fenómenos (por ejemplo, en conformidad a criterios como el interés jurídicamente protegido)". En Londoño Martínez, F. (2004). p. 173. Nota al pie n° 10.

de mecanismos informáticos. En síntesis la primera opción se centra en el fenómeno criminal; la segunda, en el bien jurídico protegido"[67].

En el caso de nuestro país, la opción de regular estos delitos ciertamente corresponde a la segunda forma, toda vez que no se tomó en cuenta los bienes jurídicos tradicionales para su agrupación sistemática dentro de nuestro ordenamiento. Esta estrategia no es innovadora ni tampoco su opuesta, así el autor señala como ejemplos que han seguido una fórmula de tratamiento de los delitos informáticos tal como Chile, los siguientes países: Francia hasta 1988, Australia, Canadá, Estados Unidos, Inglaterra y Japón. Al contrario, se mencionan como ejemplos de legislaciones que optaron por su regulación en consideración de los bienes jurídicos tradicionales, más las correspondientes adecuaciones al sistema penal general según las diferentes conductas informatizadas, las siguientes legislaciones: Francia a partir de 1988, Italia, España, Alemania, y Suiza[68].

Esta forma de consagrar los delitos relativos a la informática no fue pacífica a la hora de legislar, sino que fueron sugeridas en Cámara de Diputados algunas formas de incluir estos delitos dentro del sistema penal general[69], como también se deduce que era la intención del gobierno el que estos delitos pasaran a formar parte del sistema general[70]. Las razones dadas finalmente, para consagrar estos delitos en una ley extracódigo fueron: en primer lugar, por los inconvenientes de técnica legislativa, y en segundo lugar, la consideración de que ello acarrearía problemas en cuanto a la determinación del bien jurídico protegido. Ambas razones, son consideras por Héctor Álvarez, citado más arriba como erradas, señalando como ejemplo la forma en que fueron contemplados estos delitos en el anteproyecto de nuevo Código Penal para Chile, logrado por el Foro Penal sin mayores dificultades, adaptando las figuras tradicionales al fenómeno informático e incorporando estas al anteproyecto, según la vulneración o puesta en peligro de los diferentes bienes jurídicos protegidos. En este mismo sentido, se pronuncia Fernando

[67] Álvarez Fortte, H. (2009). Los delitos informáticos. p. 104
[68] *Ibídem*. p. 104.
[69] Sesión 24°, martes 4 de Agosto de 1992, y 33°, jueves 20 de agosto de 1992, ambas de la Cámara de Diputados; y 32°, en jueves 11 de marzo de 1993, en el Senado.
[70] Contenido en el Segundo informe de la Comisión de Constitución Legislación, y Justicia sobre el proyecto de ley sobre delito informático, Boletín oficial número 412-07.

Londoño Martínez, al afirmar que "si en algo se ha caracterizado el derecho penal informático, es el de precisamente pretender ser un derecho penal informático; es decir, un ´algo especial´ dentro del derecho penal general, un pequeño mundo dentro del gran mundo del derecho penal"[71]. Así, y citando la exposición de motivos del mensaje del Ejecutivo en el proyecto de reforma contenido en el boletín número 3083-07, el autor se refiere a las consideraciones para preferir un sistema de adecuación de los delitos informáticos orientado según el bien jurídico protegido a uno fenomenológico –guiado por las características del fenómeno informático–. El mensaje se refiere a la situación en los siguientes términos: "La aproximación fenomenológica desvincula fuertemente la nueva valoración del sistema de valoraciones subyacentes en el ordenamiento penal, dando lugar a numerosos problemas de legitimación y de coherencia normativa. En efecto (…), la regulación fenomenológica no da señales sobre su fundamento: solo vincula sanciones a determinadas conductas que aparecen como típicas, sin que se reflexione sobre las razones que legitiman tal incriminación. La puerta a la reflexión la abre recién la consideración de los bienes jurídicos protegidos. Sólo desde esa perspectiva pueden detectarse los excesos, como son las hipótesis en que no se vislumbra bien jurídico a proteger, así como, tanto más importante, sólo desde esta perspectiva se puede comprobar la coherencia interna del sistema: ¿por qué el acceso indebido a los datos contenidos en un computador personal debe sancionarse más severamente que la interceptación de correspondencia?, o ¿por qué la alteración de datos que dan cuenta de una situación patrimonial merecen mayor nivel de protección que los datos que, por ejemplo, dan cuenta de una receta de cocina? Se trata de preguntas que sólo pueden plantearse racionalmente desde la perspectiva del bien jurídico protegido (…)

Existe, además, un segundo nivel de fundamentos para optar por el modelo mencionado. Recoger estas nuevas formas comisivas en los tipos tradicionales del Código Penal significa dotarlas –de inmediato y en relación a sus bases– del importante acervo jurisprudencial y doctrinario acumulado durante años de vigencia de dicho cuerpo normativo. Evidentemente, esta ´dote´ se traduce en mayor certeza jurídica, atributo que –se comprende– es particularmente precioso tratándose de formas delictivas surgidas a partir de fenómenos como el desarrollo

[71] *Óp. cit.*, Londoño Martinez, F. (2004). p.173.

tecnológico. En consecuencia, el modelo aquí auspiciado viene a favorecer, además un más normal uso de estos tipos penales por parte de los actores del sistema: jueces y abogados"[72].

En este mismo sentido, se pronuncian Rodolfo Herrera y Alejandra Núñez al decir que "(…) la ubicación del texto fuera del Código Penal nos parece una desafortunada técnica legislativa, y lamentamos que las opiniones de algunos parlamentarios en este mismo sentido no hayan sido escuchadas. Compartimos algunas ideas que se plantearon en la discusión de la ley, tales como que al tratarse de una legislación codificada, la tendencia de los legisladores debería fortalecerla y no seguir creando legislaciones penales particulares y especiales que sólo sirven para desperdigar la normativa penal existente, lo que dificulta la labor del juez y la defensa de los inculpados. Además, pensamos que en la medida que no se incorporen los nuevos delitos que exige la realidad social en el Código Penal, dicho cuerpo legal quedará desadaptado a los tiempos actuales"[73].

En el estado actual de la situación legislativa se puede afirmar que es inminente la dictación de una reforma en esta materia[74], la que incorpora las figuras penales establecidas en el Convenio de Budapest, convenio que fue suscrito por Chile en el año 2001 y promulgado con declaraciones y reservas en el año 2017. En dicho instrumento, el tratamiento que se le dará a los tipos penales relacionados con la informática o cibercrímenes se orienta en el sentido mixto, toda vez que modifica el Código Penal, crea nuevos delitos y crea nuevos delitos en un cuerpo extra código. Derogando, por cierto la actual ley de delitos informáticos.

[72] *Ibídem.* pp. 174 y ss. Citando la exposición de motivos del mensaje en el boletín de proyecto de reforma a la ley 19.223, contenido en el boletín N° 3083-07.
[73] *Óp. cit.*, Herrera Bravo, R. y Núñez Romero, A. (1999). p. 266.
[74] Boletín 12192-25 que Establece nomas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.

II. Análisis del tipo penal contenido en el artículo 3° de la ley 19.223 a la luz de la jurisprudencia

El presente capítulo, trata la aplicación del artículo 3° de la ley 19.223 por parte de los tribunales de competencia penal de nuestro país, incluyendo sentencias de: Juzgados de Garantía, Tribunales Orales en lo Penal, Cortes de Apelaciones y Corte Suprema. La información es sistematizada y presentada conforme al orden conceptual de la teoría general del delito, esto es: bien jurídico protegido; autoría, contemplando a su vez sujeto activo y sujeto pasivo; elementos del tipo objetivo, que a su vez contiene los elementos verbo rector, objeto de ataque, medios y circunstancias comisivos; tipo subjetivo y eventuales elementos subjetivos del tipo; causas de justificación; y finalmente, causas de ausencia de culpabilidad y de exculpación. Así, se ofrece la información sistematizada y resumida conforme al orden de exposición del género del comentario de Código Penal.

El delito del artículo 3° de la ley se encuentra tipificado de la siguiente forma:

> Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

En lo sucesivo se desglosará el tipo penal de la forma antes mencionada y se aportará de forma ordenada la jurisprudencia generada a partir de cada uno de los elementos. Ello, como se verá no siempre es posible dado principalmente por lo escaso de la aplicación de la ley 19.223 en general, y particularmente del art. 3°. Ello, trae como consecuencia para el presente trabajo de investigación, que el tratamiento de los elementos del art. 3° por parte de la jurisprudencia en ocasiones deba ser justificado con la aplicación de los otros delitos de la misma ley, lo que no trae aparejado mayor inconveniente, toda vez que en la ley 19.223 se comparten muchos de los elementos contenidos en los delitos en ella tipificados.

Previamente, conviene hacer presente que este delito durante la vigencia de esta ley ha sido conocido como: un delito de sabotaje informático, alteración de datos, o bien, simplemente el delito informático contenido en el art. 3°, entre otras formas.

i. Bien jurídico protegido

En el Capítulo I se abordó el tema de los fines de protección de la ley 19.223 de forma general, esbozando las posturas que han asumido autores nacionales en cuanto al mismo, las que pueden resumirse en: aquella que está por considerar el bien jurídico protegido por todos los delitos informáticos uno nuevo y puramente informático; aquella que considera que los delitos informáticos protegerían bienes jurídicos tradicionales y por ende este nuevo bien jurídico no es más que un desacierto; y por último, la doctrina que considera a los delitos informáticos como pluriofensivos, lo que conlleva que además de el bien jurídico propiamente informático se protegerían según sea el caso, otros bienes jurídicos.

En general, la jurisprudencia reconoce como bien jurídico protegido, el establecido por los legisladores de la ley 19.223, como el bien jurídico protegido en común por todos los tipos contenidos en la misma: esto es la calidad, pureza e idoneidad de la información en cuanto tal y de los productos que de ella se obtengan[75]. Al hacerlo, no se pronuncian en el sentido de negar la tutela de otros valores jurídicos además del informático, o bien expresamente asumen una postura de considerar la calidad de pluriofensivos de los delitos informáticos contenidos en la legislación informática, tal como se mencionó en el Capítulo I, la sentencia de la Corte Suprema Rol 3951-2012, relativa al delito de acceso indebido y difusión de datos, se pronuncia en el sentido de considerar en general a los delitos informáticos como pluriofensivos, viéndose en ese caso en particular también vulnerado el derecho a la intimidad o privacidad. No obstante, dicha sentencia fue obtenida con un voto en contra, que consideró que la ley informática protegería nada más que el bien jurídico establecido en sus sesiones legislativas. Lo que nos permite afirmar que la jurisprudencia no se encuentra conteste en este punto.

[75] Historia fidedigna de la ley Boletín 412-07. Primer Trámite Constitucional: Cámara de Diputados. Moción Parlamentaria en Sesión 19. 16 de julio, 1991. p. 4.

Por lo tanto, en lo que sigue se expondrán algunas sentencias que se refieran al bien jurídico protegido por la ley 19.223, y en lo posible, en su aplicación particular al artículo 3°. Como comentario previo, se dará por establecido que según la postura que le otorga un carácter pluriofensivo a los delitos informáticos, el bien jurídico tutelado de forma indirecta diría relación con la materia en los datos contenidos en el sistema de tratamiento de información, lo que variaría dependiendo de cada caso particular, pudiendo obtener múltiples alcances, como hipotéticamente: el patrimonio, la propiedad, la honra o el valor económico de la empresa, secretos industriales, fe pública o incluso la vida.

Específicamente en lo que dice con el artículo 3°, se pronuncia la Corte de Apelaciones de Concepción[76], que en sede de nulidad, rechazó el recurso presentado por la defensa de una imputada por el delito de alteración de datos, acogiendo como motivos los siguientes relativos al bien jurídico protegido por la ley 19.223 en general y lo que según la Corte correspondería al bien jurídico protegido específicamente por el artículo 3° de la misma ley. La sentencia, razona concordantemente con la doctrina que establece como bien jurídico protegido por la ley el de "sentido, veracidad, claridad o pureza de la información", pero agregando además que:

> En el caso sub litis puede decirse, propiamente, que el bien jurídicamente protegido es colectivo y se traduce en la información como valor económico de la actividad de la empresa.

Inclinándose de esta manera por una concepción pluriofensiva del delito informático, que en este caso particular en relación al delito de alteración de datos vulneraría, además del bien jurídico puramente informático, el valor económico de la actividad de la empresa. En los hechos, se condenó en juicio oral a la imputada por haber alterado los datos del sistema informático de la empresa de combustible donde trabajaba, en el sentido de ingresar datos falsos relativos al estado los cheques de un cliente específico, lo que hacía marcándolos como pagados, para luego anularlos. Maniobra que autorizaba la extracción de combustible de la empresa por parte de

[76] SCA Concepción 844-2014 (30.01.2015), acoge la argumentación del TOP de Los Ángeles número de Ruc 0810011797-6 (11.12.2014).

dicho cliente, por encima de lo facultado. En lo relativo, en sus considerandos 6° y siguientes, la Corte señala:

> 6.- (…) La acción delictiva está destinada a alterar, destruir o dañar los datos contenidos en un sistema de tratamiento de información. Alterar los datos contenidos en un sistema sería, en consecuencia, alteraciones conductas como el ingreso o introducción de datos erróneos, el borrado de datos verdaderos, transformaciones o desfiguraciones de los datos, y en general toda conducta que implique cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla. Por lo tanto, lo afectado es el sentido, veracidad, claridad o pureza y alcance de la información contenida, la cual se verá afectada con conductas como las descritas.
>
> 7.- Que la sentencia recurrida en el motivo 8 se refiere al bien jurídico protegido señalando que "....este ilícito fue introducido por el cuerpo legal citado y, tal como se dejó constancia en sus diversos trámites legislativos, el bien jurídico a proteger por tal tipo penal es la calidad, pureza e idoneidad[77] de la información, contenida en los sistemas automatizados de tratamiento de la misma, así como los productos provenientes de la operación de dichos sistemas. (Primer Trámite Constitucional, Moción Parlamentaria, Pág. 4; Primer Trámite Constitucional, Discusión en Sala, Pág. 38 y 47; Segundo Trámite Constitucional, Segundo Informe de Comisión de Constitución, Pág. 77)"
>
> 8.- Que tal como se señaló precedentemente, en la hipótesis del artículo 3° de la ley mencionada, el bien jurídico tutelado es el sentido, veracidad, claridad o pureza de la información. Así lo señalan los autores Rodrigo Medina Jara, en su artículo Los delitos Informáticos en la Legislación Chilena, publicado en Revista Electrónica de Derecho Informático, N°44, marzo 2002; los autores Marcelo

[77] Subrayado en la original.

> Huerta y Claudio Líbano, en su obra Delitos Informáticos, Editorial Jurídica; Alejandro Vera Quilodrán en Delito e Informática, etc.
>
> En el caso sub litis puede decirse, propiamente, que el bien jurídicamente protegido es colectivo y se traduce en la información como valor económico de la actividad de la empresa. Distinto ocurre en el fraude informático, en que el verdadero bien a cautelar es el patrimonio, ya que el interés general en el adecuado funcionamiento del tratamiento electrónico de datos, de creciente importancia para la economía y la administración, resulta protegido sólo en forma refleja. (Nelson Pozo Silva, La tecno-estafa o la estafa informática, Gaceta Jurídica N°245, pág.10 y ss.)"

Manteniendo la línea jurisprudencial de considerar los delitos de la ley 19.223 como pluriofensivos, pero ya no vinculado al artículo 3°, también se encuentra la sentencia del TOP de San Bernardo causa Ruc 1100498003-6, (14.05.2016). El caso se encuentra enmarcado dentro del delito del artículo 4°, sobre difusión de datos. En su considerando 11°, literal iii, el tribunal establece el carácter pluriofensivo del mismo, que en la especie se da, en primer lugar, por la confidencialidad del soporte lógico de un sistema automatizado de información, el que constituiría el bien jurídico puramente informático, y en segundo lugar, sostiene que dicho artículo protege el bien jurídico de privacidad. En lo pertinente:

> En este mismo orden de ideas, y para efecto del correcto análisis de la configuración del tipo penal en cuestión, debe asentarse cuales son los bienes jurídicos tutelados por estas figuras, y así determinar su posible lesión. El Tribunal acoge la tesis conforme a la cual esta es una figura pluriofensiva. Existe un primer bien jurídico tutelado que fija la puerta de entrada de la punibilidad de esta conducta, ese bien jurídico es "la confidencialidad del soporte lógico de un sistema automatizado de información" (Moscoso, Romina, La ley 19223 en general y el delito de hacking en particular, revista chilena de derecho y tecnología, Vol. 3 nº 1 (2014) p. 16). "Así una conducta que no afecte datos confidenciales debe ser eximida de responsabilidad penal por faltar la

antijuricidad material" (Moscoso, Romina, ibídem). Supone tal bien jurídico evaluar la importancia de la información contenida en un sistema informático, ya que no toda la información digitalizada es merecedora del mismo grado de confidencialidad. Por otro lado, se postula que estos delitos son pluriofensivos, pues "los delitos informáticos también afectan otros intereses o valores como la intimidad…. [en todo caso] la confidencialidad de los datos de un sistema informático se convierte en la puerta de entrada, condición necesaria, para admitir la represión penal de un conducta lesiva de este interés" (Moscoso, Romina, ibídem, p. 17). Así las cosas, en lo que respectó a la conducta de los acusados Romero Román y Henríquez Morales, el Tribunal entendió no hubo antijuridicidad material que permitiera dar por configurado este tipo penal. En efecto, atendiendo al bien jurídico protegido por esta figura, la confidencialidad, y, teniendo en cuenta lo señalado supra, respecto del carácter de pública, para las partes interesadas, de toda la información que conste en un proceso penal remitido al Archivero Judicial, se debe necesariamente concluir que la información que fue obtenida y divulgada por los imputados no afectaba de ninguna forma la confidencialidad del sistema.

En este sentido aparece de manifiesto que dicha información es pública, y el sistema lo único que hace es ordenarla y facilitar su consulta. Por consiguiente, si bien los imputados divulgaron información contenida en el sistema de consulta del registro civil, en ningún caso aquella se encontraba limitada por una necesidad de confidencialidad. Luego, en su divulgación no se afectó ninguna reserva de la misma, ya que, perfectamente se pudo obtener por otra vía, respecto de la cual no rige ninguna limitación, y esta es, su directa consulta en el Archivero Judicial correspondiente. En lo que se debe poner hincapié al hacer este análisis es que, si bien la información en cuestión se encuentra digitalizada e incorporada a un sistema, no por ese solo hecho debe entenderse que sea confidencial. A su respecto debe hacerse un ejercicio de valoración que permita discernir si recae en dicha información dicha calidad. Y la conclusión a que se arribó es que no puede postularse esa calidad a su respecto, pues esa misma

información se encontraba fuera del sistema sin limitación de confidencialidad para las partes interesadas. Es decir la misma información contenida en proceso remitido al Archivero Judicial era la que en parte estaba consignada en el respectivo extracto de filiación.

Por su parte, y entendiendo que esta figura es pluriofensiva, el bien jurídico privacidad, respecto de la persona titular de esa información David Bravo Villavicencio tampoco se vio afectado con estas conductas. En primera instancia, pues de su propia parte se habría encomendado recabar esa información. Por otro lado si dicha información fue recabada, lo fue única y exclusivamente para solucionar su situación procesal conforme a los institutos penales, como la prescripción de la pena para este caso concreto. Es decir, esta información ya fue puesta al corriente de los terceros que intervinieron en el proceso por el propio titular de esa información. Luego, sólo a instancia y en su beneficio es que dicha información fue obtenida. Por ende no hay afectación alguna de su intimidad, pues hubo un acto previó de abrirla a terceros, los que se impusieron de datos relativos a condenas penales que pesaban en su contra sólo para efecto de poder verificar si aquellas podían declararse prescritas, y ante un anuencia tácita de quien solicitó se resolviera tal situación.

Algunos ejemplos, en el sentido de considerar solo como interés jurídico tutelado el establecido en la discusión de la ley informática, la sentencia del 4° TOP de Santiago en causa Ruc 1000626117-0 (08.06.2011), en lo relativo a revelaciones ilícitas y sabotaje, que haciendo referencia tanto a los artículos 3° y 4° de la ley 19.223, reconoce como bien jurídico protegido exclusivamente el informático, al considerar que la incorporación del artículo 4° sobre revelación de datos fue producto de la sugerencia de la Asociación Chilena de Empresas de Informática, y que se encontraba destinado a sancionar principalmente a quienes trabajaran en el mismo sistema de tratamiento de datos, situación que no se da en el caso particular, y por lo tanto derivó en una decisión absolutoria en esta parte. Por otro lado se absolvió a la acusada también en cuanto al artículo 3° de la ley 19.223, en razón de la falta de acreditación de la participación de ella. No obstante esta argumentación absolutoria, el tribunal condenó a otro

imputado por el delito de difusión de datos, quien si tenía acceso directo al sistema informático, haciendo coherente su interpretación. Así, en lo pertinente, su considerando 12° establece que:

> En cuanto a las imputaciones de participación en los delitos "informáticos" de revelaciones ilícitas y sabotaje, cabe señalar que el tribunal no pudo determinar responsabilidad de Margarita Cuadros Aedo, al considerar, por una parte, la historia del establecimiento de la ley 19.223, de acuerdo a la cual aparece que la incorporación de su actual artículo 4° fue producto de una idea sugerida por la Asociación Chilena de Empresas de Informática A.G., que buscaba sancionar una conducta que no estaba definida en el proyecto original, pero que guardaba estrecha relación con la idea matriz del mismo, como lo era la revelación o transmisión maliciosa de los datos contenidos en un sistema de información. Indica el informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, que en tal delito pueden incurrir principalmente quienes trabajan en el sistema, ya que los terceros ajenos a él necesariamente deberán cometer el de apropiación indebida de los datos. De esta manera, resulta evidente que los destinatarios de la conminación penal son los operadores del sistema, esto es, las personas que manejaban o accedían a esta fuente como custodios, posición que nunca ostentó la acusada Cuadros Aedo.
>
> La conclusión precedente guarda coherencia con los principios que inspiraron la dictación de la señalada ley, los que de acuerdo a los informes de la misma comisión citada precedentemente, apuntan a dar protección jurídica a la calidad, pureza e idoneidad de la información contenida en los sistemas para el tratamiento automatizado de la misma, así como de los productos provenientes de la operación de dichos sistemas.
>
> Los dos casos de este tipo que logró acreditar la fiscalía, relativos al funcionario público que accedió a esta base de datos reservada, Manuel Donoso Cáceres, da cuenta que éste, no recibió pago por la entrega de esta información. Así, si en los mismos acontecimientos hubiera mediado una recompensa económica,

> estaríamos en el escenario jurídico de atribuir a Cuadros Aedo otro delito de cohecho, pero tal cuestión ni se probó, ni tampoco está contenida en los hechos de la acusación.
>
> (…) Cuadros Aedo no era titular de la obligación de reserva ni de custodia de la referida información y la imputación a título de otras formas de autoría no elude la objeción primordial de no ser ella titular del deber que justifica la protección penal de las señaladas bases de datos que contienen la información que se pretende reservar.

En el sentido de reconocer nada más que el bien jurídico informático, el TOP de Curicó en causa Ruc 0910014546-1 (07.03.2011), enmarcada en el contexto del artículo 1° de la ley 19.223, referida a la obstaculización del funcionamiento de un sistema informático, en su considerando 9° establece que:

> (…) Se debe tener presente que la ley 19.223 lo que protege es la información de los datos contenidos en las redes informáticas y lo que se pretende con su aplicación es la constitución de un bien jurídico nuevo cual es "la calidad, pureza e idoneidad de la información" (Hernán Silva Silva) y así de algún modo impedir que dichos sistemas sean burlados para obtener beneficios tales como apropiación, uso o conocimiento de la información en ellos contenida para fines propios y diversos a aquellos para los cuales fueron creados o generados.

Así mismo, el JG de Concepción en la causa Ruc 1410003541-4 (16.05.2016), conociendo de un procedimiento abreviado, y enmarcado dentro del razonamiento de la atipicidad de la figura de fraude informático, hace suyo el entendido de que el bien jurídico tutelado por la ley 19.223 es el establecido en la historia fidedigna de la misma. Así, en su considerando 5° establece que:

> Sin embargo, al alero de nuestra deficiente legislación en materia de delitos informáticos, lo que se ha afectado como bien jurídico protegido es la información, pues conforme a la historia de la Ley 19.223, el autor de la moción

> que la origina, diputado Antonio Viera Gallo, fundamentando su propuesta señala que el propósito que se persigue es proteger la calidad, pureza e idoneidad de la información contenida en un sistema automatizado de tratamiento de la misma, y los productos que de su operación se obtengan, opinión sostenida por el autor Hernán Silva en su libro "Las Estafas, Doctrina, Jurisprudencia y Derecho Comparado", Editorial Jurídica, páginas 214 y siguientes (sobre la criminalidad informática v. también la obra de Manuel Jaén Vallejo, Estudios Penales, Editorial Lexis Nexis, páginas 136 y siguientes).

En cuanto al titular del bien jurídico lesionado o puesto en peligro, la ley tampoco distingue entre las calidades especiales de los sujetos afectados por los delitos contemplados en ella, por lo que solo cabe concluir que cualquier persona, sea natural o jurídica puede ser considerada como titular del interés en la conservación de los datos contenidos en un sistema de tratamiento de información. Esta postura es también compartida tanto por la doctrina[78] como por la jurisprudencia nacional.

La ya citada sentencia del TOP de Arica Ruc 1210014297-8 (18.07.2014), que si bien lo hace en relación art. 2°, lo hace de forma extensible al resto del articulado de la ley 19.223, estableciendo una persona jurídica como sujeto pasivo de la conducta. Así, en el mismo considerando decimotercero establece que:

> *"Ahora, en relación al* ***sujeto pasivo*** *del delito, teniendo en consideración el bien jurídico protegido por el ilícito, éste sería la persona titular del mismo, lo cual se cumple con la persona jurídica Sodimac S.A., quien además actúa en calidad de querellante".*

Si se considera el bien jurídico tutelado expresamente en la historia de la ley 19.223, como uno puramente informático, se tendría que afirmar entonces que el titular del interés protegido por

[78] *Óp. cit.*, Magliona Markovicth, C., & López Medel, M. (1999). p. 146.

las normas que prohíben estos delitos es el titular de los datos, que en su conjunto darían forma a la "información en cuanto tal", y sucesivamente a "los productos que de su operación se obtengan". Por otro lado, esto podría traer consecuencias diferentes en caso de considerar este delito como pluriofensivo.

Un ejemplo en que puede confundirse la titularidad del bien jurídico lesionado, es en la causa del JG de Quillota 1500048128-6 (30.12.2015), que en causa de responsabilidad penal adolescente, condenó a la imputada por el delito del art. 3° de alteración de datos, toda vez que la adolescente ingresó a la página web del Departamento de Evaluación, Medición y Registro Educacional (DEMRE) utilizando para ello el nombre de usuario y contraseña de quien era hasta ese entonces su amiga, y considerada en este caso como la víctima del delito, accediendo con ello a la postulación realizada por esta última para el proceso de selección universitaria, modificando sin su consentimiento no solo las universidades a las que la víctima había postulado, sino también a las carreras por las cuales había manifestado su preferencia. De esta forma, el DEMRE determinó que aquella no podía considerarse válida, teniéndola como no presentada para todos los efectos, perdiendo la víctima, la posibilidad de ingresar a la Universidad. Aunque el tribunal en cuestión no ahondó sobre esta materia, resulta interesante observar cómo es que si bien la imputada alteró los datos, cuya titularidad ostentaba el DEMRE, los efectos de la conducta lesiva recaen en otra persona, en este caso su amiga, la que a su vez es considera como la víctima del delito, por tener esta un interés jurídicamente protegido, cual podría ser en este caso su derecho de intimidad.

ii. Autoría

En el artículo 3°, al igual que el resto del articulado de la ley 19.223 se utiliza la voz "el que", lo que significa que "cualquier individuo de la especie puede ser sujeto de las acciones típicas reguladas por la ley"[79]. No exigiendo, por tanto, la concurrencia de alguna calidad

[79] *Óp. cit.*, Magliona Markovicth, C., & López Medel, M. (1999). p. 145.

determinada[80]. En cuanto al sujeto activo del tipo penal, tanto la doctrina, como la jurisprudencia nacional se encuentran contestes en dicho punto, alejando así la creencia primera que rondaba al sujeto activo de los delitos informáticos, en el cual se le tenía por un experto en materias de tecnologías de la información y comunicación. Muy por el contrario, se puede afirmar que en la mayoría de las sentencias analizadas, el sujeto activo de la conducta puede ser catalogado como *insider,* un sujeto que tiene acceso a determinados sistemas, sea por su calidad de trabajador dependiente de una institución, sea por su relación de amistad o de confianza con alguna persona, desmitificando así, al sujeto activo de los delitos informáticos como uno que requiere de determinados conocimientos o expertíz en materias informáticas. En particular, en relación al sujeto activo del delito del art. 3° los autores son, como se mencionó, en la gran mayoría de los casos *insiders,* que tienen acceso al sistema de tratamiento de información donde se encuentran los datos objeto de la conducta. Ello no quita que este delito pueda ser cometidos por personas expertas en materias informáticas, casos que si existen en la jurisprudencia nacional, y cuya comisión es ciertamente llevada a cabo con conocimientos que exceden del normal conocimiento sobre la materia informática[81], pero que corresponde a una minoría significativa en comparación con aquellas sentencias donde el sujeto activo no se valió de una expertíz informática relevante para ejecutar la conducta.

[80] Además, recordar lo establecido en la historia legislativa, en que el proyecto de ley original contemplaba un artículo referido a un aumento en la penalidad de la conducta, el que era aplicable a todos los tipos de la ley, para aquellos responsables del sistema informático. Así, salvo en el delito contemplado en el artículo 4° de la ley 19.223, relativo a la difusión de datos, el cual contempla en su inciso segundo un aumento en la pena, en el evento de que la persona que revele o difunda maliciosamente los datos contenidos en un sistema de información, sea el responsable del mismo. No se contempla dicho aumento para ninguno de los demás artículos de la ley. Esto, según Magliona y López haría del delito del art. 4°, y solo este artículo, uno de sujeto activo calificado. Magliona Markovicth, C., & López Medel, M. (1999). p. 146.

[81] Ejemplo de ello, es la sentencia del 8° J G de Santiago Ruc 1300971941-k (01.09.2014), que condenó en procedimiento abreviado por los artículos 2° y 3° de la ley a dos hackers. Es de las pocas sentencias analizadas en que el imputado se valió de operaciones un poco más complejas y no es un *insider*. Los imputados accedieron desde diversas conexiones subiendo archivos modificados a los sitios web www.ahoranoticias.cl y www.megamujeres.cl, ambas del canal de televisión Megavisión. Este archivo modificado, les permitió leer un virus previamente guardado por uno de ellos, con lo que pudo obtener las claves para controlar el twitter corporativo de la estación Mega. Además, los imputados distribuyeron un código malicioso vía correo electrónico de forma masiva y aleatoria. Los equipos de los usuarios que abrieron dicho correo fueron infectados con un virus que hacía de este equipo un *bot*, un esclavo del hacker que los domina. El hacker a su vez puede convertir estos *bots* en una red, una *botnet*, pudiendo de esta forma impartir órdenes y acceder a información de forma masiva. Lo que ocurrió en el caso.

Sin existir confusión sobre el alcance de la expresión *el que* en la doctrina nacional, en materias referentes a la ley 19.223, se puede ejemplificar su uso de forma explícita, y en este mismo sentido mediante algunas sentencias, que si bien lo hacen a raíz en conocimiento de otros artículos de la ley, la hacen extensible a todo el articulado de la misma:

El TOP de Arica en causa Ruc 1210014297-8 (18.07.2014), en su considerando 13°, establece que:

> Para estar en presencia de la figura típica de espionaje informático, en relación al **sujeto activo**, el legislador en la ley 19.223 optó por utilizar la expresión "el que", de manera que no queda restringido el tipo penal a la existencia de un sujeto activo calificado o determinado; en tal sentido, conforme al mérito de la prueba incorporada y analizada, dicho presupuesto fáctico se cumple al imputar responsabilidad al acusado Víctor Cruz Torres.

De la misma forma, referida esta vez al art. 1° de la ley, la sentencia condenatoria del TOP de Curicó. Ruc 0910014546-1 (07.03.2011), que en su considerando 9° establece que:

> Considerando, del mismo modo, que la ley no establece como requisito que se trate de un sujeto activo calificado o con conocimientos especiales en esta materia, estos jueces estiman que cualquier sujeto que ejecute alguna de las acciones mencionadas en la norma en comento, es capaz de ser el sujeto activo y en este caso, los acusados digitaron determinadas funciones, que sin bien fueron dadas por el sistema proporcionado por el empleador, importó obstaculizar el mismo.[82]

Así mismo, dada la indeterminación de sujetos contemplada en la ley 19.223 en general, es posible aseverar que le son plenamente aplicable las reglas generales contempladas en el título

[82] Los argumentos de este tribunal fueron a su vez confirmados por la Corte de Apelaciones de Talca Rol 498-2010(24.12.2010).

II del Código Penal "De las personas responsables de los delitos", de forma que se puede ser responsable del delito de alteración de datos, en calidad de autor, cómplice o encubridor[83].

iii. Tipo objetivo

Dentro de este apartado se tratarán, en el mismo orden, los elementos de: verbo rector; objeto de ataque; y, medios y circunstancias comisivas contenidas en el delito del art. 3° de la ley 19.223.

a. Verbo rector

El delito de sabotaje informático contemplado en el artículo 3° de la ley 19.223, contiene tres verbos rectores: el que maliciosamente "altere", "dañe" o "destruya" los datos contenidos en un sistema de tratamiento de la información.

Originalmente, el proyecto de ley hacía referencia al verbo "manipular datos*"* como omnicomprensivo de conductas como la introducción, transformación, difusión y alteración. Pero durante su tramitación, el verbo que se contempló para abarcar de forma general cada una de estas conductas fue el de "alterar*"*[84], además de "dañar" y "destruir".

Según la Real Academia de la Lengua Española, alterar significa "cambiar la esencia o forma de una cosa", y en general la doctrina nacional considera esta definición de alterar como apropiada para el verbo descrito en el tipo penal. Además, al igual que en la discusión legislativa, se considera por parte de la doctrina al verbo alterar como omnicomprensivo de otras conductas, como las de: ingreso o introducción de datos erróneos, el borrado de datos verdaderos, las

[83] Véase por ejemplo la sentencia del 4° TOP de Santiago, que en causa Ruc N°1000626117-0 (08.06.2011), absolvió a la acusada de su participación como autora y otras formas de participación en el delito contemplado en el art. 3°; También, la sentencia del JG 8°, que en causa Ruc N° 1400481698-7 (25.08.2016), condenó al imputado en calidad de autor por el delito de estafa y en calidad de cómplice por el delito el delito informático del art 3°.
[84] *Óp. cit.*, Huerta, M., y Líbano, C. (1998). pp. 292 y ss.

transformaciones y desfiguraciones de los datos y cualquier otra que implique cambiar la información contenida en un sistema de tratamiento de información, sin destruirla[85].

En la jurisprudencia, se refiere explícitamente a la definición y alcance del verbo alterar la sentencia de la Corte de Apelaciones de Concepción Rol 844-2014 (30.01.2015), que en su considerando 6° se expresa de la siguiente forma:

> La acción delictiva está destinada a alterar, destruir o dañar los datos contenidos en un sistema de tratamiento de información. Alterar los datos contenidos en un sistema sería, en consecuencia, alteraciones conductas como el ingreso o introducción de datos erróneos, el borrado de datos verdaderos, transformaciones o desfiguraciones de los datos, y en general toda conducta que implique cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla. Por lo tanto, lo afectado es el sentido, veracidad, claridad o pureza y alcance de la información contenida, la cual se verá afectada con conductas como las descritas.

En cuanto al verbo "dañar", según la Real Academia de la lengua, significa "maltratar o echar a perder una cosa". El significado del verbo "destruir", según la misma institución es "reducir a pedazos o a cenizas algo material, u ocasionarles un grave daño", también "deshacer o inutilizar algo no material", siendo esta última la que se adecúa mejor al tipo penal. Según los autores nacionales, también es adecuada la aplicación de esta definición a la conducta delictiva en contra de los datos contenidos en un sistema de tratamiento de información[86].

La jurisprudencia del foro penal es coincidente tanto con el sentido amplio del verbo alterar como con la aplicación de los verbos contenidos en artículo 3° a diversas situaciones, alcanzando una gran variedad de formas de ejecutar el tipo penal descrito en el artículo 3°, en las que muchas veces se superponen unas con otras. Así, por ejemplo en la causa Ruc

[85] *Ibídem*. p. 293. En el mismo sentido: Magliona Markovicth, C., & López Medel, M. (1999). p. 168.
[86] *Óp. cit.,* Huerta, M., y Líbano, C. (1998). p 293; En el mismo sentido: Magliona Markovicth, C., & López Medel, M. (1999). Delincuencia informática. p. 168.

1000464726-8 del 3° TOP de Santiago, (19.06.2012) se refiere a la conducta cometida por el imputado como una "modificación"[87] en el sistema informático. O bien, la sentencia del 4° TOP de Santiago que en causa Ruc 1000626117-0 (08.06.2011) se refiere a la conducta como el haber realizado por parte de imputado "borrones" y "borrones ilícitos" en el sistema informático[88]. Además, a modo de ejemplo en el uso variado de expresiones para referirse a este delito, la sentencia del JG 8° Santiago Ruc 1501138933-0 (31.12.2018) utiliza variados verbos rectores: "manipulación de sistema informático"[89] y "adulteración"[90] del sistema informático de contabilidad de la misma, "ingreso de datos ficticios", "ingreso datos falsos"[91], "ocultamiento en el sistema informático", "cambio de datos", "modificación de datos"; "vulnerando y adulterando los sistemas informáticos de registro, protección y control de datos" de la empresa afectada. En el mismo sentido la sentencia del JG 8° de Santiago Ruc 0910000486-8 (25.11.2015) que utiliza varios conceptos sinónimos de "alteración", como "maniobras fraudulentas en el sistema informático", "cambiar datos en el sistema", y "ocultamiento de datos". Por su parte, en JG Talcahuano Ruc 0900600732-2 (13.09.2011) se utilizan las expresiones "dañando" y "destruyendo datos", "Cancelando datos", "cancelaciones ficticias" y "adulteración de información".

[87] Hace uso del verbo modificar o alguno semejante en relación a los datos contenidos en algún sistema de tratamiento de información la sentencia JG Puerto Varas 1501011576-8 (15.03.2018). Utiliza: Alteración de sistema informático, modificando, registrando en su lugar, adulterando así la contabilidad.

[88] Hacen uso del verbo borrar o alguno semejante en relación a los datos contenidos en algún sistema de tratamiento de información la sentencia: JG 7° Santiago Ruc 1410003541-4 (02.10.2015).

[89] También hacen uso del verbo "manipular" en relación al sistema informático o datos, las siguientes sentencias: JG 7° Santiago Ruc 1510006022-9 (26.01.2017), se refiere a: Manipular el sistema computacional y modificando los datos de los clientes; JG 7° Santiago Ruc 1510011054-4 (01.12.2016), se refiere a: Alteración de base de datos informática y manipulación de cuentas contables; JG La Serena Ruc 1000571645-k (12.12.2014), se refiere a manipular y alterar un sistema; JG Concepción Ruc 1410003541-4 (16.05.2016), se refiere a Ingreso de datos falsos, manipulación de sistema y alteración de cuenta corriente.

[90] Hacen uso del verbo "adulterar" en relación al sistema informático o a los datos contenidos en ellos las siguientes sentencias: JG 7° Santiago Ruc 1610018667-9 (12.06.2018), se refiere a: Adulteración de Sistema informático, abrir irregularmente un terminal de caja, cancelar vale vistas y generar créditos; JG Arica Ruc 1500784272-1 (06.01.2017), se refiere a: Adulteración de información; JG 7° de Santiago Ruc 1700296781-2 (16.02.2018), se refiere a: Adulteración de sistema informático, modificación de sistema informático; JG La Serena Ruc 1000571645-k (12.12.2014), se refiere a manipular y alterar un sistema, adulterando la información; JG Quillota Ruc 1500048128-6 (30.12.2015), se refiere a adulterar y modificar.

[91] También hacen uso del verbo "ingresar" en relación al ingreso de datos falsos o semejantes, las siguientes sentencias: JG 4° de Santiago Ruc 1010001813-1 (30.06.2011), utiliza los términos alteró los datos, borrado de datos originales y sustitución de los mismos por datos falsos; JG Concepción Ruc 1410003541-4 (16.05.2016), se refiere a Ingreso de datos falsos, manipulación de sistema y alteración de cuenta corriente; JG La Serena 1100470439-k (18.05.2015), refiere a alteración de datos en sistema informático e ingreso de datos.

De esta forma, se puede afirmar que no existe en nuestro país gran discusión sobre el alcance de los verbos rectores de este tipo penal, ciñéndose en su base a las definiciones aportadas por la Real Academia de la Lengua Española, pero ampliando su aplicación a situaciones de relevancia jurídica e informática. Así, el verbo alterar es entendido, además de su sentido natural y obvio, como comprensivo de conductas tales como: el ingreso o introducción de datos erróneos o falsos, el borrado de datos verdaderos, las transformaciones y desfiguraciones de los datos y cualquier otra que implique cambiar la información contenida en un sistema de tratamiento de información, sin destruirla. Por otra parte los verbos dañar y destruir, no han sido objeto de mayor mención, entendiéndose en su sentido natural y obvio, los que variarían en la sola intensidad del daño generado en los datos, siendo la mayor, el efecto de destruir completamente los datos contenidos en un sistema de tratamiento de información.

b. Objeto de ataque: datos, sistema de tratamiento (automatizado) de información, e información

El objeto de ataque en un delito, se refiere al objeto contra el cual se dirige la conducta descrita en el tipo. Y, como se dijo en el Capítulo I, lo que caracteriza a los delitos informáticos en abstracto, es que las conductas castigadas por ellos están dirigidas contra el soporte lógico de un sistema de tratamiento de información. Así, se entiende a los sistemas de tratamiento de información como aquellos compuestos tanto por un componente lógico que incluye a los datos e información, como por uno físico que incluye el cableado, carcazas, y chips. Por lo que, una acción dirigida contra el soporte lógico de un sistema de tratamiento de información puede ser caracterizada propiamente como un delito informático, mientras que una acción dirigida contra el soporte físico del sistema, no sería más que un delito tradicional de daños[92]. Una de las principales críticas que se le ha hecho a la legislación sobre delitos informáticos en nuestro país, es que al momento de legislar sobre la materia se confundieron dichos conceptos, quedando como resultado, el que la actual ley 19.223 proteja conductas dirigidas tanto contra soportes

[92] *Óp. cit.*, Moscoso, R. (2014). p. 13.

lógicos como sería el caso de ataque contra los datos e información, pero también contra conductas dirigidas contra el soporte físico del sistema, como es el caso del artículo 1° de la ley.

En el caso del artículo 3° la conducta de alterar, dañar o destruir debe recaer sobre "los datos contenidos en un sistema de tratamiento de información". Por otro lado, la ley 19.223 no define ninguno de estos conceptos, pese a que son conceptos técnicos y son usados en sus cuatro artículos. Esto significa que el objeto de ataque de este delito, es inmaterial, toda vez que la conducta debe verificarse en una inmaterialidad constituida por los datos, los que a su vez están constituidos, en un sistema informático, por el *bit (binary digit)* que constituye la unidad más básica para la representación dentro de un soporte lógico, los que se encuentran contenidos en dicho sistema, o tienen lugar cuando dicho sistema se magnetiza, generando impulsos electromagnéticos[93]. Concebir el impulso electromagnético como un objeto de ataque de características inmateriales, tendría como consecuencia por ejemplo excluir la configuración del delito de apropiación de una cosa corporal mueble ajena[94]. Por su parte el anteproyecto de la ley 19.223, lo entendió como "todo hecho representado bajo una fórmula convencional apropiada para su comunicación, interpretación o tratamiento, sea por el hombre o por medios informáticos"[95]. Así también el concepto de información que en el anteproyecto sobre informática se definió como "conjunto de datos que permiten conocer o inferir una realidad, efectiva o presunta"[96].

Doctrinariamente, también se ha hecho la distinción acerca de la clasificación de este elemento, y se alude, tradicionalmente a la clasificación a la luz del artículo 576 del Código Civil, entre cosas corporales e incorporales, siendo los impulsos electromagnéticos clasificados dentro del segundo grupo por exclusión, toda vez que no pueden ser percibidos directamente por los sentidos. La crítica a ello, sin embargo es que no porque los limitados sentidos humanos no

[93] *Ibídem.* p. 14. Definición usada por la autora a partir del trabajo de Jijena Leiva, R (2008). Delitos informáticos, internet y derecho. p. 148 y s.
[94] *Ibídem.* p. 18. Definición usada por la autora a partir del trabajo de Jijena Leiva, R (2008). Delitos informáticos, internet y derecho. p. 152.
[95] *Óp. cit.,* Magliona Markovicth, C. & López Medel, M. (1999). p. 145.
[96] *Ibídem.* p. 145.

puedan percibirlos, dicho elemento no tiene una corporeidad. Así, los impulsos electromagnéticos, si bien intangibles, bien pueden ser considerados como cosas corporales[97].

En cuanto a las posiciones que ha adoptado la jurisprudencia en estas materias se puede expresar que, como primera cuestión relevante se reconoce por parte de la jurisprudencia que el objeto de ataque del artículo 3° son los datos contenidos a su vez en sistemas de tratamientos de información. Así, la Corte de Apelaciones de Concepción causa Rol 844-2014 (30.01.2015), distingue a su vez el objeto de ataque del delito, del concepto de bien jurídico protegido por el delito, situación que generó confusión a la hora de legislar y que según algunos autores fue una de las causas de la deficiente legislación. En sede de nulidad la Corte expresa que:

> La acción delictiva está destinada a alterar, destruir o dañar los datos contenidos en un sistema de tratamiento de información. Alterar los datos contenidos en un sistema sería, en consecuencia, alteraciones conductas como el ingreso o introducción de datos erróneos, el borrado de datos verdaderos, transformaciones o desfiguraciones de los datos, y en general toda conducta que implique cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla. Por lo tanto, lo afectado es el sentido, veracidad, claridad o pureza y alcance de la información contenida, la cual se verá afectada con conductas como las descritas.

En segundo lugar, en cuanto al concepto de sistema de tratamiento de información es necesario reconocer que sufrió una serie de modificaciones durante la tramitación del proyecto de ley,

[97] *Óp. cit.*, Moscoso, R. (2014). p. 19. La autora analiza este tema de una forma mucho más acabada, citando en la nota al pie n° 11 de su trabajo también la doctrina moderna, que estaría por considerar a los datos como "cosas intelectuales", que consistiría en que "(..) estas cosas intelectuales constituyen materia o movimientos de la materia pensados, y pensados con una forma determinada, reproducible o representable indefinida cantidad de veces con materia o con su movimiento físico. Esta aptitud de proyección física no afecta al modelo intelectual, desde donde pueda ser multiplicado, esto es, indefinidamente reproducido o representado, y por ello permite que el objeto intelectual llegue al conocimiento de los demás. Su consistencia, empero, no es la corporalidad del soporte material, sino la forma concebida por el intelecto y dada a la materia concebida de la misma manera. Por ello, como hemos dicho, la denominación que mejor conviene a estos objetos es la de 'cosas intelectuales o ideales'", definición tomada por la autora de Guzmán Brito, Alejandro. (2006). Las cosas incorporales en la doctrina y en el derecho positivo. p. 59 y s.

"tanto en su texto, como en las acepciones que le fueron dando"[98]. Así, lo que en la presentación del proyecto original por parte del diputado Viera-Gallo, tuvo como objeto:

> La protección de un sistema de información automatizado (…) mediante la creación de figuras penales especiales, que evitan la necesidad de hacer interpretaciones extensivas de las tradicionales normas penales, para incluir conductas indebidas en contra de los sistemas automatizados de tratamiento de la información, tanto en lo referente a su soporte lógico o programas de funcionamiento como en lo relativo a los datos que se manejan[99].

De lo que se desprende que lo que buscaba proteger el proyecto original de la ley 19.223 fue el sistema "automatizado" de tratamiento de la información, compuesto por los programas o soporte lógico *(software)* y los datos contenidos en ellos, dejando de lado el soporte físico del sistema (*hardware*) y los otros medios de tratamiento de información no automatizados. No obstante, tras distintas intervenciones –primero en la Comisión de Constitución, Legislación y Justicia, y luego en la Cámara de Diputados–, comenzaron las dudas sobre la protección de este sistema "automatizado" de tratamiento de información, fundadas principalmente en la razón de que, "[la Comisión] tuvo en vista que en la protección de los sistemas de información no tiene sentido discriminar según cuál sea el soporte físico en que ellos residan. De este modo quedan protegidos los que posean un carácter manual y estén contenidos en papel, lo mismo que otros que el desarrollo de la tecnología permita en el futuro"[100]. Finalmente, lo que nació como duda, terminó por plasmarse en el articulado final del proyecto, en el sentido de eliminar definitivamente la palabra "automatizado" de los artículos que la contenían, incluido por cierto el actual artículo 3°. De ello cabe concluir, que dentro de los sistemas de tratamiento de información protegidos por el texto de la ley 19.223 se encuentran tanto los automatizados, entendidos como computadoras, celulares, y otros similares, como también los no

[98] *Óp. cit.*, Magliona Markovicth, C., & López Medel, M. (1999). p. 139.
[99] Boletín Oficial N° 412-07 de la Honorable Cámara de Diputados y Senadores de Chile, Cámara de Diputados, sesión 19°, en martes 16 de Julio de no1991, p. 1969. Citado por Magliona Markovicth, C., & López Medel, M. (1999).p. 139.
[100] Boletín Oficial N° 412-07 de la Honorable Cámara de Diputados y Senadores de Chile, Cámara de Diputados, sesión 19°, en martes 16 de Julio de no1991, p. 1969. Citado por Magliona Markovicth, C., & López Medel, M. (1999).p. 143.

automatizados, los archivadores, bibliotecas, y otros modos de almacenamiento y tratamiento físicos de la información. Lo que por cierto desnaturalizó el sentido original del proyecto y genera inconvenientes relacionados a la doble tipicidad de ciertas conductas, como sería el caso de aquella que borrara los datos de un archivador manual, o bien, el ataque al soporte físico de información o *hardware*, ambas conductas podrían que puede subsumirse bajo el delito contemplado en el artículo 3° y 1° de la ley 19.223 respectivamente, o bien bajo el delito tradicional de daños.

La jurisprudencia por su parte, acepta como objeto de ataque del artículo 3° aquellos datos contenidos en un sistema "automatizado" de tratamiento de información. Entendiendo además a aquel, como un sistema complejo compuesto tanto por *hardware, software,* datos y personas, haciendo aplicable la ley 19.223 y específicamente su artículo 3°, a su propósito original, y obviando su posterior desnaturalización al quitarse del texto legal la palabra "automatizado". Esta conclusión se obtiene a partir de que todas las sentencias recolectadas en este trabajo se encuentran dentro de un contexto informatizado, entendiendo con ello que los delitos de la ley 19.223 fueron aplicados, entre los años 2010 y 2018 solo a conductas donde el objeto de ataque estuvieron constituidos por *softwares* o datos. En este sentido y con expresión textual de la misma idea, se pronuncia el TOP de San Bernardo Ruc 1100498003-6, (14.05.2016) en su considerando 11°, numeral iii, en relación al delito del art. 4° de la ley 19.223 sobre difusión de datos contenidos en un sistema de tratamiento de información, haciéndola extensible a todo su articulado. Textualmente señala:

> En cuanto al delito de Divulgación de información contenida en sistema informático, la conducta típica importa que maliciosamente revele o difundan los datos contenidos en un sistema de información. Dos alcances corresponden hacer a ese respecto. Primero, en cuanto a la conducta de Romero Román, no puede postularse que aquél haya hecho una revelación o difusión de los datos contenidos en un sistema de información. Esta cuestión queda meridianamente clara si se atiende al título de la ley 19223, esto es, tipifica figuras penales relativa a la informática. Por lo tanto, todas las conductas sancionadas en dicha ley se entienden configuradas sólo en la medida que estén relacionadas

> directamente con sistema informático. Esto es, sólo respecto de aquella conducta que esté directamente conectada al levantamiento de información desde el sistema informático, y que posteriormente procede a sus revelación o difusión. Únicamente en este sentido puede ser entendida dicha figura, pues si se criminalizara de esta forma cualquier difusión de información que haya estado contenida en uno de estos sistema, independiente de cómo se adquirió dicha información, se podría terminar penando acciones que jamás tuvieron el más mínimo acceso a dicho sistema. Importaría penar por esta figura cualquier cadena de información independiente de lo lejos de que se esté de la fuente de esa información, o la vía por la cual se adquirió esa información, y que puede no tener relación alguna con un sistema informático, por ejemplo el boca a boca. En este orden de ideas es claro que la persona que hizo la revelación de esta información fue Gerko Henríquez, pues fue él quien tenía el acceso al sistema, y quien recabó la información de éste para luego entregársela a Romero Román.

Por su parte, la sentencia del TOP de Coyhaique Ruc 1610036482-9(24.07.2018) absolvió a los imputados de la causa, acusados por los delitos del artículo 2° y 4° de la ley informática, entendiendo que las conductas realizadas se encuentran contenidas de igual forma en el delito de interceptación de señal televisiva, por el cual se arribó a una decisión condenatoria. El fallo fue obtenido por decisión unánime y cuenta con la prevención del Juez Sr. Edmundo Ariel Devia que se refiere de la siguiente forma al objeto material de los delitos informáticos, forma que por cierto hace eco de la doctrina nacional:

> Los delito informáticos se caracterizan porque sancionan conductas dirigidas en contra **soporte lógico** de un sistema tratamiento información, como sería por ejemplo un computador, que se compone de dos partes el soporte lógico, a saber los datos, la información contenía el sistema, es decir el software y el **soporte físico** los cables, chips, carcasa el equipo, decir el hardware, por ello una conducta dirigida contra los datos es un delito informático, mientras que una dirigida contra soporte físico, sólo es un delito de daños. De esta forma las conductas tipificadas en la Ley N° 19.223, tratándose de delitos con carácter

informático, el objeto sobre el cual recaen dichas conductas es inmaterial, distinguiéndose tres modalidades de criminalidad informática, esto es fraude informático, el sabotaje informático y el espionaje informático. Los primeros, se encuentran las alteraciones o manipulaciones, de los datos, ya sea al recopilarlos, procesarlos, estando almacenados o al transmitirlos telepáticamente, como de los programas del sistema computacional; los espionajes informáticos se encuentran las figuras de obtención ilícita, dolosa y sin autorización de datos o información relevante y de programas computacionales; y el sabotaje informático el cual se configuran las conductas de atentados que causan daños, destruyen o inutilizan un sistema computacional.

Podemos decir que, el tribunal estima que, la figura descrita el artículo 1 de la Ley N° 19.223, corresponde a lo que en doctrina se ha denominado como **sabotaje informático**, en oposición a las figuras de **espionaje informático** que regulan los artículos 2 y 4 de la misma ley. De acuerdo a ello, es posible identificar que respecto de los artículo 2 y 4 referidos, estamos en presencia de protección de la privacidad como bien jurídico penal que se encuentra sujeto a restricciones generales de custodia, estando restringida las intromisiones físicas en la vida privada de las personas bajo el concepto de morada, y por otro lado las intromisiones por medio de instrumentos regulado en el artículo 161-A del Código Penal, lo cual lo hace mediante el doble recurso de exigir, por una parte, que se trate de sucesos que ocurran en lugares que no sean de libre acceso al público y de exigir, adicionalmente, que se trate de sucesos de la vida privada, cuestión que no pasa en el caso de los tipos penales informáticos y que tiene consecuencias en la comprensión de lo protegido y además la ley penal protege el registro de papeles ajenos. En forma adicional se encuentra la Lay N° 19.223, respecto de la información contenida en soportes informáticos, apreciando algunos autores que se estaría en presencia de una posible infracción a un derecho de exclusión no necesariamente vinculado con la privacidad, sino más bien específico de la informática, cuestión que no es pacífica en las opiniones, sin embargo en forma general, podemos decir que ambos artículos protegen la

> privacidad del titular de la información, entendiéndose como la eventual posibilidad de excluir a terceros del acceso a esferas de dominio de ese titular, es decir se puede concordar esa noción de privacidad como concepto formal, pero se debe tener en cuenta el rasgo distintivo especial de excluir a terceros.

Como tercera cuestión relevante, un conflicto que se ha dado en la jurisprudencia sobre la ley 19.223 refiere a las características con las que debe cumplir un sistema de tratamiento de información para ser considerado como tal. La jurisprudencia mayoritaria esta por considerar, tanto a aquellos equipos tecnológicos que cumplen expresamente con la función de "tratar" los datos informáticos que incluiría las funciones de almacenar, procesar y transmitir datos e información, como también a aquellos sistemas que si bien no cumplen con todas aquellas funciones, pueden de igual forma ser considerados como tales para los efectos de aplicar los delitos contenidos en la ley 19.223, como sería el caso de dispositivos de "mero almacenamiento*"* de información, por ejemplo: bases de datos y *pendrives*.

Así, la ya citada sentencia de la Corte Suprema en causa Rol 3951-2012 (20.03.2013) en la que se rechazaron los recursos de casación en el fondo interpuestos en el marco de un procedimiento judicial militar, donde se condenó a tres personas por los delitos del artículo 4° de esta ley, referido al delito de difusión de datos, y el artículo 2° referido al delito de acceso indebido. La causa refiere a que en un regimiento militar un Oficial solicitó un *pendrive* a otro Oficial con la excusa de respaldo de documentos. Dicho individuo accedió sin autorización al computador personal de su vecina de oficina, copiando en el *pendrive* prestado una serie de archivos dentro de los cuales había algunas fotografías y videos de contenido sexual, el que posteriormente fue difundido por el Oficial. Fueron presentados respectivamente dos recursos de casación en el fondo ante la Corte Suprema, donde una de las alegaciones de la defensa de los acusados consistió en que "el objeto material del delito, es decir, los datos contenidos en un sistema de información, pues un pendrive sólo es un dispositivo portátil, mero contenedor de datos que no cumple las tareas básicas de todo sistema de tratamiento de información". Argumentando además, que con ello no se vulneraría el bien jurídico protegido por la ley, relativo a la calidad, pureza e idoneidad de la información, por lo que la conducta por la que fueron condenados los imputados debió haber sido tratada bajo otro supuesto penal, como lo sería el caso del artículo

161 A del Código Penal. La Corte, en su considerandos 6° y 7° rechazó la referida argumentación, estimando de esta forma que lo divulgado tenía el carácter de datos o información y que se encontraba contenida en un sistema de almacenamiento o tratamiento de la misma –*pendrive*–, lo que en ambos casos se estaría a los dispuesto por la ley. Así, La Corte en su considerando 6°:

> (…) Lo que se sanciona es el empleo de procedimientos dolosos destinados a afectar no sólo el sistema de tratamiento y almacenamiento de datos como erróneamente postulan las defensas, sino también difundir la información ilícitamente obtenida, de manera que sea conocida por terceras personas, lo que a su turno incrementa las posibilidades de que nuevamente sean utilizados y difundidos, como en la especie ocurrió. En el caso de autos quedó establecido que los sentenciados de un modo subrepticio o con un conocimiento no autorizado de la clave de acceso a un computador, vulneraron un software e información confidencial allí almacenada, la que se extrajo a través de un dispositivo externo de almacenamiento para efectos de exhibirse y difundirse a terceros.

Y en su considerando 7°, respecto de la falta del elemento de procesamiento:

> Que la alegación de la defensa de Campos Bustos acerca de la falta de procesamiento respecto de la conducta de sustracción de datos no es atendible, pues la figura penal por la que ha sido condenado sanciona hechos diversos y no exige como condición previa que sea el mismo agente quien acceda al sistema de almacenamiento de información que posteriormente se divulga.

En el mismo sentido, pero referido esta vez a hacer aplicable la figura del artículo 2° de la ley informática, sobre interceptación de un sistema de información, la sentencia de la Corte de Apelaciones de la Serena Rol 24-2017 (27.02.2017) estima, que las líneas de envío de información forman parte del sistema de tratamiento de datos. Así la Corte:

> Recordemos que un sistema automatizado de tratamiento de la información es mucho más que un computador. Las líneas a través de las cuales se envía la información de computador a computador son, por ejemplo, integrantes del sistema. Por lo tanto las acciones pueden recaer tanto en los computadores como en las líneas a través de las cuales se envía una comunicación´. (Magliona Markovitch, Claudio 1999).

Si bien la Corte Suprema y otras Cortes superiores se ha pronunciado en este sentido, en los tribunales del foro penal ha habido casos en que se considera un equipo de mero almacenamiento de información como uno que no se encuentra contenido dentro del objeto de ataque de la ley 19.223, toda vez que prescindiría de la aptitud de tratar información, quedando excluida de su ámbito de protección. Así, en relación al delito contenido en el artículo 1° de la ley, sobre destrucción de sistema informático, se pronuncia el TOP de Curicó en causa Ruc 0910014546-1 (07.03.2011) que en su considerando 9° , señala que pese a atribuirle dichas características a los sistemas informáticos, arriba a una decisión condenatoria, toda vez que en los hechos los cajeros de un supermercado obstaculizaron el sistema informático de una de las cajas para la venta de códigos telefónicos de prepago o pines telefónicos, generando así códigos prepagados de las empresas Entel, Claro y Movistar que nadie pagó al Supermercado, pero que dicha empresa debió pagar a las empresas telefónicas ya mencionadas. Así, el tribunal razona de la siguiente manera:

> Que en relación al de DELITO INFORMATICO del artículo 1° Ley 19.223 es preciso mencionar que el tipo penal contempla dentro de sus figuras penales al que maliciosamente obstaculice o modifique el funcionamiento de un sistema de tratamiento de información, al respecto es necesario hacer algunas consideraciones: Se debe tener presente que la ley 19.223 lo que protege es la información de los datos contenidos en las redes informáticas y lo que se pretende con su aplicación es la constitución de un bien jurídico nuevo cual es "la calidad, pureza e idoneidad de la información" (Hernán Silva Silva) y así de algún modo impedir que dichos sistemas sean burlados para obtener beneficios

> tales como apropiación, uso o conocimiento de la información en ellos contenida para fines propios y diversos a aquellos para los cuales fueron creados o generados.
>
> Asimismo, considerando que un sistema informático está compuesto por recursos humanos, recursos físicos (hardware), recursos lógicos (software) y datos de información, que se relacionan entre sí y cada parte o componente constituye un sistema en sí mismo, podemos llegar a concluir que un sistema de tratamiento de información es un conjunto de componentes interrelacionados, integrados y coordinados (personas, equipos, procedimientos) que transforman datos en información, permitiendo así, capturar, procesar, almacenar y distribuir la información necesaria para la toma decisiones y control.

Esta idea sobre los sistemas informáticos no es compartida en toda la jurisprudencia analizada. En contra de la interpretación anterior que considera incluidos dentro del concepto de sistemas de tratamiento de información, tanto a equipos que cuenten con la capacidad de almacenar, procesar y transmitir datos e información, como aquellos que tan solo cuenten con alguna de estas aptitudes, se encuentran algunas sentencias que estiman que dichos elementos deben darse en forma conjunta, por lo que la ausencia de alguno de ellos puede llegar a excluir un equipo de su configuración de objeto material del delito, y por ende hacer derivar en una decisión absolutoria por parte del tribunal. En este sentido se pronuncia el TOP de Temuco Ruc 1700268031-9 (22.07.2018), considerando 17°, literal B, que expresa las cualidades con las que debiera contar un sistema de tratamiento de información para ser catalogado como tal (esto es: entrada, proceso y salida de los datos), haciendo una distinción, entre sistema de tratamiento de información y una mera base de datos. Así, utiliza esta distinción para absolver al imputado, toda vez que la conducta de alteración –que en este caso particular consiste en el ingreso de datos falsos al sistema NAHUEL– no se podría verificar en este caso particular, ya que lo alterado fueron los datos contenidos en una mera base de datos y no en un sistema de tratamiento de información:

Ahora bien, para ir comprendiendo adecuadamente, dejaremos sentado que el tratamiento de la información consiste en una serie de operaciones que se realizan sobre una determinada información de forma planificada y ordenada y así poder convertirla en conocimiento; y que un sistema de tratamiento de información permite el procesamiento automático de la información, y conforme a ello, los sistemas informáticos deben realizar las siguientes tres tareas básicas: entrada, consistente en la captación de la información, normalmente datos y órdenes ingresados por los usuarios a través de cualquier dispositivo de entrada conectado a la computadora; proceso, que es el tratamiento de la información, que se realiza a través de programas y aplicaciones diseñadas por programadores que indican de forma secuencial cómo resolver un requerimiento; y salida, que es la transmisión de los resultados del proceso anterior, el producto de lo anterior, mediante dispositivos de salida a través de los cuales los usuarios pueden visualizar los resultados que surgen del procesamiento de los datos.

De lo anterior resulta que es relevante para entender si estamos delante de un sistema de tratamiento de la información, o no, que este sea capaz de almacenar, procesar y transmitir datos e información en formato digital utilizando sistemas computacionales. Lo anterior porque hay que diferenciarla de una mera base de datos.

En efecto, una base de datos es solo un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital, siendo este un componente electrónico, que dado su desarrollo ofrece un amplio rango de soluciones al problema del almacenamiento de datos.

> Ahora bien, concentrando el análisis tanto en la descripción fáctica como en el tipo penal que hemos analizado, una primera consideración tenida en vista por el tribunal es que el propio acusador estimó que lo que denominaba sistema informático "Nahuel", era una base de datos.
>
> De este modo, quedó demostrado que la conducta de solo ingresar datos para los fines que perseguía la acusada en los procedimientos irregulares de reemplazo de vehículos de transporte de pasajeros como taxis colectivos, lejos de configurar la comisión de un delito autónomo y regulado en una ley especial como el pretendido por el querellante, dado que lo que se manipulaba no era un sistema de procesamiento de datos o tratamiento de información, como exige perentoriamente el legislador, el denominado NAHUEL no era sino solo una base de datos de operación, más o menos compleja, y al efecto hay que señalar, como se arguyó por su defensa que no hubo probanzas de tipo técnico como para darle cabida y entender que si se trata de un sistema informático, la calidad precisa que exige el tipo penal invocado, ni hubo testimonio alguno en ese sentido, sino muy por el contrario, como dejamos de manifiesto, siendo la manipulación de la información que la acusada realizada en esa base de datos solo una parte del tramado de acciones que realizó en cada una de las operaciones irregulares, y por ello no puede ser objeto de reproche penal por separado.

Por su parte el TOP de Arica en causa Rol 1210014297-8 (18.07.2014), condenó al imputado por el delito del art. 2° de la ley 19.223, referido al delito de acceso informático, en su considerando 13°, parte final, señala que el programa Excel es un sistema de tratamiento de información, y además no sería necesario probar su aptitud de tal, ya que constituiría un hecho público y notorio:

> En relación a los datos contenidos en un sistema de tratamiento, conforme a los hechos acreditados, la información decía relación con un archivo Excel, conteniendo datos de trabajadores de la empresa a nivel nacional. Archivo que, por lo demás, se encontraba en un servidor de la empresa con acceso restringido

> a un número determinado de personas, entre las cuales, no se encontraba el acusado. Por su parte, es un hecho público y notorio que Excel se trata de un programa desarrollado y distribuido por Microsoft, y es utilizado normalmente en tareas financieras y contables, útil para gestionar Bases de Datos; pues permite agrupar, ordenar y filtrar la información.

En el mismo sentido, esta vez haciendo referencia a otro sistema, el JG de Copiapó en causa Ruc 1700582359-5 (31.10.2018) señala:

> Decimoquinto: En primer lugar se deben descartar algunos asertos que la defensa vertió durante el juicio tendientes a desvirtuar la convicción condenatoria del tribunal. En efecto, se indicó que se desconocía de qué plataforma o sistema de información se trataba, y de cómo esta funcionaba por un lado. Pues bien a este respecto es menester señalar que son principios generales del Derecho Procesal que los hechos públicos, notorios o ampliamente conocidos no ameritan probarse, en estas circunstancias resulta de conocimiento general por parte de los ciudadanos cada vez más inmersos en la tecnología que los bancos comerciales, cualesquiera sean estos mantienen un sistema virtual o plataforma virtual de acceso para sus clientes y que las mismas, producto de los ataques que han sido expuestos, han erigido una serie de barreras y protecciones virtuales, entre las que más se destacan el mantener sistemas de clave de acceso. En otras palabras, nadie desconoce hoy la existencia de los portales y sistemas de almacenamiento que existen en los bancos y en general como es su uso y finalidades, por lo que los dichos de la defensa en nada hacen variar la convicción del tribunal.

Esta sentencia fue objeto de un recurso de nulidad ante la Corte de Apelaciones de Copiapó Rol 448-2018 (19.12.2018), la que rechazó el recurso. En lo atingente a la materia en comento, se reclamó por parte de la defensa del condenado una vulneración a las reglas probatorias, en particular a las reglas de la sana crítica, toda vez que se dio por probada la existencia y conocimiento del elemento sistema informático en el caso, lo cual no correspondía sin antes

rendir la pertinente prueba. Si bien, la Corte rechazó esta alegación por motivos formales, alcanzó a mencionar en su considerando 9° que:

> Que, sin perjuicio de todo lo señalado precedentemente, cabe precisar, respecto del último tema reclamado por el recurrente de nulidad –atingente al sistema informático del Banco de Chile–, que aun cuando eventualmente esta Corte pudiere compartir parte de sus alegaciones de fondo, lo cierto es que las deficiencias del recurso no pueden ser subvencionadas por este Tribunal de Alzada, y a la vez impiden un pronunciamiento sobre la materia, de todo lo que se sigue que el recurso será rechazado.

Dicha sentencia fue obtenida con una votación de dos a uno, contando con el voto en contra de la fiscala María José Hernández, quien estuvo por acoger dicho recurso de nulidad.

Como cuarto punto relevante en este acápite, en cuanto al concepto de "dato", si bien es posible afirmar que no existe una definición legal del mismo por parte de la ley 19.223, teniendo en cuenta lo expuesto más arriba, existen intentos jurisprudenciales penales, de definir esta materia. Así, el JG de Concepción en causa Ruc 1410003541-4 (16.05.2016), la cual en su considerando 4°, haciendo referencia a los datos informáticos, los considera como cosas muebles incorporales:

> (…) traducida básicamente la evidencia de una cosa mueble incorporal como lo es un ´dato informático´, contenido en un sistema de tratamiento de información de un privado, banco BBVA, en que el soporte lógico de los ordenadores son en sí mismos información.

También, la sentencia del JG de Concepción en causa Ruc 1410003541-4 (16.05.2016), que hace referencia a que lo alterado fue la representación de información, que en la especie se encuentra determinada por un registro contable.

Las críticas que ha sufrido la ley 19.223 en cuanto a la materia de la protección de datos, dice relación con que esta no distingue las distintas calidades de los datos que son procesados en un

sistema de tratamiento de información, haciendo equiparables los datos personales, datos comerciales de una empresa u otros de entidad elevada, con cualquier otro tipo de dato de valor insignificante. También, se le ha criticado a la redacción de la norma que esta no hace referencia a quien pertenece la titularidad de los datos contenidos en el sistema informático, y que constituye en definitiva lo protegido por el artículo 3°, pudiendo ser autor de este delito aquel que altere, dañe o destruya datos de su propia titularidad. La jurisprudencia ha hecho eco de ello, reconociendo el déficit legislativo en la materia, pero sin caer en el absurdo de aplicar las sanciones penales de la ley informática a aquellas personas que hayan alterado, dañado o destruido datos de naturaleza insignificante, o a aquel que altere datos de su propia titularidad.

c. Medios y circunstancias comisivas

En relación al tercer elemento de tipo objetivo, esto es los medios y circunstancias comisivas, la ley 19.223 no contempla para ninguno de sus artículos alguno de estos en específico, por lo que los tipos penales contenidos en ella pueden ser clasificados en la categoría de aquellos delitos de medios libres o abiertos. Esto significa, en relación al delito de alteración de datos del artículo 3°, que cualquier medio o circunstancia comisiva es apta para provocar el resultado descrito en tipo penal, esto es: la alteración, daño o destrucción de los datos.

En el proceso de elaboración de la ley, se pensó en los delitos informáticos como algo especial dentro del Derecho Penal general, radicando su especialidad precisamente en que sus modalidades comisivas, estaban caracterizadas por un entorno informatizado, dado el avance reciente de las tecnologías de la comunicación e información. Poniendo así, esta característica por sobre los fines de protección de la norma, que estaría dada por la protección de bienes jurídicos tradicionales. Este enfoque, denominado como enfoque fenomenológico fundamentó en parte, la tipificación de los delitos informáticos en una ley especial, extra Código Penal[101]. Pero lo cierto es que en la redacción final del articulado de la ley no se recogió de forma adecuada la afectación de este nuevo bien jurídico protegido por la ley a través de las conductas descritas en ella. O, dicho de otro modo: la ley 19.223 no se hizo cargo del fenómeno

[101] Tema tratado con mayor profundidad en el Capítulo I del presente trabajo.

informático. Siendo la principal causa de ello la eliminación del término "automatizado" al referirse a los sistemas de tratamiento de información, desvirtuando completamente el sentido original del proyecto[102].

Ahora, si bien es cierto que los delitos de la ley 19.223 no tienen un medio comisivo especial, la jurisprudencia ha aplicado sus normas estrictamente en lo referente a situaciones informatizadas, como se mencionó en el acápite anterior, referente al objeto de ataque. En particular a lo referente al artículo 3°, esto ha dado lugar a que diversas conductas puedan ser encasilladas dentro del mismo.

iv. Tipo subjetivo y eventuales elementos subjetivos del tipo

La faz subjetiva del tipo está dada, en los delitos dolosos, por la "congruencia de entre el conocimiento, la voluntad de realización y los requisitos objetivos del hecho típico"[103], dicho de otra forma en el conocer y querer la concurrencia de los elementos objetivos del tipo. O en segundo término, haberla podido conocer empleando el debido cuidado o diligencia, situación que dará lugar a la configuración de un delito culposo[104]. En la ley 19.223, la faz subjetiva del tipo está constituido en tres de sus artículos, incluyendo el artículo 3° objeto de esta investigación, por la voz "maliciosamente". Como antecedente, se puede afirmar que fue introducida en la discusión del proyecto, reemplazando a la voz "indebidamente", y generando controversias desde aquel momento. El conflicto se suscitó entre quienes aconsejaron la introducción de la voz maliciosamente, en razón de que se le considera sinónimo de dolo directo y por lo tanto la ideal para referirse a aquel que ha realizado con intención, propósito y plena conciencia criminal, la conducta descrita en el tipo penal. Por otro lado, estando en desacuerdo con su introducción, y por ende de mantener la voz "indebidamente", aquellos que consideraron que su incorporación exigiría un dolo específico que no se encuentra amparado por el artículo 1° del Código Penal, en virtud de la cual las acciones y omisiones penadas por la ley se reputan

[102] *Óp. cit.*, Magliona Markovicth, C. & López Medel, M. (1999). p.142.
[103] Cury Urzúa, E. (2005). Derecho Penal parte general. p. 322.
[104] *Ibídem. p. 325 y ss.*

siempre voluntarias a no ser que conste lo contrario. El dolo específico debería probarse, y en caso contrario, quedarían al margen de sanción penal las conductas realizadas exclusivamente con dolo genérico[105].

Tres de los cuatro tipos penales contenidos en la ley 19.223 contienen la voz "maliciosamente"[106] como constituyente de su faz subjetiva. En el delito restante, contenido en el artículo 2°, la faz subjetiva del tipo la constituye la voz "indebidamente", la que además contiene exigencias subjetivas adicionales, configurado finalmente como "ánimo de apoderarse, usar o conocer indebidamente*"*. Esto es excepcional y se puede afirmar que la ley 19.223 contiene la voz maliciosamente como rectora del tipo subjetivo como regla general.

Así entonces, tanto la doctrina como la jurisprudencia se han devenido en la especificación de este concepto, unos en supuestos teóricos, los otros en su aplicación concreta. La discusión doctrinal ha girado en torno a las mismas consideraciones antes mencionadas y encontramos partidarios de ambas posturas. A modo de síntesis, y haciendo referencia a una discusión que escapa del ámbito de aplicación de la ley 19.223 y dice relación con el Derecho Penal chileno en general, estas posturas pueden ser expuestas como aquella conformada por la mayoría de la doctrina moderna, que entiende la expresión "voluntariedad" del art. 1° del Código Penal como un "conciencia de antijuridicidad" y no como sinónimo de dolo[107]. Así entonces, la expresión "malicia" es entendida en el sentido de restringir la imputación objetiva (faz subjetiva), las razones que se usa para ello son entender este concepto dentro de un sistema de *numerus clausus* respecto de la realización imprudente del tipo, dada por las reglas generales. En este sentido se entiende que si existen reglas especiales en que se atribuye responsabilidad penal a una conducta realizada con imprudencia (culpa) el sentido de la voz "maliciosamente" solo se le da el sentido de excluir la modalidad culposa de dichas conductas[108]. Mientras que, en otras situaciones en que no se admite la comisión imprudente de las conductas típicas, en aplicación de las reglas generales, el sentido de la voz maliciosamente es restringir la faz subjetiva del tipo, excluyendo

[105] *Óp. cit.*, Huerta, M., y Líbano, C. (1998). p.212.
[106] La excepción la constituye el artículo 2°, cuya faz subjetiva está constituida por el "ánimo de apoderarse, usar o conocer indebidamente"
[107] Cury Urzúa, E. (2005). Derecho Penal parte general. p. 306 y 307.
[108] Por ejemplo los arts. 490, 491 y 402 respecto de los delitos contra las personas (Título VIII del Código Penal).

la comisión de las conductas tipificadas mediando dolo eventual, quedando solo la posibilidad de su comisión mediando dolo directo, o dolo directo de segundo grado. Es en este último sentido en que se encontraría la ley 19.223, toda vez que no admitiendo la comisión culposa de los delitos contenidos en ella[109], el sentido restrictivo de la voz "maliciosamente" excluye la posibilidad de cometer los delitos informáticos de la misma bajo la modalidad de dolo eventual.

La jurisprudencia en esta materia, también ha considerado el elemento maliciosamente como sinónimo de dolo directo. Así, la Corte Suprema en la causa Rol 2024-2012 (01.06.2012), optó por rechazar el recurso de casación interpuesto, aceptando por ello el razonamiento de la Corte de Apelaciones de Santiago[110] que absolvía a una imputada de cometer el delito contenido en el artículo 3° de la ley informática en razón de que el dolo que se dio por probado podría corresponder más bien a un error, ya que no se deduciría de su comportamiento una intención de enriquecerse a sí misma o de dañar a la parte contraria, las que permitirían hacer deducible una intención dolosa. Así, en su considerando 6°, la Corte establece que:

> (…) los hechos establecidos en el proceso resultan inamovibles para estos sentenciadores, tanto en lo relativo al delito mismo como a la participación de la acusada, siendo del caso que en el presupuesto fáctico arriba transcrito no se advierte la animosidad con que pudo haber actuado la acusada y que conforma el elemento subjetivo del tipo penal, en tanto los jueces de alzada optaron por

[109] Como se mencionó en el Capítulo I, en la discusión del proyecto legislativo se excluyó expresamente la aplicación de los tipos penales contenidos en la ley 19.223 a las conductas cometidas con culpa, dejando por ello sin tipificar los llamados "cuasidelitos informáticos".

[110] La referida sentencia de la Corte de Apelaciones de Santiago Rol 2347-2011 (13.01.2012) acoge apelación y absuelve a la imputada por el art. 3°, cuyo considerando 2° establece que:

> en la especie, se encuentra establecido que las conexiones a la página www.sii.cl para realizar la alteración de los datos contenidos en el sistema de información tributaria de la empresa querellante, así como dichas mismas alteraciones, fueron realizadas por la acusada. No obstante, no se ha establecido en el proceso de modo alguno que tal actuación la realizó con la intención de cometer la acción tipificada como delito en el artículo 3º de la ley 19.223, ni existe indicios de la motivación que la habría llevado a realizar esa conducta, esto es, si lo fue para obtener algún beneficio económico, para defraudar a esta empresa, para robar información, como extorsión, espionaje, amenazas, o para otra cualquiera finalidad que el sistema informático le pudiere permitir. La ausencia de esta motivación descarta la existencia de dolo pues impide establecer con certeza que la acusada actuó con la intención de causar daño a la querellante.

> entender que bien pudo responder a un simple error de aquélla, lo que resulta incompatible con la exigencia de malicia que contiene el tipo penal investigado.

Esta doctrina de la Corte Suprema encuentra sustento en dos sentencias anteriores del mismo tribunal. La primera, en causa Rol 370-02 (24.06.2004), en que pese a que se condenó al imputado por el artículo 1° de la ley 19.223 se estableció la doctrina que considera el elemento maliciosamente como exigencia de dolo directo, excluyendo de esta forma la figura de dolo eventual. Y, en el mismo sentido lo establece la sentencia de Rol 4245-2008 (02.04.2009)[111].

En aplicación de este criterio, se pronuncia la sentencia de la Corte de Apelaciones de Concepción en causa Rol 844-2014 (30.01.2015), en su considerando 19°:

> Que del mérito de los antecedentes se desprende con claridad que las conductas desplegadas por la acusada Sandra Gouet San Martín, tuvieron un solo propósito, cual fue lograr que el sistema computacional no registrara que el cliente Jorge Barbieri Luarte excedía el crédito otorgado por la empresa ($3.000.000) y así poder efectuarle otras ventas de combustible. Como se acreditó en el juicio, consignaba como pagados o depositados cheques que recibía de Barbieri, en circunstancias que eran a fecha y no eran depositados en ese momento, para luego anular el ingreso de esa información.
> Al prestar declaración en estrados señaló que fingía el depósito y luego lo anulaba, lo que permitía, según lo expresa, aumentar por una parte el crédito del cliente y por otra, darle tiempo para pagar los documentos. (Considerando 6°).
> De este modo posibilitó que las ventas no autorizadas superaran los $80.000.000.- pesos.

Esta sentencia confirma la sentencia condenatoria del TOP de Los Ángeles que en causa Ruc 0810011797-6 (11.12.2014), se refirió al elemento subjetivo del artículo 3°. En primer lugar, en

[111] Estas referencias a sentencias anteriores al año 2010 y que por ende no forman parte de la muestra de sentencias analizadas, fueron tomadas del texto Estado de internet en Chile: aspectos generales, regulación y actores relevantes. De los autores J. Carlos Lara Gálvez, Francisco Vera Hott & Pablo Viollier Bonvin. p 25.

su considerando 8°, expresando que acusador y defensa concordaron en que la expresión maliciosamente se refería al dolo, y luego en su considerando 23° refiriéndose a la inexistencia de elementos subjetivos adicionales en el artículo 3°, señala:

> Que, finalmente, la defensa de la acusada también ha exigido que concurra ánimo de lucro y un perjuicio patrimonial para la configuración del tipo penal, sin embargo, dicha exigencia es menester para el delito de fraude informático; que es, así como el delito de sabotaje o alteración de datos, una especie dentro de la gama de delitos informáticos, mas, no resulta necesaria para la configuración de éste último, y materia del presente juicio.
>
> En efecto, el delito de alteración de datos implica cambiar la esencia o forma de una cosa, y "comprende, por ejemplo la introducción de datos erróneos, las trasformación y desfiguración de datos y el suprimir datos correctos", y "lo que protege el interés en la utilización de datos en perfecto estado", (Claudio Paul Magliona Markovicth y Macarena López Medel en su obra "Delincuencia y Fraude Informático. Ed. Jurídica, pág. 168 y 169), lo que se condice, a su vez, con el fundamento para la tramitación de la Ley 19.22[3], en orden a la importancia que revisten hoy en día dichos soportes para la mantención de datos en una organización, las que constituyen respaldos en procesos de adopción de decisiones. Aquello también se vio reflejado en el rechazo de los legisladores en adoptar el sistema propuesto por el ejecutivo en sus indicaciones, que, en síntesis, regulaba el sistema informático como un medio para la comisión de ilícitos, y no como un fin en sí mismo, consagrando expresamente la figura del fraude informático. (Primer Trámite Constitucional. Discusión en Sala, Historia de la Ley Pág. 37 a 61).
>
> Por su parte, el fraude informático, ha sido definido por la doctrina como "la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento

informático, con ánimo de lucro y en perjuicio de tercero" (Ramón Casabona, Citado por Claudio Paul Magliona Markovicth y Macarena López Medel en su obra "Delincuencia y Fraude Informático. Ed. Jurídica Pág. 184), cuyo bien jurídico protegido es el patrimonio por una parte, y la confianza en el funcionamiento de los sistemas informatizados, por otra, pero como un interés social. Es decir, en esta figura sí es exigencia los requisitos del ánimo de lucro y perjuicio patrimonial. Sin embargo, los autores citados hacen presente la falta de regulación que abarque el fenómeno del fraude informático en la Ley 19.223, sin perjuicio de tipificar el sabotaje informático, en su artículo 1°; el espionaje informático en su artículo 2°; la alteración de datos en el artículo 3°, materia de esta juicio, y la revelación o difusión de datos, en su artículo 4°. Terminología que también utiliza la propia historia de la ley 19.223 en la Moción Parlamentaria; y en cuyo proyecto se contenía un artículo 5° que aumentaba las penas si las conductas de los artículos anteriores –entre ellas la alteración de datos, primitivamente regulada en el artículo 4°- eran efectuadas con ánimo de lucro.

De este modo, no se comparte con la defensa la exigencia del perjuicio netamente económico ni el elemento subjetivo adicional, no obstante que, en la especie, y tal como lo sostuvieron los testigos pertenecientes a la Empresa Cruz y Cía., el perito informático y la acusada en su declaración, ésta efectuó los movimientos en el sistema computacional con el objeto de proporcionar más crédito que el autorizado al cliente, de modo que si obró con ánimo de lucro, en este caso, para un tercero. Crédito que, por lo demás fue efectivamente utilizado por el acusado, quien adquirió combustible, y sin perjuicio de las razones que alude, no lo pagó, como el mismo lo reconoció en su declaración.

En aplicación textual de este criterio, pero en relación al artículo 1° de la ley, la sentencia del TOP de la Serena en causa Ruc 0910021731-4 (22.03.2012), absolvió a la acusada en razón de la falta de conocimiento que tenía esta sobre la vulnerabilidad del sistema, no pudiendo establecer entonces lo malicioso de su actuar. Así, en su considerando 11°:

> Que, así las cosas, no quedando acreditado en juicio que la acusada conociera real y efectivamente la vulnerabilidad del sistema informático, y en consecuencia deliberadamente produjera el error en éste, tampoco resulta posible dar por concurrente el delito consagrado en el artículo 1 de la ley 19.223, ya que tal delito exige que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento.

Y también la sentencia del TOP de San Bernardo, que refiriéndose al art. 4° en causa Ruc 1100498003-6 Considerando 11° numeral iii (14.05.2016), absolvió al imputado explicitando la exigencia de dolo directo, y la improcedencia de cometer este delito con dolo eventual:

> En segundo lugar debe tenerse en cuenta que la faz subjetiva de esta figura exige que aquella sea cometida con dolo directo al utilizarse en su descripción típica la voz "maliciosamente". Luego, desde la perspectiva de su faz subjetiva, si es que el imputado Gerko Henríquez hubiere actuado con dolo eventual no podría tenerse por configurado este delito. Al respecto debe tenerse en consideración que el convenio de cooperación que prescribía la confidencialidad de ciertas informaciones contenidas en el sistema monito web nunca les fue informada ni instruida a los funcionarios del Tribunal.
>
> Por lo tanto, Henríquez bien pudo haberse representado la posibilidad de que infringía una prohibición de difundir la información de ese sistema informático, pudo hasta haber aceptado esa consecuencia, y sin embargo, en dicho contexto sólo habría actuado con dolo eventual y, por lo tanto, no se podría tener por configurada esta figura penal.

En la causa TOP 3° Santiago Ruc 1000464726-8 (19.06.2012)[112] se condenó a un médico del Hospital de Carabineros por los delitos de homicidio culposo y el delito informático del art. 3° de la ley 19.223. Los hechos que se tuvieron por acreditados demuestran que el imputado, un médico radiólogo, que en ese momento estaba encargado de realizar este tipo de exámenes, informó un examen de Angio TAC de tórax realizado a la paciente, por orden del médico tratante, este concluía que 'No hay hallazgos compatibles con TEP'[113]. Días más tarde la paciente murió, siendo la causa de muerte un tromboembolismo pulmonar (TEP). Transcurridos algunos días de la muerte de la paciente, el médico radiólogo encargado de dicho examen, ingresaría al sistema computacional del Hospital de Carabineros (RISC) y modificaría el examen primigenio, concluyendo en este segundo examen que: ´No hay hallazgos categóricos compatibles con TEP. Se sugiere controlar y revaluar según evolución clínica. Tenues imágenes nodulares subpleurales de aspecto inespecífico que se sugiere controlar´. En lo pertinente al elemento subjetivo del tipo, en este caso la malicia, el Tribunal Oral equipara el dolo con malicia, dándola por probado por una serie de elementos, así en su considerando 27°, establece que :

> A su vez, en virtud de los registros históricos existentes en el HOSCAR y particularmente en lo referente al examen de Angio TAC de tórax practicado a la joven Bárbara Anahí Velásquez Caro, el Tribunal obtuvo ilustración suficiente, concatenado a los dichos del mencionado testigo Ayala Martínez en correspondencia con lo expuesto por el Sub-comisario de la Policía de Investigaciones de Chile Mauricio Díaz Albornoz, en cuanto a la razones de la dualidad de existir ambos informes, a raíz de la investigación que se hizo como parte del sumario interno que se llevó por el propio Hospital y que arrojó como resultado la intervención dentro de dicho sistema de parte del acusado HERNÁNDEZ CANALES, situación que acaeció pocos días después del fallecimiento de la víctima, lo cual, por lo demás se vio complementado con los propios dichos de HERNÁNDEZ CANALES, quien además reconoció en

[112] Cuya sentencia fue objeto de recurso de nulidad, al que no se le dio lugar por la Corte de Apelaciones de Santiago. 1803-2012. (30.08.2012).
[113] Tromboembolismo pulmonar.

> estrados que para tales efectos contaba con una clave personal e intransferible que se le había entregado por el propio Servicio, reconociendo por lo demás que dicha clave personal nunca se la reveló a ninguna persona, aunado a la circunstancia que de acuerdo al citado registro histórico, quedó acreditado de la misma manera que el doctor HERNÁNDEZ ingresó al referido sistema informático y modificó mediante dictado de voz, el contenido del citado informe, una vez producida la muerte en referencia, indicio que dejó en evidencia el dolo o faz subjetiva con que aquél actuó en cuanto a la configuración del tipo penal en cuestión, previsto en el artículo 3° de la Ley N° 19.223, en su verbo rector "alterar" de manera maliciosa los datos contenidos en un sistema de tratamiento de información.[114]

La jurisprudencia ha seguido un criterio uniforme al considerar el elemento maliciosamente como el único elemento subjetivo del tipo en el art. 3° de la ley, haciéndolo equiparable con una exigencia de dolo directo, eliminando de esta forma las posibilidades de comisión de este delito mediante el dolo eventual[115]. Además, como se mencionó en el apartado de historia fidedigna de la ley 19.223, quedando expresamente fuera de esta ley la posibilidad de comisión de cuasidelitos informáticos.

v. Causas de justificación

En materia de causales de justificación es posible afirmar que se aplican al delito de alteración de datos, al igual que al resto del articulado de la ley 19.223 las reglas generales del derecho penal. De esta forma, se podría hacer uso de una justificante tanto en su aspecto formal de la

[114] Además la sentencia del TOP de Viña Ruc 0910023307-7 (23.04.2012) que en su considerando 16° señala: "no concurre la faz subjetiva del tipo penal, esto es, un actuar malicioso, que debe entenderse como la conciencia positiva de estar realizando cada una de las conductas del tipo penal, que sólo se satisface con dolo directo", cuyos argumentos fueron acogidos por el CA de Valparaíso Rol 837-2012 (08.08.2012) al rechazar el recurso de nulidad presentado en su contra; Además, la sentencia del JG Villa Alemana Ruc 0910024674-8 (03.01.2011), confirmada por la CA de Valparaíso Rol 34-2011 (17.01.2011).

[115] Aunque este entendimiento no es absoluto, como es el caso de la sentencia del TOP de Curicó Ruc 0910014546-1 en su considerando 9° parte final confunde las exigencias subjetivas especiales del artículo 2° de la ley 19.223 como exigencias generales de la misma ley, otorgándoselas al resto del articulado de la ley, pero principalmente al artículo 1° que es del cual trata la sentencia.

misma, como también en su aspecto material. Si bien no se cuenta con registros de sentencias, que entre los años que cubre este trabajo de investigación, hayan hecho uso de una causal de justificación formal, ni tampoco de su uso en su aspecto material, si hay un ejemplo de absolución por parte de los tribunales penales, en razón de la ausencia del elemento de antijuricidad. Esto es, cuando no se ha verificado en los hechos del caso particular una efectiva lesión al bien jurídico protegido por la norma penal que sea merecedor de una reacción penal, perdiendo por ello el sentido la aplicación de la norma penal para el caso particular. Esto traería consecuencias diferentes teniendo presente la discusión acerca del bien jurídico protegido por la ley 19.223, a saber si es protectora de un bien jurídico nuevo de "calidad, pureza e idoneidad de la información"*;* simplemente protectora de bienes jurídicos tradicionales como sería el caso de la intimidad y la propiedad; o bien, una norma que tipifica delitos pluriofensivos, protegiendo a la vez bienes jurídicos tradicionales y un nuevo bien jurídico específicamente informático.

Así, como único ejemplo de aplicación de las reglas generales a esta de esta categoría de la teoría del delito, es posible citar la sentencia del TOP de San Bernardo en causa Ruc N° 1100498003-6 (14.05.2016) considerando 11°, literal iii, en que absolvió al imputado, principalmente por la ausencia del elemento antijuricidad material, aunque lo hace en relación al artículo 4° de lay 19.223 referido al delito de difusión de datos, y acogiendo la tesis de que en esta norma estaría tipificada una conducta pluriofensiva, que se traduciría en la protección del bien jurídico informático establecido por los legisladores de la ley 19.223, como también uno tradicional, en este caso el de privacidad.

vi. Causas de ausencia de culpabilidad y exculpación

La culpabilidad como elemento del delito no está definida expresamente en nuestra legislación. Doctrinariamente se han generado diversas acepciones de lo que debe entenderse por esta, principalmente a partir de la casuística y algunas de las circunstancias eximentes del artículo 10° del Código Penal. Para este trabajo se entendió la culpabilidad como elemento de la teoría del delito aquel juicio de reproche que se le hace al autor de un hecho típico y antijurídico, toda vez que ha obrado con una disposición interna contraria a la norma penal vulnerada, y existiendo

además en su situación una posibilidad de haber actuado de acuerdo a la misma. Concibiéndola de esta forma de acuerdo a la teoría normativa de la culpabilidad, y teniendo como consecuencia que las eventuales causas de inimputabilidad a grandes rasgos: causas derivadas de trastornos mentales, desarrollo insuficiente de la personalidad, error de prohibición, inexigibilidad de otra conducta[116].

Si bien, no se cuenta con registros de sentencias que hagan referencia a este elemento del delito en aplicación sobre la legislación informática, se puede aseverar que le son aplicables, a la ley 19.223 en general los elementos generados por la doctrina y jurisprudencia sobre este elemento.

[116] *Óp. cit.*, Cury Urzúa, E. (2005). Derecho Penal parte general. p. 385 y ss.

III. Conclusiones

El presente trabajo de investigación tuvo como primer objetivo la recolección de material jurisprudencial relativo a la ley informática número 19.223, abarcando un determinado margen de tiempo entre los años 2010 y 2018, ambos incluidos, para poner a disposición de lectores expertos e interesados en la materia esta información de forma más expedita. Este objetivo fue satisfactoriamente cumplido, tanto en términos cuantitativos como en términos cualitativos, dejando constancia de ello en los dos anexos que acompañan el presente trabajo.

En una segunda etapa, se procedió a la exposición de dicho material en relación la vigencia de la normativa informática, marcando como hitos de dicha vigencia aquellos sub-capítulos que componen el capítulo primero de esta investigación. En aquel, si bien se conceptualizó y se presentó información tratada en extenso por la doctrina nacional, se ejemplificó con sentencias judiciales aquellas conceptualizaciones jurídicas derivadas de la teorización en materia de criminalidad informática. Cobrando relevancia en esta parte el entendimiento que se ha dado, por parte de los tribunales de competencia penal, en primer término sobre concepto de delito informático. Luego, en un segundo término, el sentido de protección que se ha dado a la ley 19.223, que si bien fue creada con una intención teleológica específica, en su aplicación ha recibido muchas veces un tratamiento más extensivo, considerándose de esta forma a los delitos informáticos como figuras pluriofensivas y supliendo de alguna forma la restricción inicial de aquellos.

Posteriormente, en lo que respecta al núcleo de la investigación, la información recopilada se presentó de forma ordenada según el género de comentario de Código Penal, desglosando el tipo penal del artículo 3° según los elementos del delito. Así se especificó, en lo relativo al bien jurídico protegido, su comportamiento en la práctica judicial, considerado mayoritariamente –aunque no de forma conteste- como una figura pluriofensiva. Así también, se pone de manifiesto en el trabajo, situaciones que podrían derivar de dicha consideración, al considerar como sujetos diferentes, al titular de los datos y del bien jurídico informático, y el titular de un bien jurídico protegido accesoriamente con el delito de alteración de datos como lo serían hipotéticamente el

patrimonio, la propiedad, la honra o el valor económico de la empresa, secretos industriales, fe pública o incluso la vida.

Luego, en materia de autoría no se presenta mayores problemas, dando aplicación a las consideraciones del Derecho Penal general, la falta de distinción entre la titularidad del sujeto activo y el titular de los datos, que en primer momento produjo en doctrina una reacción de descontento, fue suplida en la aplicación de la norma, al referirse esta exclusivamente a casos en no había coincidencia entre ambos. Además se entiende por parte de la jurisprudencia nacional que no es necesario ser un experto para cometer las conductas descritas en los delitos informáticos.

Por su parte, en cuanto al verbo rector del delito de alteración de datos, se extrae de la aplicación del mismo que la gran variedad de conductas que se enmarcan dentro de los verbos rectores del delito (alterar, dañar y destruir), permite considerarlos como óptimamente flexibles ante las distintas posibilidades de ejecución que permite el avance de la tecnología. De igual forma ocurre en cuanto a los medios y circunstancias comisivas de este delito, el que admite una fórmula abierta de medios comisivos, la que permite adaptarse de mejor manera al rápido y permanente avance tecnológico. En cuanto al objeto de ataque en el delito de alteración de datos, la información presentada en el presente trabajo expone un avance jurisprudencial en especificar lo que debe entenderse por dato, por sistema de tratamiento de información e información, y aunque no se logra una doctrina consistente, si se logran identificar los problemas y consecuencias a los que dichas conceptualizaciones dan lugar.

En cuanto a lo que al tipo subjetivo respecta, se logra apreciar que en la aplicación de la voz "maliciosamente" el grueso de la doctrina judicial opta la por la consideración de aquella como restrictiva de la faz subjetiva del tipo, en el sentido de excluir, dentro del contexto de la ley 19.223, la posibilidad de comisión mediando dolo eventual, quedando como única posibilidad la comisión del delito de alteración de datos, aquella cometida con dolo directo, o bien, dolo directo de segundo grado.

Finalmente, en cuanto a las consideraciones sobre la aplicación de causales de justificación y causas sobre ausencia de culpabilidad, si bien se cuenta con escasa información respecto de esta, se logra apreciar una aplicación de las reglas generales del Derecho Penal nacional.

Bibliografía

Doctrina

Álvarez Fortte, H. (2009). Los delitos informáticos. Corpus iuris regiones: Revista Jurídica Regional y Subregional Andina, 9, 101-128.

Balmaceda Hoyos, G. (2009). El delito de estafa informática (1° ed.). Santiago de Chile: Ediciones Jurídicas de Santiago.

Cárdenas Aravena, C. (2008). El lugar de comisión de los denominados ciberdelitos. Política Criminal, 6, 1-14.

Cury Urzúa, E. (2005). Derecho Penal parte general (8° ed.) Santiago: Ediciones Universidad Católica de Chile.

Donoso, M. (2002). Bien jurídico protegido y delincuencia informática. Viña del Mar, Universidad Adolfo Ibáñez.

Escalona Vásquez, E. (2004). El hacking no es (ni puede ser) delito. Revista chilena de derecho informático, 4, 149-167.

González Marín, P. (2013). Desde el delito computacional al delito de alta tecnología: Notas para una evolución hacia el concepto y estructura del delito informático. En Alex Van Weezel (editor), Humanizar y renovar el derecho penal. Estudios en memoria de Enrique Cury, 1.073-1095. Santiago: Legal Publishing Thomson Reuters.

Hermosilla, J.P. y Aldoney, R. (2002). Delitos informáticos. En Íñigo de la Maza Gazmuri (coordinador), Derecho y Tecnologías de la información, 415-429. Santiago: Universidad Diego Portales.

Hernández Basualto, H. (2001). Tratamiento de la criminalidad informática en el derecho penal chileno. Diagnóstico y propuestas. Informe solicitado por la División Jurídica del Ministerio de Justicia. Inédito

Hernández Basualto, H. (2008). Uso indebido de tarjetas falsificadas o sustraídas y de sus claves. Política Criminal, 5, 1-38.

Herrera Bravo, R. y Núñez Romero, A. (1999). Derecho informático. Santiago: Jurídicas La Ley

Herrera Bravo, R. (1998). Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la ley chilena N° 19.223. Ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile en agosto de 1998.

Huerta Miranda, M., & Líbano Manzur, C. (1998). Delitos informáticos. (2°. ed.). Santiago de Chile: Jurídica ConoSur.

Jijena Leiva, R. (1992). Chile, la protección penal de la intimidad y el delito informático (1a. ed.). Santiago de Chile: Jurídica de Chile.

Jijena Leiva, R. (2008). Delitos informáticos, Internet y derecho. En Luis Rodríguez Collao (coordinador), Delito, pena y proceso, 145-162. Santiago: Jurídica.

Lara Gálvez, J. C.; Martínez, Maraboli M.; y Viollier Bonvin, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. Revista Chilena de Derecho y Tecnología, 3, 1, 101-137.

Lara Gálvez, J.C.; Vera Hott, F. & Viollier Bonvin, P. (2014). Estado de internet en Chile: aspectos generales, regulación y actores relevantes. ONG Derechos Digitales, N° 6.

Londoño Martínez, F. (2004). Los delitos informáticos en el proyecto de reforma en actual trámite parlamentario. Revista Chilena de Derecho Informático, 4, 171-190.

Magliona Markovicth, C., & López Medel, M. (1999). Delincuencia y fraude informático: Derecho comparado y ley no. 19.223 (1a. ed.). Santiago de Chile: Jurídica.

Magliona Markovicth, C. (2002): Análisis de la normativa sobre delincuencia informática en Chile. En de la Maza, Iñigo (coord.), Derecho y tecnologías de la información, 383-395. Santiago, Fundación Fueyo: Universidad Diego Portales.

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. Revista chilena de derecho 44, 1, 261–285.

Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Ius et Praxis, 24, 1, 159–206.

Medina Schulz, G. (2014). Estructura típica del delito de intromisión informática. Revista Chilena de Derecho y Tecnología, 3, 1, 79-99.

Moscoso Escobar, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista Chilena de Derecho y Tecnología, 3, 1, 11-78.

Vera Quilodrán, A. (1996). Delito e informática. La informática como fuente de delito. Santiago, Chile: Ediciones Jurídicas La Ley.

Jurisprudencia citada[117]

Corte Suprema, Rol N° 370-2002 (24.06.2004)

[117] Las sentencias se presentan en orden de jerarquía del tribunal que las dictó, incluyendo cuando corresponda las sentencias de tribunales inferiores dictadas en la misma causa, que fueron utilizadas para la investigación. En sentencias de la misma jerarquía se ordenan por fecha de dictación, desde la más reciente a la más antigua.

Corte Suprema, Rol N° 4245-2008 (02.04.2009)

Corte Suprema, Rol N° 2024-2012 (01.06.2012); Corte de Apelaciones de Santiago Rol 2347-2011 (13.01.2012)

Corte Suprema, Rol N° 3951-2012 (20.03.2013)

Corte de Apelaciones de Talca, Rol N° 498-2010 (20.12.2010); Tribunal de Juicio Oral en lo Penal de Curicó, Ruc N° 0910014546-1 (07.03.2011)

Corte de Apelaciones de Valparaíso, Rol N° 34-2011 (17.01.2011); Juzgado de Garantía de Villa Alemana, Ruc N° 0910024674-8 (03.01.2011)

Corte de Apelaciones de Valparaíso, Rol N° 837-2012 (08.08.2012); Tribunal de Juicio Oral en lo Penal de Viña del Mar, Ruc N° 0910023307-7 (23.04.2012)

Corte de Apelaciones de Santiago, Rol N° 1803-2012 (30.08.2012); 3° Tribunal de Juicio Oral en lo Penal de Santiago, Ruc N° 1000464726-8 (19.06.2012)

Corte de Apelaciones de Concepción, Rol 844-2014 (30.01.2015); Tribunal de Juicio Oral en lo Penal de Los Ángeles, Ruc N° 0810011797-6 (11.12.2014)

Corte de Apelaciones de Valdivia, Rol N° 312-2018 (22.05.2018)

Corte de Apelaciones de Copiapó, Rol N° 448-2018 (19.12.2018); Juzgado de Garantía de Copiapó, Ruc N° 1700582359-5 (31.10.2018)

4° Tribunal de Juicio Oral en lo Penal de Santiago, Ruc N° 1000626117-0 (08.06.2011)

Tribunal de Juicio Oral en lo Penal de La Serena, Ruc N° 0910021731-4 (22.03.2012)

Tribunal de Juicio Oral en lo Penal de Arica, Ruc N° 1210014297-8 (18.07.2014)

Tribunal de Juicio Oral en lo Penal de San Bernardo, Ruc N° 1100498003-6 (14.05.2016)

Tribunal de Juicio Oral en lo Penal de Temuco, Ruc N° 1700268031-9 (22.07.2018)

Tribunal de Juicio Oral en lo Penal de Coyhaique, Ruc N° 1610036482-9 (24.07.2018)

4° Juzgado de Garantía de Santiago, Ruc N° 1010001813-1 (30.06.2011)

Juzgado de Garantía de Talcahuano, Ruc N° 0900600732-2 (13.09.2011)

8° Juzgado de Garantía de Santiago, Ruc N° 1300971941-k (01.09.2014)

Juzgado de Garantía de La Serena, Ruc N° 1000571645-k (12.12.2014)

Juzgado de Garantía de La Serena, Ruc N° 1100470439-k (18.05.2015)

Juzgado de Garantía de Curicó, Ruc N° 1301170732-1 (04.09.2015)

7° Juzgado de Garantía de Santiago, Ruc N° 1410003541-4 (02.10.2015)

8° Juzgado de Garantía de Santiago, Ruc N° 0910000486-8 (25.11.2015)

Juzgado de Garantía de Quillota, Ruc N° 1500048128-6 (30.12.2015)

Juzgado de Garantía de Concepción, Ruc N° 1410003541-4 (16.05.2016)

8° Juzgado de Garantía de Santiago, Ruc N° 1400481698-7 (25.08.2016)

7° Juzgado de Garantía de Santiago, Ruc N° 1510011054-4 (01.12.2016)

Juzgado de Garantía de Arica, Ruc N° 1500784272-1 (06.01.2017)

7° Juzgado de Garantía de Santiago, Ruc N° 1510006022-9 (26.01.2017)

7° Juzgado de Garantía de Santiago, Ruc N° 1700296781-2 (16.02.2018)

Juzgado de Garantía de Puerto Varas, Ruc N° 1501011576-8 (15.03.2018)

7° Juzgado de Garantía de Santiago, Ruc N° 1610018667-9 (12.06.2018)

8° Juzgado de Garantía de Santiago, Ruc N° 1501138933-0 (31.12.2018)

Anexo I: Listado de sentencias referentes a la ley 19.223, con fecha de dictación entre 2010 a 2018[118]

Tribunal	ROL/RUC	Año dictación
Corte Suprema	9238-2013	2013
Corte Suprema	3951-2012	2013
Corte Suprema	2024-2012	2012
Corte Suprema	2249-2012	2012
Corte Suprema	7777-2011	2012
Corte Suprema	742-2011	2011
Corte de Apelaciones de Copiapó	448-18	2018
Corte de Apelaciones de Valdivia	312-2018	2018
Corte de Apelaciones de La Serena	24-2017	2017
Corte de Apelaciones de Santiago	2143-2017	2017
Corte de Apelaciones de Santiago	1760-2017	2017
Corte de Apelaciones de Valparaíso	1763-2017	2017
Corte de Apelaciones de Concepción	844-2014	2015
Corte de Apelaciones de Santiago	1967-2012	2013
Corte de Apelaciones de Santiago	2091-2012	2013
Corte de Apelaciones de Santiago	1803-2012	2012
Corte de Apelaciones de Santiago	2347-2011	2012
Corte de Apelaciones de Valparaíso	837-2012	2012
Corte de Apelaciones de Chillán	100-2010	2011

[118] Las sentencias se presentan en orden de jerarquía del tribunal que la dictó, y dentro de la misma jerarquía ordenadas por fecha, desde la más reciente hasta la más antigua.

Corte de Apelaciones de Santiago	1398-2011	2011
Corte de Apelaciones de Santiago	638-2011	2011
Corte de Apelaciones de Valparaíso	34-2011	2011
Corte de Apelaciones de Santiago	2573-2009	2010
Corte de Apelaciones de Santiago	2705-2009	2010
Corte de Apelaciones de Talca	498-2010	2010
Corte de Apelaciones de Santiago	2447-2007	2009
4º Tribunal de Juicio Oral en lo Penal de Santiago	1501254486-0	2018
Tribunal de Juicio Oral en lo Penal de Coyhaique	1610036487-9	2018
Tribunal de Juicio Oral en lo Penal de Temuco	1700268031-9	2018
Tribunal de Juicio Oral en lo Penal de Valparaíso	1600109716-8	2017
Tribunal de Juicio Oral en lo Penal de la Serena	1400644806-3	2015
Tribunal de Juicio Oral en lo Penal de Arica	1210014297-8	2014
Tribunal de Juicio Oral en lo Penal de Los Ángeles	0810011797-6	2014
3º Tribunal de Juicio Oral en lo Penal de Santiago	1310023323-6	2013
1° Tribunal de Juicio Oral en lo Penal de Santiago	0900350109-1	2012
3° Tribunal de Juicio Oral en lo Penal de Santiago	1000464726-8	2012

Tribunal de Juicio Oral en lo Penal de la Serena	0910021731-4	2012
Tribunal de Juicio Oral en lo Penal Viña del Mar	0910023307-7	2012
4º Tribunal de Juicio Oral en lo Penal de Santiago	1000626117-0	2011
4º Tribunal de Juicio Oral en lo Penal de Santiago	1001109352-9	2011
7º Tribunal de Juicio Oral en lo Penal de Santiago	0710028046-3	2011
Tribunal de Juicio Oral en lo Penal de Curicó	0910014546-1	2011
11º Juzgado de Garantía de Santiago	1810005322-1	2018
14° Juzgado de Garantía de Santiago	1800453522-3	2018
1º Juzgado de Garantía de Santiago	1601114389-3	2018
1º Juzgado de Letras y Garantía de Peumo	1600985002-7	2018
4º Juzgado de Garantía de Santiago	1500754624-3	2018
7º Juzgado de Garantía de Santiago	1610018667-9	2018
7º Juzgado de Garantía de Santiago	1700296781-2	2018
8º Juzgado de Garantía de Santiago	1501135350-6	2018
8º Juzgado de Garantía de Santiago	1501138933-0	2018
8º Juzgado de Garantía de Santiago	1600069485-5	2018
8º Juzgado de Garantía de Santiago	1700417037-7	2018
8º Juzgado de Garantía de Santiago	1700687472-K	2018
8º Juzgado de Garantía de Santiago	1701065592-7	2018

9º Juzgado de Garantía de Santiago	1700977530-7	2018
Juzgado de Garantía de Chillán	1700852761-K	2018
Juzgado de Garantía de Concepción	1710024936-7	2018
Juzgado de Garantía de Copiapó	1700582359-5	2018
Juzgado de Garantía de Los Ángeles	1600162684-5	2018
Juzgado de Garantía de Puerto Varas	1501011576-8	2018
Juzgado de Garantía de Punta Arenas	1701088612-0	2018
Juzgado de Garantía de Temuco	1600578370-8	2018
Juzgado de Letras y Garantía de Licantén	1400871048-2	2018
Juzgado de Letras y Garantía de Pichilemu	1600784691-K	2018
3º Juzgado de Garantía de Santiago	1600262493-5	2017
6º Juzgado de Garantía de Santiago	1600974831-1	2017
7º Juzgado de Garantía de Santiago	1010034106-4	2017
7º Juzgado de Garantía de Santiago	1300491398-6	2017
7º Juzgado de Garantía de Santiago	1500784272-1	2017
7º Juzgado de Garantía de Santiago	1500986607-5	2017
7º Juzgado de Garantía de Santiago	1510006022-9	2017
7º Juzgado de Garantía de Santiago	1600365596-6	2017
8º Juzgado de Garantía de Santiago	1600076091-2	2017
8º Juzgado de Garantía de Santiago	1600096085-7	2017
Juzgado de Garantía de Arica	1500691742-6	2017
Juzgado de Garantía de Copiapó	1600621489-8	2017

Juzgado de Garantía de Rengo	1600299000-1	2017
Juzgado de Garantía de San Bernardo	1710020214-K	2017
Juzgado de Garantía de Temuco	1400974702-9	2017
Juzgado de Garantía de Valdivia	1400215106-6	2017
Juzgado de Garantía de Valdivia	1501255135-2	2017
Juzgado de Garantía de Valdivia	1700019546-4	2017
2° Juzgado de Garantía de Santiago	1600624220-4	2016
4º Juzgado de Garantía de Santiago	1500571770-9	2016
7º Juzgado de Garantía de Santiago	1510011054-4	2016
8° Juzgado de Garantía de Santiago	1300772456-4	2016
8° Juzgado de Garantía de Santiago	1401188406-8	2016
8º Juzgado de Garantía de Santiago	1200358361-7	2016
8º Juzgado de Garantía de Santiago	1301252012-8	2016
8º Juzgado de Garantía de Santiago	1400481698-7	2016
8º Juzgado de Garantía de Santiago	1500330341-9	2016
8º Juzgado de Garantía de Santiago	1510015652-8	2016
8º Juzgado de Garantía de Santiago	1600356068-K	2016
Juzgado de Garantía de Concepción	1410015476-6	2016
Juzgado de Garantía de Coyhaique	1400534287-3	2016
Juzgado de Garantía de Valdivia	1300771259-0	2016
Juzgado de Garantía de Valdivia	1400365350-2	2016
Juzgado de Garantía de Valparaíso	1500670451-1	2016
Juzgado de Garantía de Viña del Mar	1401174769-9	2016
7° Juzgado de Garantía de Santiago	1310032588-2	2015

7° Juzgado de Garantía de Santiago	1401159799-9	2015
7º Juzgado de Garantía de Santiago	1310027331-9	2015
7º Juzgado de Garantía de Santiago	1410003541-4	2015
7º Juzgado de Garantía de Santiago	1510013640-3	2015
8º Juzgado de Garantía de Santiago	0910000486-8	2015
8º Juzgado de Garantía de Santiago	1101206060-4	2015
8º Juzgado de Garantía de Santiago	1300235719-9	2015
8º Juzgado de Garantía de Santiago	1301018212-8	2015
Juzgado de Garantía de Curicó	1301170732-1	2015
Juzgado de Garantía de Curicó	1510003134-2	2015
Juzgado de Garantía de Iquique	1410023383-6	2015
Juzgado de Garantía de la Serena	1100470439-K	2015
Juzgado de Garantía de Quillota	1500048128-6	2015
Juzgado de Garantía de Valdivia	1400229791-5	2015
Juzgado de Garantía de Viña del Mar	1500082601-1	2015
14º Juzgado de Garantía de Santiago	1201043218-7	2014
7º Juzgado de Garantía de Santiago	1300365840-0	2014
7º Juzgado de Garantía de Santiago	1300427073-2	2014
7º Juzgado de Garantía de Santiago	1301115464-0	2014
8º Juzgado de Garantía de Santiago	1200473077-K	2014
8º Juzgado de Garantía de Santiago	1300971941-K	2014
8º Juzgado de Garantía de Santiago	1400529583-2	2014
Juzgado de Garantía de Chillán	1400050382-8	2014
Juzgado de Garantía de Coquimbo	1200859257-6	2014

Juzgado de Garantía de Iquique	1000544350-K	2014
Juzgado de Garantía de la Serena	1000571645-K	2014
Juzgado de Garantía de Valdivia	1200490063-2	2014
12º Juzgado de Garantía de Santiago	1200166874-7	2013
4° Juzgado de Garantía de Santiago	1110009853-0	2013
4° Juzgado de Garantía de Santiago	1200564274-2	2013
Juzgado de Garantía de Cauquenes	1200244914-3	2013
Juzgado de Garantía de Concepción	0901009275-K	2013
Juzgado de Garantía de Concepción	1100788925-0	2013
Juzgado de Garantía de la Serena	0901136485-0	2013
Juzgado de Garantía de Loncoche	1200676447-7	2013
Juzgado de Garantía de Viña del Mar	0901242626-4	2013
Juzgado de Letras y Garantía de Pucón	1200347520-2	2013
4º Juzgado de Garantía de Santiago	0910023762-5	2012
7° Juzgado de Garantía de Santiago	1000513809-K	2012
7º Juzgado de Garantía de Santiago	0800707626-7	2012
7º Juzgado de Garantía de Santiago	1000798695-0	2012
7º Juzgado de Garantía de Santiago	1010015205-9	2012
7º Juzgado de Garantía de Santiago	1100299934-1	2012
Juzgado de Garantía de Curicó	0900810060-5	2012
Juzgado de Garantía de Curicó	1010010665-0	2012
Juzgado de Garantía de Lautaro	1100764645-5	2012
Juzgado de Garantía de Talca	1010026055-2	2012
Juzgado de Garantía de Valdivia	1200063441-5	2012

4º Juzgado de Garantía de Santiago	0801035405-7	2011
4º Juzgado de Garantía de Santiago	1010001813-1	2011
8° Juzgado de Garantía de Santiago	1000897066-7	2011
8º Juzgado de Garantía de Santiago	0901185869-1	2011
8º Juzgado de Garantía de Santiago	0901240546-1	2011
8º Juzgado de Garantía de Santiago	1010000225-1	2011
8º Juzgado de Garantía de Santiago	1010014390-4	2011
8º Juzgado de Garantía de Santiago	1100023556-5	2011
Juzgado de Garantía de Angol	1000913187-1	2011
Juzgado de Garantía de Arica	1000510991-K	2011
Juzgado de Garantía de Concepción	1010008200-K	2011
Juzgado de Garantía de Iquique	1001206389-5	2011
Juzgado de Garantía de Lautaro	1000913699-7	2011
Juzgado de Garantía de Punta Arenas	1010023142-0	2011
Juzgado de Garantía de Talcahuano	0900600732-2	2011
Juzgado de Garantía de Temuco	0901155715-2	2011
Juzgado de Letras y Garantía de Traiguén	1100296829-2	2011
13º Juzgado de Garantía de Santiago	0900421772-9	2010
4º Juzgado de Garantía de Santiago	0800680998-8	2010
7° Juzgado de Garantía de Santiago	0910000588-0	2010
8º Juzgado de Garantía de Santiago	0900673164-0	2010
8º Juzgado de Garantía de Santiago	1000077397-8	2010
9º Juzgado de Garantía de Santiago	0800082583-3	2010

Juzgado de Garantía de Arica	0910014535-6	2010
Juzgado de Letras y Garantía de Traiguén	1000783152-3	2010

Anexo II: Ficha jurisprudencial de cada sentencia citada

- **Tribunal:** Corte Suprema (Segunda Sala)
- **Ministros:** Milton Juica A., Hugo Dolmestch U., Carlos Künsemüller L., Juan Escobar Z. y Jorge Lagos G. (abogado integrante)
- **Fecha:** 01.06.2012
- **Rol:** 2024-12
- **Recurso:** Recurso de casación en el fondo
- **Tribunal de origen:** Segundo Juzgado del Crimen de Santiago
- **Síntesis de los hechos:**

Entre los días 24 y 25 de enero de 2004, en esta ciudad, se alteraron datos contenidos en el sistema de información tributaria de la empresa Importadora y Exportadora HJ Limitada, en cuanto los folios originales de declaraciones del formulario 29 de los años 2001 a 2003 habían sido anulados, generándose treinta tres giros automáticos por un total aproximado de $911.000.000 y la declaración original de formulario 22 del año tributario 2003 había sido rectificada en dos ocasiones en el mes de enero de 2004 agregándose ingresos antes no declarados por $152.000.000 lo que generó otro giro automático. Para ello, las conexiones a la página www.sii.cl se realizaron en el domicilio de la querellada, obteniéndose una clave inicial y una nueva clave secreta de la empresa querellante".

Si bien por estos hechos se estimó constitutivo del delito que sanciona el artículo 3° de la ley 19.223 en la sentencia de primera instancia, ello no fue así corroborado en el fallo de alzada y que ahora se analiza, puesto que aquel tipo ordena sancionar a: "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información…", y como en todo delito, es precisa la concurrencia del elemento dolo, el que no se estimó probado en la causa, puesto que para aquellos jueces apareció verosímil la versión de la acusada que esgrimió la posibilidad de haber cometido un error al desempeñar su trabajo en el portal de internet del

S.I.I., lo que se vio reforzado por el hecho que no se estableció de modo alguno que la imputada reportara algún beneficio de cualquier índole con su proceder, como tampoco que la empresa sufriera un perjuicio irreparable.

En consecuencia, los jueces de alzada revocaron el fallo de primera instancia y absolvieron a la acusada por considerar que en el hecho denunciado no quedó comprobada la concurrencia del elemento dolo en el actuar de la imputada, requisito indispensable para la configuración del tipo, lo que el recurrente impugnó, por estimarlo configurado –de acuerdo a la infracción de normas reguladoras de la prueba que no prosperó- y a la supuesta aplicación de la presunción del artículo 1° del Código Penal.

- **Decisión del tribunal:**

Se rechazó el recurso de casación en el fondo deducido por la parte querellante contra la sentencia de trece de enero de dos mil doce.

- **Considerandos relevantes:**

SEXTO: Que, sin embargo, como ya se anticipó, los hechos establecidos en el proceso resultan inamovibles para estos sentenciadores, tanto en lo relativo al delito mismo como a la participación de la acusada, siendo del caso que en el presupuesto fáctico arriba transcrito no se advierte la animosidad con que pudo haber actuado la acusada y que conforma el elemento subjetivo del tipo penal, en tanto los jueces de alzada optaron por entender que bien pudo responder a un simple error de aquélla, lo que resulta incompatible con la exigencia de malicia que contiene el tipo penal investigado.

- **Tribunal:** Corte Suprema (Segunda Sala)
- **Ministros:** Milton Juica A., Hugo Dolmestch U., Carlos Künsemüller L., Haroldo Brito C., Jorge Lagos G. (abogado integrante), y el Auditor General del Ejército Waldo Martínez C.
- **Fecha:** 20.03.2013
- **Rol:** 3951-2012
- **Recurso:** Recurso de casación en el fondo
- **Tribunal de origen:** Segundo Juzgado Militar de Santiago
- **Síntesis de los hechos:**

En el interior del Regimiento Logístico N° 3 Limache un oficial del grado de Capitán le pidió a otro Capitán que le facilitase un pendrive ya que tenía que obtener unos antecedentes. Obtenido el pendrive fue hasta su oficina y sin autorización accedió al computador personal de la Subteniente Vargas que ocupaba un escritorio al lado del suyo, pero que en ese momento no estaba en el lugar. Una vez que ingresó accedió a un archivo oculto y copió en el pendrive unas fotografías íntimas de la mencionada Subteniente. Acto seguido se reunió con el oficial que le había prestado el pendrive, y junto a otros tres oficiales fueron hasta la oficina del Capitán Soto Acuña en donde instaló en su computador el pendrive, procediendo todos a ver las fotografías. Posteriormente el dueño del pendrive, quien también ostentaba el grado de Capitán, en su domicilio particular colocó el mismo dispositivo extraíble en su computador personal y accedió a otro archivo oculto que tenía el nombre de "porno"; vio otras fotografías de la Subteniente en las cuales mantenía relaciones sexuales con su novio. Al día siguiente se reunieron los mismos oficiales y el Capitán dueño del pendrive, utilizando este dispositivo, mostró las nuevas fotografías. El día 12 de julio de 2007 una Oficial del mismo regimiento que tenía el grado de Teniente, informó acerca de las fotografías al Segundo Comandante de la Unidad luego de ingresar sin autorización a la oficina del Capitán dueño del pendrive donde copió en un pendrive las fotografías de la Subteniente para entregarlo a sus superiores jerárquicos.

- **Decisión del tribunal:**

Se rechazaron los recursos de casación en el fondo deducidos condenados Sebastián Campos Bustos y Sergio Valenzuela Cruz contra la sentencia de dos de mayo de dos mil doce.

- **Considerandos relevantes:**

SEXTO: Que desestimada la motivación anterior, corresponde el análisis de la causal 3ª que es común a los recursos de ambos condenados.

El artículo 4° de la Ley N° 19.223 sanciona al que maliciosamente revele o difunda los datos contenidos en un sistema de información.

Lo que se sanciona es el empleo de procedimientos dolosos destinados a afectar no sólo el sistema de tratamiento y almacenamiento de datos como erróneamente postulan las defensas, sino también difundir la información ilícitamente obtenida, de manera que sea conocida por terceras personas, lo que a su turno incrementa las posibilidades de que nuevamente sean utilizados y difundidos, como en la especie ocurrió. En el caso de autos quedó establecido que los sentenciados de un modo subrepticio o con un conocimiento no autorizado de la clave de acceso a un computador, vulneraron un software e información confidencial allí almacenada, la que se extrajo a través de un dispositivo externo de almacenamiento para efectos de exhibirse y difundirse a terceros.

En lo que respecta al bien jurídico, el legislador dispensa en este caso una protección penal especial entre otros, a los denominados datos sensibles o el llamado "núcleo duro" de la intimidad personal, entre los que se encuentran aquellos que recaen en la vida sexual de las personas, carácter que tenía la información a la que los sentenciados accedieron y compartieron con otros sujetos.

Así las cosas, en el caso de autos debe concluirse que al hacerse aplicación de la norma sancionatoria que se estima conculcada no se ha incurrido en infracción de ley, pues en la sentencia atacada han sido declarados aquellos hechos señalados en la disposición y que constituyen el acto típico, lo que hace que los recursos no puedan ser acogidos.

SÉPTIMO: Que la alegación de la defensa de Campos Bustos acerca de la falta de procesamiento respecto de la conducta de sustracción de datos no es atendible, pues la figura penal por la que ha sido condenado sanciona hechos diversos y no exige como condición previa

que sea el mismo agente quien acceda al sistema de almacenamiento de información que posteriormente se divulga.

Voto en contra Haroldo Brito: (…) acoger los recursos de casación en el fondo fundados en la causal 3ª del artículo 546 del Código de Procedimiento Penal, por estimar que el hecho de haberse copiado una información contenida en un registro computacional para, luego, mostrarla a terceros, no importa el ilícito del artículo 4° de la Ley N° 19.223, por cuanto del examen de su artículo 1° deriva que el bien jurídico protegido dice relación con la seguridad de los sistemas de información o sus partes, su funcionamiento, su indemnidad o el uso indebido de la información, lo cual no ha sido lesionado en modo alguno, en su entendimiento, el fallo impugnado incurre en la infracción de ley denunciada.

- **Tribunal:** Corte de Apelaciones de Concepción
- **Ministros:** María Leonor Sanhueza Ojeda, Camilo Álvarez Órdenes y Liliana Acuña Acuña
- **Fecha:** 30.01.2015
- **Rol:** 844-2014
- **Recurso:** Recurso de Nulidad
- **Tribunal de origen:** Tribunal de Juicio Oral en lo Penal de Los Ángeles, RUC 0810011797-6
- **Síntesis de los hechos:**

Que "Sandra Gouet San Martin, maliciosamente, y con el fin de evitar que los mecanismos de control de la empresa, a partir del sistema informático y contable, tomaran conocimiento de su autorización a las ventas de combustible a Jorge Barbieri Luarte, toda vez que estas excedían latamente el monto de crédito autorizado a este cliente, sucesiva y reiteradamente entre los meses de febrero de 2008 y mayo del mismo año, alteró los datos contenidos en el sistema de tratamiento de información de la empresa mediante el ingreso de información falsa, en orden a que los cheques del cliente habían sido pagados para luego anular ese falso ingreso de información, evitando así que fuera detectado el exceso de crédito que sin facultades para ello otorgó, de hecho, a favor de Jorge Barbieri Luarte".

En el razonamiento 25 concluyó que la conducta antes descrita es constitutiva del delito previsto y sancionado en el artículo 3 de la Ley 19.223, el cual se consumó toda vez que la alteración se efectuó en su totalidad en el sistema computacional.

- **Decisión del tribunal:**

Se rechazaron, los recursos de nulidad interpuestos por el abogado defensor de la inculpada Sandra Elizabeth Gouet San Martín y por el abogado de la víctima Sociedad Cruz y Cía Ltda.

- **Considerandos relevantes:**

5.- Que, son delitos informáticos 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 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. (Marcelo Huerta y Claudio Líbano, Delitos Informáticos)

Siguiendo la clasificación efectuada por los autores antes citados, la Ley 19.923 contempla dos figuras delictivas: I Sabotaje informático y II Espionaje Informático, las cuales se subdividen en categorías distintas atendiendo al objeto contra el cual se atenta y/o el modus operandi.

El sabotaje informático tiene tras manifestaciones que se consagran atendiendo el objeto que se afecta con la acción punible:

a) atentados contra un sistema de tratamiento de la información o de sus partes componentes; (art.1, primera parte)

b) atentados en contra del funcionamiento de un sistema de tratamiento de la información; (art.1 segunda parte)

c) atentado contra los datos contenidos en un sistema automatizado de tratamiento de la información. (art.3)

6.- Que el artículo 3 de la ley 19.223 dispone que: " El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigados con presidio menor en su grado medio".

La acción delictiva está destinada a alterar, destruir o dañar los datos contenidos en un sistema de tratamiento de información. Alterar los datos contenidos en un sistema sería, en consecuencia, alteraciones conductas como el ingreso o introducción de datos erróneos, el borrado de datos verdaderos, transformaciones o desfiguraciones de los datos, y en general toda conducta que implique cambiar la información contenida en un sistema de tratamiento de la

misma sin destruirla. Por lo tanto, lo afectado es el sentido, veracidad, claridad o pureza y alcance de la información contenida, la cual se verá afectada con conductas como las descritas.

7.- Que la sentencia recurrida en el motivo 8 se refiere al bien jurídico protegido señalando que "....este ilícito fue introducido por el cuerpo legal citado y, tal como se dejó constancia en sus diversos tramites legislativos, el bien jurídico a proteger por tal tipo penal es la calidad, pureza e idoneidad de la información, contenida en los sistemas automatizados de tratamiento de la misma, así como los productos provenientes de la operación de dichos sistemas. (Primer Trámite Constitucional, Moción Parlamentaria, Pág. 4; Primer Trámite Constitucional, Discusión en Sala, Pág. 38 y 47; Segundo Trámite Constitucional, Segundo Informe de Comisión de Constitución, Pág. 77)"

8.- Que tal como se señaló precedentemente, en la hipótesis del artículo 3° de la ley mencionada, el bien jurídico tutelado es el sentido, veracidad, claridad o pureza de la información. Así lo señalan los autores Rodrigo Medina Jara, en su artículo Los delitos Informáticos en la Legislación Chilena, publicado en Revista Electrónica de Derecho Informático, N°44, marzo 2002; los autores Marcelo Huerta y Claudio Líbano, en su obra Delitos Informáticos, Editorial Jurídica; Alejandro Vera Quilodrán en Delito e Informática, etc.

En el caso sub litis puede decirse, propiamente, que el bien jurídicamente protegido es colectivo y se traduce en la información como valor económico de la actividad de la empresa. Distinto ocurre en el fraude informático, en que el verdadero bien a cautelar es el patrimonio, ya que el interés general en el adecuado funcionamiento del tratamiento electrónico de datos, de creciente importancia para la economía y la administración, resulta protegido sólo en forma refleja. (Nelson Pozo Silva, La tecno-estafa o la estafa informática, Gaceta Jurídica N°245, pág.10 y ss.)

9.- Que, por las razones expresadas en los motivos precedentes resulta evidente que la sentencia ha hecho un correcto razonamiento de los hechos establecidos y acreditados en el proceso, que conduce, lógicamente, a la decisión de condena de la imputada, de la manera como se hizo, no vislumbrándose la errónea aplicación del derecho que hubiere influido sustancialmente en lo dispositivo del fallo.

19.- Que del mérito de los antecedentes se desprende con claridad que las conductas desplegadas por la acusada Sandra Gouet San Martín, tuvieron un solo propósito, cual fue lograr que el sistema computacional no registrara que el cliente Jorge Barbieri Luarte excedía el crédito otorgado por la empresa ($3.000.000) y así poder efectuarle otras ventas de combustible. Como se acreditó en el juicio, consignaba como pagados o depositados cheques que recibía de Barbieri, en circunstancias que eran a fecha y no eran depositados en ese momento, para luego anular el ingreso de esa información.

Al prestar declaración en estrados señaló que fingía el depósito y luego lo anulaba, lo que permitía, según lo expresa, aumentar por una parte el crédito del cliente y por otra, darle tiempo para pagar los documentos. (considerando 6°). De este modo posibilitó que las ventas no autorizadas superaran los $80.000.000.- pesos.

20.- Que por las razones esgrimidas, estima esta Corte que el fallo impugnado por vía de nulidad, no ha incurrido en la causal del artículo 373 letra b) del cuerpo legal antes citado, pues existió por parte de la sentenciada una unidad de acción, porque cada una de las acciones que realizó, considerada independientemente, cumplen con las condiciones necesarias para tipificar el delito, pero en conjunto constituyen uno solo, porque se encuentran ideológicamente conectadas, media una relación especial entre ellas, ejecutadas con un propósito unitario, como se señaló.

- **Tribunal:** 3° Tribunal de Juicio Oral en lo Penal de Santiago
- **Magistrado(s):** Rodrigo Carrasco Mez, Verónica Sabaj Escudero e Isabel Mallada Costa
- **Fecha:** 19.06.2012
- **RUC:** 1000464726-8
- **RIT:** 24-2012
- **Procedimiento:** Ordinario
- **Síntesis de los hechos:**

El día 14 de mayo de 2010, aproximadamente a las 21:00 horas, el médico cirujano ALAN ENRIQUE HERNÁNDEZ CANALES, quien se desempeñaba como radiólogo en el Servicio de Imagenología del Hospital de Carabineros, ubicado en Simón Bolívar 2.200, comuna de Ñuñoa, informó el examen que había sido tomado horas antes, denominado Angio TAC de tórax de la paciente Bárbara Anahí Velásquez Caro, la que se encontraba internada desde el día anterior en dicho recinto asistencial con el diagnóstico de tromboembolismo pulmonar (TEP). Dicho examen había sido ordenado por el médico tratante de la paciente para confirmar el diagnóstico clínico de TEP, estando en conocimiento de esa circunstancia Hernández Canales. Pues bien, en el referido informe radiológico el Dr. Hernández Canales concluyó: 'Grandes vasos de calibres normales y permeables. Arteria pulmonar de calibre normal, permeable, así como sus ramas principales derecha e izquierda, ramas lobares, segmentarias y subsegmentarias visualizadas. No se identifican defectos de llenamiento compatibles con fenómenos trombóticos. No hay adenopatías. Tráquea y bronquios fuente de calibre normal y permeables. Corazón de morfología y tamaño normal. Pleura y pericardio libre. Parénquimas pulmonares de arquitectura conservada sin imágenes de significado patológico. Impresión diagnóstica: 'No hay hallazgos compatibles con TEP'. Este informe fue dictado y luego archivado por el acusado en la carpeta digital denominada como 'DEFINITIVO', en el sistema computacional utilizado para estos efectos en el Hospital de Carabineros llamado RISC por sus siglas en inglés de Radiologhy Informatic System, utilizando su clave personal para la realización de estos movimientos en el sistema computacional.

Con fecha 22 de mayo de 2010, la paciente Bárbara Velásquez Caro falleció a consecuencia de un 'tromboembolismo pulmonar masivo' en el mismo hospital, sin haber recibido tratamiento alguno para la patología presentada, la que había sido descartada.

Con posterioridad, los días 29 de mayo de 2010 y 14 de noviembre de 2010, Hernández Canales utilizando su clave personal ingresó a la carpeta digital denominada 'DEFINITIVO', existente en el sistema RISC del Informe del Angio TAC de tórax de la paciente, ya referido, y modificó el contenido de dicho informe en el siguiente sentido: 'Grandes vasos de calibres normales y permeables. Arteria pulmonar de calibre normal, permeable así como sus ramas principales derecha e izquierda, ramas lobares, segmentarias y subsegmentarias visualizadas. No se identifican defectos de llenamiento categóricos que comprometan significativamente el lumen de vasos visualizados compatibles con fenómenos trombóticos. Es necesario revaluar según su evolutividad. No hay adenopatías. Traquea y bronquios fuente de calibre normal y permeables. Corazón de morfología y tamaño normal. Pleura y pericardio libre. Parénquimas pulmonares de arquitectura conservada tenues imágenes nodulares subpleurales en ambas bases de aspecto inespecífico, que sería puede correlacionar comparando con exámenes previos y controlar según evolución clínica. Impresión diagnóstica: No hay hallazgos categóricos compatibles con TEP. Se sugiere controlar y revaluar según evolución clínica. Tenues imágenes nodulares subpleurales de aspecto inespecífico que se sugiere controlar". .

- **Decisión del tribunal:**

Se decidió condenar a Alan Enrique Hernández Canales en calidad de autor-ejecutor en los términos del artículo 15 N° 1 del Código Penal del Cuasidelito de homicidio de Bárbara Velásquez. Y además, condenarlo en calidad de autor por el delito Informático que preceptúa y sanciona el artículo 3° de la Ley N° 19.223, en etapa de ejecución consumado.

- **Considerandos relevantes:** a

Vigesimoséptimo: 2 °.-) Imputación en relación al delito previsto en el artículo 3° de la Ley N° 19.223: Que, por otra parte, tanto el Ministerio Público como la parte Querellante emplazaron individualmente a este juicio a don ALAN ENRIQUE HERNÁNDEZ CANALES, por el delito Informático contenido en el artículo 3° de la Ley 19.223, que sanciona entre otras hipótesis a quien "altere los datos contenidos en un sistema de tratamiento de información". Que, atingente

a dicho requerimiento punitivo se tuvo presente fundamentalmente, el mérito de las probanzas rendidas en juicio, a saber, documental, específicamente dos informes imagenólogicos de Angio TAC de tórax cuyos resultados son disímiles, toda vez que el primero en lo sustancial indicó como impresión diagnóstica "No hay hallazgos compatibles con TEP"; lo anterior sin firma digital del médico que lo expidió, en tanto que el segundo señaló a su vez "No hay hallazgos categóricos compatibles con TEP. Se sugiere controlar y revaluar según evolución clínica. Tenues imágenes nodulares subpleurales de aspecto inespecífico que se sugiere controlar", con dicha rúbrica digital. En este sentido, a través de la prueba testimonial y pericial aportada al juicio, se pudo acreditar acorde con lo expuesto por el tecnólogo médico Jaime Edmundo Ayala Martínez, quien ejerce labores de Coordinador del Sistema Computacional de Radiología - RISC - del Hospital de Carabineros, en qué consistía dicho sistema y cómo funcionaba al interior del citado centro de salud, detallando in extenso cada fase de operatividad del aquél en los términos que latamente fueron expuestos en el razonamiento decimoquinto de este fallo, atingente a la declaración de este testigo, lo cual fue confirmado en lo esencial con el relato que a su vez brindaron las enfermeras universitarias Leyton Domínguez y Mahfud Muñoz, quienes coincidieron con éste acerca de dicho funcionamiento. Es así, que los tres fueron contestes en señalar que en cada Servicio de dicho Hospital existe un punto computacional con impresora en pantalla desde el cual el personal de salud que labora al interior del mismo, pueden ver los procedimientos que se hacen en Imagenología a raíz de los exámenes ordenados por los médicos respecto de algún paciente en específico, una vez que se encuentran finiquitados y puestos en la carpeta de "DEFINITIVO", a través de otro sistema que se denomina SYNAPSE, en el cual se pueden apreciar las imágenes y la correspondiente impresión diagnóstica, pudiendo ser imprimidos en cada estación de enfermería, al ser requerida dicha información, siempre y cuando aquéllos se encuentren en el estado de "DEFINITIVOS", sin necesidad de recurrir al Servicio de Radiología. Al respecto Ayala Martínez fue categórico en señalar, que desde que se instaló un sistema digital en el Servicio de Imagenología del HOSCAR - finales del año 2009, mes de diciembre - a través de la red o servidor, el resto del Hospital únicamente podía acceder como visualizadores de los procedimientos que se efectuaban en Imagenología, vale decir, el sistema estaba destinado para que en su unidad se pudiesen realizar todos los procesos imagenológicos, los que pueden estar guardados en carpetas digitales, pero el Hospital en sí, solamente podía acceder a revisar imágenes e informes que estuviesen en la carpeta de

"DEFINITIVOS", según quedó dicho en el párrafo anterior, especificando que cualquier examen o informe que quedara inconcluso o en estado de revisión o estuviese para transcripción, de modo alguno podía estar disponible para el resto de los profesionales que quisieran visualizar tal examen dentro del Hospital. Precisó en otras palabras que podía suceder que un examen realizado en Imagenología no se terminara de la forma que correspondía; que en dicha situación quedaba "trabado" el sistema, no llegando a las carpetas médicas, no llegando las imágenes correspondientes, no llegando las carpetas para informe etc; que el proceso normal implicaba ingresar claves; que se tienen que terminar órdenes de trabajo, escanear órdenes, asociar profesionales y una serie de pasos, las que de no cumplirse el examen estaba disponible como imagen no más, pero no estaba dirigido a las carpetas médicas para que pudiesen realizarse tales informes. Asimismo, quedó sentado a través del testimonio de este deponente y del médico Jaime Edgardo Cotroneo Escobar, que el citado sistema digital de rayos se denomina "RISC", que son las siglas en inglés de "Radiologhy Informatic System" y, está asociado a un sistema de visualización de imágenes que se llama "PACS". De otro lado y en relación a las objeciones planteadas por la Defensa de HERNÁNDEZ CANALES, en orden a que el primer informe no presentaba firma digital en tanto que el segundo si la tenía, quedó claro en el devenir de todas estas probanzas y por los testimonios antes indicados, a los que se sumaron los dichos de los co-acusados DEL VALLE, MONCADA, MARINCOVIC y el resto de los facultativos que laboraba al interior de dicho Hospital y que fueron citados como testigos ante estrados, entre otros, la interna Cavada, los doctores Cotroneo y Huerta, que tal circunstancia carecía de toda relevancia, toda vez que los reportes que venían sin firma eran intra sistema, ello con la finalidad de obtener prontamente el resultado de algún examen en concreto; en tanto que aquéllos que presentaban firma digital, correspondían a los pacientes extra sistema cuando éstos los requerían y obtenían directamente desde el Servicio o de la Unidad de Radiología del Hospital con la finalidad de llevárselos materialmente. Por lo demás, en todas las evaluaciones y exámenes físicos que se realizaron a la paciente por distintos médicos y enfermeras universitarias que la atendieron dentro del establecimiento de salud en cuestión, al momento de dejar constancia de su intervención profesional, sea en la ficha clínica o en la hoja HOCLIA CAR, la negatividad del informe de Angio TAC de tórax siempre quedaba consignada dentro de sus anotaciones bajo la expresión TEP (-), lo que ratifica aún más que era el primer informe y no otro el emitido de manera original. Con todo, es dable tener presente que el acusado HERNÁNDEZ y su propia

Defensa reconocieron como válido el informe de Eco Doppler venoso de extremidades inferiores de Bárbara Velásquez Caro, de fecha 14 de mayo de 2010, el que se condice en términos formales con el de Angio TAC de tórax, atendido que de igual forma aparece sin firma y en el estado de "correction". En este orden de ideas, ambos informes de los exámenes imagenológicos guardaron el mismo formato, lo que permite otorgarle mayor fuerza al hecho que la primitiva interpretación del Angio TAC de tórax fue aquélla en que se descartaba de manera categórica el TEP. A su vez, en virtud de los registros históricos existentes en el HOSCAR y particularmente en lo referente al examen de Angio TAC de tórax practicado a la joven Bárbara Anahí Velásquez Caro, el Tribunal obtuvo ilustración suficiente, concatenado a los dichos del mencionado testigo Ayala Martínez en correspondencia con lo expuesto por el Sub-comisario de la Policía de Investigaciones de Chile Mauricio Díaz Albornoz, en cuanto a la razones de la dualidad de existir ambos informes, a raíz de la investigación que se hizo como parte del sumario interno que se llevó por el propio Hospital y que arrojó como resultado la intervención dentro de dicho sistema de parte del acusado HERNÁNDEZ CANALES, situación que acaeció pocos días después del fallecimiento de la víctima, lo cual, por lo demás se vio complementado con los propios dichos de HERNÁNDEZ CANALES, quien además reconoció en estrados que para tales efectos contaba con una clave personal e intransferible que se le había entregado por el propio Servicio, reconociendo por lo demás que dicha clave personal nunca se la reveló a ninguna persona, aunado a la circunstancia que de acuerdo al citado registro histórico, quedó acreditado de la misma manera que el doctor HERNÁNDEZ ingresó al referido sistema informático y modificó mediante dictado de voz, el contenido del citado informe, una vez producida la muerte en referencia, indicio que dejó en evidencia el dolo o faz subjetiva con que aquél actuó en cuanto a la configuración del tipo penal en cuestión, previsto en el artículo 3° de la Ley N° 19.223, en su verbo rector "alterar" de manera maliciosa los datos contenidos en un sistema de tratamiento de información. En este orden de ideas, adquirió relevancia también lo expuesto por el doctor Cotroneo Escobar, quien aportó por su lado, que luego de enterarse del fallecimiento de la paciente Bárbara Velásquez, acaecido el día 22 de mayo de 2010, en virtud de una reunión que mantuvo con la Subdirectora médica del Hospital, así como de todo el procedimiento policial que sobrevino a continuación, supo durante la semana que siguió a la muerte de ésta, que dentro del período de estadía hospitalaria de la misma había intervenido en el manejo de dicha enferma el Servicio de Apoyo Diagnóstico y Terapéutico a su cargo,

concretamente a través de la realización de los mentados exámenes de Angio TAC de tórax y Eco Doppler venoso de extremidades inferiores y, que el facultativo a cargo de tales exámenes fue el doctor ALAN HERNÁNDEZ CANALES, razones por las cuales conversó con éste el día 26 de mayo de 2010, solicitándole la revisión de las imágenes aludidas debido a la ocurrencia de la defunción de la citada paciente, diálogo que a su vez corroboró el acusado HERNÁNDEZ al momento de declarar ante la audiencia, especificando por otra parte el doctor Cotroneo que por su lado personalmente efectuó una lectura del informe de Angio TAC de tórax evacuado por HERNÁNDEZ, donde aparecía como resultado que "No habían hallazgos compatibles con TEP", de lo cual se colige que existió un lapso de tiempo casi inmediato entre la intervención que hizo el encartado HERNÁNDEZ al aludido sistema computacional con el diálogo que mantuvo con su colega y superior jerárquico Cotroneo, toda vez que a través del este último tomó cabal conocimiento de la muerte de la citada joven, así como de la magnitud de su error en cuanto al resultado que consignó en su primitivo informe, situación que lógicamente lleva a estos Jueces adquirir convicción de que el mentado HERNÁNDEZ viéndose enfrentado a tal panorama de sucesos, se sintió constreñido ante tal acontecimiento e intervino el referido sistema computacional, concretamente tres días después, de enterarse de las consecuencias acarreadas por su equivocación, ingresando así al sistema, esto es, específicamente el día 29 de mayo de 2010. A lo anterior, cabe agregar que el doctor Cotroneo indicó además que en el mes de marzo de 2011 y en circunstancias que estaba haciendo uso de su permiso administrativo, recibió un llamado del Director del Hospital, quien le preguntó si sabía que había dos informes, respondiéndole que sólo conocía de uno de ellos, ante lo cual dicho Director le replicó que él tenía a la vista dos informes y le solicitó que revisara el sistema. Fue así que alrededor de las 14:00 horas, concurrió a la Unidad de Imagenología donde se contactó con el Coordinador del sistema RISC-PACS, don Jaime Ayala, fueron a la parte informe Angio TAC pulmonar de la paciente Velásquez Caro, percatándose que existían diferencias con el que originalmente Cotroneo había tenido a la vista, esto es, con antelación y a propósito de la Auditoría interna del Hospital, documento que por lo demás le fue exhibido por la Fiscal al inicio de su declaración en estrados reconociéndolo sin mayor titubeo. Puntualizó que al analizar este segundo informe advirtió que las diferencias más bien establecían evaluaciones que debían ser adjuntadas a nivel clínico; que el nuevo informe no era tan categórico en cuanto a descartar TEP y sugería evaluar la conclusión en base a otros antecedentes clínicos que el radiólogo no tenía en ese momento.

Refrendó luego sus dichos, al serle exhibida la prueba documental N° 16 aportada tanto por la Fiscalía como por el Querellante, correspondiente a un segundo informe de Angio TAC de tórax de la paciente Bárbara Velásquez Caro, en el que se señala como impresión diagnóstica: "No existen hallazgos compatibles con TEP. Se sugiere controlar y reevaluar según evolución clínica. Tenues imágenes nodulares, subpleurales, de aspecto inespecífico que se sugiere controlar". Este informe aparece igualmente suscrito por el reseñado doctor HERNÁNDEZ y firmado de manera impresa sobre la individualización del anterior. Agregó Cotroneo Escobar que en razón de lo anterior, le solicitó al señor Ayala, que verificara en su computador de control el "historial", a fin de determinar las intervenciones que había tenido el mentado examen de Angio TAC de tórax, quien a continuación le manifestó que revisó desde su computador de control percatándose que una vez que el examen fue informado, quedó en el carácter de "DEFINITIVO" a "REVISIÓN" durante cinco minutos, dentro de una fecha mayo de 2010, siendo devuelto a "DEFINITIVO". En este este aspecto puntual ratificó además lo señalado por Ayala, al afirmar que si el examen se encuentra en estado de "REVISIÓN" al interior de la unidad de Imageología no puede ser visto fuera de ella. Detalló también que en el estado de "REVISIÓN" se pueden modificar el contenido de los informes. Asimismo resaltó que en el mes de noviembre de 2010, nuevamente fue pasado a "REVISIÓN" para posteriormente dejarlo a "DEFINITIVO", dentro del lapso de cinco minutos; que una vez que confirmó dicha situación consultó con el doctor HERNÁNDEZ, quien le negó toda intervención en relación a tal ingreso. Profundizando respecto de lo señalado anteriormente re sultó útil recordar que Ayala Martínez explicó latamente en audiencia que si se realizaba un informe y se mandaba a "DEFINITIVO", y posteriormente al informe se entregaban nuevos antecedentes que no se tuvieron a la vista al momento de realizar dicho informe, se podía acceder a la carpeta que estaba en estado de "DEFINITIVO", sacarlo y mandarlo a otra carpeta, vale decir, que se podía intervenir, correspondiendo a la carpeta de "REVISIÓN", verificar seguidamente las modificaciones consideradas relevantes en relación a los antecedentes nuevos y posteriormente mandarlas nuevamente a "DEFINITIVO"; que en este ejemplo, lo que se tenía era un informe modificado que iba a ser el mismo que se va a representar en el Sistema PACS; que las modificaciones o las intervenciones que se hicieron en el sistema quedaban borradas y salía sólo lo que se modificó. Recalcó asimismo que todos los funcionarios de Imagenología poseían claves personales, con distinto perfil, de acuerdo a sus responsabilidades labores y procedimientos a efectuar, a saber,

los tecnólogos médicos, paramédicos y finalmente los médicos todo ello de acuerdo a su especialidad, que les fueron entregadas al principio de la instauración del sistema; además de un número interno con el cual podía identificarse cada uno de ellos; que en la especie pudo inferir que la clave con la que se ingresó a la carpeta para realizar la modificación en comento, era la del doctor HERNÁNDEZ, ya que al acceder al sistema RISC, éste abre el perfil de la clave que se ingresó. De este modo, si se ingresó la clave del doctor HERNÁNDEZ se abre su perfil, su reconocimiento de voz, las plantillas que pudiese tener archivadas y la firma digital previamente registrada por el citado doctor.

Aclaró que los registros aludidos están cuando se realiza un informe en el sistema de dictado, el sistema guarda un registro de voz y un registro escrito, de lo que se informó, si una persona interviene el informe y modifica algo del informe va a quedar lo que se modificó, pero lo que se reemplazó no se guarda sino solamente lo que se modificó. Por tanto, si no se tiene lo primero difícilmente se va a saber que hay una modificación viendo el informe, pero cada vez que se ingresa al sistema y cambia un archivo de carpetas a otra carpeta que permite modificar queda registrada la clave de quien ingresó, el día y la hora. Procedió a continuación este testigo a describir tal como quedó señalado en el mencionado apartado decimoquinto del fallo todo el proceso en cuestión, lo quese da por integrante reproducido, sin perjuicio de lo cual vale nuevamente recordar que precisó que existían seis carpetas, la primera para grabación, la segunda para tipeo, la tercera para revisión, la cuarta para definitivo, la quinta entregado y la sexta sin informe. Añadió que particularmente el día 14 de mayo de 2010 en dicho registro se indica el código 428 de HERNÁNDEZ CANALES ALAN, el 14 de mayo de 2010, a las 20:59:14 de la consola RISC dictado, toma un examen y lo envía a DEFINITIVO. Seguidamente, el mismo código 428 que corresponde a HERNÁNDEZ CANALES ALAN, toma la carpeta que está en DEFINITIVO, lo envía a la carpeta de REVISIÓN, el día 29 de mayo de 2010 a las 17:18:41 horas y la manda posteriormente a DEFINITIVO, código 428, el mismo día 29 de mayo de 2010 a las 17:25:12 horas. A continuación nuevamente el código 428 de HERNÁNDEZ CANALES ALAN, el día 14 de noviembre de 2010 a las 20:11:23 horas de la consola RISC dictado toma la carpeta nuevamente que está en DEFINITIVO y la manda a REVISIÓN. El siguiente registro indica que el mismo código 428 - HERNÁNDEZ CANALES ALAN - mandó la carpeta a DEFINITIVO el día 14 de noviembre de 2010 a las 20:13:27 horas.

De este modo, en el entender de estos Juzgadores quedó plasmado objetivamente en un registro computacional histórico, cada intervención que con su código hizo el acusado HERNÁNDEZ en dicho sistema. Añadio Ayala Martínez, que en dicho documento en el campo de paciente se lee: VELAS - CA – BAR, lo cual para el Tribunal equivale lógica y únivocamente acorde al enlace armonico de con todos los antecedentes probatorios que se han ido detallando a lo largo del juicio, al nombre de la occisa Bárbara Velásquez Caro. Asimismo quedó objetivado también que desde las 17:18:41 horas del día 29 de mayo de 2010 hasta las 17:25:12 del mismo día el informe en cuestión estuvo ese rango de tiempo en "REVISIÓN". Conjuntamente, lo anterior se vio complementado con Prueba Nueva cuya incorporación legal a la causa fue accedida por este Tribunal por cumplirse los presupuestos exigidos en artículo 336 inciso primero del Código Procesal Penal, consistente en el Registro de Audio grabado sistema WAP del informe de Angio TAC de Tórax, de fecha 14 de mayo de 2010, conforme el cual estos sentenciadores junto con oír ante la audiencia una voz que Ayala Martínez identificó como perteneciente al doctor HERNÁNDEZ CANALES y que se condice por lo demás con el registro de su voz que quedó en la carpeta digital del Tribunal en el momento que brindó su declaración voluntaria ante estrados, lo cual fue percibido por estos sentenciadores a través de sus propios sentidos.

Finalmente, todos estos antecedentes probatorios se vieron refrendados a mayor abundamiento con la posterior incautación y fijación digital que de la Ficha clínica realizó la Policía de Investigaciones de Chile, el mismo día y a pocas horas del fallecimiento de la paciente Velásquez Caro, donde únicamente dentro del archivo de las hojas pertinentes tan sólo aparecía el informe que señalaba en su impresión diagnóstica "No hay hallazgos compatibles con TEP". Para terminar, es menester señalar que, si bien, quedó suficientemente demostrado en el desarrollo de este juicio el acusado HERNÁNDEZ CANALES, luego de emitir el informe original en los términos que han quedado dichos, ingresó en dos ocasiones más al sistema RISC del Servicio de Imagenología donde prestaba sus servicios, a saber, el día 29 de mayo y muy posteriormente el 14 de noviembre del año 2010, únicamente fue en la primera fecha -29 de mayo- que ejecutó la conducta típica que sanciona la norma jurídica que se trajo a nuestro estudio, bajo el presupuesto de "alterar" los datos originales del sistema informático en mención, desde que acorde las mismas probanzas se pudo establecer que en la segunda oportunidad

únicamente su afán fue visualizarla sin realizar modificación alguna, razones por las cuales en definitiva el reproche y sanción que se le impondrá será por un sólo hecho.

- **Tribunal:** 4° Tribunal de Juicio Oral en lo Penal de Santiago
- **Magistrado(s):** Graciela Gómez Quitral, José Flores Ramírez y Cristián Soto Galdámes
- **Fecha:** 08.06.2011
- **RUC:** 1000626117-0
- **RIT:** 21-2011
- **Procedimiento:** Ordinario
- **Síntesis de los hechos:**

Hecho uno: El 15 de mayo del año 2007, el funcionario de la BIRO Metropolitana de la Policía de Investigaciones de Chile, Inspector Manuel Donoso Cáceres, en dos oportunidades realizó búsquedas en la base de datos del sistema informático GEPOL, para revelar a Margarita Cuadros, las órdenes de detención y arraigo que mantenía Roberto Patricio Flores Moran.

Hecho dos: El 15 de mayo de 2007, el funcionario de la BIRO Metropolitana de la Policía de Investigaciones de Chile, Inspector Manuel Donoso Cáceres, en dos oportunidades realizó búsquedas en la base de datos del sistema informático GEPOL, para revelar a Margarita Cuadros Aedo la información sobre órdenes de aprehensión y arraigo que mantenía Ariel Eduardo Morales Duque.

- **Decisión del tribunal:**

Se condenó a el acusado Manuel Alejandro Donoso Cáceres, funcionario público e ya que los hechos constituyen dos delitos de revelaciones ilícitas, figura típica contemplada en el artículo 4° de la ley N° 19.223, en grado de consumado, por los que deberá responder a título de autor ejecutor, según el artículo 15 N° 1.

Que se le absolvió de los cargos a Margarita Elena Cuadros Aedo como autora de falsificación de instrumento público, obstrucción a la investigación, revelación y sabotaje informático y como partícipe de una asociación ilícita.

- **Considerandos relevantes:** a

Décimo segundo: Absoluciones en beneficio de Margarita Cuadros Aedo.

Que este tribunal tomó la decisión de absolver a Cuadros Aedo en una serie de cargos formulados por los acusadores, en primer término respecto de los delitos de falsificación aludidos en el razonamiento anterior.

El motivo de tal decisión radica en la convicción que la conducta dolosa de Margarita Cuadros se agotó –como se dijo precedentemente- en la solicitud de cada acto en particular, por lo que su aporte respecto de los datos de cada cliente captado para que se forjaran los documentos públicos falsos, solo constituye la actividad propia que es reprochada por la vía del cohecho, y que agota la configuración del mismo. En efecto, la aludida Cuadros Aedo, de acuerdo a la prueba rendida, siempre estuvo lejos de la ejecución material de las falsificaciones y la imputación de autoría mediata o cooperativa, que de acuerdo a los cargos formulados, en opinión del Ministerio Público, permitiría atribuirle además la responsabilidad por las aludidas falsificaciones no resulta satisfactoria para solucionar el problema de su participación en estos actos, sin incurrir en la prohibida doble incriminación.

En cuanto a la absolución por los cargos por el delito de sustracción de expedientes, el tribunal consideró que no existió prueba contundente acerca de la participación Margarita Cuadros en tal hecho, lo que justificaría una condena en una calidad similar a la de Elizondo Uribe. Así, en la especie no se rindió ninguna prueba que revista el carácter de imputación directa verosímil en su contra que la vincule con este hecho, salvo el dicho de Uberlinda Elizondo, que da cuenta de su supuesta participación, en circunstancias que el resto de las probanzas unívocamente afirman un fuerte vínculo entre la actuaria Elizondo Uribe y el "beneficiado por el extravío", el denunciado Cristian Barriga Barriga, lo que relativiza negativamente sus dichos en contra de Margarita Cuadros.

Refuerza esta convicción, lo referido e incorporado en la audiencia relativo a la causa administrativa instruida por el Sr. Ministro Mario Carroza Espinosa, de acuerdo a la cual en tal investigación se acreditó la responsabilidad disciplinaria de una funcionaria judicial encargada de resguardar tales documentos.

Por otra parte, los demás antecedentes genéricos incorporados, como el video aportado como otro medio de prueba consistente en una conversación entre Gloria Navarrete, su madre y Margarita Cuadros, en un restorán de esta ciudad -imágenes registradas por el Departamento

OS 9 de Carabineros de Chile- tampoco son concluyentes. En efecto, dicho medio de prueba ha sido traído a colación en este punto por el Ministerio Público y la parte querellante a propósito de las expresiones de Cuadros: "La Joaqui anda urgida por el asunto del expediente… me llama a cada rato.", asertos que pueden perfectamente decir relación con el mero relato de la natural aflicción de la funcionaria investigada por la pérdida del proceso. Y tampoco lo son las escuchas telefónicas en las que Margarita Cuadros Aedo menciona la quema de un expediente a los ojos del cliente, ya que ellos no se pueden conectar inequívocamente con el cargo puntual levantado por los acusadores, como lo es la sustracción y ocultamiento de la causa instruida en contra de Barriga Barriga, ya que el referido expediente no fue quemado ni destruido, sino que fue encontrado íntegro en el domicilio de Elizondo.

En cuanto a las imputaciones de participación en los delitos "informáticos" de revelaciones ilícitas y sabotaje, cabe señalar que el tribunal no pudo determinar responsabilidad de Margarita Cuadros Aedo, al considerar, por una parte, la historia del establecimiento de la ley 19.223, de acuerdo a la cual aparece que la incorporación de su actual artículo 4° fue producto de una idea sugerida por la Asociación Chilena de Empresas de Informática A.G., que buscaba sancionar una conducta que no estaba definida en el proyecto original, pero que guardaba estrecha relación con la idea matriz del mismo, como lo era la revelación o transmisión maliciosa de los datos contenidos en un sistema de información. Indica el informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, que en tal delito pueden incurrir principalmente quienes trabajan en el sistema, ya que los terceros ajenos a él necesariamente deberán cometer el de apropiación indebida de los datos. De esta manera, resulta evidente que los destinatarios de la conminación penal son los operadores del sistema, esto es, las personas que manejaban o accedían a esta fuente como custodios, posición que nunca ostentó la acusada Cuadros Aedo.

La conclusión precedente guarda coherencia con los principios que inspiraron la dictación de la señalada ley, los que de acuerdo a los informes de la misma comisión citada precedentemente, apuntan a dar protección jurídica a la calidad, pureza e idoneidad de la información contenida en los sistemas para el tratamiento automatizado de la misma, así como de los productos provenientes de la operación de dichos sistemas.

Los dos casos de este tipo que logró acreditar la fiscalía, relativos al funcionario público que accedió a esta base de datos reservada, Manuel Donoso Cáceres, da cuenta que éste, no recibió pago por la entrega de esta información. Así, si en los mismos acontecimientos hubiera mediado una recompensa económica, estaríamos en el escenario jurídico de atribuir a Cuadros Aedo otro delito de cohecho, pero tal cuestión ni se probó, ni tampoco está contenida en los hechos de la acusación.

Lo mismo puede predicarse respecto de la revelación de los datos contenidos en el sistema informático GEPOL de: Juan Gabriel Abarca Moya, Juan Marcelo Villaseca Orellana, Daniel Hernán Albornoz Iturra, Cristian Hernán Barriga Barriga, Juan Darío Scanu Hermosilla, Alfonso Patricio Vásquez Parker, Patricio Salame Morales, Cristian Gonzalo Jiménez Tapia y Juan García Lillo. Cuadros Aedo no era titular de la obligación de reserva ni de custodia de la referida información y la imputación a título de otras formas de autoría no elude la objeción primordial de no ser ella titular del deber que justifica la protección penal de las señaladas bases de datos que contienen la información que se pretende reservar.

En cuanto a las conductas imputadas a Margarita Cuadros Aedo, por el delito de sabotaje informático del artículo 3° de la misma ley N°19.223, respecto de los datos contenidos en la base de datos del sistema GEPOL, de: Gonzalo Cristian Lecaros Piffre, Roberto Patricio Flores Moran, Luis Acosta Valdivia, Manuel Fernando Berrios Fernández, Juan Francisco Cortes Gutiérrez, Ricardo Agustín Lopresti Guilardi y Rodrigo Sebastián Muñoz Zúñiga, estos sentenciadores concluyeron que no es posible atribuir responsabilidad a la citada acusada, por cuanto no se acreditó su participación en los mentados ilícitos, ya que los medios de prueba rendidos no permitieron adquirir convicción más allá de toda duda razonable sobre tal extremo.

Así, tenemos que el Ministerio Público innominadamente indicó que el saboteador era un funcionario de la BICRIM de la ciudad de Calama y que la investigación interna de la que dieron cuenta los funcionarios de la Policía de Investigaciones de Chile Ricardo Pavez Rojas y Marcel Infante Mercado, no pudo determinar desde qué punto se accedía al sistema y qué persona modificaba los datos de GEPOL, cuestión ratificada posteriormente por la auditoría realizada a dicho sistema por el perito Richard Rubilar Reyes.

Las referencias que Margarita Cuadros habría hecho a las coimputadas sobre los "cabros del norte" o la posibilidad de realizar borrones, no alcanzan para determinar la identidad del saboteador, ni la forma en la que habría operado tal ilícito y cómo la aludida acusada participaba. Elaborar a partir de estos dichos y de la evidencia informática –que tampoco arroja luces sobre la identidad del ejecutor- una hipótesis positiva para los acusadores, máxime en calidad de autoría, excede los límites que tiene nuestro sistema probatorio que, si bien determina libertad de medios y valoración de acuerdo a lo que la doctrina denomina sana crítica, no permite asentar responsabilidad de carácter penal, sin determinar previamente la forma de comisión del hecho, en sus diversas aristas, y las modalidades de intervención de los partícipes, aspectos todos que se echan en falta en este caso, y que impiden formar convicción condenatoria a su respecto.

Por lo demás, la ponderación de los elementos aportados al juicio, conforme a la sana crítica, permite al tribunal consolidar su duda razonable asentada en la siguiente cuestión: Si la acusada Margarita Cuadros tenía semejante contacto con el saboteador del sistema informático, no se acierta a entender la necesidad que le asistía de chequear previa y posteriormente las presuntas eliminaciones de datos con funcionarios dotados de claves de acceso al sistema más básicas, ya que la posesión de semejante herramienta descarta la necesidad de mantener a todas las otras, las que solo dejarían rastros que evidenciarían su intervención. De lo anterior se sigue que el tribunal atisba que los hechos son más complejos que los atribuidos por la fiscalía, y no permiten atribuirle en este estado de cosas, participación en calidad de autora en el mencionado sabotaje.

En cuanto a los cargos por el delito de asociación ilícita, estos se acordarán en el siguiente considerando.

- **Tribunal:** Tribunal de Juicio Oral en lo Penal de La Serena
- **Magistrado(s):** Iván Corona Albornoz, Nury Benavidez Retamal y Lilian Tapia Carvajal
- **Fecha:** 22.03.2012
- **RUC:** 0910021731-4
- **RIT:** 185-2012
- **Procedimiento:** Ordinario
- **Síntesis de los hechos:**

En fechas y horas no precisadas durante el mes de enero de 2008, comprendidas entre el día 11 al día 30 de dicho mes, en Avenida Francisco de Aguirre, La Serena, en el interior del Supermercado Líder, se efectuaron 13 transacciones asociadas a 46 "pines", códigos de recarga, por un monto en recarga de 720.000 pesos, en la caja donde se desempeñaba la acusada Patricia Alejandra Valera Guerra, dicha generación de pines no quedaba registrada en las boletas respectivas a consecuencia de pasar el cartón de recarga por el escáner, luego de presionar las teclas "6, 4 y conex".

- **Decisión del tribunal:**

Se absolvió a Patricia Alejandra Valera Guerra, usando principalmente para ello motivos probatorios.

- **Considerandos relevantes:**

DÉCIMO: Que de lo establecido en el considerando octavo, y lo expuesto en el considerando séptimo, es que estos sentenciadores, sólo pueden explicar la creación de pines que se realizaron en dicha caja y que no quedaron constancia en las boletas, conforme a lo que el perito de cargo y Cristian Jaure Jaure indicaron, es decir, que la acusada debió haber presionado las teclas "6, 4 y conex" antes de pasar por el escáner el tarjetón de la empresa de telecomunicaciones, generándose así los "pines" sin quedar registro de ello en la boleta, adelantándose desde ya, que no se logró probar en juicio que la encausada estuviese consiente de ésta falla del sistema ni que se aprovechará de ella para generar "pines", menos aún se probó en juicio que ésta se apoderada real y efectivamente de estos, ya que como se señaló no se logró dar por establecido que los

boucher efectivamente salieran de la caja registradoras, ni menos aún se dio cuenta que los "pines" que se generaron, fueron usados por ella o un tercero.

Que, se debe señalar, que es del caso que no se probó en juicio, más allá de toda duda razonable, el real conocimiento que de esta operación tenía la encausada, es más, tampoco se logró establecer bajo el estándar legal que efectivamente hubo apropiación y perjuicio, por lo que mal podría darse por establecido el elemento subjetivo del tipo en examen. Esto es así, en atención, a que el modo de operar para poder obtener pines, según dio cuenta Jaure Jaure, analista de sistema de D&S, el que expresó que es el único que conoce el sistema con que operaban las cajeras, en conjunto con otra persona pero que tiene menos experiencia, indicó que se demoraron varios meses en descubrir cómo es que se realizaban estas generaciones de pines sin quedar registrados en las boletas, al exponer que alrededor de agosto o septiembre del año 2007, tomó conocimiento de que se estaban emitiendo más pines que los que quedaban registrados y que en la tercera semana de enero de 2008 recién pudo descubrir cómo se realizaba dicha operación, señalando luego en su declaración que cree, que la primera persona que utilizó esta vulnerabilidad debió haber sido por azar, es decir, por casualidad, concordante a los dichos de Patricio Campos Montecinos, quien coincide en que se investigó por meses, ya que señaló ante la pregunta dirigida a este punto que "se investigó por meses", al menos unas cinco a seis semanas, expresando además que el encargo de dicha investigación si bien era él por ser el subgerente del área de sistemas, delegó las funciones en Cristian Jaure Jaure, el que fue categórico en señalar, como se indicó anteriormente, el tiempo en que tomó conocimiento de la situación y cuándo logró entender como se generaban los pines sin quedar registrados en las boletas, agregando Patricio Campos Montecinos que fueron dos cajeras que estaban involucradas las que confesaron la maniobra, dando de esta forma "luces" respecto de la operación, señalando que supo el modo de operar por los dichos de las cajeras lo que posteriormente se corroboró por la empresa, y que al ser una situación compleja, bien puede Cristian Jaure Jaure indicar que fue él quien descubrió la forma de operar que se comenta; que así las cosas es que éste tribunal no puede menos que concluir y concordar con Jaure Jaure en que debió ser por azar el descubrimiento de esta maniobra, y por ende de forma involuntaria se debió haber pasado el tarjetón por el lector de la caja, ya que si la persona profesional en el área, encargado de dicho sistema le fue dificultoso encontrar esta modalidad, con mayor razón a los

cajeros que no tienen instrucciones en la materia a nivel de dicho testigo, por lo que la acusada, de quien no se dio cuenta que fuera profesional en el área informática, sólo podría haber sabido de esta maniobra ya sea porque "descubrió" la "falla" en el sistema por azar y se diera cuenta de ello o porque alguien le contara, que respecto de este último punto no se acreditó en juicio ni existen indicios de que a ella se le haya informado de esta forma de operar, ni en el local comercial existieron otros casos según dio cuenta el perito de cargo, por lo que es posible que de manera involuntaria o errada una cajera como la acusada pase por el escáner el tarjetón, luego de haber presionado el "potenciador presto". Que, teniendo presente lo anterior, este tribunal estima que no se acreditó en juicio que la acusada conociera real y efectivamente la vulnerabilidad del sistema informático, y en consecuencia deliberadamente produjera el error en éste, en razón de que, el hecho que ella realmente se diera cuenta que estaba generando pines conforme a esta maniobra no aparece a juicio de estos sentenciadores probado, toda vez que existen serias dudas al respecto, en atención a que el perito de cargo señaló que le extrañaba que en el supermercado Líder de La Serena sólo fuera una persona la que generó pines a través del potenciador presto, puesto que en otros lugares eran más de una persona la que los generaba de esta forma, dando cuenta Patricio Campos Montecinos que esta forma de operar se dio a lo largo del país con cajeros que tenían una cifra bastante elevada de transacciones, utilizando la palabra "millones" para ejemplificarlo, agregando acto seguido que era por montos de "millones" de pesos, considerando éste tribunal que ambas situaciones, esto es, que en centros comerciales exista más de una persona que realizase esta operación, repetidas veces y que sea por montos elevados, es lo que se puede esperar, ya que aparece como razonable que si un cajero descubre esta forma de burlar el registro que hace la caja de las transacciones, lo comente con algún compañero de labores, y que como no queda huella de la generación de pines en el sistema informático de la caja lo realice en repetidas ocasiones generando en consecuencia altos montos; que es del caso, que en juico no se dio cuenta que existiera otra persona aplicando el descuento presto para generar pines que no quedaran registrados en el local comercial en cuestión, ni tampoco estamos en un caso en que se generaron grandes montos como indicó Campos Montecinos, ni fue durante un transcurso de tiempo prolongado, pues los propios dichos del perito señalaron que las transacciones generadoras de pines sin registro en la boleta efectuadas en la caja que manejaba la acusada, se realizaron únicamente en el período comprendido entre el día 11 a 30 de enero de 2008 y sólo en nueve días, por lo que éste tribunal no se explica

porque ella –si es que supuestamente sabía de la vulnerabilidad del sistema– no siguió generando pines que no se registraban en las boletas todos los días y después del 30 de enero, teniendo en consideración que si bien el deponente Jaure Jaure, indicó que terminada la investigación (al descubrir la falla), se realizaron los cambios de aplicación de cajas, dando vuelta los módulos, para que cuando se escaneara un cartón de prepago se incluyera en la boleta, señaló que esto ocurrió la segunda semana de febrero, por lo que aún en el caso que se hubiese arreglado el problema la segunda semana de febrero, es oportuno preguntarse que ocurrió que no siguió generando pines después del 30 de enero, que a mayor abundamiento este tribunal debe manifestar, que, como se explicará a continuación, lo depuesto por Jaure Jaure respecto de este punto no aparece creíble a juicio de estos sentenciadores, en atención a que es contradictorio con lo expresado por testimonio de cargo, Campos Montecinos, el que señaló que en este caso debe existir (luego del descubrimiento del problema) un tiempo de codificación y de prueba para testear la funcionalidad de la modificación al sistema de la situación anómala, expresando que no puede ocurrir en uno o dos días, lo que comparte este tribunal; además lo señalando por Luis Fernández Larenas, ingeniero informático de la Policía de Investigaciónes, a quien por ser un ente extraño y no interesado en el presente juicio se le otorgará plena credibilidad de lo que le manifestó Jaure Jaure, declarnado que Cristian Jaure Jaure le informó que la vulnerabilidad fue detectada en febrero de 2008, siendo modificada posteriormente por D&S, y finalmente remplazada por "Assat", señalándole Jaure Jaure que la aplicación estuvo en funcionamiento hasta el 14 de marzo de 2008, por lo que indicó este perito que no pudo ver en terreno la vulnerabilidad del sistema, señalando que no puede dar fe del cambio de aplicación o versión ya que si bien solicitaron "el control de cambio de aplicación o control de cambio de versión de aplicación", D&S no tenía estos documentos, de donde éste tribunal sólo puede deducir que cuando concurrió este perito a la empresa Líder, esto es, el 02 de junio de 2008, probablemente ya no estaba vigente la falla, no quedado fehacientemente probado en juicio hasta cuando ésta les afecte, sin perjuicio de que éste tribunal estima, como ya se señaló, que lo lógico y lo que las máximas de la experiencias indican, es que una vez detectado la falla, se iniciare el estudio de cómo solucionarlo, codificándose en este caso la modificación al sistema como dio cuenta Campos Montecinos, luego probándose su efectividad, para recién después de eso empezar a aplicarla en las cajas, lo que indudablemente requiere cierto tiempo; sin perjuicio, que posteriormente se hiciera el cambió por otra sistema informático llamado "Assat" como

Fernández Larena expresara, ya que eso sería concordante con lo declarado por Mariela Castro Pérez, operadora del sistema en su rol de cajera, la que apareció ante estos sentenciadores, veraz y creíble en sus dichos, expresando que el sistema se modificó en octubre de ese año, lo que éste tribunal estima plausible en atención que quién más que los operadores del sistema pueden dar cuenta que se cambió el formato y funcionamiento del sistema, más aún cuando ella misma profirió que era todo diferente, y que incluso las cajas eran nuevas. Que, parece razonable a éste tribunal que la encausada desconociera que se estaban creando "pines", toda vez que como explicó Jaure Jaure y el perito de cargo, luego de presionar la tecla "6, 4 y conex" y pasar cualquier producto por el lector o escáner existente en las cajas, la misma máquina señalaba una leyenda como "producto no a la venta", por lo que perfectamente es posible que ella entendiera que no se habían solicitado "pines", y si a eso se suma que la única transacción de la que dio cuenta detalladamente el perito de cargo se había reversado la aplicación del potenciador presto, y que tanto Enque Fredes Parra como Mariela Castro Pérez fueron concordantes y coincidentes, en señalar que para reversarlo se debía llamar a la supervisora, generándose en consecuencia una boleta nueva, y que si el pin no era anulado se perdía en el sistema, como ya se acreditó; que es del caso que si a la acusada le ocurrió que pasó el tarjetón por el lector por casualidad, luego de apretar el "potenciador presto" o "teclas 6, 4, y conex"–ya sea una o varias veces–, le debió haber aparecido que el producto no estaba a la venta, por lo que hasta ese momento no tenía por qué ésta pensar que los pines se habían requerido a la central, por lo que, si por ejemplo, el cliente no tuviere cupo en su tarjeta, se arrepintiere de pagar con la tarjeta, quisiere llevar otro producto más en la misma boleta o quisiera efectivamente llevarse la recarga de teléfono celular –escenarios indicados por las testigos de descargo–, a la encausada no le quedaba más que llamar a la supervisora para que anulara la venta y botara la caja, por lo que si ésta le preguntaba por si había una venta de recarga telefónica, ésta no tenía cómo saber que efectivamente para el sistema central si lo había, porque en su caja no aparecía a la venta y no se marcaba como tal, por lo que lo lógico es que ésta respondiera que no tenía ninguna recarga marcada, por lo que la supervisora nunca realizaría la operación de anular la solicitud de "pin", perdiéndose éste en consecuencia en el sistema como dieron cuenta las testigos de descargo, y así cuando se generare la transacción finalmente requerida, sólo aparecería ante sus ojos una boleta en que figuraran los productos que ella vendió efectivamente, no emitiéndose nunca entonces el boucher, del tarjetón que pasó después de presionar las "teclas 6, 4 y conex", porque como estas mismas

cajeras depusieron éste se perdía en el sistema luego de "botar" la caja si no era anulado, por lo que la acusada jamás pudo enterarse que generó pines para el sistema. Que el hecho de que una vez anulada y botada la caja se perdían los pines quedó plenamente acreditado con los dichos de las cajeras mencionadas anteriormente, como se razonó en el considerando anterior, párrafo final, las que explicaron circunstanciadamente como podía ocurrir, expresando estas testigos que esa era una de las fallas que ellas podían apreciar del sistema en comento en transacciones normales y válidas, agregando Campos Montecinos que es normal que a ellos les reporten fallas, descartándose en consecuencia los dichos de Katherine Vergara Reyes, Jefa de Caja de empresas Líder, en cuanto a que desconoce que el sistema de recargas presentara fallas, declaración que por lo demás éste tribunal estimó como acomodaticia a las pretensiones que legítimamente pudo tener su empleador. Que finalmente la única opción en que efectivamente supuestamente debía aparecer el boucher con el código de recarga en el caso en comento, es que después de apretar la "tecla 6, 4 y conex", simplemente se recibiese el pago de la transacción con el medio adecuado, de lo que éste tribunal no tiene seguridad si ocurrió en el caso de la acusada, porque como ya se dijo reiteradamente el perito sólo dio cuenta de un caso en que se reversó el potenciador presto, desconociendo éste mismo, cómo se reversaba; además, en este caso, faltó una prueba pericial que afirmara que la encausada había realizado operaciones sin reversar el "potenciador presto" y que determinará con toda seguridad que efectivamente salía el boucher, como se razonó en el considerando anterior, no que "debía" salir, ya que tanto Jaure Jaure como el perito de cargo, sólo hablaron de que realizaron cruce de información o de datos, no señalando ninguno si realizaron pruebas de campo que confirmara el procedimiento y que efectivamente salía el boucher, menos aún explicando a este tribunal en qué podrían haber consistido estas pruebas, más cuando en juicio se dio cuenta por las mismas cajeras que depusieron como prueba de la defensa que el sistema presentaba errores con las recargas telefónicas incluso en una transacción válida, donde aún podía no aparecer el boucher, y que en esos casos se debía llamar a la supervisora quien anulaba la venta y recarga para luego "botar" la caja, y así finalmente poder realizar la venta de la recarga telefónica, agregando estas testigos que si no se reiniciaba con la operación que debía hacer la supervisora se llamaba a "sistema"; dando cuenta además, Enque Fredes Parra que incluso una vez cuando inició el procedimiento en la caja, salieron automáticamente tres boletas y los pines respectivos, por lo que con mayor razón faltó una prueba por parte del ente persecutor destinada a probar más allá de toda duda razonable que

efectivamente salían estos boucher en el caso específico que se analiza, teniendo especialmente en cuenta que no existen otros indicios para presumir dicha situación, ya que no se probó en juicio que estos pines fueran usados por persona alguna. Que no sólo en juicio no se acreditó el conocimiento que de la falla tenía la acusada, sino que tampoco se acreditó consecuencialmente el dolo requerido. Asimismo, y consecuencia de lo anterior, tampoco se acreditó que la acusada se apoderara del código de recarga, y por tanto, que se apropiara del boucher, inclusive no se dio cuenta en juicio que los "pines" que se generaron efectivamente se usaron por ella o un tercero. Que existiendo otros casos en que en una operación legítima se generaban "pines" que se perdían y de los que la empresa D&S estaba en conocimiento, ya que intervenían las supervisoras y "sistema", y desconociendo éste tribunal si respecto de esos "pines" D&S y las empresas de telecomunicaciones tenían, previstos y estipulados tales escenarios, este tribunal no puede en este caso presumir que efectivamente se pagaran o se adeudaran dichos bienes, especialmente si no se tiene acreditado que se usaron por un tercero, más aún si se tiene presente que Patricio Campos Montecinos señaló que se solicitan los pines a las compañías telefónicas directamente, y que sólo manejan stock de pines de la empresa Entel, es que éste tribunal no sabe cómo es la relación contractual entre la empresa D&S y las compañías telefónicas puesto que si se pedían directamente los "pines" a las compañías telefónicas al momento de efectuar la transacción o venta en las cajas de los establecimientos comerciales, perfectamente D&S podía ser intermediario simplemente, y si estos pines nunca se usaron, no puede considerarse que existe perjuicio para las compañías telefónicas. Es más, el perito de cargo reconoció en juicio, luego de una pregunta aclaratoria formulada por éste tribunal, que no vio documento alguno que diera cuenta que se pagaron por empresas D&S o Empresas Líder los pines que generó la caja de Patricia Valera Guerra a las empresas de telefonía, que tampoco vio que existiera un crédito por dichos pines, sino que vio sólo la base de datos en que aparece el valor del pin solicitado, a lo que se agregó que tampoco de la aseveración de que D&S había repetido el valor de los pines pudo dar cuenta el perito de cargo ya que al momento de ser preguntado por el tribunal, señaló no recordar la forma en que se realizó. Que en razón de lo antes dicho, al no acreditarse el dolo del delito, la apropiación y el perjuicio, es suficiente ara dictar sentencia absolutoria respecto de este cargo, sin embargo, parece oportuno agregar que aún cuando hubiese existido el dolo de apropiarse de especie corporal mueble ajena, se debe señalar que la apropiación indebida descrita en el artículo 470 N°1 del Código del ramo, sanciona a los que en perjuicio de otro se

apropiaren o distrajeren cosa mueble que hubiera recibido por un título que produzca la obligación de entregarla o devolverla. Que aquí, en consecuencia, el objeto jurídico protegido es la propiedad indudablemente, y como la doctrina mayoritaria sostiene el derecho real de exigir la entrega de la cosa, siendo por ende el núcleo de esta figura el abuso de confianza. Que en este delito "el objeto material de la acción (dinero, efectos o cosa mueble) se encuentra ya en manos del agente, en virtud de un negocio jurídicamente válido y preexistente; el abuso de su parte radica en que con posterioridad se apropia unilateralmente de ese bien e infringe la obligación de restituirlo, causando así un perjuicio al sujeto pasivo". En consecuencia, en el delito se visualizan dos acontecimientos, uno formado "por la entrega voluntaria que hace la víctima del dinero o especie mueble al agente, mediante un acto legalmente válido que conlleva la obligación de devolverlos en el tiempo oportuno", y el otro por la apropiación propiamente tal expresado por el incumplimiento de la obligación de devolverlo, suponiendo en consecuencia éste delito "siempre y necesariamente un título válido en su origen, y no un título viciado o sólo aparente…, si no se ha valido de ardides o engaños para provocar la entrega, su delito es de apropiación indebida, y no de estafa", de lo que se deriva que necesario es concluir, que aún cuando se estimase que la cajera actuó dolosamente para generar los pines en su beneficio y perjuicio de D&S, ésta no recibe ningún bien corporal –corporalidad que incluso es discutible en este caso– mueble legítimamente, sino que generaría éstos engañando al sistema informático, lo que a lo más se parece a una estafa informática que no se encuentra tipificada, porque no hay persona engañada, que para configurar el delito de apropiación indebida se requiere que se recibieran legítimamente los pines con la consecuente obligación de restituirlos, pero en este caso se daría que la cajera no recibió los pines de su empresa –como cosa corporal mueble (si así se estimasen), ella los generaría, antes no existían–; para que se diera el delito de apropiación indebida, la empresa en que trabajaba debía haber entregado los "pines" o el boucher voluntariamente a la cajera por un título válido, como lo es cuando se esta realizando una transacción normal, y ésta se quedara con el precio o pago que efectuara el cliente, cosa que estuvo lejos de ocurrir. Que, como consecuencia de todo lo razonado en este considerando, es que se deberá dictar sentencia absolutoria respecto de estos cargos.

- **Tribunal:** Tribunal de Juicio Oral en lo Penal de Arica

- **Magistrado(s):** Mauricio Petit Moreno, Oscar Huenchual Pizarro y Mauricio Vidal Caro.
- **Fecha:** 18.97.2014
- **RUC:** 1210014297-8
- **RIT:** 75-2014
- **Procedimiento:** Ordinario
- **Síntesis de los hechos:**

Desde el año 2001 a la fecha, Víctor Cruz Torres se desempeñaba como trabajador de la empresa Sodimac S.A., siendo su cargo de operador de sistemas, cuyo objeto es controlar el adecuado funcionamiento de los equipos de la tienda, tanto software como hardware, asignándosele para ello, un equipo computacional identificado como PCSCLA SISTEMAS 32. Víctor Cruz Torres, el año 2011, a través de la intranet de la empresa, accedió a una planilla Excel denominada básica, apoderándose y conociendo indebidamente su contenido, para lo cual la almacenó –encriptada - en el equipo asignado, PCSCLA SISTEMAS 32, bajo el archivo de nombre Víctor. La referida planilla se encontraba en el servidor del área de recursos humanos de la empresa Sodimac a nivel central, protegida por protocolos de seguridad, cuyo acceso era restringido para el personal de dicha área; ello por cuanto su contendido tenía el carácter de reservado y privilegiado para la empresa, pues contenía información relativa a nombre de los trabajadores, antigüedad en la empresa, escala de remuneraciones, bonos y afiliación sindical, entre otros.

- **Decisión del tribunal:**

Se condenó a Víctor Alex Cruz Torres a sufrir la pena de 41 días de prisión en su grado máximo, en su calidad de autor del delito consumado de espionaje informático, previsto y sancionado en el artículo 2 de la ley 19.223, cometido en perjuicio de Sodimac S.A., un día no determinado del año 2011, en esta ciudad.

- **Considerandos relevantes:**

Decimotercero: Calificación Jurídica. Que la unión lógica y sistemática de los hechos consignados en el razonamiento undécimo y valorados en el considerando duodécimo, permiten calificarlos jurídicamente como constitutivos del delito de espionaje informático, previsto y

sancionado en el artículo 2 de la ley 19.223, a saber: “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”. Para estar en presencia de la figura típica de espionaje informático, en relación al sujeto activo, el legislador en la ley 19.223 optó por utilizar la expresión “el que”, de manera que no queda restringido el tipo penal a la existencia de un sujeto activo calificado o determinado; en tal sentido, conforme al mérito de la prueba incorporada y analizada, dicho presupuesto fáctico se cumple al imputar responsabilidad al acusado Víctor Cruz Torres. Ahora, en relación al sujeto pasivo del delito, teniendo en consideración el bien jurídico protegido por el ilícito, éste sería la persona titular del mismo, lo cual se cumple con la persona jurídica Sodimac S.A., quien además actúa en calidad de querellante. Ahora, respecto de los elementos objetivos del tipo penal, la ley en el artículo 2 de la ley 19.223, trata de diversas conductas a través de las cuales se pueden realizar las acciones típicas, a saber: • Interferencia, entendida como la acción de “cruzar, interponer algo en el camino de una cosa, o en una acción. Causar interferencia”. • Interceptación, entendida como la acción de “apoderarse de una cosa antes que llegue al lugar o a la persona a quien se destina”. • Acceso, entendida como “a la entrada o paso a un lugar”. Por su parte, las referidas conductas utilizan el adverbio “indebido”, lo cual entrega la idea de ilicitud, injustica, carencia de equidad, no autorizado. Que, los hechos acreditados, especialmente los referidos en los supuestos 2° y 3° del considerando undécimo, se ajustan a la conducta típica de acceso indebido a la información, pues consistió en las pericias tendientes a introducirse en un sistema de tratamiento de la información burlando todas las medidas de seguridad y resguardo programadas en su entrada, con el fin de allegarse a la información reservada contenida en un sistema, recabarla y utilizarla.

En relación a los elementos subjetivos del tipo, el artículo 2 de la ley 19.223, dispone que la motivación del agente comisivo pueda ser de tres clases, a saber, apoderarse, usar o conocer. Apoderarse, en el sentido de hacerse dueño de alguna cosa, ocuparla, ponerla bajo su poder; en tal sentido, cabe señalar que conforme a dicho verbo, es suficiente el sólo hecho de que la información entre en la esfera personal del transgresor. Usar, consiste en hacer servir una cosa para algo, o bien, disfrutar uno alguna cosa, sea o dueño de ella; ahora, en la ley, no se exige ánimo de lucro en el uso, por lo tanto, se trata de utilización lato sensu por lo que se incurre en

la conducta típica al usar la información en cualquier cosa. Conocer, implica averiguar por el ejercicio de las facultades intelectuales la naturaleza, cualidades y relaciones de las cosas. En relación a la ley 19.223, se traduce en un ejercicio intelectual destinado a conocer y saber acerca de distintos datos que se encuentran contenidos en un programa determinado o en un banco de datos. Finalmente, las expresiones verbales apoderarse, usar o conocer, van acompañadas del adverbio indebidamente, por ello, cualquiera que sea el ánimo que desarrollo el sujeto activo deberá necesariamente ir empapado de un elemento de ilicitud, de una violación de las prohibiciones.

Que, los hechos acreditados, especialmente los referidos en los supuestos 2° y 3° del considerando undécimo, dan cuenta de que la acción ejecutadas por el acusado Cruz Torres se ajustan a todas las conductas, pues, se apoderó (guardando los datos en el computador asignado e incluso la encripto con una clave); usó la información (filtró la información para conocer las remuneraciones de diversos trabajadores) y conoció (se enteró del contenido de la información), todo ello indebidamente, pues, conforme y al mérito de las labores para las cuales estaba contratado y desarrollaba no tenía modo alguno para acceder a la información.

En relación a los datos contenidos en un sistema de tratamiento, conforme a los hechos acreditados, la información decía relación con un archivo Excel, conteniendo datos de trabajadores de la empresa a nivel nacional. Archivo que, por lo demás, se encontraba en un servidor de la empresa con acceso restringido a un número determinado de personas, entre las cuales, no se encontraba el acusado. Por su parte, es un hecho público y notorio que Excel se trata de un programa desarrollado y distribuido por Microsoft, y es utilizado normalmente en tareas financieras y contables, útil para gestionar Bases de Datos; pues permite agrupar, ordenar y filtrar la información. Finamente, en atención a que Víctor Cruz Torres ejecutó todas y cada uno de los elementos del tipo penal ya descrito, el delito se encuentra en grado de ejecución consumado, de conformidad a lo dispuesto en el artículo 7 del Código Penal.

- **Tribunal:** Tribunal Oral en lo Penal de San Bernanrdo
- **Magistrado(s):** Andrea Gloria González Araya, Julio Jáuregui Medina y Pablo Orlando Contreras Guerrero.

- **Fecha:** 14.05.2016
- **RUC:** 1100498003-6
- **RIT:** 110-2015
- **Procedimiento:** Ordinario
- **Síntesis de los hechos:**

Que Francisco Antonio Montano Vásquez, a partir del día 10 de Mayo del año 2011, contactó a Osvaldo Romero Román, funcionario público del Tribunal de Juicio Oral en lo Penal de San Bernardo, solicitándole que le informare la situación procesal de David Salomón Bravo Villavicencio, en razón de su calidad de egresado de derecho; esto es, si mantenía una condena pendiente, si tenía algún impedimento para ingresar al país, y si era procedente la prescripción penal. Por esta labor se le pagaría una remuneración a Romero Román. Para esos efectos Romero Román le pidió al Administrador del Tribunal de Juicio Oral en lo Penal de San Bernardo, Gerko Henríquez Morales, que le obtuviera la información en los sistemas computacionales del Registro Civil, al que tiene acceso el Tribunal. Ante dicha solicitud, Henríquez Morales, obtuvo y rescató de los sistemas informáticos a los que tiene acceso en su calidad de Administrador del Tribunal Oral en lo Penal de San Bernardo la información pedida, y se la entregó a Romero Román; quien luego proporcionó los antecedentes existentes en el extracto de filiación de David Bravo a Montano Vásquez.

- **Decisión del tribunal:**

Se absolvió a Osvaldo Romero Román de la acusación deducida en su contra que lo sindicó como autor de los delitos de cohecho, de violación de secreto, y de divulgación de información contenida en sistema informático.

- **Considerandos relevantes:**

Undécimo: (…) iii.- En cuanto al delito de Divulgación de información contenida en sistema informático, la conducta típica importa que maliciosamente revele o difundan los datos contenidos en un sistema de información. Dos alcances corresponde hacer a ese respecto. Primero, en cuanto a la conducta de Romero Román, no puede postularse que aquél haya hecho una revelación o difusión de los datos contenidos en un sistema de información. Esta cuestión

queda meridianamente clara si se atiende al título de la ley 19223, esto es, tipifica figuras penales relativa a la informática. Por lo tanto, todas las conductas sancionadas en dicha ley se entienden configuradas sólo en la medida que estén relacionadas directamente con sistema informático. Esto es, sólo respecto de aquella conducta que esté directamente conectada al levantamiento de información desde el sistema informático, y que posteriormente procede a sus revelación o difusión. Únicamente en este sentido puede ser entendida dicha figura, pues si se criminalizara de esta forma cualquier difusión de información que haya estado contenida en uno de estos sistema, independiente de cómo se adquirió dicha información, se podría terminar penando acciones que jamás tuvieron el mas mínimo acceso a dicho sistema. Importaría penar por esta figura cualquier cadena de información independiente de lo lejos de que se esté de la fuente de esa información, o la vía por la cual se adquirió esa información, y que puede no tener relación alguna con un sistema informático, por ejemplo el boca a boca. En este orden de ideas es claro que la persona que hizo la revelación de esta información fue Gerko Henríquez, pues fue él quien tenía el acceso al sistema, y quien recabó la información de éste para luego entregársela a Romero Román.

(…)

En segundo lugar debe tenerse en cuenta que la faz subjetiva de esta figura exige que aquella sea cometida con dolo directo al utilizarse en su descripción típica la voz “maliciosamente”. Luego, desde la perspectiva de su faz subjetiva, si es que el imputado Gerko Henríquez hubiere actuado con dolo eventual no podría tenerse por configurado este delito. Al respecto debe tenerse en consideración que el convenio de cooperación que prescribía la confidencialidad de ciertas informaciones contenidas en el sistema monito web nunca les fue informada ni instruida a los funcionarios del Tribunal.

Por lo tanto, Henríquez bien pudo haberse representado la posibilidad de que infringía una prohibición de difundir la información de ese sistema informático, pudo hasta haber aceptado esa consecuencia, y sin embargo, en dicho contexto sólo habría actuado con dolo eventual y, por lo tanto, no se podría tener por configurada esta figura penal. Sin perjuicio de lo anterior, el óbice más manifiesto a la configuración de esta conducta viene dado por la falta de antijuricidad material de las conductas de Henríquez y Romero. Al respecto se entiende que “una acción

antijurídica es formalmente antijurídica en la medida en que contraviene una prohibición o mandato legal; y es materialmente antijurídica en la medida en que en ella se plasma una lesión de bienes jurídicos socialmente nociva y que no se puede combatir suficientemente con medios extrapenales" (Roxin, Claus, Derecho Penal, Parte General, Tomo I, Thompson Civitas 1997, 558). La consecuencia más relevante de tal distinción radica en que "desde el punto de vista de la antijuricidad, el injusto material de la lesión de bienes jurídicos puede excluirse por el hecho de que no se produce un daño social jurídicopenalmente relevante" (Roxin, Claus, ibídem). Por consiguiente, sólo en la medida que pueda establecerse en el caso concreto que la sustancia en cuestión constituye un peligro real –aunque sólo potencial- para el bien jurídico es que se podrá afirmar a su respecto la configuración del tipo. En este mismo orden de ideas, y para efecto del correcto análisis de la configuración del tipo penal en cuestión, debe asentarse cuales son los bienes jurídicos tutelados por estas figuras, y así determinar su posible lesión. El Tribunal acoge la tesis conforme a la cual esta es una figura pluriofensiva. Existe un primer bien jurídico tutelado que fija la puerta de entrada de la punibilidad de esta conducta, ese bien jurídico es "la confidencialidad del soporte lógico de un sistema automatizado de información" (Moscoso, Romina, La ley 19223 en general y el delito de hacking en particular, revista chilena de derecho y tecnología, Vol. 3 nº 1 (2014) p. 16). "Así una conducta que no afecte datos confidenciales debe ser eximida de responsabilidad penal por faltar la antijuricidad material" (Moscoso, Romina, ibídem). Supone tal bien jurídico evaluar la importancia de la información contenida en un sistema informático, ya que no toda la información digitalizada es merecedora del mismo grado de confidencialidad. Por otro lado, se postula que estos delitos son pluriofensivos, pues "los delitos informáticos también afectan otros intereses o valores como la intimidad…. [en todo caso] la confidencialidad de los datos de un sistema informático se convierte en la puerta de entrada, condición necesaria, para admitir la represión penal de un conducta lesiva de este interés" (Moscoso, Romina, ibídem, p. 17).

Así las cosas, en lo que respectó a la conducta de los acusados Romero Román y Henríquez Morales, el Tribunal entendió no hubo antijuridicidad material que permitiera dar por configurado este tipo penal. En efecto, atendiendo al bien jurídico protegido por esta figura, la confidencialidad, y, teniendo en cuenta lo señalado supra, respecto del carácter de pública, para las partes interesadas, de toda la información que conste en un proceso penal remitido al

Archivero Judicial, se debe necesariamente concluir que la información que fue obtenida y divulgada por los imputados no afectaba de ninguna forma la confidencialidad del sistema. En este sentido aparece de manifiesto que dicha información es pública, y el sistema lo único que hace es ordenarla y facilitar su consulta. Por consiguiente, si bien los imputados divulgaron información contenida en el sistema de consulta del registro civil, en ningún caso aquella se encontraba limitada por una necesidad de confidencialidad. Luego, en su divulgación no se afectó ninguna reserva de la misma, ya que, perfectamente se pudo obtener por otra vía, respecto de la cual no rige ninguna limitación, y esta es, su directa consulta en el Archivero Judicial correspondiente. En lo que se debe poner hincapié al hacer este análisis es que, si bien la información en cuestión se encuentra digitalizada e incorporada a un sistema, no por ese solo hecho debe entenderse que sea confidencial. A su respecto debe hacerse un ejercicio de valoración que permita discernir si recae en dicha información dicha calidad. Y la conclusión a que se arribó es que no puede postularse esa calidad a su respecto, pues esa misma información se encontraba fuera del sistema sin limitación de confidencialidad para las partes interesadas. Es decir la misma información contenida en proceso remitido al Archivero Judicial era la que en parte estaba consignada en el respectivo extracto de filiación.

Por su parte, y entendiendo que esta figura es pluriofensiva, el bien jurídico privacidad, respecto de la persona titular de esa información David Bravo Villavicencio tampoco se vio afectado con estas conductas. En primer instancia, pues de su propia parte se habría encomendado recabar esa información. Por otro lado si dicha información fue recabada, lo fue única y exclusivamente para solucionar su situación procesal conforme a los institutos penales, como la prescripción de la pena para este caso concreto. Es decir, esta información ya fue puesta al corriente de los terceros que intervinieron en el proceso por el propio titular de esa información. Luego, sólo a instancia y en su beneficio es que dicha información fue obtenida. Por ende no hay afectación alguna de su intimidad, pues hubo un acto previó de abrirla a terceros, los que se impusieron de datos relativos a condenas penales que pesaban en su contra sólo para efecto de poder verificar si aquellas podían declararse prescritas, y ante un anuencia tácita de quien solicitó se resolviera tal situación.

- **Tribunal:** Tribunal de Juicio Oral en lo Penal de Temuco
- **Magistrado(s):** Jorge Gabriel González Salazar, José Ignacio Rau Atria y Luis Emilio Sarmiento Luarte.
- **Fecha:** 22.07.2018
- **RUC:** 1700268031-9
- **RIT:** 54-2018
- **Procedimiento:** Ordinario
- **Síntesis de los hechos:**

Hecho 1: Que desde marzo del año 2008 y hasta diciembre del año 2016 la imputada María Alejandra Rodríguez Henríquez se desempeñó como funcionaria administrativa en la Secretaria Regional Ministerial (SEREMI) de Transporte y Telecomunicaciones de la Región de la Araucanía, ejerciendo funciones en la Unidad de Registro de dicha repartición pública, correspondiéndole, entre otras funciones, aquellas relativas a la inscripción, reemplazos y cancelación de vehículos correspondientes a taxis básicos, taxis colectivos y taxis de turismo que componían el parque automotriz del transporte público de pasajeros.

Es así que en el ejercicio de las funciones públicas antes mencionadas la imputada, infringiendo gravemente los deberes de su cargo y aprovechando el acceso que por su calidad de empleada pública y las funciones desempeñadas, tenía a las bases de datos de la SEREMI de Transportes, relativas al parque automotriz del transporte público de pasajeros, el cual se encontraba congelado para efectos de ingreso de nuevos vehículos, conforme a lo dispuesto en el artículo único de la Ley N° 20.474 de 15 de noviembre de 2010 y Ley N° 20.867 de 22 de octubre de 2015, durante los meses de marzo de 2014 a diciembre de 2016 y mediando la solicitud o aceptación de un beneficio económico consistente en valores que oscilaban entre los $4.000.000 a $8.000.000 por cada cupo, procedió a vender cartones de recorrido que habilitaban para ejercer el transporte público de pasajeros en modalidad de taxis básicos, taxis de turismo y taxis colectivos a diversas personas.

En concreto, la imputada a cambio del beneficio económico solicitado realizaba esta tramitación irregular simulando estar efectuando un reemplazo de un determinado vehículo, el cual se encontraba válidamente inscrito en el Registro de la SEREMI de Transporte para ejercer el

transporte público de pasajeros, pero cuya inscripción en realidad se encontraba caducada, como era de conocimiento de la imputada y no era posible de ser reemplazada de acuerdo con el procedimiento regulado en el D.S. 212 de fecha 21 de noviembre de 1992, Reglamento de los Servicios Nacionales de Transporte Público de Pasajeros, para lo cual formaba expedientes físicos con las respectivas solicitudes, los que posteriormente desaparecían de las dependencias de la SEREMI de Transportes.

Hecho 2: Que entre los meses de marzo del año 2014 a diciembre del año 2016 la imputada Rodríguez Henríquez y en su calidad de funcionaria pública de la SEREMI de Transportes y Telecomunicaciones de la IX Región, procedió a la tramitación irregular de 165 reemplazos irregulares, que habilitaban para ejercer el transporte público de pasajeros en la Región de La Araucanía. Para llevar adelante tal conducta, la imputada procedió a confeccionar expedientes administrativos de tramitación ficticios, en los cuales consigno antecedentes falsos tendientes a dar apariencia de veracidad en la información contenida en los mismos. Fue así que, entre otros, consigno en los Formularios Únicos de Reemplazos información falsa a fin de aparentar que estábamos frente a una tramitación de reemplazos de vehículos destinados al transporte público de pasajeros de manera licita, todo ello con el objeto de dar apariencia de licitud al trámite de reemplazo y lograr así la dictación del acto administrativo, que era en definitiva la firma de la autoridad regional en la cartola de recorrido que habilita para ejercer el transporte público de pasajeros. Asimismo y con la misma finalidad, la imputada ingresó información falsa en las bases de datos del Registro Nacional de Transporte Público de la SEREMI de Transportes, entre ellos la información de Placas Patentes Únicas, fechas de ingresos, entre otros, quedando indebidamente autorizados y habilitados para el transporte público de pasajeros.

- **Decisión del tribunal:**

Se condenó a María Alejandra Rodríguez Henríquez como autora del delito consumado de cohecho, descrito y sancionado en el artículo 248 Bis del Código Penal, en carácter de reiterado. Además se le condenó como autora del delito consumado de falsificación de documento público, descrito y sancionado en el artículo 193 N° 4 del Código Penal, en carácter de reiterado, perpetrado en la comuna de Temuco enero de 2015 y diciembre de 2016, a la pena privativa de libertad de cuatro años de presidio menor en su grado máximo.

No obstante fue absuelta de los cargos por los que fue sindicada, por parte de la parte querellante, como autora de los delitos de lavado de activos y de alteración maliciosa de sistemas de tratamiento de información.

- **Considerandos relevantes:**

Décimo séptimo: (…) B) Finalmente, y en forma independiente, la querellante y acusadora particular por el Consejo de Defensa del Estado, también endilgó responsabilidad criminal en contra de la acusada Rodríguez, por los hechos descritos en la segunda parte del párrafo primero del Hecho 2, señalando que estos constituían el delito de alteración maliciosa de sistema informático, reiterado, tipificado y sancionado por el artículo 3º de la Ley Nº 19.223, toda vez que la imputada, según afirma textualmente, "en numerosas ocasiones ingresó al sistema informático "Nahuel", que administra el Registro Nacional de Servicios de Transporte de Pasajeros dependiente del Ministerio de Transportes y Telecomunicaciones y procedió a alterar la información fidedigna contenida en dicha base de datos, ingresando indebidamente vehículos nuevos en reemplazos de otros antiguos con total vulneración de la normativa vigente".

La ley 19.223 del año 1993 tipificó adecuadamente el delito de alteración maliciosa de sistemas de tratamientos de información en su artículo 3°, señalando expresamente que 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.

Según se lee de la historia fidedigna de la ley en comento , la idea matriz o fundamental del proyecto es proteger la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma, y los productos que de su operación se obtengan. El delito informático puede definirse como cualquier conducta ilegal, no ética o no autorizada, que involucra el procesamiento automático de datos o la trasmisión de los mismos (según la Organización para la Cooperación Económica y el Desarrollo), o como toda acción típica, antijurídica y culpable, para cuya consumación se utiliza o afecta una computadora o sus accesorios (según el criterio de la Comisión que redactara uno de los anteproyectos sobre informática). Y se indica asimismo que los métodos empleados en la comisión de estos delitos son variados, habiendo sido objeto de sistematización por diversos autores, entre los cuales cabe mencionar a Donn B. Parker ("Computer Crime"), en lo que nos podría ser atingente a la

pretensión del acusador particular, el data diddling (datos engañosos), que consiste en la alteración de los datos al momento de la entrada al computador, mediante manipulaciones imposibles o difíciles de detectar. Los datos son ingresados con omisiones o agregaciones que los alteran en su sentido y contenido. Desde un punto de vista doctrinal, castigaría la manipulación de datos informatizados, el delito de fraude informático, que se comete mediante la alteración de los datos que se introducen o que están ya contenidos en el ordenador, en cualquiera de las fases de su procesamiento o tratamiento informático.

Ahora bien, para ir comprendiendo adecuadamente, dejaremos sentado que el tratamiento de la información consiste en una serie de operaciones que se realizan sobre una determinada información de forma planificada y ordenada y así poder convertirla en conocimiento; y que un sistema de tratamiento de información permite el procesamiento automático de la información, y conforme a ello, los sistemas informáticos deben realizar las siguientes tres tareas básicas: entrada, consistente en la captación de la información, normalmente datos y órdenes ingresados por los usuarios a través de cualquier dispositivo de entrada conectado a la computadora; proceso, que es el tratamiento de la información, que se realiza a través de programas y aplicaciones diseñadas por programadores que indican de forma secuencial cómo resolver un requerimiento; y salida, que es la transmisión de los resultados del proceso anterior, el producto de lo anterior, mediante dispositivos de salida a través de los cuales los usuarios pueden visualizar los resultados que surgen del procesamiento de los datos.

De lo anterior resulta que es relevante para entender si estamos delante de un sistema de tratamiento de la información, o no, que este sea capaz de almacenar, procesar y transmitir datos e información en formato digital utilizando sistemas computacionales. Lo anterior porque hay que diferenciarla de una mera base de datos.

En efecto, una base de datos es solo un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital,

siendo este un componente electrónico, que dado su desarrollo ofrece un amplio rango de soluciones al problema del almacenamiento de datos.

Ahora bien, concentrando el análisis tanto en la descripción fáctica como en el tipo penal que hemos analizado, una primera consideración tenida en vista por el tribunal es que el propio acusador estimó que lo que denominaba sistema informático "Nahuel", era una base de datos.

Al respecto, la testigo Sra. Cavada (pág. 54) contratada para hacer una auditoría en la SEREMI de Transporte por la denuncia del caso que nos ocupa, manifestó que las irregularidades detectadas en su trabajo, se re reflejaban en el sistema "NAHUEL" y en un anexo que le llamaba "la maravilla" que permitía hacer todas las modificaciones en el sistema, pues NAHUEL no lo permitía directamente y que el cambio de patentes no se cerraba al cabo de 18 meses de manera automática, sino hasta que alguien no los cancelara, pues el "sistema" solo arroja la patente, y no que no fue dañado ni destruido. Luego, consultado por la defensa de la acusada el testigo sr. Donoso (pág. 58) afirmó que el sistema no hacía caducar automáticamente las patentes.

Asimismo, relevante resultó la declaración de Ghislein San Martin (pág. 68) para considerar que el denominado NAHUEL no era un sistema de tratamiento de información, sino una mera base de datos, cuando asevera que María Alejandra Rodríguez debía proporcionar información proveniente de otra base de datos una vez a la semana al nivel central a con la información o datos de las placas patentes que debían caducar para luego informar a todos los Registros Civiles del país, y que el que denomina sistema, refiriéndose a NAHUEL "solo registraba datos", al punto que en sus propias palabras ese sistema, que fue cambiado en 2017, "no permitía generar alertas".

Y terminó por asentarse la convicción respecto de lo razonado, finalmente, la respuesta aclaratoria entregada por la testigo Deysi López (pág. 55), cuando responde que el sistema no detectaba patentes caducadas, ni RUT que no correspondieran con los dueños.

De este modo, quedó demostrado que la conducta de solo ingresar datos para los fines que perseguía la acusada en los procedimientos irregulares de reemplazo de vehículos de transporte de pasajeros como taxis colectivos, lejos de configurar la comisión de un delito autónomo y regulado en una ley especial como el pretendido por el querellante, dado que lo que se

manipulaba no era un sistema de procesamiento de datos o tratamiento de información, como exige perentoriamente el legislador, el denominado NAHUEL no era sino solo una base de datos de operación, más o menos compleja, y al efecto hay que señalar, como se arguyó por su defensa que no hubo probanzas de tipo técnico como para darle cabida y entender que si se trata de un sistema informático, la calidad precisa que exige el tipo penal invocado, ni hubo testimonio alguno en ese sentido, sino muy por el contrario, como dejamos de manifiesto, siendo la manipulación de la información que la acusada realizada en esa base de datos solo una parte del tramado de acciones que realizó en cada una de las operaciones irregulares, y por ello no puede ser objeto de reproche penal por separado.

- **Tribunal:** Tribunal Oral en lo Penal de Coyhaique
- **Magistrado(s):** Pablo Andrés Freire Gavilán, Luis Rolando del Río Moncada, Edmundo Ariel Devia González.
- **Fecha:** 24.07.2018
- **RUC:** 160036487-9
- **RIT:** 40-2018
- **Procedimiento:** Ordinario
- **Síntesis de los hechos:**

El imputado es representante de la empresa nombre de fantasía "Daygon Tv cable". Desde el año 2010 a septiembre del año 2016, de manera continuada, en las sucursales de calle Gabriela Mistral N° 558 Puerto Cisnes y Antonio Varas esquina Patricio Lynch de La Junta, el imputado prestó servicios de TV cable a título oneroso a diversos clientes de ambas ciudades cobrando por esta prestación.

Las supuestas acciones que realizó el imputado, fueron la utilización de la señal de televisión de la empresa Directv Chile Televisión Ltda., interceptando e interfiriendo maliciosamente el servicio de telecomunicaciones que ella presta, adquiriendo en forma previa, por sí y por medio de terceras personas, con la finalidad referida, diversos decodificadores y sus respectivas tarjetas inteligentes de propiedad de Directv, en seguida apoderándose, usando, reproduciendo y difundiendo indebidamente la información contenida en este sistema de tratamiento de la misma, esto es, diversos canales de televisión, y además incurriendo en la utilización no autorizada de la marca comercial sin autorización de su titular y sin pagar los derechos correspondientes.

La forma práctica que realizó estas acciones fue adquiriendo por sí y por terceros los decodificadores y tarjetas inteligentes, los cuales conectaba a un artefacto denominado mezcladora, formando una parrilla programática de canales de televisión, en seguida les daba salida a las señales mediante un cable coaxial para ser finalmente conducido y distribuido a cada uno de sus clientes o consumidores finales.

Además de ello también adquirió y utilizó con la finalidad más arriba referida, 2 decodificadores con sus respectivas tarjetas inteligentes de empresa "Claro Comunicaciones S.A".

Con estas señales utilizaba y emitía obras de propiedad intelectual de Empresas Fox y Foxla, entre otras, las que fueron reproducidas y difundidas por el imputado en contravención a la Ley, sin autorización de sus titulares y sin pagar los derechos correspondientes.

- **Pretensiones de las partes:**

Ministerio público: La pretensión de la Fiscalía en cuanto los delitos del art. 36 B letra b) Ley 18.168, art. 2 y 4 Ley 19.223 y art. 28 letra a) Ley 19.039, es el de concurso ideal del artículo 75 del Código Penal, siendo la pena mayor del delito más grave art. 36 B letra b) Ley 18.168, atendida la extensión del mal causado, la fiscalía solicitó se imponga al imputado Luis Alberto González Nauto la pena de cinco años de presidio menor en su grado máximo, más el comiso de los equipos incautados, accesorias generales que en derecho procedan.

En cuanto a las infracciones al artículo 79 letras a) y b) en relación a artículo 18 Ley 17.366, atendido que el perjuicio supera las 40 Unidades Tributarias mensuales, la Fiscalía solicitó se imponga al imputado, la pena de quinientos cuarenta días de presidio menor en su grado mínimo y multa de mil unidades tributarias mensuales, accesorias.

Defensa: Por su parte la defensa argumentó en cuanto a las dos primeras leyes, de telecomunicaciones e informática, que en el tipo penal el verbo rector es, en esas dos figuras, la interferencia. Que de acuerdo a la RAE es introducirse en la recepción de otra (señal) y perturbarla. Cómo su representado intercepta, cómo se introduce en las señales y las perturba. Pero esto no ocurrió en caso, ya que no se ha intervenido o interceptado o interferido la señal satelital. Tampoco se ha intervenido el tratamiento de datos que vienen en los decodificadores. El decodificador es un sistema que no se tocó.
Y, respecto a los delitos de propiedad industrial e intelectual, la argumentación giró en torno a que los querellantes no probarán el dominio de lo que fue usado. No habrá prueba sobre la inscripción, ya que no fue ofrecida.

- **Decisión del tribunal:**

En definitiva, se absolvió a al acusado Luis Alberto González Nauto, de las acusaciones del Ministerio Público y acusadores adherentes, Directv, FOX y FOXLA, y CLARO, de los delitos tipificados en los artículo 2 y 4 de la ley 19.223, relativa a los delitos informáticos; del delito tipificado en el artículo 28 letra a) de la ley 19.039, relativa al uso malicioso de marca industrial inscrita; artículo 79 letra a) y b) de la ley 17.366, sobre propiedad intelectual. Mientras que se condenó a la pena dos años de presidio menor en su grado mínimo, como autor directo del delito de interceptación de una señal televisiva usada por Directv.

- **Considerandos relevantes:**

Décimo cuarto: Se estimó absolver al acusado González Nauto, de los delitos sobre propiedad intelectual, delitos relativos a informática y de propiedad industrial, por las razones siguientes:

A este respecto la acusación no cumple con las exigencias establecidas en el artículo 259, letra b, del Código Procesal Penal. El acusador debe entregarnos una relación circunstanciada de los hechos y su calificación jurídica. Simplemente no lo hizo. Dice, por ejemplo, se utilizó la marca comercial, sin indicar cuál es la marca comercial. Este hecho escuetamente enunciado en la acusación no da cuenta qué delito constituye el hecho. A eso se refiere la norma cuando habla de la calificación jurídica. Más adelante, en lo conclusivo, sólo cita la norma legal, cumpliendo con el requisito exigido por la letra de la misma disposición, pero en el desarrollo de los hechos, no articula éstos a al concepto jurídico que corresponde.

Así, en relación al delito mencionado en los artículos dos y cuatro de la ley 19.223, sobre figuras penales informáticas, no hay un desarrollo circunstanciado de los hechos ni se explica cómo ellos se relacionan con las disposiciones legales anteriores. Estos jueces no podemos suplir estos vacíos a riesgo de vulnerar el artículo 341 inciso primero del Código Procesal Penal, ya que excederíamos el contenido de la acusación al asentar hechos o circunstancias de tiempo o modo asociados a los hechos; por ejemplo, no se indica qué obras de propiedad intelectual de FOX y FOXLA utilizaba el acusado y no hay cómo saber si esas empresas eran legítimas

poseedoras de esos programa; tampoco, cómo eran utilizadas las marcas por parte del acusado y los verdaderos titulares de aquella, ni nada sabemos de sus respectivos registros.

b) En efecto, no se acreditó por medios que generaran plena convicción que los acusadores adherentes fueran los titulares de marcas comerciales o propietarios de obras intelectuales, debidamente inscritas en los registros respectivos. La marca registrada, por ejemplo, como su nombre lo indica, consta en Registros. Lo señala ley, y la forma cómo ella debe expresarse, también, pero ello se ignora.

c) Aun, también se advierte un concurso aparente de leyes penales, por cuanto, para cometer este delito que consistente en interferir un servicio de telecomunicaciones, era necesario contar con los programas, que en este caso, transportaba la señal satelital. Es por esa razón que un cliente contrata, para que, una vez vaciados los contenidos en la pantalla, el usuario pueda disfrutar de ellos. Sin esos contenidos, el delito no se produciría. En consecuencia, el delito de apoderarse indebidamente de la información contenida en la comunicación satelital y revelar o difundir estos mismos datos, se estiman subsumidos en el delito de interceptación del servicio de telecomunicaciones. Éste no se cometería si no se integran esos programas. En otras palabras los delitos relativos a delitos informáticos están ínsitos en el delito de telecomunicaciones.

El fallo fue adoptado con la **prevención del Juez Devia** quien, a mayor abundamiento, en relación a los delitos mencionados en los artículo 2 y 4 de la ley 19.223 profundiza en su naturaleza y conceptualización y sobre el bien jurídico tutelado en estos delitos: Los delito informáticos se caracterizan porque sancionan conductas dirigidas en contra soporte lógico de un sistema tratamiento información, como sería por ejemplo un computador, que se compone de dos partes el soporte lógico, a saber los datos, la información contenía el sistema, es decir el software y el soporte físico los cables, chips, carcasa el equipo, decir el hardware, por ello una conducta dirigida contra los datos es un delito informático, mientras que una dirigida contra soporte físico, sólo es un delito de daños. De esta forma las conductas tipificadas en la Ley N° 19.223, tratándose de delitos con carácter informático, el objeto sobre el cual recaen dichas conductas es inmaterial, distinguiéndose tres modalidades de criminalidad informática, esto es fraude informático, el sabotaje informático y el espionaje informático. Los primeros, se encuentran las alteraciones o manipulaciones, de los datos, ya sea al recopilarlos, procesarlos,

estando almacenados o al transmitirlos telepáticamente, como de los programas del sistema computacional; los espionajes informáticos se encuentran las figuras de obtención ilícita, dolosa y sin autorización de datos o información relevante y de programas computacionales; y el sabotaje informático el cual se configuran las conductas de atentados que causan daños, destruyen o inutilizan un sistema computacional.

Podemos decir que, el tribunal estima que, la figura descrita el artículo 1 de la Ley N° 19.223, corresponde a lo que en doctrina se ha denominado como sabotaje informático, en oposición a las figuras de espionaje informático que regulan los artículos 2 y 4 de la misma ley. De acuerdo a ello, es posible identificar que respecto de los artículo 2 y 4 referidos, estamos en presencia de protección de la privacidad como bien jurídico penal que se encuentra sujeto a restricciones generales de custodia, estando restringida las intromisiones físicas en la vida privada delas personas bajo el concepto de morada, y por otro lado las intromisiones por medio de instrumentos regulado en el artículo 161-A del Código penal, lo cual lo hace mediante el doble recurso de exigir, por una parte, que se trate de sucesos que ocurran en lugares que no sean de libre acceso al público y de exigir, adicionalmente, que se trate de sucesos de la vida privada, cuestión que no pasa en el caso de los tipos penales informáticos y que tiene consecuencias en la comprensión de lo protegido y además la ley penal protege el registro de papeles ajenos. En forma adicional se encuentra la Lay N° 19.223, respecto de la información contenida en soportes informáticos, apreciando algunos autores que se estaría en presencia de una posible infracción a un derecho de exclusión no necesariamente vinculado con la privacidad, sino más bien específico de la informática, cuestión que no es pacífica en las opiniones, sin embargo en forma general, podemos decir que ambos artículos protegen la privacidad del titular de la información, entendiéndose como la eventual posibilidad de excluir a terceros del acceso a esferas de dominio de ese titular, es decir se puede concordar esa noción de privacidad como concepto formal, pero se debe tener en cuenta el rasgo distintivo especial de excluir a terceros.

En definitiva, respecto del ánimo apoderarse, interceptar la información, hacer uso de la misma, y el ánimo apoderarse no se encuentran suficientemente probados.

En cuanto al ánimo apoderarse, es decir a lo indebido, la norma exige que el acceso se realice con el ánimo de conocer indebidamente del contenido de la información, a pesar de ello, no se

ha establecido en forma cierta, la vulneración de la privacidad por parte del acusado en forma dolosa y que además sea sin autorización del titular de la información por ello no se vislumbra que la conducta desplegada por el acusado en relación a los equipos entregados, tenga el ánimo que exige la norma es decir apoderarse de ellos como señores y dueños, por el contrario existían contratos respecto de los mismos.

En cuanto a la interceptación nuevamente, no se encuentra acreditado que la conducta del sujeto activo haya sido la de interceptación, puesto que la misma a pesar, que los autores acogen la definición del diccionario de la real academia de la lengua española, tal descripción no resulta adecuada para el fenómeno informático, puesto que de información contenida transmitida en un sistema de tratamiento de la misma no dejará de llegar por la intercepción a su destino utilitario, pues por su naturaleza deben incorporar no se ve limitada por el apoderamiento, uso oconocimiento a un solo poseedor. Entonces debe ser entendido como la interposición o superposición de señales, ya sea ópticas, acústicas, electrónicas etc. u ondas que resulta en ciertas condiciones, aumento, disminución o neutralización de los impulsos magnéticos. Dicha interferencia no fue acreditada respecto de las señales que llegaban a su vez a los decodificadores entregados al acusado.

En cuanto al acceso, y debe tomarse en sentido técnico, y específico para el campo de la informática, en el sentido de ingresar al sistema tratamiento información desde un disco o de cualquier otro periférico, lo que permite dependiendo de la parte el sistema al cual se ha accesado, sólo conocer datos o información, o además modificar o ingresar o sacar datos información contenida en él, durante el juicio se estima que independientemente de lo razonado, no se aprecia además que se haya acreditado las exigencias del tipo penal del artículo 2 de la ley señalada, en esta parte puesto que en cuanto al acceso ya indicado, es decir penetrar o ingresar a un sistema de tratamiento de la información, permaneciendo en él o no, considerando que se entiende que es en un espacio cerrado, ya se físico o virtual.

Definitiva, no es posible apreciar la ejecución de la conducta descrita, porque no se podía acreditar un acceso indebido al información, puesto que la acceso, interferencia o interceptación conlleva que la conducta se cometa en el sistema tratamiento información y no sobre la información misma, es decir lo que se intercepta, interfiere o a lo que se accede es a un sistema

y no al información contenida en él, no se aprecia entonces que sistema haya sido vulnerado por lo que no es posible como ya se indicó apreciar la ejecución de la conducta descrita sin el acceso indebido a la información que se reclama.

- **Tribunal:** 4° Juzgado de Garantía de Santiago
- **Magistrado(s):** María Carolina Herrera Cortés-Monroy
- **Fecha:** 30.06.2011
- **RUC:** 1010001813-1
- **RIT:** 868-20100
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Durante los años 2006, 2007, 2008 y 2009, en circunstancias que el imputado Patricio Manuel Varela Bravo trabajaba como funcionario administrativo contable para la sociedad Agrupación de Médicos de la Clínica Alemana S.A. (AMCA S.A.), ubicada en Av. Manquehue Norte Nº 1404, comuna de Vitacura, maliciosamente alteró los datos contenidos en el sistema informático de dicha sociedad, correspondientes a los pagos recaudados por la Cínica Alemana, remitidos por la clínica a AMCA y facturados por esta última sociedad, por prestaciones realizadas en la Cínica Alemana por profesionales de la salud que forman parte de AMCA (correspondientes principalmente a bonos electrónicos por consultas médicas); borrando los datos originales y sustituyéndolos por datos falsos, con el fin de engañar a los funcionarios de AMCA encargados de la liquidación y realización de tales pagos a los asociados a AMCA, obteniendo de esta forma que estos fueran desviados y asignados a los otros imputados, esto es, a la matrona María Soledad Sánchez Berríos y a la auxiliar de enfermería Eleodora Carvallo Contreras, quienes sí trabajan en la Clínica Alemana, y también a Bárbara Díaz Sanhueza, quien no es arsenalera (sino secretaria) y ni siquiera trabaja en dicha clínica, pero se le hizo figurar con tal calidad para efectos de este fraude. A todas ellas el imputado Patricio Varela Bravo semanalmente generó pagos irregulares por servicios nunca prestados. De esta forma, durante el periodo antes indicado, los imputados defraudaron y causaron un perjuicio, tanto a AMCA S.A. como a los médicos a quienes correspondían tales pagos, por un total de $110.435.896.

- **Decisión del tribunal:**

Se condenó a Patricio Manuel Varela Bravo, como autor de los delitos de estafa reiterada, previsto y sancionado en el artículo 467 inciso final, en concurso ideal con el delito previsto en el artículo 3° de la ley 19.223, a la pena única de tres años de presidio menor en su grado medio

y al pago de una multa de una unidad tributaria mensual, a las accesorias de suspensión de cargos y oficios públicos durante el tiempo de la condena, cometido en perjuicio de AMCA S.A.

Se condenó a Eleodora Raquel Carvallo Contreras, como autora de los delitos de estafa reiterada, previsto y sancionado en el artículo 467 inciso final, a la pena de dos años y diez meses de presidio menor en su grado medio y al pago de una multa de una unidad tributaria mensual. Y a Bárbara Schlomit Díaz Sanhueza, como autora de los delitos de estafa, previsto y sancionado en el artículo 467 inciso final, a la pena de dos años de presidio menor en su grado medio y al pago de una multa de una unidad tributaria mensual.

- **Considerandos relevantes:**

Sexto: (…) Que respecto de la imputación del delito previsto en el artículo 3 de la ley 19.223, que fue parte de las operaciones que tuvo que efectuar el imputado, Patricio Varela Bravo, para efectuar el delito de estafa, es decir alteró, dañó y destruyó datos contenidos en el sistema de tratamiento informático, el tribunal estima que se encuentra acreditada la existencia de ese delito, pero en el marco de lo dispuesto en el artículo 75 del Código Penal, es decir, fue un medio para perpetrar el ilícito principal, si no hubiera cometido este delito no habría podido perpetrar la estafa, es el medio necesario para cometer este delito principal, motivo por el cual, estima también que el imputado Patricio Varela Bravo, incurrió en aquel ilícito de la manera que se acaba de señalar.

- **Tribunal:** Juzgado de Garantía de Talcahuano
- **Magistrado(s):** Raúl Reinaldo Martínez Henríquez
- **Fecha:** 13.09.2011
- **RUC:** 0900600732-2
- **RIT:** 4783-2010
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

En el mes de junio del año 2009, el Comisario Jefe de la Policía de Investigaciones de Chile, Bicrim Talcahuano, Constata ciertas irregularidades cometidas en el sistema administrativo Policial, sistema computacional de la Policía de Investigaciones, denominado SAP, y en ciertos informes policiales de la Brigada de Investigación Talcahuano, en los que no había correspondencia entre los informes remitidos a la Fiscalía local de Talcahuano y los que se mantenía en la Brigada de Talcahuano, constatándose en definitiva que el encartado Marcos Teamar Arancibia Campos, había alterado maliciosamente en el sistema informático señalado, cancelando intencionadamente y maliciosamente diversas órdenes de investigar emanadas del Ministerio Público a la Policía de Investigaciones de Chile, dirigidas al esclarecimiento de crímenes o simples delitos, que le habían sido encomendadas para su investigación, tramitación y diligenciamiento, utilizando para ello la clave de acceso al sistema SAP de otra funcionaria de la misma policía, asignándoles a estas cancelaciones números de informes policiales ya evacuados con anticipación relativos a otras materias, o simplemente inventando números de oficio inexistentes. Luego, el propio Arancibia Campos, simplemente faltó a la verdad en los informes que remitía a la superioridad cuando se le consultaba por dicha situación, generando que la policía de investigaciones, formalmente informara a la Fiscalía que las ordenes encargadas e instrucciones impartidas ya estaban cumplidas y que habían sido informadas en los oficios que mencionaba, que en resumen no correspondía a la realidad. Además, el señor Arancibia campos, no solo realizó las acciones descritas respecto de las ordenes de investigar e instrucciones emanadas de la Fiscalía Local de Talcahuano, sino que también adulteró la información relativa a órdenes de aprehensión y arresto emanadas de los tribunales de Justicia.

- **Decisión del tribunal:**

Se condenó a Marcos Teamar Arancibia Campos, a cumplir una pena de sesenta y un dias, de presidio menor en su grado mínimo accesoria legal de suspensión para cargos y oficios públicos por el tiempo de la condena, en su calidad de autor del delito que previene el artículo 22 de la ley orgánica Constitucional de la Policía de investigaciones de Chile en grado de consumado. Igualmente al pago de una multa ascendente a una unidad tributaria mensual. Además, se condenó a Arancibia Campos, a una pena de sesenta y un días de presidio menor en su grado medio, accesoria legal de suspensión de cargo u oficio público por el término de la condena, como autor del delito informático que previene el artículo 3° de la Ley 19.223 en grado de consumado. Finalmente se condenó también a cumplir una pena de cuarenta y un días de prisión en su grado máximo, accesoria legal de suspensión de cargo u oficio público por el término de la condena en su calidad de autor del delito de Obstrucción a la Justicia, artículo 269 Bis del Código Penal, consumado.

- **Considerandos relevantes:** No procede.

- **Tribunal:** 8° Juzgado de Garantía de Santiago
- **Magistrado(s):** Alicia Gemma Rosende Silva
- **Fecha:** 01.09.2014
- **RUC:** 1300971941-k
- **RIT:** 9186-2013
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Everth Joshua Phillips Provoste Álvarez, Fernando Mateluna Bascuñán y Pablo Videla Yáñez, accedieron desde diversas, conexiones, entre ellas desde el domicilio particular, subiendo archivos modificados nombrados FOOTER HTML a los sitios web www.ahoranoticias.cl y www.megamujeres.cl, ambas administradas por el canal de Televisión Mega, el archivo modificado le permitió leer el virus previamente guardado por él, en el servidor FTP en la carpeta public_htm/jwebsite/especiale/megatestigos/ con lo que pudo obtener las claves para controlar el twitter corporativo de la estación Mega. Adicionalmente, efectuaron la distribución de un código malicioso que hacía referencia a un software de seguridad el cual utilizaba el nombre del plan de desarrollo institucional de la PDI llamado "minerva", posteriormente surgió una nueva distribución de código malicioso a través de un correo masivo relacionado con una cobranza judicial que mantenía el receptor del mensaje con DICOM e igual situación con Presto de la empresa Líder, es decir, mediante el envío de correos masivos con información que aparenta ser seria (como es el caso de la PDI o cobranzas judiciales de presto o Dicom) consiguieron infectar los computadores de aquellos usuarios que inadvertidamente abren estos correos. El denominado virus Minerva.exe, el cual fue enviado a un número indeterminado de personas, corresponde a un troyano que no tan sólo infecta a un computador, si no que más bien transforma al equipo computacional infectado en un robot esclavo o, en términos informáticos, en un terminal bot. Por definición los bot's pueden ser múltiples y, sin importar su ubicación geográfica, pueden mantenerse activos y conectados a través de internet a un servidor de IRC (Internet Relay Chat, protocolo de comunicación en tiempo real), pasando a ser "esclavos" del hacker que los domina. Lo anterior quiere decir que la suma de estos equipos conforma una red de bot's, es decir, una botnet. El creador de dicho código malicioso imparte instrucciones

directamente a través de un canal de conversación mediante las cuales puede obtener información de forma masiva de cada uno de los equipos infectados.

Todas estas redes de servidores institucionales fueron espiadas indebidamente mediante el uso de este mecanismo como se ha descrito, esta misma actividad la realizaron con los servidores del canal de Televisión Megavisión y con el programa Ahora Noticias, de este canal, que mantenía una cuenta activa en la red social twitter de nombre "ahora noticiascl" perfil que es administrado por el equipo de internet de prensa, y el día 01 octubre de 2013, alrededor de las 21 00 horas, las claves de acceso habían sido cambiadas por los imputados no logrando acceder a la cuenta quienes modificaron el contenido de la cuenta, adjudicándose esta acción como un hackeo el grupo denominado "santuario de la fiebre CCA" conformada por los imputados. La cuenta de Twitter tenía al momento del ataque más de 250.000 seguidores. A partir de ese momento los imputados controlaron la cuenta con los 250 mil seguidores y comenzaron a postear twitts con contenidos ideados por ellos entre otros relevando antecedentes personales de figuras públicas tales como ministro de estado. El imputado Provoste Álvarez, además de las conductas realizadas anteriormente, realizo otras conductas consistentes que en conocimiento de la cedula de identidad de funcionarios públicos tales como el Subcomisario Marcelo Gómez Cea, la Senadora Isabel Allende Busi, y del Subcomisario Andrés Godoy, a cargo de los informes policiales de la presente causa, obtuvo certificados de nacimiento para posteriormente proceder a bloquear su cedula de identidad, lo que luego público en la cuenta Twitter @hakerchilenos.

- **Decisión del tribunal:**

Se condenó a los acusados Pablo Andrés Videla Yáñez, Fernando Esteban Mateluna Bascuñán, y Everth Joshua Phillips Provoste Álvarez, a sufrir cada uno de ellos la pena de quinientos cuarenta y un días de presidio menor en su grado medio, suspensión de cargo u oficio público por el mismo plazo de la condena, más el comiso de las especies incautadas, por su participación de autores en el delito consumado de espionaje y sabotaje informático, al acusado Everth Joshua Phillips Provoste

- **Considerandos relevantes:** No procede.

- **Tribunal:** Juzgado de Garantía de La Serena
- **Magistrado(s):** Carlos Lorenzo Jorquera Peñaloza
- **Fecha:** 12.12.2014
- **RUC:** 1000571645-k
- **RIT:** 648-2009
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Hecho uno: En el período comprendido entre el 01 de febrero de 2010 y el 29 de abril de 2010, en horario de atención de público del Servicio de Registro Civil e Identificación, el acusado, actuando como funcionario de dicho servicio y en razón de su cargo en caja, utilizando su cuenta en el sistema computacional del referido servicio, manipuló y alteró dicho sistema, disminuyendo o rebajando fraudulentamente la valoración de los bienes del inventario en las solicitudes de posesiones efectivas de los usuarios, adulterando la información del Formulario de Solicitudes de Posesión Efectiva en a los menos 18 oportunidades dentro del período indicado, no ingresó a caja el dinero de los aranceles hereditarios, apropiándose indebidamente mediante el fraude y en su interés propio de una suma de dinero no inferior a $ 1.013.715, por cobros indebidos a usuarios del servicio, originando una pérdida al fisco por la suma indicada.

Hecho dos: Con fecha 05 de Febrero de 2010 y 17 de Febrero de 2010, en horas de la mañana, en horario de atención de público del Servicio de Registro Civil e Identificación, actuando como funcionario de dicho servicio y en razón de su cargo, falsificó las firmas de la solicitud de posesión efectiva de dos usuarios, ingresándolas al servicio con la firma adulterada, para la tramitación de la posesión efectivas impetradas por ellos.

- **Decisión del tribunal:**

Se condenó César Horacio Ireland Castillo, a la pena única de cuatrocientos dieciocho días de presidio menor en su grado mínimo más la accesoria de suspensión de cargo u oficio público durante el tiempo de la condena, como autor en un concurso medial de los delitos reiterados de sabotaje informático y de malversación de caudales públicos en grado de consumados. Se le

condena además, al pago de una multa de 6 Unidades Tributarias Mensuales. Además se le condenó a sufrir dos penas de sesenta y un días de presidio menor en su grado mínimo cada una de ellas más la accesoria de suspensión de cargo u oficio público durante el tiempo de la condena, como autor en dos delitos de falsificación de instrumento público.

- **Considerandos relevantes:** No procede.

- **Tribunal:** Juzgado de Garantía de La Serena
- **Magistrado(s):** Erick Fabián Ríos Leiva
- **Fecha:** 18.05.2015
- **RUC:** 1100470439-k
- **RIT:** 1751-2014
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Entre los meses de febrero de 2009 y noviembre de 2010, en el interior de las dependencias de la Universidad de La Serena, los acusados, en el ejercicio de sus cargos, en su calidad de funcionarios administrativos de la sección de remuneración del departamento de personal de la referida institución educacional pública, intervinieron en el proceso de pago de remuneraciones del personal universitario, aumentando indebidamente sus liquidaciones de sueldo correspondientes a los meses de marzo de 2009 a noviembre de 2010. Para ello, el acusado Carlos Javier Rojas Herrera, alteró maliciosamente los datos del sistema informático financiero denominado Phoenix, sistema que contenía la información relativa a las remuneraciones del personal universitario, consignando e ingresando a este software en los formularios de pago de remuneración de ambos acusados, mes a mes, en 21 oportunidades, durante el período antes referido, dos asignaciones universitarias, la primera por un porcentaje equivalente al 100 % de su sueldo base, suma que fluctuaba entre $536.237 y $560.368 y la segunda, por un monto de $110.000, en circunstancias que por concepto de asignación universitaria, a ambos funcionarios sólo les correspondía una suma equivalente al 3 % de su sueldo, por un monto aproximado de $17.000. Posteriormente, las referidas propuestas de liquidaciones de sueldo fueron revisadas y aprobadas por el acusado Carlos Hernán Latorre Silva, quien sabía de la alteración de los datos ingresados a los formularios de remuneraciones, logrando de esta forma obtener la respectiva resolución de pago de sueldo percibiendo indebidamente, cada imputado de parte del Fisco la suma de $13.514.034, causando un perjuicio económico al erario fiscal que asciende a la suma de $ 27.028.068.

.

- **Decisión del tribunal:**

Se condenó a Carlos Hernán Latorre Silva y a Carlos Javier Rojas Herrera , ya individualizados, por su participación en calidad de autores de veintiún delitos consumados de fraude al fisco previsto y sancionado en el artículo 239 del Código Penal, a sufrir cada uno las penas de quinientos cuarenta y un días de presidio menor en su grado medio, multa de un diez por ciento del monto defraudado. Se condenó asimismo a Carlos Javier Rojas Herrera, por su participación en calidad de autor de veintiún delitos consumados de sabotaje informático previsto y sancionado en el artículo 3 de la Ley 19.223, a sufrir las penas de sesenta y un días de presidio menor en su grado mínimo y la accesoria legal de suspensión de cargo u oficio público durante el tiempo de la condena, eximiéndosele del pago de las costas de la causa.

- **Considerandos relevantes:** No procede.

- **Tribunal:** Juzgado de Garantía de Curicó
- **Magistrado(s):** Jorge Omar Valenzuela Navarro
- **Fecha:** 04.09.2015
- **RUC:** 1301170732-1
- **RIT:** 7226-2013
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Hecho uno: Que desde el mes de octubre de 2013 y hasta a principios de diciembre del mismo año el imputado Miguel Ángel Ruiz Ceballos, utilizando sus conocimientos computacionales se apoderado de las claves computacionales del listado de personas señalados en la acusación, sin consentimiento ni conocimiento de estas, suplantándose por ellos y solicitando a terceros dineros de los que se apropió y que se indican en la acusación.

Que para operar en la forma descrita utilizaba correos electrónicos. Primero buscaba a una persona de su confianza, reclutador, el que debe suministrar una cuenta donde depositar el dinero y un Rut. Luego accede a los computadores de sus víctimas, los que interviene a través de un virus, captura sus claves bancarias (pharming) y transfiere dineros a la cuenta que le señala el reclutador. Una vez que el dinero es retirado de esta última cuenta se reparten el producto entre ambos, mitad y mitad. Señala además que vulneraba las cuentas de correos electrónicos gmail y hotmail. Que registró el sitio www.lanzadorx.com portal dedicado a modificar datos de los correos electrónicos, los que ingresaba al citado portal, las desencriptaba previo pago vía paypal donde se le cobraba entre dos a cinco dólares por clave. Que una vez tomado el control del correo, modificaba la casilla secundaria y así su legítimo titular no podía acceder a su cuenta.

Hecho dos: A contar del año 2010 en adelante Miguel Ángel Ruiz Ceballos, en la Región del Maule, capturó información de las cuentas corrientes de diversas personas y transfirió fondos de estas a cuentas de terceros sin la voluntad de sus titulares. En una segunda modalidad infectó equipos informáticos con el objetivo de apoderarse de cuentas electrónicas, principalmente correos y perfiles de redes sociales a fin de controlarlas y mediante engaños hacerse de dineros ajenos los que eran depositados en cuentas de terceros que eran reclutados por Agustín Villagra González, con quien se repartía las utilidades.

- **Decisión del tribunal:**

Se condenó a Miguel Ángel Ruiz Ceballos, a la pena de ochocientos días de presidio menor en su grado medio , suspensión de cargo u oficio público durante el tiempo que dure la condena, como autor del delito de sabotaje informático reiterado, previsto y sancionado en el artículo 2 de la ley 19.223 y a la pena de quinientos cuarenta y un días de reclusión menor en su grado medio como autor del delito de estafas reiteradas, previsto y sancionado en el artículo 473 del Código Penal, multa de once Unidades Tributarias Mensuales.

Se condenó a Ulises Aguilar Bravo, a la pena de trescientos días de presidio menor en su grado mínimo, accesorias legales de suspensión de cargo u oficio público durante el tiempo que dure la condena, como autor en grado de consumado del delito de sabotaje informático, previsto y sancionado en el artículo 2 de la ley 19.223, como autor del delito de y a la pena de cien días de presidio menor en su grado mínimo y suspensión de cargo u oficio público mientras dure la condena, por el delito de estafas reiteradas, multa de tres Unidades Tributarias Mensuales por los hechos previstos y sancionados en el artículo 470 y 468 inciso final del Código Penal.

- **Considerandos relevantes:**

16° Que en cuanto a la petición de la defensa de RUIZ CEBALLO, en el sentido que se trata de un solo delito, lo cierto y concreto que el artículo 2 de la ley 19.223, sanciona una conducta diferente al delito de estafa tipifica 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. Que el modus operandi fue la interceptación y apoderamiento de la información contenida en un correo electrónico, en una cuenta bancaria y esa sola conducta tipifica el delito informático. Basta invadir la privacidad de un sistema informático para cometer el delito.

- **Tribunal:** 7° Juzgado de Garantía de Santiago
- **Magistrado(s):** No consta de la Sentencia.
- **Fecha:** 02.10.2015
- **RUC:** 1410003541-4
- **RIT:** 2365-2014
- **Procedimiento:** No consta de la Sentencia.
- **Síntesis de los hechos:**

Durante los días 16 de diciembre de 2013 y 23 de enero de 2014, desde las oficinas del Banco Consorcio, el imputado Javier Eduardo Oyarce Salinas procedió a alterar maliciosamente las base de datos informáticas del Banco consorcio sin la autorización de este utilizando el lenguaje de consulta de base de datos "pl/sql", a través del usuario "joyarce", procediendo a realizar abonos por $16.750.000 pesos a través de siete operaciones dirigidas a la cuenta bancaria de Nataly Consuelo Orrego Flores, las que después fueron transferida desde esta última a la cuenta corriente, a nombre de Gabriel Oyarzún, que en realidad pertenece al imputado. Luego de realizado los abonos, el imputado utilizó un comando de consulta para borrar en los registros informáticos los abonos realizados, utilizando para ello el usuario "FISA CREDITOS".

- **Decisión del tribunal:**

Se condenó a Javier Eduardo Oyarce Salinas a la pena de 541 días de presidio menor en su grado medio, y al pago de una multa de 1 UTM, más la accesoria de suspensión de cargo u oficio público durante el tiempo que dure la condena. Por la participación en calidad de autor en los delitos de Espionaje Informático y Estafa, en grado de desarrollo consumado.

- **Considerandos relevantes:** No procede.

- **Tribunal:** 8° Juzgado de Garantía de Santiago
- **Magistrado(s):** Sergio Guillermo Córdova Alarcón
- **Fecha:** 25.11.2015
- **RUC:** 0910000486-8
- **RIT:** 199-2009
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Los imputados Germán Gutiérrez Smith y Roberto Fredes Besoaín, desde al menos el día 16 de junio de 2005 y hasta el día 30 de junio de 2008, se concertaron para que Gutiérrez Smith, a la sazón encargado de crédito y cobranza de la víctima Petroquim S.A., procediera a realizar una serie de maniobras fraudulentas en el sistema informático de la misma, denominado JD_EDWARDS, con el fin de alterar el mismo de manera maliciosa, para beneficiar de esta manera a la empresa Bagsa chile S.A., cliente habitual de Petroquim S.A., de la cual el acusado Fredes Besoaín era su dueño, controlador y representante, alterando en tal sistema los datos de individualización de Bagsa Chile S.A. y las fechas de vencimiento de las facturas de venta respectivas, prorrogándolas sin que ello fuera procedente o autorizado por los superiores de Gutiérrez Smith, con el fin de mantenerlas indefinidamente en estado de pendientes de vencimiento en el sistema y de esta forma, evitar o retardar lo máximo posible el subsecuente cobro de las mismas. De esta manera, el imputado Gutiérrez Smith procedió a realizar diversos actos que tendieran a alcanzar los fines señalados. Así, procedió en primer lugar a cambiar en el sistema JD_EDWARDS el nombre del cliente Bagsa Chile S.A. por el de otro cliente de Petroquim S.A., la compañía de Mallas y plásticos S.A., cliente que ya figuraba registrado en el sistema, quedando en consecuencia, Bagsa Chile S.A., registrado dos veces en el mismo. Una de ellas con su Rut verdadero y con las operaciones que le correspondían y la segunda de ellas con el Rut de Mallas y plásticos S.A., con las operaciones que le correspondían a tal empresa, cuestión que ocasionó el ocultamiento de todas las ventas a dicha empresa, puesto que en el sistema quedaron entonces registradas como hechas a la compañía Mallas y plásticos S.A., para luego, adicionalmente, procedió alterar en el sistema informático mencionado, las fechas de vencimiento de las facturas emitidas por Petroquim S.A. a Bagsa Chile S.A. con ocasión de ventas de productos a esta última, prorrogándolas indefinidamente, evitando de este modo la

cobranza de las sumas respectivas, que no eran pagadas por Bagsa Chile S.A. Adicionalmente, procedió a imputar en el sistema informático de la víctima, un pago que realizaron otros clientes de la misma otro cliente de la misma: las empresas Polifilm, Norsac, Plastisacks y Embalex.

Lo anterior provocó entonces, que una serie de deudas contraídas por Bagsa Chile S.A., con el actuar concertado de ambos imputados, quedaran impagas y en definitiva, perjudicada la víctima en dichos montos y beneficiado, principalmente, el acusado Fredes Besoaín de dicha circunstancia.

- **Decisión del tribunal:**

Se condenó a German Eduardo Gutiérrez Smith a la pena corporal única de quinientos cuarenta días de presidio menor en su grado mínimo, en calidad de autor de 4 delitos de sabotaje informático, previstos y sancionados en el artículo 3° de la ley 19.223 en grado de desarrollo de consumados y 4 delitos de estafa, previstos y sancionados en el Art. 473 del Código Penal, en carácter de reiterados.

- **Considerandos relevantes:** No procede.

- **Tribunal:** Juzgado de Garantía de Quillota
- **Magistrado(s):** Nancy Amalia Riffo Zúñiga
- **Fecha:** 30.12.2015
- **RUC:** 1500048128-6
- **RIT:** 1911-2015
- **Procedimiento:** Simplificado
- **Síntesis de los hechos:**

El día 30 de diciembre de 2014, en diferentes horas del día, la imputada V.J.M.N., de 17 años a la fecha de los hechos, ingresó desde su computador personal y desde uno de los computadores de la oficina de su madre, a la página web del Departamento de Evaluación, Medición y Registro educacional (DEMRE) utilizando para ello el nombre de usuario y contraseña de la víctima V.V.S.A., accediendo con ello a la postulación realizada por esta última para el proceso de selección universitaria, alterando maliciosamente los datos ingresados por la víctima en el sistema de postulación del DEMRE, modificando no solo las universidades a las que la víctima había postulado, sino también a las carreras por las cuales había manifestado su preferencia. De esta forma, y atendida la adulteración ocurrida en la ficha de postulación de la víctima, el DEMRE determinó que aquella no podía considerarse válida, teniéndola como no presentada para todos los efectos, perdiendo la posibilidad de ingresar a la Universidad a través de ese proceso de selección.

- **Decisión del tribunal:**

Se condenó V.J.M.S. la pena del pago de una multa de una (1) unidad tributaria mensual a beneficio fiscal, por su responsabilidad de autora del delito de Sabotaje informático, del artículo 3 de la Ley 19.223, ejecutado en grado de consumado.

- **Considerandos relevantes:** No presenta.

- **Tribunal:** Juzgado de Garantía de Concepción
- **Magistrado(s):** Ana María Fierro Oyarzo
- **Fecha:** 31.12.2018
- **RUC:** 1410003541-4/1410015476-6
- **RIT:** 4775-2014
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Ricardo Romualdo Domínguez Pérez, en el período junio de 2012 a mayo de 2013, utilizando de manera indebida las claves de acceso y privilegio que se le habían otorgado, en su calidad de jefe de gestión operativa de banca grandes empresas, del banco BBVA sucursal Concepción, procedió a acceder al sistema de tratamiento de información del Banco BBVA, alterándolo ingresando en al menos dieciséis oportunidades, datos falsos consistentes en registrar como canceladas dieciséis boletas de garantía de diversos clientes tomadas al contado, que se encontraban vencidas, registrando el valor de cada una de esas boletas en otras cuentas contables del banco, traspasando luego parte de esos valores a su propia cuenta corriente y parte a cuentas de terceros, apropiándose de las sumas así sustraídas, destinándolas a sus fines particulares, causando un perjuicio al banco, quien sigue obligado a pagar a sus clientes, ascendente a un total de $ 11.592.999.

- **Decisión del tribunal:**

Se condenó a Ricardo Romualdo Domínguez Pérez, ya individualizado, a la pena de quinientos cuarenta días de presidio menor en su grado mínimo y accesoria legal de suspensión de cargo u oficio público durante el tiempo de la condena, por su responsabilidad como autor de un delito continuado de hurto simple agravado, previsto y penado en el artículo 446 N°1 en relación a los artículos 432 y 447 del Código Penal y de dieciséis delitos de sabotaje informático, bajo la figura de “alteración de datos”, previstos y penados en el artículo 3 de la Ley N°19.223, en concurso ideal impropio, perpetrados en el territorio jurisdiccional de este tribunal, en el periodo comprendido entre el mes de junio de 2012 al mes de mayo de 2013, en perjuicio de Banco BBVA.

- **Considerandos relevantes:**

Quinto: Que, los hechos establecidos, se enmarcan en primer término dentro del tipo penal de hurto agravado, previsto y sancionado en el artículo 446 N°1 del Código Penal en relación al artículo 447 del mismo código, desde que ha existido una apropiación de dinero, la suma ascendente a $11.592.999, cosa mueble ajena, perteneciente al banco BBVA, para el que el hechor se desempeñaba en el cargo de jefe de gestión operativa de banca grandes empresas sucursal Concepción, apropiación que realizaba mediante los privilegios que tal cargo le proporcionaba, por el uso de una clave personal e intransferible que le permitía registrar como canceladas boletas de garantía de clientes tomadas al contado y registrar sus valores en otras cuentas contables del banco afectado, para traspasar finalmente esos valores a su propia cuenta corriente y a cuentas de terceros, algunos de ellos familiares, accionar ignorado por su empleador y por tanto, efectuado sin su voluntad y con ánimo de lucro, desprendiéndose este último elemento del tipo de su propia declaración en la que reconoce que el asumir una deuda clínica por un monto aproximado de catorce millones de pesos gatilló el desorden de sus cuentas personales, realizando lo que coloquialmente denomina “bicicleta bancaria”, haciendo uso de sus niveles de acceso y privilegios bancarios, radicándose el perjuicio causado por el ilícito en el que era a la época de los hechos y desde el año 1993 su empleador, que configura el tipo agravado, por ser un dependiente del banco que debió y deberá asumir la fraudulenta (en sentido profano) cancelación registral de las boletas de garantía, que permanecen en su materialidad y funcionalidad en poder, por lo general del beneficiario, conforme a las obligaciones garantizadas por tal documento hasta su cobro efectivo, desde que este acto ilegítimo no afectó a la materialidad ni funcionalidad de la boleta bancaria de garantía.

Más adelante, en cuanto a la independencia entre un sistema informático y las obligaciones generadas por el tráfico mercantil: Establecida la posibilidad de emisión de tal instrumento como una de las operaciones de banco consagrada por el legislador en el artículo 69 N°13 de la Ley General de Bancos y definida en el apartado 1.1. del Capítulo 8-11 de la Recopilación Actualizada de Normas de la Superintendencia de Bancos e Instituciones Financieras como una caución que constituye un banco, a petición de su cliente llamado el 'Tomador' a favor de otra persona llamada 'Beneficiario' que tiene por objeto garantizar el fiel cumplimiento de una obligación contraída por el tomador o un tercero a favor del beneficiario, el blindaje otorgado

por su inembargabilidad, permite concluir que una cancelación indebida, fuera de los parámetros estrictos establecidos tanto por la costumbre mercantil como por la legislación traída a colación, no puede comprometer un mecanismo de garantía bancarizada de gran solidez y eficacia, ergo el tráfico jurídico-mercantil, por la falibilidad de un sistema de tratamiento informático. De ahí que concluye esta sentenciadora la absoluta independencia de estos instrumentos de lo registrado en un sistema informático de un privado, manteniéndose intacta tanto la relación causada de tomador y beneficiario y sus obligaciones como las que vinculan a tomador y beneficiario con el banco, conservando plena vigencia la comisión de pagar sin condición, debiendo asumir las pérdidas por su falta de control de las boletas vencidas por parte de los gestores o los jefes de operaciones.

Más adelante, en cuanto a la no tipificación del delito de fraude informático en nuestro país: Desechada la posibilidad de que la afectación patrimonial se radique en los depósitos constituidos por los tomadores de las boletas bancarias de garantía, corresponde ahora determinar la concurrencia de los elementos del tipo en base a los antecedentes investigativos. Para la acreditación de la apropiación de cosa mueble, se cuenta en los antecedentes que obran en la carpeta investigativa fiscal con la declaración de Andrea Bugmann Quezada, contenida en el informe policial N°2459/00816 de la Brigada Investigadora de Delitos Económicos de Concepción de la Policía de Investigaciones de Chile, al referir en su calidad de agente de la sucursal en que el imputado se desempeñaba como jefe de operaciones grandes empresas, la génesis de la develación del ilícito, al ser notificada en el mes de agosto del año 2013 que un cliente solicitó el reintegro de una boleta de garantía que ya había sido cancelada contablemente, lo que originó una investigación interna que reveló la cancelación de nueve boletas de garantía que sumaban un valor total de $7.039.142, que habían sido cancelados y transferidos a la cuenta personal del denunciado sin dejar respaldo por escrito de dichas operaciones, de las cuales existe registro en los sistemas, que es el núcleo del elemento objetivo de la conducta apropiatoria de cosa mueble, de paso ajena, como lo es el dinero perteneciente al banco, en ausencia de un delito de fraude informático o estafa de computación (Computerbetrug &263 a) StGB) tipificado en nuestro país, pues el dato informático adulterado por el hechor, con esta cancelación ficticia, pero registrada como tal, de boletas de garantía que tanto en su materialidad como en las obligaciones personales que de ella emanan se mantienen intactas, hace recaer precisamente la

apropiación en el dinero perteneciente al activo del banco, pues en realidad esta cancelación registral no produce efecto de extinguir los derechos y obligaciones de tomador y beneficiario del documento, por la falibilidad del sistema de tratamiento de información del banco a quien se mandató esta operación.

Más adelante y en relación con la naturaleza de dato informático: conforme a los dichos de la auditora del banco y testigo Claudia Oyarce, quien clarifica la conducta apropiatoria efectuada por el imputado en el marco de sus posibilidades, desglosando cada una de las boletas canceladas, traducida básicamente la evidencia de una cosa mueble incorporal como lo es un "dato informático", contenido en un sistema de tratamiento de información de un privado, banco BBVA, en que el soporte lógico de los ordenadores son en sí mismos información, tanto la extraída del terminal CQ09, que era el equipo usado por el imputado, a la que accedía con su clave H090693(…)

Se trata de un hurto calificado por la calidad del sujeto activo, llamado también hurto doméstico, pues el señor Domínguez era ni más ni menos que el jefe de gestión operativa de banca grandes empresas del banco BBVA, con quien existió una relación trabajador-empleador, que se extendió por veinte años, como dan cuenta copia del finiquito, declaración de los testigos Bugmann, Díaz y Medina Müller, que si bien puede o no penarse con mayor severidad, conlleva tanto la violación de la confianza puesta en el dependiente como el debilitamiento de la defensa del afectado, sobre todo al alero de una relación extendida por tanto tiempo, que lo habilitaba con un código usuario de amplias facultades, con capacidades supervisoras incluso de quienes han declarado como testigos en esta causa, los ejecutivos a cargo de cuentas de empresas, perpetrados en la misma sucursal en la que se desempeñó desde el año 2010 en su último cargo.

Esta conducta desplegada por el hechor en el transcurso de aproximadamente un año, conforme a la fecha de abono de los dineros sustraídos en su cuenta corriente desde el 18 de junio de 2012 a 5 de junio de 2013, si bien comprende pluralidad de acciones, por los dieciséis abonos en la cuenta del imputado de dineros provenientes supuestamente de las boletas bancarias mal

canceladas, pudiendo cada una de ellas satisfacer el tipo de hurto mediando este año entre la primera y la última acción, resultando ser el sujeto pasivo en todas éstas el empleador del hechor Banco BBVA, constituyen la violación necesariamente fraccionada de una misma norma de deber, pues conforme a la representación del autor, no era posible consumarla sino en esta forma. Hemos llegado a la conclusión de que existe un delito continuado y no un concurso material, analizando la imposibilidad del hechor de acceder a la suma de $11.592.999 en un solo acto conforme a su modus operandi, que requería por cierto, que las boletas de garantía se encontraran vencidas y contando todas ellas con distintas fechas de vencimiento, consta en los antecedentes que obran en la carpeta investigativa fiscal que los abonos a la cuenta corriente del imputado o de terceros relacionados con él, se realizaron en cada una de las ocasiones en fechas muy próximas al vencimiento, la mayor parte de los traspasos a menos de un mes, inmediatez que guarda relación con los motivos que reconoce en su declaración, lo condujeron a perpetrar este ilícito, la deuda clínica que mantenía por catorce millones de pesos derivada de la enfermedad de su hermana María Angélica Domínguez Pérez, que padeció de cáncer terminal y falleció hace unos cuatro años (…)

En cuanto a la forma de ejecución de delito informático del artículo 3° de la ley 19.223: Si bien el hechor admite en su declaración que iba cubriendo lo sustraído a medida que podía, manipulando el sistema por la alteración de la cuenta corriente del beneficiario, accionar que podría denotar el tratar de impedir el descubrimiento del ilícito, agrega a continuación que su intención fue rembolsar los dineros dubitados, movido en su accionar por la desesperación de cubrir sus deudas, las que se corroboran con el registro de once páginas de sus doscientas cuarenta y tres acreencias y doscientas sesenta deudas desde el año 2009 a 2014, por lo que fluye con mayor naturalidad de los antecedentes investigativos un accionar fraccionado por la necesidad impuesta por la naturaleza de los documentos cancelados contablemente, a través de la manipulación del sistema efectuado por el hechor.

Dicho delito configurado se encuentra en concurso ideal impropio con dieciséis delito reiterados y consumados de sabotaje informático en la forma de alteración de datos, previstos y penados en el artículo 3 de la Ley 19.223.

Mas adelante y en cuanto al modo de ejecución del delito del artículo 3° de la ley 19.223: (...) el modus operandi de éste consistía en modificar e intervenir los sistemas, borrando la cuenta corriente asociada al beneficiario de la boleta y colocar otra cuenta de carácter contable, de la cual realizaba otra transacción, para posteriormente transferirlas a cuentas personales o de terceros.

(…)Como corolario de todos estos antecedentes investigativos el propio imputado en su declaración se refiere a su accionar señalando que su nivel de acceso "H090693" era el que lo identificaba como funcionario del banco, con atribuciones completas de supervisor en el área de operaciones, teniendo acceso al control de las cajas, sistemas computacionales y cuentas de todo tipo en calidad de autorizador, privilegios bancarios de los que se valió para cancelar diversas boletas de garantía que pertenecían a varios clientes de la banca empresas, manipulando el sistema por la alteración de la cuenta corriente del beneficiario, para que se cancelaran en una cuenta contable del banco BBVA, de la cual posteriormente transfería a su cuenta corriente personal N°96010001407 del banco BBVA, lo que no hace más que corroborar la documentación

que integra los set a los que la testigo Oyarce (…) incurriendo en dieciséis delitos de sabotaje informático, bajo la figura de alteración de datos, prevista y penada en el artículo 3 de la Ley 19.223, resultando ser el sujeto activo del delito un empleado del banco con un puesto de confianza, con el fin de provocar una transferencia de activo patrimonial del banco, en perjuicio de éste y si bien en principio doctrinalmente enfrentamos un fraude informático, no encontrándose éste tipificado en nuestra legislación, se ha dado por establecido el referido delito, descartando cualquier otro no cubierto en todos sus elementos como éste de mayor simpleza, que requiere sólo de alteración de datos, aunque no existiese perjuicio alguno para el administrador del sistema de tratamiento de información, pues lo relevante es que se afecte el soporte lógico del sistema, lo que hizo al ingresar información no fidedigna en el sistema registral mediante una cancelación improcedente, que sólo en el sistema puede producir efecto no así en la boleta de garantía como evidencia de la caución que involucra tal documento.

En cuanto al bien jurídico Protegido: (...)Sin embargo, al alero de nuestra deficiente legislación en materia de delitos informáticos, lo que se ha afectado como bien jurídico protegido es la

información, pues conforme a la historia de la Ley 19.223, el autor de la moción que la origina, diputado Antonio Viera Gallo, fundamentando su propuesta señala que el propósito que se persigue es proteger la calidad, pureza e idoneidad de la información contenida en un sistema automatizado de tratamiento de la misma, y los productos que de su operación se obtengan, opinión sostenida por el autor Hernán Silva en su libro "Las Estafas, Doctrina, Jurisprudencia y Derecho Comparado", Editorial Jurídica, páginas 214 y siguientes (sobre la criminalidad informática v. también la obra de Manuel Jaén Vallejo, Estudios Penales, Editorial Lexis Nexis, páginas 136 y siguientes).

En cuanto al modo de ejecución del delito del artículo 3° de la ley 19.223: Los antecedentes investigativos llevan a concluir que entre todas las maniobras realizadas por el hechor, alambicadas y difíciles de rastrear, para conseguir la apropiación de dinero del banco sin su voluntad, obteniendo el fin ilícito que pretendía, ingresando datos falsos al sistema de tratamiento de información del banco con el uso indebido de su clave privilegiada, de paso personal e intransferible, esta alteración de datos fue una más de las acciones de que debió valerse para conseguir su fin, pues adicionalmente los respaldos de las boletas de garantía físicos, consistentes en el set de contrataciones la boleta, que debían estar en la oficina, no fueron encontrados en ésta, pensando la auditora que el imputado debió destruirlos y si bien es cierto no lo afirma como conclusión en su declaración, dicha desaparición resultaba indudablemente indispensable para que el hechor consiguiera su propósito y si como asevera, en este accionar no intervino ninguna otra persona, las normas de la experiencia llevan a concluir que debió tener injerencia en esta pérdida, pues con este respaldo físico ningún sentido tendría manipular los datos del sistema si se buscaba la impunidad, en un engranaje en que la manipulación de datos era una acción no sólo de relevancia sino el medio necesario para la comisión del hurto continuado, desde que sin esta alteración de datos de nada hubieran servido el resto de sus maniobras, resultando imposible de eludir cualquiera fuese la forma que imprimiese a la ejecución material de su designio, de lo que aparece razonable conceder al autor un tratamiento más benévolo que si hubiera incurrido en un concurso real de delitos, pues aunque en verdad ejecutó dos acciones, unificadas en su exteriorización, abarcadas por su voluntad de realización, una de ellas, la alteración de datos fue impuesta por las circunstancias concurrentes, que limitó su libertad de decisión dentro de sus posibilidades.

En cuanto a la relación concursal del delito de hurto agravado y el delito de alteración de datos: Octavo: Respecto al concurso ideal impropio, por lo dispuesto en el inciso 2° del artículo 75 del Código Penal, corresponde imponer la pena mayor asignada al delito más grave, que en la especie resulta ser la asignada al delito de sabotaje informático por alteración de datos y no la del delito continuado de hurto agravado como han impetrado los intervinientes. En efecto, la pena asignada al delito informático de alteración de datos es la de presidio menor en su grado medio, luego tratándose de una reiteración de delitos de la misma especie, conforme a la regla establecida en el artículo 351 del Código Procesal Penal, la pena se puede aumentar en uno o dos grados y de aumentarse sólo en uno, estaríamos ya en el margen de presidio menor en su grado máximo, resultando más benévolo este tratamiento que la acumulación material de la pena, para dieciséis delitos.

Resolviendo primeramente este concurso material corresponde ahora estudiar cuál es el tratamiento penal de un delito continuado, desechando en este punto las alegaciones del persecutor en cuanto a considerar que debe penarse conforme a lo dispuesto en el artículo 451 del Código Penal, puesto que no hay casi discusión en la actualidad de que esta norma se refiere a reiteración de hurtos, en que existen varios delitos y por ello toma por base el importe total de lo sustraído, sumatoria improcedente para lo que hemos establecido en el considerando quinto de esta sentencia como un delito continuado de hurto, siendo aplicable la regla del inciso 2° del artículo 75 del código punitivo, por el ineludible fraccionamiento de las acciones apropiatorias continuadas en relación de "medio a fin", debiendo imponerse la pena mayor asignada al delito más grave, que es la de hurto del artículo 446 N°1 del Código Penal, castigado con presidio menor en su grado medio a máximo y multa de once a quince unidades tributarias mensuales, al exceder lo sustraído cuarenta unidades tributarias mensuales (…)

Sin la facultativa regla de elevación de pena para el hurto agravado de dependiente, que como arbitrio judicial no puede servir para analizar cuál es la pena mayor asignada al delito más grave, conforme al tenor literal del artículo 447 del código punitivo, lo cierto es que si bien ambos ilícitos, resuelto previamente el concurso material, cuentan con idéntico límite superior, comparando el inferior, resulta ser que el hurto es castigado con menor severidad en este tramo, al ser sancionado con presidio menor en su grado medio si tenemos presente que cada grado es una pena.

Decidido por esta sentenciadora que el delito más grave es el sabotaje informático, corresponde aplicar al concurso ideal la pena de presidio menor en su grado máximo, pues efectivamente se elevará la pena sólo en un grado, a pesar de su número, considerando que esta manipulación de datos reiterada obedece a la necesidad de disminuir el riesgo de ser descubierto, por eso no se configura un delito continuado en este caso, confiriendo los dichos de la testigo Oyarce, asidero a la búsqueda de impunidad del autor, quien en lo que a la alteración de datos incide, expresa que fue muy difícil de rastrear cada una de estas acciones, a tal punto que finalmente termina por relacionar sólo la cancelación de la boleta con la cuenta corriente del imputado o terceras personas, pero no es capaz de conocer el destino final de todo lo sustraído ni los movimientos entre distintas cuentas del propio banco, existiendo un ámbito que queda en una nebulosa en información que puede rastrearse, pero que requiere una investigación minuciosa que implica la intervención del sistema informático del banco en su totalidad y que asegure debidamente la cadena de custodia de evidencia digital, que como tal requiere interpretación, conservación oportuna y eliminación de cualquier duda sobre su legitimidad, rescatando archivos enmascarados y borrados que implican el empleo de herramientas técnicas diseñadas al efecto, contrariedades que pueden explicar el optar por un procedimiento en que se juzga un caso en base a actas con información que emana básicamente del propio afectado por el delito, conductas que deslindan tenuemente con el delito continuado, pero que atendidas las manifestaciones de un fin de impunidad cuando el objeto del delito es la alteración de datos de un sistema de tratamiento de información, sea el bien jurídico protegido la pureza de la información o su confidencialidad, no el patrimonio, descartado un fraude informático no tipificado en nuestro país, aceptando el análisis de todas estas conductas bajo el lente del injusto - en palabras de Cury- debe concluirse necesariamente la existencia de pluralidad de delitos informáticos. Favoreciendo al acusado dos circunstancias atenuantes, sin que lo perjudiquen agravantes, conforme a lo establecido en el artículo 67 del Código Penal, esta sentenciadora se encuentra facultada para rebajar la pena hasta en dos grados a partir de este nuevo marco, procediendo a la rebaja en dos grados, ponderando la entidad de las atenuantes concurrentes, conforme a lo razonado en el considerando séptimo de esta sentencia en lo que dice relación a la aminorante de colaboración sustancial, al que este tribunal se remite en su apreciación y en relación a la mayor entidad de la de irreprochable conducta anterior basta resaltar el hecho de que el imputado no sólo no registra condena alguna en su extracto de filiación y antecedentes penales sino que

tampoco existe antecedente en el registro de sistema de apoyo a fiscales de otra causa en que intervenga en calidad de imputado como tampoco existe orden de detención en su contra, suspensión condicional del procedimiento o medidas cautelares, estimando esta sentenciadora muy meritoria esta ausencia de antecedentes para una persona de cincuenta y un años de edad. En el tramo de presidio menor en su grado mínimo, estando a la extensión del mal causado, por el ilícito que en concepto de esta sentenciadora es el más grave no sólo por la pena, sino por el bien jurídico afectado, el delito de sabotaje informático, que aun en ausencia de la tipificación de fraude informático, no impide a esta sentenciadora evaluar la vulneración que implica para la víctima ver burlados sus sistemas registrales, pues ciertamente más allá del patrimonio perdido, que el imputado se vio en imposibilidad de restituir, a pesar de su oferta inicial, plasmada en su declaración en sede policial, lo que causa y causará mayor perjuicio al banco BBVA, es admitir una falla en sus mecanismos de control de boletas de garantía vencidas, por parte de los gestores o jefe de operaciones (que debe ser la razón para no sancionar a otros funcionarios del banco) una de las conclusiones de la auditoría efectuada por la testigo Oyarce, al admitir que no existe normativa al respecto, lo que a la vez descarta el engaño a una persona determinada, pero no por ello deja de asombrar la falibilidad de sus sistemas de tratamiento de información, por alguien que no cuenta con mayores conocimientos informáticos, tratándose sólo de un usuario con acceso privilegiado, con un puesto de control, pero que igualmente fue capaz de introducir modificaciones que provocaron la transmisión no consentida de activos patrimoniales de una institución que se supone debe resguardar los dineros puestos a su recaudo, por todos sus clientes, comprometiendo no sólo los intereses del banco que asumió finalmente los costos de su falta de adecuado control, pues podría tener implicancia en bienes jurídicos diversos al patrimonio e información, de llegar a otra instancia, desde que los registros informáticos generan rastros que los clientes del banco asumen como privados y que pueden ser monitoreados más allá de lo que implica la investigación de una causa, sin que exista método alguno de manejo forense de evidencia digital, que resguarde apropiadamente esta privacidad, por lo que se impondrá la pena dentro de este tramo en su máximo (En cuanto a la prueba informática v. al autor Daniel Petrone en su obra “Prueba Informática”. Ediciones Didot. Buenos Aires, 2014).

- **Tribunal:** 8° Juzgado de Garantía de Santiago
- **Magistrado(s):** Daniel Aravena Pérez
- **Fecha:** 25.08.2016
- **RUC:** 1400481698-7
- **RIT:** 4602-2014
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

El 16 de mayo de 2014, a las 13:00 horas aproximadamente, el requerido Rodrigo Candia Salas concertado con sujetos desconocidos y con el ánimo de defraudar a la víctima concurrió a una sucursal del Banco de Chile y una vez allí se acercó al mesón de atención de clientes donde presentó su cédula de identidad consultando por un vale vista que debía serle emitido, el asistente de atención le indicó que tal documento no figuraba en el sistema, procediendo el requerido de inmediato a comunicarse con un tercero mediante el celular que portaba a quien señaló "jefe no está el vale vista", para en seguida volver al mesón a consultar si el vale vista ya aparecía en el sistema, verificando el asistente que efectivamente ahora sí estaba el referido documento a nombre del requerido, atendido lo cual el asistente emitió el vale vista solicitado y lo entregó al requerido quien se acercó a la caja donde presentó a cobro el vale vista recién por la suma de $23.800.000. El vale vista en cuestión había sido tomado en favor del requerido a través de la plataforma internet que el banco proporciona a sus clientes para gestionar sus cuentas corrientes, por un tercero cuya identidad se desconoce que concertado con el requerido y con el ánimo de defraudar a la víctima y al banco accedió indebidamente a la cuenta corriente del cliente Achondo y Cía Ltda. que operó desde un ciber-café, previa captura de sus claves secretas mediante correos supuestos del banco en que éstas les fueron requeridas.

El cajero que atendió al requerido entregó el vale vista a su supervisor para ser autorizado el pago, resultando que el documento fue objetado por el representante de la empresa Achondo y Cia Ltda don Francisco Achondo Bastian, quien negó haber efectuado tal operación en beneficio del requerido, percatándose recién de la gestión fraudulenta que se había ejecutado en la plataforma de internet, razón por la cual no le fue pagado al requerido el vale vista, siendo detenido.

- **Decisión del tribunal:**

Se condenó a Rodrigo Fernando Candia Salas, como autor del delito consumado de estafa y como cómplice del delito consumado de sabotaje informático, a la pena única de 21 días de prisión en su grado medio, suspensión de cargo público por el mismo plazo y multa de 1/3 de unidad tributaria mensual.

- **Considerandos relevantes:**

SEGUNDO: Que habiendo admitido responsabilidad el imputado en los hechos señalados en el requerimiento, se tiene por establecido la existencia de los mismos, así como –también- la participación culpable que ha correspondido al requerido; se califican los hechos como un delito de estafa en grado de consumado, previsto y sancionado en el artículo 473 del Código Penal, en el cual correspondió al acusado participación de autor, y un delito consumado de sabotaje informático, previsto y sancionado en el artículo 3 de la Ley Nº 19.223 en el que correspondió al requerido participación en calidad de cómplice .

- **Tribunal:** 7° Juzgado de Garantía de Santiago
- **Magistrado(s):** Mario Alfredo Cayul Estrada
- **Fecha:** 01.12.2016
- **RUC:** 1510011054-4
- **RIT:** 6523-2015
- **Procedimiento:** No consta de la Sentencia.
- **Síntesis de los hechos:**

Entre junio de 2011 a marzo de 2015 el imputado, Adolfo Hernán Inostroza Palma, ejerciendo el cargo de "Ejecutivo de Apoyo de Gerencia de Operaciones de Finanzas", del Banco de Créditos e Inversiones BCI, procedió a realizar abonos a sus cuentas personales, desde fondos provenientes de la cuenta del Banco BCI denominada "pasivo provisorio de la sucursal", para lo cual, maliciosamente alteró la base de dato informática del banco utilizando las claves y cuentas de acceso de otros funcionarios del Banco. Con lo anterior ingresaba al sistema 'portal' del banco, generando las transacciones ya indicadas, de modo que apareciera en el sistema interno del banco que las transacciones eran efectuadas por otros funcionarios. El imputado para ocultar los abonos realizados, manipulaba cuentas contables transitorias, las cuales presentan controles de razonabilidad y no de detalle, lo que el imputado aprovechó para generar contabilidad por un lado y el abono a sus cuentas personales por el otro sin que existieran diferencias contables que alertaran a la víctima sobre su actuar realizando una maniobra que le permitió apropiarse indebidamente y en perjuicio de la víctima de la suma de $479.369.063 pesos.

- **Decisión del tribunal:**

Se condenó, al requerido a la pena de 100 días de presidio menor en su grado mínimo, mas las accesorias de suspensión de cargo u oficio público mientras dure la condena.

- **Considerandos relevantes:** No presenta.

- **Tribunal:** Juzgado de Garantía de Arica
- **Magistrado(s):** Paulina Andrea Zúñiga Lira
- **Fecha:** 06.01.2017
- **RUC:** 1500784272-1
- **RIT:** 7878-2015
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Luego de una denuncia efectuada por el Servicio Nacional de Aduanas, y en el contexto de las pesquisas que estaba desarrollando la Policía de Investigaciones de Chile en el marco de una investigación sobre liberación de vehículos desde la Zona Franca de Arica, el acusado Pedro Ruz, con fecha 14 de agosto de 2015, en Arica, en el contexto de su declaración adujo que había contactado nuevamente a JOSE GUAJARDO a objeto de obtener un nuevo certificado de viaje, haciendo entrega de un documento denominado certificado de viaje n° 3445 de fecha 06 de agosto del 2015 del Departamento de Extranjería y Policía Internacional de Iquique, al verificar este documento por parte de los funcionarios policiales del BRIDEC de Arica, se percataron que el documento era original, pero en el sistema GEPOL de la PDI se habían registrado estos viajes en el sistema, el día 28 de julio del 2015, por parte un usuario con la clave de acceso al sistema informático QHQN, el cual pertenece al funcionario policial Subinspector Francisco Espinoza Fariña y de la estación de trabajo IP 172.25.150.246, la cual se encuentra asignado a la Jefatura Nacional de Inteligencia Policial de la PDI. De esa forma, se pudo determinar que la acusada Tamara Inostroza Montoya, quien se desempeñaba como Subcomisario de la Policía de Investigaciones de Chile en la Jefatura Nacional de Inteligencia Policial, a Francisco Espinoza si le podía facilitar su clave de acceso al sistema GEPOL, de esa forma Espinoza accede a dicha petición. Fue así que contando con esta clave, Tamara Inostroza fue contactada por la acusada Silvia Méndez Otárola, la cual a su vez había sido contactada por el imputado Pedro Ruz, a objeto de alterar el sistema GEPOL, adulterar la información sobre movimiento migratorio de José Guajardo y de esa forma, obtener luego en la ciudad de Iquique, Silvia Méndez, a petición de Ruz, un nuevo certificado de viajes de José Guajardo,

documento ideológicamente falso, en la cual en su confección participó en la forma señalada la imputada Inostroza. Asimismo este documento fue retirado por la acusada Silvia Méndez, el cual luego fue entregado al imputado Pedro Ruz, justificando de esa forma que efectivamente Guajardo si presentaba viajes al extranjero. Por esta acción la imputada Silvia Méndez pagó la suma de $500.000 pesos, los cuales depositó en la cuenta bancaria de la madre de Tamara Inostroza. Asimismo el imputado Pedro Ruz, quien necesitaba de dicho certificado, pago la suma de $1.000.000 de pesos a Silvia Méndez, la cual se realizó mediante transferencia electrónica.

- **Decisión del tribunal:**

En lo relativo a la autora del delito informático, el tribunal condenó a Tamara Soledad Inostroza Montoya a la pena de quinientos cuarenta y un días de presidio menor en su grado medio y accesoria de suspensión de cargo u oficio público durante el tiempo de la condena, como autora del delito consumado de falsificación de instrumento público del artículo 193 del Código Penal; a la pena de sesenta y un días de presidio menor en su grado mínimo y accesoria de suspensión de cargo u oficio público durante el tiempo de la condena, como autora del delito consumado de sabotaje informático del artículo 3° de la Ley n° 19.223; y a la pena de quinientos cuarenta y un días de presidio menor en su grado medio y accesoria de suspensión de cargo u oficio público durante el tiempo de la condena, y a una multa equivalente al doble del provecho solicitado, correspondiente a $3.100.000 como autora del delito consumado de cohecho, previsto y sancionado en el artículo 248 y siguientes del Código Penal, cometidos en Arica en el año 2015.

- **Considerandos relevantes:** No presenta.

- **Tribunal:** 7° Juzgado de Garantía de Santiago
- **Magistrado(s):** Carla Valeria Cappello Valle
- **Fecha:** 26.01.2017
- **RUC:** 1510006022
- **RIT:** 4000-2015
- **Procedimiento:** No consta de la Sentencia.
- **Síntesis de los hechos:**

Entre el 1 de diciembre de 2011 hasta el 25 de agosto de 2014 el imputado, Christián Andrés Flores Valderrama, ejerciendo el cargo de "Analista de Recaudación", de la empresa BCI Seguros generales, procedió a manipular el sistemáticamente el sistemas computacional AS-400 de la empresa, modificando los datos de clientes y emitir devoluciones de dinero a nombre de familiares o amigos, las que posteriormente retiraba personalmente desde las cajas de la empresa, aprovechándose de un permiso especial para el cobro de cheques por clientes, apropiarse indebidamente en perjuicio de la víctima de la suma de $13.365.353.

- **Decisión del tribunal:**

Se condenó al imputado a la pena única de 541 días de presidio menor en su grado mínimo, y al pago de una multa de un tercio de UTM, mas las penas accesorias de suspensión de cargo u oficio mientras dure la condena, por los delitos de Apropiación indebida del artículo 470 N°1 e infracción al artículo 3 de la ley 19.223, en los que le corresponde participación en calidad de autor.

- **Considerandos relevantes:** No presenta

- **Tribunal:** 7° Juzgado de Garantía de Santiago
- **Magistrado(s):** Freddy Cubillos Jofré
- **Fecha:** 16.02.2018
- **RUC:** 1700296781-2
- **RIT:** 21769-2017
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Entre los meses de octubre del año 2016 a marzo del 2017, en las dependencias del 4° Juzgado de Policía Local de Santiago, el imputado Nelson José Pino Bravo, en el ejercicio de sus funciones como funcionario del tribunal, engañó a 24 infractores de tránsito distintos, indicándoles que debían pagar una multa supuestamente fijada por la Jueza consistente en una suma de dinero que variaba entre $65.000 a $130.000 pesos. De esa manera tendrían por pagada su multa y recuperarían sus licencias de conducir, que se encontraban retenidas en el Juzgado de Policía Local.

Luego de que las personas entregaban el dinero, el imputado, usurpando las funciones propias de un Juez de Policía Local y de un Secretario del Tribunal, decidía entregar un boucher firmado por el juez y secretario del tribunal que les permitía retirar las licencias de conducir y además, haciendo uso del usuario y clave de otros administrativos del tribunal, modificaba en el sistema informático del Cuarto Juzgado de Policía Local de Santiago el estado de causa de cada una de los infractores, incorporando sentencia de "Amonestación". De esta manera defraudó de modo reiterado al fondo municipal provocándole perdida o privándole de un lucro legítimo en cada ocasión por montos que fluctúan entre 1.5 y 3 UTM, además de provocar que no se generara la pena de suspensión de licencia asociada a la infracción. El imputado Nelson José Pino Bravo, recibió de los distintos infractores o por medio de terceros el dinero mencionado.

- **Decisión del tribunal:**

Se condenó a Nelson José Pino Bravo, a la pena de cuatro años de presidio menor en su grado máximo, accesoria de inhabilitación absoluta perpetua para derechos políticos y la inhabilitación absoluta para cargos y oficios públicos durante el término de la condena, y multa de un millón

de pesos ($1.000.000), como autor de delitos reiterados de fraude al fisco, adulteración de sistema informático, estafa y usurpación de funciones, en grado de consumados.

- **Considerandos relevantes:** No presenta.

- **Tribunal:** Juzgado de Garantía de Puerto Varas
- **Magistrado(s):** Ximena Cristina Bertin Pugin
- **Fecha:** 15.03.2018
- **RUC:** 1501011576-8
- **RIT:** 2276-2015
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Desde el año 2006 hasta agosto de 2015, el imputado Egon Walter Heim Aguirre, desempeñó funciones de Cajero Municipal, cargo administrativo dependiente de la Dirección de Administración y Finanzas de la Municipalidad de Puerto Varas, en las dependencias de calle San Francisco 413, Puerto Varas.

Entre las funciones y responsabilidades propias del cargo de cajero municipal, el imputado tenía, entre otras, la obligación de recaudar y recepcionar los fondos correspondientes a pagos de los permisos de circulación, efectuar su contabilización, enterarlos en arcas del municipio y efectuar su registro contable en el sistema informático de tesorería municipal CAS., sistema de tratamiento de información al cual accedía mediante una cuenta y clave personal y exclusiva proporcionada por el servicio para el desempeño de sus funciones.

En esas circunstancias, entre el mes de noviembre de 2011 y agosto de 2015, el imputado en el ejercicio de sus funciones como cajero municipal, aprovechando su posición funcionaria privilegiada en directa relación con los recursos económicos públicos del municipio recaudados, recepcionó personalmente los pagos de permisos de circulación efectuados y luego omitió enterarlos en arcas fiscales, sustrayendo la suma de total de $58.600.520 pesos, equivalente a 1.413,12 UTM a la época de los hechos.

Para burlar el control contable y encubrir la sustracción antes señalada, el imputado altero maliciosamente el sistema informático de tesorería municipal, modificando el monto real indicado en el formulario de ingreso municipal, y registrando en su lugar el valor ficticio de $0 pesos, adulterando así la contabilidad general del municipio.

- **Decisión del tribunal:**

Se condenó a Egon Walter Heim Aguirre, como autor en delitos consumados de malversación de caudales públicos previsto y sancionado en el artículo 233 y 238 inciso 2 del Código Penal en concurso medial con el delito informático de alteración maliciosa de sistema y tratamiento de información del artículo 3 de Ley 19.223, a la pena única de cinco años de presidio menor en grado máximo, accesoria de inhabilitación absoluta perpetua para derechos políticos, e inhabilitación absoluta perpetua para cargos y oficios públicos y multa de doce unidades tributarias mensuales.

- **Considerandos relevantes:** No Presenta.

- **Tribunal:** 7° Juzgado de Garantía de Santiago
- **Magistrado(s):** Marcia Irene Figueroa Astudillo
- **Fecha:** 12.06.2018
- **RUC:** 1610018667-9
- **RIT:** 9204-2016
- **Procedimiento:** Abreviado
- **Síntesis de los hechos:**

Durante el período comprendido entre el mes de abril de 2014 a julio de 2015, en la sucursal del Banco de Chile, ubicada en Ahumada N° 251, piso 3, comuna de Santiago, el imputado Patricio Javier Orellana Alarcón, aprovechándose de su cargo de Jefe de Servicios al Cliente, cobró a los menos sesenta y un vale vistas nominativos, los cuales supuestamente pertenecían a Fernando Patricio Ramírez Cabezas.

Lo anterior lo realizaba solicitando a los funcionarios encargados de la custodia de papeles valorados, los formularios respectivos para imprimir los vale vistas. Una vez impresos fingía la firma del titular del vale vista, Fernando Patricio Ramírez Cabezas, en el comprobante de entrega, simulando que éste era recibido por el titular, agregando, además, los datos personales del afectado. Luego de esto, la colilla del retiro del vale vista era entregada nuevamente a los encargados de custodia.

Para adulterar el sistema informático y con el objeto de cancelar vale vistas masivos y luego con los fondos obtenidos crear acreencias en nombre de Fernando Ramírez y así cobrarlos a su nombre, el imputado abría irregularmente un terminal de caja bajo su usuario y clave personal, utilizando la terminal identificada como "pcdl2b", equipo computacional ubicado en su puesto de trabajo y desde ese equipo y con su LOG de acceso, procedía a cancelar los vale vistas y generar los créditos antes mencionados.

Posteriormente, el imputado procedía a imprimir los vale vistas y cobrarlos por caja, sosteniendo que estos pertenecían a su amigo Fernando Ramírez y que éste tenía su autorización para cobrarlos por él. De esta manera defraudó al Banco de Chile en la suma de $ 79.893.111.

- **Decisión del tribunal:**

Se condenó a Patricio Javier Orellana Alarcón, a la pena cuatro años de presidio menor en su grado máximo, a la multa a beneficio fiscal de cinco unidades tributarias mensuales y a las accesorias de inhabilitación absoluta o perpetua para derechos políticos y la inhabilitación absoluta para cargos u oficios públicos mientras dure la condena, por su responsabilidad como autor del delito reiterado de estafa en concurso medial con el delito de adulteración de sistema informático, previstos y sancionados en los artículos 467 n°s 1 y 2 en relación al artículo 468, ambos del código penal y artículo 3° de la ley 19.223, que se encuentran en grado de ejecución de consumados.

- **Considerandos relevantes:** No presenta.

- **Tribunal:** 8° Juzgado de Garantía de Santiago
- **Magistrado(s):** Ely Rothfeld Santelices
- **Fecha:** 31.12.2018
- **RUC:** 1501138933-0
- **RIT:** 10444-2015
- **Procedimiento:** Abreviado.
- **Síntesis de los hechos:**

Hecho 1: En circunstancias que el imputado WILSON BARROS MONCADA, contador, ejerció labores en el área de contabilidad desde el año 2003 y hasta fines del año 2015 para la víctima Echeverría Izquierdo Montajes Industriales S.A. -cuyo giro es dentro del rubro de la construcción, la de montaje industrial de obras complejas- y específicamente en su desempeño como Supervisor del Departamento de Subcontratos y Costos, en el que dentro de sus funciones se encontraban la de estar a cargo de los trabajadores asociados a la digitación y validación de los subcontratos en el sistema informático computacional, la de gestionar el proceso de proveedores, desde el ingreso de la Orden de Compra o Estado de Pago, hasta la confección de la nómina de pago masivo a proveedores, ideó un sistema de defraudación a dicha empresa, que se extendió durante 5 años (desde 2010 a 2015), lo que le permitió, en conjunto con el imputado PATRICIO PÉREZ SEPULVEDA, apropiarse de dineros de dicha empresa, mediante la manipulación y adulteración del sistema informático de contabilidad de la misma, como más adelante se referirá, para así apropiarse de una cifra de al menos $2.392.496.567. Esta actividad, se mantuvo sostenida en dicho periodo de tiempo, con diferenciación de roles y actuaciones por cada imputado.

En efecto, esta manipulación del sistema informático, consistió en el ingreso por parte del imputado BARROS MONCADA, de obligaciones ficticias asociadas a falsos proveedores de la víctima, generando de este modo el correspondiente informe de pago, que habilitaba para que luego se subiera o cargara la denominada “nómina de pago” al banco y finalmente se autorizara el pago (bajo esta simulación y engañando al contador general, al tesorero, gerente de finanzas y demás empleados, que no podían advertir lo ocurrido y por tanto autorizaban el pago) y

cobrado el dinero mediante vales vista, por 17 testaferros, los que eran contactados especialmente al efecto por el imputado PEREZ SEPÚLVEDA, quién también cobraba dineros en tal sentido. La manipulación del sistema informático, fue llevada a cabo por el imputado BARROS MONCADA, a través de 2 modalidades:

La primera modalidad, utilizada hasta el año 2013, consistió en la emisión de facturas de compra por la empresa, respaldadas en un estado en un estado de pago falso por él mismo generado, puesto que no correspondía a un estado de pago emitido en la obra que la víctima ejecutaba y a que hacía referencia, y que daba cuenta de diferentes servicios prestados por los testaferros. La segunda modalidad, utilizada a partir del año 2014, fue la de ingresar una factura (también falsa) al sistema de contabilidad, pero solo para cargar una nómina de pago, ingresándola con una nomenclatura especial llamada OT (otros documentos) y de ese modo aprovechar una vulnerabilidad del sistema en tanto aquello reducía las capacidades de control sobre tales operaciones, y que también daban cuenta de operaciones ficticias, pues ningún servicio fue prestado por ellos al efecto.

En ambos casos además, y conforme lo exigía el sistema informático contable, el imputado marcaba que el pago debía efectuarse a través de vale vista, lo que permitía que estos falsos proveedores de la empresa, al haber sido ingresados a las nóminas de pago y cargada dicha información en el banco para su pago, pudieran cobrar los vales vista en diversas sucursal del Banco Chile (aquel al que pertenece la cuenta bancaria de la víctima), dinero que posteriormente entregaban al imputado PÉREZ SEPULVEDA, quién era el encargado de contactar a los imputados para el cobro de los mismos.

Posteriormente, el imputado BARROS MONCADA, llevaba a cabo diversas maniobras de ocultamiento en el sistema informático contable, como son el ingreso de una falsa nota de crédito, cambios en la nómina de pagos y modificación de los informes de costos de las obras, con lo cual evitaba ser descubierto y mantenía las cuentas contables en orden.

Hecho 2: En circunstancias que el imputado WILSON BARROS MONCADA, contador, ejerció labores en el área de contabilidad desde el año 2003 y hasta fines del año 2015 para la víctima Echeverría Izquierdo Montajes Industriales S.A. (cuyo giro es dentro del rubro de la construcción, la de montaje industrial de obras complejas), con fecha 22 de julio de 2015, y para efectos de realizar las labores propias de su cargo, la víctima le hizo entrega de un computador

notebook marca Hewlett Packard 450. Al momento de ser desvinculado de la empresa, el imputado no realizó la devolución del computador notebook antes referido.

Hecho 3: El imputado Daniel Madrid Castro, a través de su empresa montajes industriales Daniel Madrid Castro E.J.R.L., aprovechando la circunstancia de ser proveedor de la víctima Echeverría e Izquierdo Montajes Industriales S.A. (EIMISA) desde hace varios años, y previamente concertado con el imputado Wilson Barros Moncada, a la sazón, Supervisor del Departamento de Subcontratos y Costos de la víctima, en el que dentro de sus funciones se encontraban la de estar a cargo de los trabajadores asociados a la digitación y validación de los subcontratos en el sistema informático computacional, la de gestionar el proceso de proveedores, desde el ingreso de la Orden de Compra o Estado de Pago, hasta la confección de la nómina de pago a proveedores, en las oficinas ubicadas en Avenida Nueva Providencia N° 1480, oficina 141, comuna de Providencia, desde el año 2010 al año 2014, efectuaron diversas maniobras defraudatorias para con la víctima, consistentes en la simulación de prestaciones de servicios y/o trabajos efectuados por el imputado a la víctima, de entre las varias otras que si correspondían a operaciones reales, las que no se referían a operaciones verdaderas, y que en el sistema de registro y contabilidad de la víctima fueron respaldados mediantes falsos estados de pago, lo que permitió que se expidieran sendas facturas de compra por la víctima, conforme más delante se señalará, por un total de $180.355.186, dinero que fue pagado y transferido por la víctima al imputado, el que de ningún otro modo le hubiera correspondido recibir.

- **Decisión del tribunal:**

Se condenó, al requerido a la pena de 5 años de presidio menor en su grado máximo, accesorias de inhabilitación absoluta perpetua para derechos políticos e inhabilitación absoluta para cargos y oficios públicos durante el tiempo de la condena y multa de 10 (diez) Unidad Tributaria Mensual, sin costas, por no haberse éstas pedido, como autor de los delitos reiterados de Estafa de los artículos 468 y 467 inciso final del Código Penal, reiteradas; sabotaje informático del artículo 3° de la Ley 19.223; asociación ilícita de los artículos 292 y 293 del Código Penal y Apropiación indebida del artículo 470 N° 1 y 467 N° 2 del Código Penal, hechos ocurridos entre los años 2010 y 2015 en la comuna de Providencia de esta ciudad, en perjuicio de Echeverría Izquierdo Montajes Industriales S.A.

- **Considerandos relevantes:**

3º Que los antecedentes fundantes de la acusación apreciados todos ellos resultan concordantes y coherentes entre sí y llevan necesariamente a la conclusión de que los hechos ocurrieron en la forma reseñada en el relato del Ministerio Público, coincidiendo con éste en su calificación Jurídica, correspondiendo al imputado participación en calidad de autor, toda vez que ha quedado acreditado que, mediante maniobras engañosas, y coludido con diversos otros partícipes; vulnerando y adulterando los sistemas informáticos de registro, protección y control de datos de la empresa afectada, con ánimo consiguió apropiarse por una parte de $2.392.496.567.- y por la otra, de $ 180.355.186.- Sumado a ello, se apropió de un notebook de la empresa, avaluado en la suma de $737.800.