Delitos Informáticos. Chile y legislación extranjera

En Chile, la Ley N° 19.223, que tipifica figuras penales relativas a la informática, cubre adecuadamente las figuras tradicionales de comisión de delitos informáticos, distinguiendo entre sabotaje, espionaje y fraude, informáticos, pero no se adecua a las nuevas formas de comisión, dadas por el avance de la tecnología y la modificación de los conceptos normativos utilizados en la ley, relativos a la tecnología.

Además se presentan dificultades procesales relativas a la competencia de los tribunales, debido al lugar de comienzo de ejecución del delito, originando muchas veces la impunidad de delitos cometidos contra chilenos desde el extranjero. También hay algún grado de confusión sobre el bien jurídico protegido por la norma, lo que ocasiona dificultades de interpretación.

Pese a no ser exigible para Chile, la legislación nacional se adapta a las recomendaciones internacionales de incriminación de estas conductas, formuladas por el Consejo de Europa y la Unión Europea, aunque no totalmente, pues en Chile no se incrimina el simple acceso no autorizado a un computador o sus datos por medios informáticos.

El proyecto de ley que tipifica y sanciona los delitos informáticos y deroga la ley N° 19.223 (Boletín N°) modifica el delito de destrucción o inutilización de sistema informático de tratamiento computacional de datos, y crea delitos nuevos, tales como: acceder o usar, sin derecho, información contenida en un sistema informático; impedir a otro por vía informática, acceder a sus datos personales u otros de su propiedad intelectual; alterar, dañar o destruir los datos contenidos en un sistema informático; cualquier forma de puesta a disposición de elemento informático que permitan o faciliten la comisión de delitos; y el delito de exacción patrimonial.

También se crea una agravante especial consistente en incurrir en estos delitos, siendo responsable del sistema de información, y se crea una nueva circunstancia agravante, genérica, en el artículo 12, circunstancia 22ª en el Código Penal, consistente en emplear medios informáticos para ejecutar el delito.

Se sancionan la tentativa y la frustración de los delitos contemplados en esta ley.

Asimismo, se modifica el Código Procesal Penal para introducir normas procesales penales que fortalecen al Ministerio Público y a las Policías.

En síntesis, las modificaciones propuestas coinciden con lo observado en la legislación extranjera analizada.

Sin perjuicio de ello, la mayoría de los delitos previstos exigen dolo directo, contrariamente a lo observado en las legislaciones extranjeras analizadas.

Biblioteca del Congreso Nacional. Juan Pablo Cavada Herrera. Asesoría Técnica Parlamentaria. jcavada@bcn.cl, Anexos: 1873 y 3905, 22.12.2015.

Tabla de Contenido

I. Introducción

El presente trabajo describe la legislación nacional y los principales tipos penales relativos a ésta materia, y describe y explica someramente algunas normas internaciones del Consejo de Europa y de las Naciones Unidas, y de las legislaciones de Alemania, Argentina, Francia, Francia, Gran Bretaña, Portugal y Suiza, dado que en ellas se ha encontrado disposiciones al respecto.

Los delitos informáticos se encuentran regulados en Chile en tres normas legales: Ley N° 19.223[1], que tipifica figuras penales relativas a la informática; Ley N° 17.336[2], sobre Propiedad Intelectual; y la Ley N° 19.927[3], que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil.

[1] Disponible en: http://bcn.cl/mts (Diciembre, 2015).
[2] Disponible en: http://bcn.cl/9nkx (Diciembre, 2015).
[3] Disponible en: http://bcn.cl/qkl (Diciembre, 2015).

De la misma manera se analiza el Proyecto de Ley que modifica los delitos informáticos, introduce modificaciones en materia procesal penal para facilitar la persecución de éstos delitos, y deroga la Ley N° 19.223.

El tema que aborda el presente Informe y sus contenidos están delimitados por los parámetros de análisis acordados y por el plazo de entrega convenido. No es un documento académico y se enmarca en los criterios de neutralidad, pertinencia, síntesis y oportunidad en su entrega.

I. Análisis Legislación Nacional[4]

De acuerdo a Marcelo Huerta y Claudio Líbano[5] las figuras penales nacionales de la Ley Nº 19.223 pueden clasificarse de la siguiente manera:

1. Delitos de sabotaje informático: Este delito se tipifica de la siguiente manera en la Ley Nº 19.223:

a. Atentados contra un sistema de tratamiento de la información o de sus partes componentes (artículo 1º, primera parte).
b. Atentados contra el funcionamiento de un sistema de tratamiento de la información (artículo 1º, segunda parte).
c. Atentados contra los datos contenidos en un sistema automatizado de tratamiento de la información (artículo 3º).

2. Delitos de espionaje informático: Se tipifican de la siguiente manera en la Ley Nº 19.223:

a. Delitos de apoderamiento, uso o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información (artículo 2º).
b. Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información (artículo 4º).

Los autores agregan a esta clasificación, dos más, doctrinarias:

3. Delitos de piratería de programas: Copia indebida de programas u obras por medios informáticos, sancionada en los artículos 79 y 80, en relación al 81 quater, de la Ley Nº 17.336.
4. Delitos de *hacking*: Acceso no autorizado o indebido a sistemas[6].

[4] La información, análisis, referencias y citas de este capítulo fueron extractadas de minuta titulada Delitos Informáticos. Legislación Comparada, elaborada por Williams O., Guido, Abogado del Área de Análisis Legal de la Biblioteca del Congreso Nacional.

[5] Huerta, Marcelo y Líbano, Claudio. Delitos Informáticos, Editorial Jurídica Conosur Ltda., Santiago. 1996, p. 123, citado por Williams O., G., OP. Cit., y Piedrabuena R., Guillermo, en "Boletín de Jurisprudencia. Ministerio Público", Nº 6, octubre de 2001, p. 86. Los antecedentes fueron vueltos a citar en Oficio N° 422, de 27/09/2001, del Ministerio Público, sobre Informe Relativo a las Diligencias e Investigación de los Delitos Informáticos contemplados en la Ley N° 19.223 y al Fraude Informático". Disponible en: http://bcn.cl/h3ma (Diciembre, 2015).

Guillermo Piedrabuena sostiene que a estos delitos debe agregarse el de "fraude informático", es decir, defraudaciones cometidas mediante el uso de elementos informáticos o computacionales. En Chile, por no existir norma especial, se aplican los delitos clásicos de defraudación del Código Penal (artículos 463 y ss.)[7].

En este punto, la Ley Nº 19.927 incorpora al Código Penal dos delitos nuevos que pueden ser cometidos por medios informáticos:

- Artículo 366 quinquies: Sanciona a quien participa en la producción de material pornográfico, cualquiera que sea el soporte del mismo.
- Artículo 374 bis: Sanciona a quien comercializa, importa, exporta, distribuye, difunde o exhibe material pornográfico, cualquiera sea su soporte y a quien, maliciosamente, adquiere o almacena dicho material.

Como se verá mas adelante, el análisis de la clasificación legal y doctrinaria de Líbano y Huerta, en relación con lo señalado por Piedrabuena, y las disposiciones de las Leyes Nº 17.336 y Nº 19.927, permiten constatar que las figuras penales nacionales coinciden con los tipos propuestos por la Convención de Delitos Informáticos del Consejo de Europa y por la Organización de las Naciones Unidas.

II. Bien Jurídico Protegido

En la historia fidedigna de la Ley N° 19.223, se dejó expresa constancia de que este proyecto de ley tenía "por finalidad proteger un nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: 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" [8].

Sin embargo no solamente se protege ese bien sino que, además, otros tales como el patrimonio, en el caso de los fraudes informáticos; la privacidad, intimidad y confidencialidad de los datos, como el espionaje informático; la seguridad y fiabilidad del tráfico jurídico y probatorio en el caso de las falsificaciones de datos probatorios vía medios informáticos; el derecho de propiedad sobre la información y sobre los elementos físicos, materiales de un sistema informático, en el caso de los delitos de daños[9]. Además, el nacimiento de esta nueva tecnología, proporciona nuevos medios o mecanismos para atentar contra bienes jurídicos ya existentes[10].

---

[6] Líbano y Huerta sostienen que éste delito ha sido entendido por algunos como medio o herramienta de comisión de otros delitos informáticos y no uno en sí mismo. OP. Cit., p. 169. Citado por Williams O., G., OP. Cit., y Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[7] Piedrabuena R., Guillermo. Boletín de Jurisprudencia. Ministerio Público, Nº 6, octubre, 2001, p. 98.
[8] Oficio N° 422, de 27/09/2001, del Ministerio Público, ya citado.
[9] Magliona Marcocicht, Claudio Paul, y López Medel, Macarena, Delincuencia y Fraude Informático, Editorial Jurídica, 1999, p. 66. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[10] Ibídem.

III. Historia Fidedigna de la Ley N° 19.223

La Ley N° 19.223 se origina en una moción del diputado José Antonio Viera Gallo, presentada en la Cámara de Diputados el 16 de julio de 1991. En base a la historia de la ley, se puede afirmar que los fundamentos de la Ley N° 19.223 son[11]:

1. La dependencia de las sociedades modernas en la utilización de los sistemas automatizados de tratamiento de información, mediante computadores o redes.
2. Lo anterior muestra la gran vulnerabilidad a la que se encuentran expuestas los organizaciones, frente a abusos contra los sistemas informáticos.
3. Surge un nuevo bien jurídico que requiere de protección: "La calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de la misma y de los productos que de su operación se obtengan". Sin embargo, como señalamos, éste no es el único bien afectado sino que, además, concurren otros tales como: seguridad, patrimonio, intimidad, confianza en el buen funcionamiento de los sistemas de información, etc.
4. Necesidad de crear nuevos tipos penales autónomos para evitar la interpretación extensiva de los tipos penales clásicos. Es decir, se reconoce que las conductas reprochables son de una estructura y contenido diverso.

IV. Análisis de los tipos penales de la Ley N° 19.223

La estructura, análisis y consideraciones contenidas en este punto se han extraído y transcrito casi íntegramente del Oficio N° 422, del Ministerio Público, de 27/09/2001, sobre Informe Relativo a las Diligencias e Investigación de los Delitos Informáticos contemplados en la Ley N° 19.223 y al Fraude Informático", ya citado.

Desde un punto de vista general, siguiendo la clasificación efectuada por Marcelo Huerta M. y Claudio Líbano M., contenida en su obra titulada Delitos Informáticos[12], la Ley N° 19.223 contempla dos figuras delictivas: I) Sabotaje Informático; II) Espionaje Informático. A su vez estas dos figuras se subdividen en categorías distintas atendiendo al objeto contra el que se atenta y/o al modus operandi.

1. Sabotaje Informático

Este delito se encuentra previsto en sus diversas modalidades en los artículos 1° y 3° de la ley. Para facilitar el estudio de los tipos penales se transcriben los artículos pertinentes.

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.

[11] Oficio N° 422, de 27/09/2001, del Ministerio Público, Ob. Cit.
[12] Huerta, Marcelo, y Líbano, Claudio. Op. Cit., p. 123, citado por Williams O., G., OP. Cit., Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

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

a) Sujeto Activo y Pasivo

En cuanto al sujeto activo del delito, la ley no exige la concurrencia de ningún requisito específico, lo que se desprende de la expresión "El que...", empleada en los artículos 1° y 3° de la ley. En cuanto al sujeto pasivo, es el titular del bien jurídico lesionado o puesto en peligro. Sin embargo, estos delitos serían pluriofensivos, es decir, afectan bienes que trascienden al particular afectado o a un conglomerado social o a toda la Nación.

b) Conductas tipificadas como sabotaje informático:

b.1. Atentados contra el sistema de tratamiento de información o sus partes o componentes. Artículo 1°, inciso primero primera parte.

i. Destrucción de un sistema de tratamiento de información o sus partes o componentes. Según el Diccionario de la Lengua Española de la Real Academia española, el verbo rector es destruir, entendido como "deshacer, arruinar". Dada la amplitud del tipo penal, la acción punible se circunscribe a la destrucción del soporte físico de un sistema de tratamiento de información (*hardware*) y a lo que se denomina soporte lógico (*software*). Esto se fundamenta en el Diario de Sesiones de la Cámara de Diputados, donde, al analizarse el artículo 1°, se dejó constancia que el tipo penal "se refiere a lo que en doctrina se denomina "delito de sabotaje informático", que consiste en la destrucción o inutilización del soporte lógico, esto es, de los datos o programas contenidos en un computador, pudiendo, según algunos, afectar el soporte físico del sistema informático (*hardware*)"[13].

La anterior explicación coincide con las ideas centrales de la moción parlamentaria, en cuanto a que el proyecto buscaba evitar la interpretación extensiva de los tipos penales clásicos, creando figuras delictivas nuevas. El *software*, por su naturaleza jurídica especial, escapa a la protección penal común, precisando una tutela judicial diversa cuando las acciones punibles son llevadas a cabo mediante la utilización de mecanismos de tecnología

[13] Diario de Sesiones de la Cámara de Diputados. Sesión 20° Ord. (28/07/1992). Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

computacional, con resultado de destrucción como por ejemplo, los virus[14], bombas lógicas[15], rutinas cáncer[16], etc.

El texto legal se coloca en el evento de una destrucción de la totalidad del sistema de tratamiento de información o de una de sus partes o componentes.

Un problema que se presenta es el caso de la destrucción de los soportes físicos del sistema, pues en tal caso se produciría un concurso aparente de leyes penales entre el tipo común del delito de daños y el artículo 1°, debiendo por tanto ser resuelto por el Tribunal en base a los principios de especialidad, accesoriedad, o subsunción. La legislación española, en el caso de destrucción por procedimientos físicos, de elementos materiales del sistema (destrucción de un monitor, incendio de una unidad de proceso, inutilización de una impresora, etc.), aplica el tipo penal básico de daños. En casos de destrucción del soporte lógico mediante mecanismos informáticos, se ha contemplado una previsión legislativa especial, pues tal destrucción no se manifiesta en una necesaria afectación material del soporte[17].

Por esta razón se interpreta que el artículo 1° se aplica a aquellos casos de destrucción de soporte lógico a través de mecanismos informáticos, pues ellos no dejan huella material en el soporte que los contiene (*disquetes, CD-ROM*), haciendo inaplicable en estos casos el tipo clásico de daños. Además, al analizar la historia de la ley se observa que el objetivo propuesto era proteger los programas o datos, al no ser posible su debida tutela bajo los tipos penales comunes.

ii. Inutilización de un sistema de tratamiento de información o de sus partes o componentes. Según la RAE, el verbo rector inutilizar, quiere decir hacer inútil, vana o nula una cosa. El sistema de tratamiento de información no ha sido destruido, sin embargo, no es apto o idóneo para tratar la información, o si sirve, sólo presenta una utilidad limitada para el fin asignado. En este caso

[14] Son programas informáticos diseñados específicamente para realizar dos funciones: replicarse de un sistema informático a otro y situarse en los computadores de forma que pueda destruir o modificar programas y ficheros de datos interfiriendo los procesos normales del sistema operativo (vid Sneyers, El fraude y otros delitos informáticos, cit., pp. 101 – 105). Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

[15] Consiste en introducir en un programa un conjunto de instrucciones no autorizadas para que en una fecha o circunstancia predeterminada se ejecuten desencadenando la destrucción de información almacenada en el computador, distorsionando el funcionamiento del sistema, provocando paralizaciones intermitentes (Camacho Losa, Luis, El Delito Informático, cit., p. 44). Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

[16] Sieber expresa que este delito "consiste en unas instrucciones que consumen poco tiempo de programa, y en una serie de comandos que producen una auto reproducción del "programa cáncer" en otra parte del programa de aplicación, arbitrariamente escogida, durante cada uso. Cuando el programa de aplicación disminuya debido al aumento del número de rutinas de cáncer, esas rutinas deberían detectarse y extraerse del programa por el usuario. De todas formas, sólo con que se deje una de estas rutinas, el cáncer continuará reproduciéndose y expansionándose". Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

[17] El artículo 264.2, Código Penal Español 1995, recoge como modalidad agravada de daños la conducta de quien "por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

hay procedimientos físicos e informáticos, como por ejemplo, la introducción de papel esmerilado sobre las partes electrónicos leíbles de una tarjeta con la finalidad de destruir los lectores de símbolos y de tarjetas; insertar hierro cortante, sujeta papeles o pequeños trozos de hojas finas de aluminio en el mecanismo de los computadores para causar cortocircuitos eléctricos; verter café, etc.[18].

b.2. Atentados contra el funcionamiento de un sistema de tratamiento de información (Artículo 1°, parte final). La ley contempla tres modos de afectar el funcionamiento:

i. Impedir el funcionamiento del sistema. Concurren dos verbos "funcionar" e "impedir". El Diccionario de la Lengua Española de la Real Academia Española[19] (RAE) define funcionamiento como la "acción y efecto de funcionar" y, a su vez, define funcionar como "ejecutar una persona, máquina, etc., las funciones que le son propias". Luego define impedir como "estorbar, imposibilitar o impedir que el sistema ejecute sus funciones propias, cuales son el tratamiento de información.". Ejemplo de ello son los virus que se sitúan en el sector de arranque del computador, impidiendo su utilización, ocasionando el envío masivo y constante de *spams* o serie de correos electrónicos para saturar el sistema, pudiendo impedir su funcionamiento.

ii. Obstaculizar el funcionamiento del sistema. La expresión obstaculizar alude a versión un poco más atemperada que la anterior, pues según los términos de la RAE consiste en impedir o dificultar la consecución de un propósito. Su finalidad es que el sistema no pueda cumplir con su función, o si lo logra, que lo haga de manera dificultosa, es decir, al igual que en el caso anterior, habrá un trastorno grave pero no insuperable. "Como ejemplo podríamos señalar la incorporación de un virus computacional a un sistema automatizado de tratamiento de información, para que éste funcione más lento, o funcione imperfectamente, o que finalmente no pueda funcionar"[20].

iii. Modificar el funcionamiento del sistema. La expresión modificar, según consta de la historia fidedigna de la ley, fue tomada por el legislador en su sentido más amplio; así dejó constancia el senador Otero: "Finalmente, quiero dejar constancia, para la historia fidedigna de la ley, de que en opinión de los integrantes de la Comisión a quienes consulté el tema de la palabra 'modificar', consignada en el artículo 1°, comprende el concepto 'alterar', es decir, la expresión 'modifique' se usa en su sentido más amplio"[21]. En

[18] Sieber señala que incluso la aproximación de un simple imán a un disco magnético, golpear o mover el computador cuando se están grabando los datos, un corte en el suministro de energía eléctrica o alteraciones intermitentes de tensión, aumento o descenso de la temperatura o la humedad más allá de los límites de funcionamiento óptimo del sistema, pueden suponer pérdidas y perturbaciones importantes en el almacenamiento de los datos capaces de dañarlos. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[19] Disponible en: http://www.rae.es/rae.html (Diciembre, 2015).
[20] Magliona M., Claudio, y López M., Macarena, Delincuencia y Fraude Informático. Ed. Jurídica, P. 163. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[21] Boletín N° 412-07 de la Honorable Cámara de Diputados y Senado de Chile, sesión 50°, martes 11 de mayo de 1993, p. 5914. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

conclusión, la expresión modificar alude a un concepto diverso al del mero funcionamiento, apuntando a la utilidad, pues el sistema seguirá cumpliendo sus funciones (procesar información), pero el beneficio o utilidad para el usuario se verá trastocada.

El orden de los verbos rectores parece no ser arbitrario, sino que se basaría en la intensidad de sus consecuencias, por lo que cabe hacer dos reflexiones al respecto:

- La impedición y la obstaculización comparten una base común: ambas afectan el funcionamiento en sí del Sistema, sin embargo, el carácter insuperable del trastorno permite determinar si una acción es impeditiva u obstructiva. Igualmente, una acción puede comenzar por obstaculizar el funcionamiento del Sistema, derivando luego en su impedimento.

- La diferencia entre la impedición y la obstaculización, con la modificación radica en que esta última no afecta el funcionamiento en sí del computador, de modo que éste sigue cumpliendo con su función: procesar información, sin embargo, el computador no prestará al usuario la utilidad perseguida, pues su funcionamiento se ha visto alterado.

iv. Agravante de Responsabilidad. Artículo 1°, inciso 2°.

Las hipótesis de sabotaje informático contempladas en el inciso primero del artículo 1° contemplan la siguiente circunstancia agravante: "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".

El fundamento de esta agravante radica en que cualquier persona puede prever que si realiza las acciones del inciso primero, los datos contenidos en el sistema pueden resultar afectados. El problema de la agravante es la indeterminación de la intensidad de la afectación de los datos, aunque pareciera ser que la finalidad de la norma es castigar mas severamente en caso que haya una irreversibilidad definitiva y absoluta, es decir, que los datos no puedan recuperarse.

a.3. Atentados contra los datos contenidos en un sistema. Artículo 3°.

Esta modalidad de sabotaje informático se distingue de las anteriores por la circunstancia que la acción delictiva está destinada a alterar, destruir o dañar los datos contenidos en un sistema de tratamiento de información; mientras que las modalidades anteriores buscan afectar el sistema de tratamiento de información, ya sea a sus elementos físicos o a su soporte lógico (programas o *software*).

Una definición del término dato se encuentra en el anteproyecto de legislación informática de 1987, que entendía por dato, "todo hecho representado bajo una fórmula convencional apropiada para su comunicación, interpretación o tratamiento

sea por el hombre, sea por medios informáticos."[22]. *Software* o soporte lógico se entiende como "Parte inmaterial formada por un conjunto de programas[23] que determinan el funcionamiento de los circuitos físicos que se contiene en el sistema informático."

La tipología de las conductas contempladas en la ley son las siguientes, en orden de menor a mayor intensidad:

i. Alterar los datos contenidos en un sistema. Según la RAE, alterar significa "Cambiar la esencia o forma de una cosa". Serían, en consecuencia, alteraciones, conductas como ingresar o introducir datos erróneos o "*data diddling*", borrar datos verdaderos, transformaciones y desfiguraciones de datos, por ejemplo, mediante la introducción de virus informáticos, y en general toda conducta que implique cambiar la información contenida en un sistema de tratamiento, sin destruirla. Por tanto lo afectado es el sentido, veracidad, claridad o pureza y alcance de la información contenida, que se verá afectada con estas conductas.

ii. Dañar los datos contenidos en un sistema. Según la RAE, dañar implica "maltratar o echar a perder una cosa"; se entiende como una conducta destinada a perjudicar la integridad de la información, lo que plantea la noción de perjuicio, maltrato o afectación de una cosa. Sin embargo, como veremos, lo que distingue al daño de la destrucción es que en ésta última el resultado es irreversible y permanente. Por lo tanto, si es posible recuperar la información o datos mediante instrucciones o comandos como *unerase*, *undelete* u otros, o se disponen de programas de respaldo (*back up*), estaremos frente a un daño informático.

iii. Destrucción de los datos en un sistema. Según la RAE, destruir significa "deshacer, arruinar o asolar una cosa". Ello implica una pérdida irreversible y permanente de los datos a través de la desfiguración de los mismos.

En los verbos dañar y destruir se involucra la noción de perjuicio, de tipo integral, a los datos o información almacenada; mientras que en la alteración se compromete su aspecto teleológico.

En este tipo penal se aprecia la protección al bien jurídico de la calidad, pureza, idoneidad e integridad de la información.

Los elementos subjetivos de los tipos de sabotaje informático serán analizados conjuntamente con la figura de revelación o difusión de datos contenidos en sistema de información, contenida en el artículo 4°, pues todas coinciden en la utilización de la expresión "maliciosamente".

[22] El Diccionario de la RAE define también adecuadamente, el concepto de dato informático "Representación de una información de manera adecuada para su tratamiento por el computador".
[23] A su vez programa se entiende como aquél conjunto de instrucciones para ser usadas directamente o indirectamente en un computador a fin de efectuar u obtener un determinado proceso o resultado, contenidas en un cassette, diskette, cinta magnética, discos compactos, memories sticks u otro soporte material. Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

2. Espionaje Informático de los artículos 2 y 4 de la Ley N° 19.223

Los artículos 2° y 4° de la Ley N° 19.223 contemplan dos modalidades distintas, doctrinariamente conocidas bajo la denominación "espionaje informático":

Artículo 2°. "El que con ánimo de apoderarse, usar, o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

Artículo 4°. "El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio.
Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

Por lo tanto se dividirá este tipo penal en grupos:

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

a. Elementos Objetivos

a.1. Sujetos Activos: La expresión "el que ..." contiene una formulación amplia, pero debe de tratarse de sujetos sin autorización para ingresar al sistema de tratamiento de información, pues se trata de intercepciones, interferencias o accesos indebidos.

a.2. *Modus Operandi*: La Ley circunscribe los medios por los cuales se logre el apoderamiento, uso o conocimiento de la información contenida en el sistema. Estas modalidades son tres:

i. Interceptar. Interceptar, según la RAE, implica "apoderarse de una cosa antes que llegue a su destino, o bien, detener una cosa en su camino o interrumpir, obstruir una vía de comunicación". Sin embargo, debido a la naturaleza incorporal de la información contenida y transmitida en un sistema de información, no es posible "evitar que llegue a su destino o destinatario", pese a que haya apoderamiento, uso o conocimiento de la misma, configurándose de igual manera la conducta de interceptación.

   La interpretación anterior parece correcta, pues "de lo contrario se caería en el absurdo de que en caso de que se interceptara la información con el fin de apoderarse, usar y conocer de ella, ésta de todas formas llegara a su destino o destinatario, no existiría interceptación y la conducta quedaría impune"[24].

ii. Interferir. Según la RAE, interferir significa "cruzar, interponer algo en el camino de una cosa, o en una acción. Causar interferencia. Introducirse en la

[24] Huerta M., Marcelo y Líbano M., Claudio, Op. Cit., pp. 300 y 301. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

recepción de una señal otra extraña y perturbadora". Esta definición parece insuficiente para el ámbito punitivo, por ello, desde el punto de vista de la informática y del bien jurídico protegido por la ley, se concluye que la interferencia supone "una alteración de la calidad, pureza e idoneidad de la técnica de la ciencia informática, mediante la acción recíproca de las ondas de la que resulta un aumento, disminución o neutralización del movimiento ondulatorio original de los impulsos eléctricos, operada utilizando métodos tecnológicos modernos, ya sea con el fin de apoderarse de ella, de usarla , o, conocerla"[25].

Lo anterior hace relevante destacar la diferencia entre las conductas de interceptación e interferencia, pues ambas se asemejan en el hecho que la información se conocerá pero, de igual manera, llegará a su destinatario. En consecuencia, tal elemento es insuficiente, sin embargo, el factor diferenciador se sitúa en que en la interceptación la información llegará incólume al destinatario, mientras que en la interferencia la información captada será enviada al receptor en forma imperfecta en lo que toca a su veracidad y fidelidad. Por lo tanto la interferencia implica interceptar y, a la vez, se suma la acción del agente en orden a modificar la información, a fin que, el destinatario reciba un contenido diverso.

iii. Acceder. Según la RAE el acceso "es la entrada o paso a un lugar", el que tendrá distintas connotaciones de si el acceso es lícito o ilícito.

Existe una diferencia entre los conceptos de acceso e interceptación. El acceso implica el ingreso al sistema automatizado de tratamiento de información, pudiéndose conocer la totalidad de la información contenida en el computador; mientras que mediante la interceptación sólo se puede conocer la información que está siendo transmitida o emitida, pero no se puede inmiscuir en otras bases de datos contenidas en el sistema. Ambos procederes permiten conocer la información, pero el ámbito de intromisión es más limitado en la interceptación que en el acceso, siendo entonces éste último más peligroso para los sistemas.

Por último, el diputado Viera-Gallo señaló que "la idea, para que quede bien precisa, es que esta interceptación, interferencia o acceso al sistema se haga mediante métodos tecnológicos. No se trata de que una persona, por casualidad, entre a una sala donde hay un computador y lea en la pantalla lo que ahí aparece, aunque lo haga con el ánimo de apoderarse de la información, sino que, utilizando métodos tecnológicos modernos realice algunas de las conductas tipificadas en el artículo 2°".

b. Elementos Subjetivos

El tipo del artículo 2° exige la realización objetiva de las conductas descritas, debiendo además concurrir elementos subjetivos que integran el tipo penal. No basta con que el sujeto activo intercepte, interfiera o acceda a un sistema de

[25] Huerta M., Marcelo y Líbano M., Claudio, Op. Cit., p. 300. Citado por Piedrabuena R., Guillermo.

tratamiento de la información, sino que es indispensable que se realice tales conductas con el ánimo de apoderarse, usar, o conocer indebidamente la información contenida en él. No es necesario para la configuración del tipo, que objetivamente haya apoderamiento, conocimiento, o uso de información, sino que basta que se pruebe que se ha interceptado, interferido, o accedido a un sistema con la intención de adueñarse, conocer o utilizar información contenida en el computador.

En consecuencia, se entiende por los términos apoderarse, usar, conocer e indebidamente:

i. Apoderarse: "Hacerse uno dueño de alguna cosa, ocuparla, ponerla bajo su poder". A este respecto durante la discusión en el Senado del proyecto de ley, en la sesión 50, el senador Otero expresó:" El artículo 2° comienza con la frase: 'el que con ánimo de apoderarse indebidamente de la información' (…) Pero las expresiones "apoderarse indebidamente", en materia informática, significan hacerse para uno, quedando fuera dos elementos que también deberían estar en el tipo que son "usar y conocer", porque debe castigarse no sólo al que se apodera de información para hacerse de ella, sino también al que interfiere para usarla y al que interfiere para conocerla, pues muchas veces conocer la información es suficiente como para caer dentro de los términos del proyecto".
   No es necesario para que se configure el apoderamiento que el sujeto utilice o lucre con la información, bastando con que ella ingrese a su esfera personal.

ii. Usar: "Hacer servir una cosa para algo, o bien, disfrutar uno alguna cosa" (RAE). Esta acción remite al aprovechamiento de la información obtenida, de forma más amplia que el apoderamiento. Sin embargo es preciso conocer que quien se apodera de información no buscará su mero atesoramiento. El tipo penal no exige para su configuración que la utilización o aprovechamiento de la información deba ir acompañada de un ánimo de lucro, sino que basta que se utilice la información para cualquier fin.

iii. Conocer: Implica averiguar por el ejercicio de las facultades intelectuales la naturaleza, cualidades y relaciones de las cosas.

   Aunque parece difícil, es posible la hipótesis del mero conocimiento, bastando solamente la interceptación, interferencia o acceso a un sistema de tratamiento de información, con el ánimo de saber cierta información que se encuentre en él, pero sin que la persona luego la use.

iv. Indebidamente: Este término es fundamental pues tiñe a todo el tipo penal de una connotación de ilicitud, antijuridicidad, de un procedimiento contrario a derecho, de una violación de prohibiciones. Con lo anterior se resalta la carencia de ética en la utilización de conocimientos específicos con el solo objetivo de vulnerar las medidas de seguridad e ingresar, de esa manera, a los sistemas de información a fin de utilizar para su propio beneficio la información contenida en ella.

La historia de la ley contribuye al esclarecimiento del sentido del vocablo en cuestión. De acuerdo a ella el término indebidamente significa "sin derecho"[26]. "Sin derecho significa que la persona no tiene la posibilidad legal de acceder, sin embargo, lo hace cometiendo abuso. Quien debe determinar eso en última instancia es el magistrado. Obviamente, existen tres situaciones: en el primer caso, el sistema de información al que simplemente el público no tiene acceso, porque es privado y nadie puede tenerlo, salvo el propietario o personas que él autorice; en el segundo, puede haber sistemas de información en los que, para acceder, se cobre una determinada cuota o pago, y pudiera ocurrir que alguien ingresara a ese sistema burlando el pago correspondiente, y, en el tercero, existen sistemas de información que, además, están protegidos por ciertos resguardos de la seguridad nacional, relacionados con sistemas de información de las Fuerzas Armadas o de los aparatos de inteligencia"[27].

El principal problema del adverbio "indebidamente" se produce en el acceso a los sistemas automatizados de información. El acceso indebido implica la realización de conductas o pericias tendientes a penetrar a un sistema automatizado de tratamiento de información, burlando todas las medidas de seguridad, para lograr la información reservada que contiene, recabarla y eventualmente utilizarla en beneficio o en perjuicio de terceros. La anterior conducta es lo que se conoce como el delito de *hacking*.

Sin embargo la ley chilena solo considera como delito el *hacking* que se realiza con el fin de apoderarse, usar o conocer información (espionaje informático), o para cometer sabotaje informático, fraude informático (hecho atípico). Es decir, el acceso indebido en estos casos es solamente un medio necesario para la comisión de un delito. Lo anterior se conoce en doctrina como *hacking* indirecto, el cual se considera como delito, a la luz de la legislación chilena, en la medida que haya espionaje informático o sabotaje.

En cuanto al *hacking* propiamente tal, esto es, el acceso a un sistema vulnerando las medidas de seguridad sin la concurrencia de un ánimo de apoderarse, conocer o usar indebidamente la información contenida en él, acá la finalidad es una satisfacción de carácter intelectual, consistente en el desciframiento de *passwords*, que en jerga informática se conoce como *joy riding*. Esta forma de *hacking* es atípica en nuestra legislación, pese a poner en peligro múltiples bienes jurídicos tales como la idoneidad, pureza y calidad de la información, la propiedad, seguridad, etc.

[26] En el proyecto original el tipo del artículo 2° tenía el siguiente tenor en su parte primera:" El que sin derecho intercepte, interfiera o acceda a un sistema...".
[27] Boletín Oficial N° 412-07 de la Honorable Cámara de Diputados y Senadores de Chile, Cámara de Diputados, sesión N° 24, en martes 4 de agosto de 1992, p. 1970. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

2.2. Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información. Artículo 4°.

a. Sujetos Activos

Esta figura delictiva se diferencia de la anterior en cuanto al sujeto activo, pues no obstante la formulación amplia con la que comienza el artículo 4°, "El que...", su ámbito de aplicación se restringe sólo a aquellos sujetos que tengan autorización para ingresar al sistema automatizado de tratamiento de información, debiendo agravarse la penalidad respecto de aquellos que, además, sean los responsables del mismo[28] (inciso 2° artículo 4°).

Esta conclusión resulta de la lectura conjunta de los artículos 2° y 4°, ya que el primero sanciona los accesos indebidos, los cuáles serán efectuados, obviamente, por quienes carecen de autorización para penetrar al sistema y lo hacen a través de maniobras tendientes a burlar las medidas de seguridad del mismo. Es más, la agravante del inciso 2° del artículo 4° sirve de argumento de texto, pues si se está agravando la sanción de quien es responsable del sistema se sub entiende que, además, tiene autorización para acceder a él.

Esta interpretación no implica afirmar que aquellos que carezcan de permiso para acceder al sistema e incurran en conductas de revelación o difusión, no cometerían una acción típica, fundamentalmente por dos razones:

1. La conducta de "revelación indebida" apunta precisamente a sujetos que tienen una obligación de reserva o secreto respecto de la información contenida en el sistema, y necesariamente dicha obligación debe emanar de un vínculo previo entre el sujeto activo y el propietario o encargado del sistema, pues hay un depósito de confianza en virtud de éste vínculo. El vocablo "indebida" implica la carencia de derecho para dar a conocer la información "reservada", o lo que es lo mismo, que se carece de autorización expresa para excepcionar la obligación de reserva; mientras que en el artículo 2° la expresión "indebida" reviste de ilicitud los procedimientos utilizados (interceptación, interferencia, o, acceso) para conocer la información, no porque ellos sean ilícitos en sí mismos, sino por la circunstancia que se han dirigidos a una base de datos restringida o cerrada, es decir, solo pueden ingresar aquellos que tengan la posibilidad legal de hacerlo.

2. La conducta de difusión sí que es posible que la ejecuten los sujetos activos del artículo 2°, pues la conducta de difundir no implica necesariamente que quien lo haga tenga, a su vez, obligación correlativa de guardar secreto de ella, en consecuencia, la acción puede ser ejecutada por quienes tienen derecho para acceder al sistema y por quienes carecen de él.

[28] Persona responsable del sistema de tratamiento de información será aquella que tiene a su cargo la dirección y vigilancia del mismo siendo absolutamente irrelevante, a estos efectos, su eventual o especial capacidad técnica superior. Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

b. *Modus Operandi*

El texto legal castiga dos conductas: la revelación y la difusión maliciosa de datos. Ambas persiguen resguardar la fidelidad en la custodia de información, evitándose la vulneración del deber de reserva que pesa sobre el sujeto sea el responsable o no del sistema.

- Revelación de los datos contenidos en un sistema de información.

Según la RAE, revelar significa descubrir o manifestar lo ignorado o secreto. Tal acción presupone a lo menos la existencia del derecho para que el operador dé acceso a la información, con la correlativa obligación de reserva, de suerte que ésta no pueda ser conocida por terceros que carezcan de acceso a ella.

- Difusión de los datos contenidos en un sistema de información.

Según la RAE, difundir significa propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc. Al igual que en la letra anterior, se requiere que la información difundida tenga el carácter de reservada o secreta.

El tipo penal no exige que los datos sean secretos, pero puede interpretarse que sólo deben protegerse o quedar bajo el amparo del tipo penal, aquellos datos que sean de interés, por ejemplo, económico, estratégico, íntimos, etc., para el sujeto pasivo. Al ocuparse la expresión revelar parece confirmarse esta apreciación.

3. Sentido y Alcance de la expresión "maliciosamente", utilizada en los artículos 1°, 3° (ambos constitutivas de sabotaje informático), y 4° (espionaje informático)

Este término ha originado numerosas divergencias jurisprudenciales y doctrinales. Son dos los aspectos que abarcan este punto: a) Contenido de la expresión maliciosamente; y b) Incidencia en la carga probatoria.

Los siguientes fallos se han hecho cargo de los puntos en cuestión[29]:

a. Corte de Apelaciones de Valparaíso, año 1981: "Las expresiones 'maliciosamente' y 'maliciosa' utilizadas en el número 4° del artículo 97 del Código Tributario, no importan la exigencia de un requisito anímico especial ni dan origen a un elemento subjetivo del tipo penal. Su significado no es otro el de 'intencional' y su finalidad es exigir del tribunal una especial atención a la prueba del dolo, sin que baste la sola presunción del mismo, contemplada en el artículo 1° del Código Penal" (Revista Derecho y Jurisprudencia (RDJ), tomo LXXVIII, N° 2°, sección IV, año 1981, p. 199).

[29] Estos fallos son a propósitos de otros tipos penales, pues a la fecha no hay jurisprudencia que interprete el término maliciosamente en la Ley N° 19.223. Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

b. Corte de Apelaciones de Santiago, año 1985: "La presunción establecida en el inciso 2° del artículo 1° del Código Penal no tiene aplicación si la existencia del delito requiere del llamado dolo específico, que importa la intención precisa de causar determinadas consecuencias. Cuando la ley lo exige emplea la palabra 'maliciosamente' o la frase 'con malicia', como ocurre en el artículo 198 del mencionado Código, corresponde probar al sentenciador que el inculpado obró con intención criminal de hacer uso o aprovecharse del documento falso" (RDJ, tomo LXXXII, N° 2°, sección IV, año 1985 p. 182).

c. Corte de Apelaciones de Santiago, año 1997: "Para la configuración de la infracción tributaria del N° 7° del artículo 97 del Código Tributario, se requiere un dolo específico respecto de las declaraciones incompletas de impuestos hecha por el contribuyente, denotado por el adverbio "maliciosamente". Esta especie de dolo debe ser probado por la parte acusadora, por no tratarse del dolo común del artículo 1° del Código Penal" (Gaceta Jurídica N° 207 página 227, año 1997).

d. Corte de Apelaciones de Santiago, año 1990: "El dolo específico existe cuando la voluntad se orienta hacia una meta especial contenida en la finalidad general que persigue el delincuente y, cuando la ley lo exige, emplea las palabras "con malicia" o el adjetivo "malicioso". Esta modalidad del dolo directo, no queda comprendida en la presunción del inciso 2° del artículo 1° del Código Penal". (Gaceta Jurídica N° 117, página 82, año 1990).

e. Corte Suprema de Justicia, año 1995: "En resumen, la sentencia que se impugna por el recurso de casación absolvió al procesado únicamente por estimar que su acción estuvo desprovista de dolo, de modo que, aunque se daban todos los demás elementos del delito, cabía concluir que no había incurrido en el delito de daños por carecer de dolo su acción.

El sentenciador exigió un requisito que no exige la ley para configurarlo, al requerir un dolo específico, o sea acto deliberadamente encaminado al propósito de perjudicar a un tercero.

Que la sentencia que se impugna ha estimado probado los hechos que acepta el recurrente, de modo que la infracción de las leyes que denuncia del Código Penal es clarísima, toda vez que los artículos 484 y 487 del Código Punitivo sancionan a aquellos que causen daño en propiedad ajena, sin requerir dolo específico o directo, como se expresa en aquellas sentencia, para lo cual basta la simple lectura de esos preceptos, de los que se infiere claramente que el legislador no ha contemplado tal requisito, como sucede en otros hechos punibles en que emplea las expresiones 'actuar maliciosamente' o 'a sabiendas' o 'con conocimiento de causa'. Fluye así infracción al artículo 1° del CP. Toda vez que el delito de daños tipificado en los artículos 484 y 487 de dicho Código se rige por la presunción de dolo que se establece en el artículo 1° recién citado". (RDJ, tomo XCII, sección IV, año 1995, p.230).

La jurisprudencia citada permite extraer dos conclusiones:

- Cuando el legislador emplea la expresión "maliciosamente", traslada la carga probatoria sobre el dolo a la parte que lo alega. En otros términos, la presunción de dolo contemplada en el inciso 2° del artículo 1° del Código Penal[30] no opera, y consiguientemente debe rendirse prueba para acreditar el conocimiento e intención de realizar una determinada figura delictiva y de querer la consecución de su resultado.

- En relación al tipo de dolo que abarca la expresión "maliciosamente", el término en su acepción natural y obvia indica la idea de una voluntad conciente y determinada no solo de realizar una conducta típica y antijurídica sino que, además, el agente se encuentra animado a lograr la producción del hecho punible y, su plasmación en la realidad mediante la consecución de sus resultados. Por lo tanto los tipos penales (artículos 1°, 3° y 4°) requieren de dolo directo, quedando excluidos el dolo de consecuencias seguras o necesarias y el dolo eventual.

  Igualmente, una acción puede iniciarse sin la concurrencia de dolo directo, enmarcándose dentro de algunos de los tipos descritos, pero, los actos que componen el hecho pueden adquirir dolo directo; por ejemplo, un *hacker* puede quebrantado los sistemas de seguridad de un computador sin el propósito de apoderarse de su información, es decir, solo busca efectuar un *joy riding*, sin embargo, puede ocurrir que dentro del sistema detecte información de relevancia y decida apoderarse de ella.

V. El Fraude Informático

1. Concepto

Para Casabona[31], el fraude informático es "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 computador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de tercero". Por su parte, Corcoy y Joshi señalan que las estafas por computador son las manipulaciones del proceso de elaboración electrónica de cualquier clase y en cualquier momento de este, con la intención de obtener un beneficio económico, causando a un tercero un perjuicio patrimonial[32].

---

[30] "Las acciones u omisiones penadas por la ley se reputan siempre voluntarias, a no ser que conste lo contrario".
[31] Citado por Magliona Marcovicth, Claudio y López Medel, Macarena; Delincuencia y Fraude Informático, Ed. Jurídica, 1999, p. 184.
[32] Corco y Bidasolo, Mirentxu y Joshi, Ujala, Delitos contra el patrimonio cometidos por medios informáticos, en Revista Jurídica de Catalunya, 1988, p. 687. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

2. Bien Jurídico protegido[33]

A diferencia del delito informático, del que puede decirse propiamente que el bien jurídicamente protegido es colectivo y se traduce en la información (almacenada, tratada y transmitida a través de sistemas informáticos) como valor económico de la actividad de la empresa[34], respecto del fraude informático el verdadero bien jurídico a tutelar 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[35]. Esta es la perspectiva europea, donde autores como González Rus clasifican los delitos entre aquellos en que los sistemas informáticos o sus elementos son el objeto material del mismo, y aquellos en que son el instrumento del mismo. En este último grupo, el autor incluye a los delitos cometidos mediante sistemas informáticos o utilizando elementos de naturaleza informática, que son entonces el medio utilizado para la comisión de un ilícito patrimonial o socio económico[36].

3. Elementos del delito

De acuerdo con la definición señalada, los elementos del delito de fraude informático, en general, son los siguientes:

a. Modificaciones en el sistema de procesamiento de datos.
b. Animo de lucro o de obtención de beneficios ilícitos.
c. Utilización de elementos propios del fraude[37].

4. Las modificaciones o manipulaciones de datos

La doctrina señala que el computador debe ser considerado como una instalación de procesos de datos, esto es, como una instalación en la que se introducen los datos que se tienen que procesar (el denominado *input*) y la forma de proceso deseada (a través del programa los recursos de consola complementarios), obteniéndose automáticamente el resultado del proceso (el denominado *output*)[38].

---

[33] Piedrabuena R., Of. N° 422, del Ministerio Público.
[34] Reyna Alfaro, Luis Miguel; Perú: El Bien Jurídico en el delito informático, en Revista Electrónica de Derecho Informático Nº 33, abril de 2001. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[35] Kindhäuser, Urs; La estafa mediante computadoras en el Código Penal Alemán (§ 263ª StGB), mimeo, trad. de Héctor Hernández B. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[36] González Rus, Juan José; Protección penal de sistemas, elementos, datos, documentos y programas informáticos, en Revista Electrónica de Ciencia Penal y Criminología, Nº 1, 1999. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[37] Camacho Losa señala que debe existir un comportamiento o manipulación que reúna las notas configuradoras de una defraudación y no basta con la simple alteración de los elementos informáticos, citado en Magliona Marcovitch, Claudio y López Medel, Macarena; Op. Cit., p. 185 y 186. Asimismo, en la clasificación de delitos informáticos de Davara Rodríguez se habla de "Utilización del computador con fines fraudulentos", y Gutiérrez Frances se refiere a los "delitos económicos vinculados a la informática", citados en Villalobos, Carlos; El delito informático, disponible en: http://bcn.cl/1tr79 (Febrero, 2010).
[38] Sieber, Ulrich; Criminalidad informática: peligro y prevención, en Mir Puig, Santiago (comp.); Delincuencia Informática, PPU, Barcelona, 1992, p. 15 y 16; González Rus, Juan José; Ob. cit., nota 92. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

a. Manipulaciones de *input*

Consisten en el suministro de datos falsos al computador, mediante la modificación de datos reales, o introduciendo datos completamente ficticios. También puede producirse por la omisión de registro de datos[39].

b. Manipulaciones en el programa

Lo que se modifica son los programas (*set* de instrucciones entregados a un computador que debe conformarse con las tareas actuales que deben ser realizadas[40] o la conducción fijada en forma de datos de cada uno de los pasos del tratamiento de datos[41]), modificándolos o interfiriéndolos, rescribiendo la totalidad de las instrucciones o adicionando o alterando un determinado paso del programa.

El sujeto activo transforma o modifica los programas existentes en una empresa (especialmente añadiendo rutinas del tipo "caballo de Troya"[42] o usando virus) o aplica programas adicionales para alterar los datos almacenados en un banco de datos.

c. Manipulaciones de consola

En este caso, al igual que en el anterior, se trata de una manipulación de computador pero no de programas, sino de los elementos del servicio mecánicos de la instalación del proceso de datos, en el *hardware* o en la consola[43].

d. Manipulaciones del *output*

En este caso se produce un cambio o alteración de los datos de salida, es decir, el resultado del procesamiento de estos, el que, siendo correcto, no se compadece con los datos producidos por causa de una manipulación posterior, cuando son reflejados por escrito, o cuando son registrados por una banda magnética[44], etc.

Esto ocurre cuando se interviene la parte mecánica de la emisión (impresión, video, teles, teléfono). Por ejemplo, puede intervenirse el cable telefónico para interceptar los datos y manipularlos[45].

---

[39] Magliona Marcovitch, Claudio y López Medel, Macarena; O. Cit., p. 192, citando a Romeo Casabona. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[40] Ibídem, p. 328. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[41] Kindhäuser, Urs. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[42] Esta manipulación consiste en introducir modificaciones en el programa que permite la realización por el computador de actividades rutinarias privilegiando a un sujeto determinado, por ejemplo, incorporando un paso al programa por el cual, cada vez que se digita una clave de acceso, se transfieran fondos a una persona determinada, en Corcoy Bidasolo, Mirentxu y Joshi, Ujala; Op. Cit., p. 135, nota 11, y Sieber, Ulrich; Documentación para una aproximación al delito informático, en Mir Puig (comp.); Santiago; Op. Cit., p. 87. Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[43] Sieber, Ulrich; Criminalidad Informática, p. 20. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[44] Sieber, Ulrich; Criminalidad Informática, p. 21; Magliona Marcovitch, Claudio y López Medel, Macarena; Op. Cit., p. 194. Citados por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
45 Corcoy y Bidasolo, Mirentxu y Joshi, Ujala; Op. Cit., p. 136. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

VI. Fraude Informático en Chile

En el ámbito internacional existe una serie de denominaciones para clasificar algunos casos que derivan en principalmente de la clonación de tarjetas. Dentro de ellas, a modo meramente ejemplar, podemos destacar las conductas denominadas "*piggybacking*" e "*impersonation*"[46].

Como se señaló, la Ley N° 19.223, que tipifica figuras relativas a la informática, contiene cuatro artículos que sancionan preferentemente algunas conductas de espionaje y sabotaje informático.

Una posible falencia de esta ley es que no incorpora una figura penal de fraude informático, que es una de las formas utilizadas por la doctrina internacional para sancionar los casos de clonación de tarjetas.

El tipo penal que normalmente se emplea para abordar este tipo de conductas es el artículo 2 de la Ley N° 19.223.

Artículo 2°: "El que con ánimo de apoderarse, usar, o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

Este tipo penal presenta algunas dificultades para su aplicación, especialmente en los casos de clonación de tarjetas, principalmente respecto a los siguientes puntos:

1. ¿Por qué medio se accedió a la información?

El acceso según la RAE "es la entrada o paso a un lugar"[47].

En el caso de la clonación, los medios tecnológicos son utilizados para copiar la banda magnética de la tarjeta, pero no para lograr un acceso al sistema, ya que normalmente se accede mediante una tarjeta clonada, de la cual se conocen sus claves de acceso. Distinto sería, si mediante un computador conectado al cajero o a la red del banco, se lograra obtener la clave de acceso de la tarjeta, vulnerando los sistemas informáticos.

2. ¿Cuál es el ánimo especial que debe concurrir en el sujeto activo?

Respecto del sujeto activo el tipo penal contempla una formulación amplia, utilizando la expresión "el que". La única restricción es que este sujeto no se encuentre autorizado para ingresar al sistema. En este sentido, no existen mayores inconvenientes, dado que quienes utilizan Tarjetas clonadas no están autorizados para ingresar al sistema.

---

[46] "Huerta Miranda, Marcelo y Líbano Manzur, Claudio, Delitos Informáticos, 2ª edición, Editorial Conosur Ltda. Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.
[47] Disponible en: http://bcn.cl/1tr7a (Diciembre, 2015). Citado por Piedrabuena R., Guillermo, en Of. N° 422, del Ministerio Público.

El problema se presenta con el ánimo especial que debe concurrir en el sujeto (ánimo de apoderarse, usar, o conocer indebidamente la información contenida en él sistema de tratamiento de datos). Se entiende que este ánimo está presente en el sujeto al momento de realizar la copia de la banda magnética, pero cuando ya tiene esta información y ha clonado la tarjeta, su ánimo es apoderarse del dinero o crédito que pudiese existir en la cuenta, pero no de la información que ella contiene. Este punto es importante cuando se pretende aplicar este tipo penal, ya que como se señaló, el bien jurídico protegido por esta Ley es la calidad, pureza e idoneidad de la información.

VII. Competencia Territorial. Problemas de Jurisdicción

Básicamente, los ataques informáticos son de dos tipos: si la conducta se despliega dentro de la estructura donde se encuentra el sistema de tratamiento de información (*insiders*) como bancos, empresas, organismos públicos, etc., o si se lleva a cabo desde a fuera de ellas, es decir, por vía remota (*outsiders*).

El grueso de los delitos informáticos más relevantes (fraude informático, sabotaje informático, espionaje informático, *hacking* directo, etc.) puede realizarse remotamente, es decir, el hechor puede infiltrarse mediante un computador en otro sistema automatizado de tratamiento de información, y hurtar o alterar datos, introducir virus informáticos, etc. La modalidad remota puede plantear los siguientes escenarios:

1. El sujeto activo realiza la acción dentro del mismo País o Estado en que se ubicada el sistema automatizado de tratamiento de información afectado por el ataque informático. Por ello pueden darse las siguientes variantes:

a. Sujeto activo y sistema de tratamiento de información están ubicados en distintas regiones.

b. Sujeto activo y sistema de tratamiento de información están ubicados dentro de la misma región pero en territorios jurisdiccionales diferentes.

2. El sujeto activo realiza la conducta desde un Estado distinto del cual en que se encuentra ubicado el computador objeto del ataque informático.

Los escenarios planteados descansan sobre una base común: víctima y actor están separados, nacional o transnacionalmente. El punto es crucial, pues la distancia produce problemas en cuanto a la legislación aplicable y la jurisdicción o competencia de los tribunales. A este respecto cabe tener presente el artículo 157 del Código Orgánico de Tribunales señala en su inciso primero que "será competente para conocer de un delito el tribunal en cuyo territorio se hubiere cometido el hecho que da motivo al proceso"; conjuntamente, el inciso final dispone: "el delito se considerará cometido en el lugar donde se dio comienzo a su ejecución". Por lo tanto, el lugar donde el sujeto activo cometió la conducta típica a distancia mediante un computador, es el elemento determinante, pues desde aquél espacio el sujeto tiene el control de las acciones tendientes a la realización del

ataque informático. Lo anterior es aplicable tanto al ámbito nacional como internacional.

VIII. Proyecto de Ley que tipifica y sanciona los delios informáticos y deroga la Ley N° 19.223 (Boletín N° 10.147-07)

El proyecto de ley que tipifica y sanciona los delitos informáticos y deroga la ley N° 19.223 modifica los delitos informáticos, introduce modificaciones en materia procesal penal para facilitar la persecución de éstos delitos, y deroga la Ley N° 19.223.

Pese a que el objetivo de este Informe no es analizar exhaustivamente el proyecto de ley mencionado, se pueden señalar algunas características de él:

a) Artículo 1°:

- Se mantiene el delito de destrucción o inutilización de sistema informático de tratamiento computacional de datos.
- Se mantiene la pena de presidio menor en su grado medio a máximo.
- Se modifica el objeto del delito "sistema de tratamiento de información o sus partes o componentes" por "sistema informático de tratamiento computacional de datos, o sus partes o componentes lógicos".
- Se crea una nueva circunstancia agravante de responsabilidad penal consistente en que la conducta "recayere sobre sistemas de los cuales dependan la defensa nacional, la seguridad pública o la infraestructura crítica del país, como por ejemplo servicios públicos de agua potable, alcantarillado, electricidad, transporte, redes domiciliaras de gas o redes cableadas o inalámbricas de telefonía o computación, caso en que la pena será de presidio menor en su grado máximo a presidio mayor en su grado mínimo.
- Se mantiene exigencia de dolo directo en el tipo penal.

b) Artículo 2°:

- Se crea un nuevo delito consistente en acceder o usar, sin derecho, información contenida en un sistema informático de tratamiento de datos, sancionándose con presidio menor en su grado mínimo a medio.
- Este delito no exige explícitamente dolo directo.
- Se crea el delito de impedir a otro por vía informática, acceder a sus datos personales u otros de su propiedad intelectual.

c) Artículo 3°:

- Se crea el delito de alterar, dañar o destruir los datos contenidos en un sistema informático de tratamiento de datos, sancionado con presidio menor en su grado medio. Hasta ahora esta hipótesis constituye una agravante del delito de destrucción o inutilización contenido en el artículo 1 de la Ley N° 19.223.
- El delito requiere de dolo directo.
- Se reitera la agravante de que la conducta recaiga sobre sistemas de los cuales dependan la defensa nacional, la seguridad pública o la infraestructura crítica del país, como por ejemplo servicios públicos de agua potable,

alcantarillado, electricidad, transporte, redes domiciliaras de gas o redes cableadas o inalámbricas de telefonía o computación, aplicándose la misma pena.

d) Artículo 4°:

- Se modifica el delito de revelar o difundir los datos contenidos en un sistema informático de tratamiento de datos. La modificación recae sobre el objeto del delito, que hasta ahora consiste en que los datos deben ser contenidos en un sistema de información, pasando a ser ahora, "datos contenidos en un sistema informático de tratamiento de datos".
- Las pena sigue siendo de presidio menor en su grado medio.
- Se crea una agravante consistente en que si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumenta en un grado.
- Se reitera la agravante de que los datos correspondan a un sistema del cual dependa la defensa nacional, la seguridad pública o la infraestructura crítica del país, como por ejemplo servicios públicos de agua potable, alcantarillado, electricidad, transporte, redes domiciliarias de gas o redes cableadas o inalámbricas de telefonía o computación, aplicándose la misma pena.

e) Artículo 5°

- Se crea un delito consistente en "La tenencia, posesión, producción, venta, difusión, o cualquier otra forma de puesta a disposición de dispositivos, programas informáticos, aplicaciones, claves, códigos de acceso u otro tipo de elemento informático que permitan o faciliten la comisión de delitos.
- La pena es de presidio menor en su grado mínimo a medio.
- La norma no señala de que delitos se trata, pudiendo ser delitos de la ley que se propone, o de otra ley.
- La norma no distingue entre elementos ilícitos o lícitos, como por ejemplo, una antena de wifi, pendrives, etc.

f) Artículo 6°

- Se introducen las figuras de interceptación o grabación de comunicaciones, e intervención de agentes encubiertos, en caso de sospechas fundadas de que una persona o una organización delictiva, hubiere cometido o preparado la comisión de alguno de los delitos previstos en esta ley, y la investigación lo hiciere imprescindible.
- La facultad judicial es previa petición del Ministerio Público.
- El Tribunal podrá autorizar a Carabineros de Chile o la Policía de Investigaciones para mantener un registro reservado de producciones del carácter investigado. No se detalla de que tipo de "producciones" se trata.
- Se permiten las entregas vigiladas de material respecto de la investigación de hechos que se instigaren o materializaren a través del intercambio de dichos elementos, en cualquier soporte.

g) Artículo 7°

- Se crea un delito especial de exacción patrimonial consistente en: "El que sin la voluntad de su dueño y con ánimo de lucrar, transfiriere u obtuviere la transferencia de cualquier activo patrimonial de un tercero empleando medios informáticos", sancionado con presidio mayor en sus grados mínimo a medio.

h) Artículo 8°

- Se crea una agravante especial nueva consistente en que si quien incurriere en las conductas descritas en los artículos anteriores fuere responsable del sistema de información, la pena se aumentará en un grado.

i) Artículo 9°

- Se crea una nueva circunstancia agravante, genérica, en el artículo 12, circunstancia 22ª en el Código Penal, consistente en: "22a. Emplear, en cualquiera de sus etapas, medios informáticos para ejecutarlo, entendiéndose por tales cualquier sistema informático de tratamiento de datos de la información.".

j) Artículo 10°

- Se modifica el Código Procesal Penal para introducir las normas procesales penales recién señaladas.

k) Artículo 10º

- Toda persona natural o jurídica que, a cualquier título, mantenga o provea acceso a sistemas informáticos de tratamiento de datos, tales como empresas telefónicas, de comunicaciones o de cualquier naturaleza, bancos, establecimientos educacionales, establecimientos comerciales que presten servicios de comunicación digital al público, así como los titulares de redes públicas de conexión inalámbrica, queda obligada a interceptar y grabar comunicaciones por orden judicial, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera.
- Además deberán mantener, en carácter reservado por un lapso no inferior a quince años, a disposición del Ministerio Público, un listado actualizado de los números IP asignados a las conexiones que realicen sus abonados con sus correspondientes fechas y horas, así como de las direcciones físicas asociadas.
- El encargado de estos registros deberá poner esos datos técnicos a disposición del Ministerio Público, previo requerimiento de información del fiscal a cargo de la investigación, dentro del plazo de veinticuatro horas o del que señale la petición.
- La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación autorizada judicialmente será constitutivo del delito de desacato, en tanto que el incumplimiento frente al requerimiento de información del Ministerio Público constituirá el delito de obstrucción a la investigación.
- El fiscal respectivo deberá ejercer las acciones penales que procedan contra el responsable de la negativa, entorpecimiento o incumplimiento tan pronto

se haya cumplido el plazo dentro del cual la empresa haya debido cumplir con la obligación que se establece en este inciso.

- El fiscal que incumpliere esta obligación dentro del plazo prescrito en el artículo 176, incurrirá en el delito previsto y sancionado en el artículo 177.
- Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento.

l) Artículo 11

Se sancionan la tentativa y la frustración de los delitos contemplados en esta ley, de acuerdo con las reglas generales contenidas en el Párrafo 4°, del Título III del Libro Primero del Código Penal.

IX. Legislación Comparada

A continuación se analizan someramente algunas normativas internacionales, y algunas legislaciones extranjeras en las que se ha encontrado coincidencias. Las normativas y los países seleccionados responden a que en ellos se ha normas aplicables a la materia.

1. Convenio del Consejo de Europa sobre la Cibercriminalidad

En el seno del Consejo de Europa[48] se suscribió la Convención sobre Cibercriminalidad[49] (Budapest, 23 de Noviembre de 2001), cuya firma está abierta a todos los países del Mundo, sean o no parte del Consejo.

Rueda Martín, en "Cuestiones político – criminales sobre las conductas de *hacking*"[50], señala: "El Convenio del Consejo de Europa sobre Cibercriminalidad recoge en su capítulo II un conjunto de medidas que deben ser adoptadas por todos los estrados parte para prever como infracción penal una serie de conductas contempladas en dicho Convenio: el acceso ilícito a la totalidad o a una parte de un sistema informático (art. 2°), la interceptación ilícita de transmisiones privadas de datos informáticos (art. 3°), atentados contra la integridad de datos informáticos (art. 4), atentados contra la integridad de un sistema (art. 5°), la producción, venta, utilización, importación, distribución o cualquier forma de hacer posible cualquier dispositivo, password electrónico, código de acceso o datos similares con la finalidad de cometer las infracciones de los arts. 2°, 2°, 4° y 5° (art. 6°), falsedades informáticas (art. 7°), fraude informático (art. 8°), infracciones relacionadas con la pornografía infantil (art. 9°) e infracciones relacionadas con las violaciones de los derechos de propiedad intelectual y derechos afines (art. 10°) (…)".

[48] El Consejo de Europa es una organización creada en 1949 con el fin de promover el desarrollo de todos los países europeos basado en los principios democráticos comunes y en la Convención Europea de Derechos y Libertades Fundamentales, entre otros instrumentos suscritos en su seno.
[49] Disponible en: http://bcn.cl/8bd0 (Diciembre, 2015).
[50] Rueda Martín, María, Derecho Penal Contemporáneo, Revista Internacional, N° 28, Enero, 2009, Editorial Legis, Bogotá, Colombia, N° 28, pp. 151 y ss.

El artículo 2° del Convenio establece: "Los Estados Parte deberán adoptar las medidas legislativas y otras que resulten necesarias para establecer como infracción criminal, conforme a su derecho interno, el acceso intencional si autorización a ls totalidad o parte de un sistema informático. Los Estados podrán requerir que el hecho sea cometido infringiendo medidas de seguridad o con la finalidad de obtener datos u otra finalidad deshonesta o, en relación con los sistemas informáticos, que se encuentren conectados a otros sistemas informáticos.".

Luego, el n° 1 del artículo 6° del Convenio ordena a los Estados Partes "… a adoptar las medidas legislativas o de otro género que fuesen necesarias para establecer como infracción criminal la comisión dolosa y antijurídica …" de una serie de conductas enumeradas.

En síntesis, los delitos informáticos, de acuerdo al Consejo de Europa, pueden ser clasificados en los siguientes cuatro tipos:

a. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: Sanciona el acceso y la interceptación ilegal, interferencia de datos y sistemas y el mal uso de dispositivos.
b. Delitos de fraude informático: Falsificación y fraude computacional.
c. Delitos por su contenido: Producción, diseminación y posesión de pornografía infantil.
d. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: La amplia gama de reproducciones ilícitas, por medios informáticos, de obras protegidas por el derecho de autor.

2. Decisión Marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información

La Unión Europea ha adoptado dos Directivas para la aproximación de las normas nacionales sobre protección de la intimidad en lo que se refiere al tratamiento de datos personales. El artículo 24 de la Directiva 95/46/CE obliga claramente a los Estados miembros a adoptar las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la misma y a determinar, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones de las leyes nacionales. Los derechos fundamentales a la intimidad y la protección de datos se incluyen, además, en la Carta de los Derechos Fundamentales de la Unión Europea[51].

María Ángeles Rueda Martín[52] señala que "En el ámbito de la Unión Europea destaca la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea, relativa a los ataques contra los sistemas de información, que tiene como objetivo aproximar "la legislación penal en materia de ataques contra los sistemas de información para conseguir la mayor cooperación policial y judicial posible respecto de las infracciones penales vinculadas a ataques contra los sistemas de información y para contribuir a

[51] Comunicación de la Comisión COM (2000) 890 final. Disponible: http://bcn.cl/8bcv (Diciembre, 2015).
[52] Op. Cit., pp. 158 y ss.

la lucha contra el terrorismo y la delincuencia organizada". A continuación, Rueda Martín clasifica las obligaciones normativas establecidas por la Decisión Marco, de la siguiente manera:

a. El artículo 2° obliga a cada Estado a adoptar las medidas necesarias contra el acceso ilegal a los sistemas de información.
b. El artículo 3° obliga a cada Estado a adoptar las medidas necesarias contra la intromisión ilegal en los sistemas de información.
c. El artículo 4° obliga a cada Estado a adoptar las medidas necesarias contra la intromisión ilegal en los datos.
d. El artículo 7° establece algunas circunstancias agravantes consistentes en actuar en el marco de una organización delictiva, y el hecho de haber ocasionado graves daños o haber afectado a intereses esenciales.

En síntesis, de los dos textos normativos internacionales se puede concluir[53]:

a. Se protegen los sistemas informáticos mediante la propuesta de tipificar como delito determinadas conductas de simple acceso no autorizado a sistemas informáticos, y también aquellas que suponen una obstaculización o interrupción de su funcionamiento.
b. Se protegen los datos y la información resguardada en los sistemas informáticos mediante la propuesta de considerar como delito las conductas que suponen un atentado o una intromisión lesiva en los datos o la información contenida en dichos sistemas.

3. Alemania

La Segunda Ley contra la Criminalidad Económica de 1986 de Alemania[54] modificó el Código Penal, contemplando delitos relacionados con la informática. Se optó por incorporar estos delitos en capítulos en los que ya estaban reguladas figuras similares de la realidad análoga. No sólo se modificaron tipos penales, sino que también se incorporaron nuevas figuras[55].

El Código Penal alemán contempla diversos delitos informáticos, entre ellos, el espionaje de datos (Sección 202.a), *phishing* (Sección 202b), Actos preparatorios de espionaje de datos y *phishing* (Sección 202c), estafa mediante ordenador o fraude informático (Sección 263.a), falsificación de datos probatorios (Sección 269), modificaciones complementarias del resto de las falsedades documentales (Sección 270, 271, 273, 274 y 348), engaño en el tráfico jurídico mediante sistemas de procesamiento de datos (Sección 270), modificación de datos (Sección 303.a) y sabotaje informático (Sección 303.b)[56].

[53] Ambas conclusiones son compartidas también por María Ángeles Rueda Martín. Op. Cit., pp. 158 y ss.
[54] Alemania también suscribió la Convención contra delito informático, pero hasta Junio de 2009 no la había ratificado.
[55] Rovira del Canto, Enrique. Delincuencia informática y fraudes informáticos. Editorial Comares. Madrid. 2002. Pp. 382 y ss.
[56] Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto. Análisis de los delitos informáticos en el derecho chileno y comparado. Tesina para optar al grado de Licenciado en Ciencias Jurídica, Santiago de Chile, 2013. Disponible en: http://bcn.cl/1tr0o (Diciembre, 2015).

Siguiendo con la clasificación del Consejo de Europa, es posible constatar la existencia de los siguientes delitos en materia de confidencialidad, integridad, disponibilidad y fraude informático:

a. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Artículo 202: Violación del secreto de correspondencia: Es sancionado quien procure el conocimiento del contenido de una carta cerrada, bajo utilización de medios técnicos.
- Artículo 202a: Piratería Informática. Se sanciona la conducta de conseguir para si o para otro, sin autorización, datos de un tercero que se encuentren protegidos del acceso no autorizado[57].

  La redacción recién señalada dio por superadas las discusiones sobre si la figura penal anterior contemplaba o no las conductas de *hacking*, al exigir el tipo antiguo, la adquisición de datos no autorizados[58]. Sin embargo, en opinión de Schünemann, dichas conductas sí quedaban comprendidas en la norma, cuando suponían la apropiación de algunos datos, como un *password*[59].

- Artículo 269: Falsificación de datos de pruebas relevantes: Se estiman ilícitas las siguientes conductas.
  - Almacenar o alterar datos probatorios relevantes para configurar un documento electrónico no auténtico o falsificado.
  - Utilizar los datos almacenados o alterados, antes mencionados.

- Artículo 303a: Constituye delito las siguientes conductas y sus tentativas: Borrar, eliminar, inutilizar o alterar ilícitamente datos.
- Artículo 303b: Es tipificado como delito la destrucción de datos considerados esenciales para una industria.
- Artículo 348: Falsedad ideológica en el ejercicio de sus funciones. Se sanciona a quien estando encargado de la recepción de documentos públicos introduzca falsamente en registros públicos archivos de datos.

b. Delitos de fraude informático:

- Artículo 263a: Estafa por computador. Se tipifica como delito el perjuicio patrimonial a otro, con el afán de ventaja propia, mediante: influencia en el resultado de la elaboración de datos utilizando una errónea configuración del programa; uso de datos incorrectos o incompletos; o por el empleo no autorizado de datos. Se debe considerar, en éste tipo, que serán circunstancias agravantes, respecto del autor:

[57] Estos datos son: "aquellos que no sean almacenados, transmitidos electrónica, magnéticamente, o de forma inmediatamente accesibles." (Artículo 202 a, apartado II, Código Penal Alemán).
[58] Rueda Martín, María Ángeles, Op. Cit., pp. 163 y ss.
[59] Ibídem.

- Que, actúa profesionalmente o es miembro de una banda asociada para la comisión continua del delito de falsificación;
- Cuando ocasiona una pérdida patrimonial de grandes dimensiones o actúa con el propósito de conducir a un gran número de personas al peligro de perdida de activos mediante la comisión continuada de estafas.
- Su actuar conduzca a una persona a necesidad económica.
- Abuse de sus competencias o de su posición como titular del cargo, o
- Simule una contingencia de seguro después de haber puesto fuego él u otro con este fin a una cosa de significativo valor o haberla destruido total o parcialmente por incendio o haber hecho hundir o naufragar un buque.

- Artículo 270: Engaño en el tráfico jurídico en sistematización de datos. Tipifica como delito, la falsificación de una base de datos.
- Artículo 273: Alteración de documentos oficiales. Sanciona como delito hacer uso de datos falsos almacenados, con la finalidad de engañar, en el tráfico jurídico.

A continuación se detallan los delitos señalados

a) Espionaje de datos.

El artículo 202.a[60] dispone: "quien consiga sin autorización, para sí o para otro, datos que no estaban destinados a él y que estén especialmente protegidos contra el acceso ilegítimo será castigado con pena privativa de la libertad de hasta tres años o con multa.
Los Datos, a efectos del apartado I, serán sólo aquellos que sean almacenados, transmitido electrónica, magnéticamente, o de forma no inmediatamente accesible".

Este delito contiene los siguientes elementos:

- Los datos contenidos en el sistema de tratamiento de la información deben ser de carácter privado.
- La accesibilidad de los datos debe estar especialmente protegida contra el acceso ilegítimo.
- El sujeto activo debe poseer la condición de restricción a los datos a los que accede.

b) Phishing

El artículo 202.b[61] dispone: "Todo aquel que intercepta ilegalmente datos (sección 202a (2)) no previstos por él, por sí mismo o mediante otra técnica de una

[60] "Abschnitt 202.a: "(1) Wer rechtswidrig Daten erhält für sich selbst oder anderen, die nicht für ihn bestimmt waren und wurden besonders gegen unbefugten Zugriff geschützt, wenn er umgangen hat den Schutz, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. (2) Im Sinne des Absatzes (1) oben genannten Daten werden nur diejenigen gespeichert oder übertragen werden elektronisch oder magnetisch oder sonst in einer Weise, die nicht sofort spürbar sein". Citado por Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto, Op. Cit.
[61] "Abschnitt 202.b: "Wer widerrechtlich fängt Daten (§ 202a (2)) nicht für ihn bestimmt sind, für sich selbst oder andere mit technischen Mitteln aus einem nicht-öffentlichen Datenverarbeitungsanlage oder

instalación de procesamiento de datos que no sea pública o de la emisión electromagnética de un centro de procesamiento de datos, será castigado con pena de prisión no superior a dos años o una multa, a menos que el delito incurra en una pena más grave en virtud de otras disposiciones.".

Esta norma reafirmaría que el bien jurídico protegido "privacidad de la información" sea resguardado con mayor efectividad, ya que, para que se configure el tipo penal es necesario que la información a que el sujeto activo accede se encuentre protegida del acceso público. A diferencia con la sección 202.a, este delito apunta a aquellos datos que si bien son privados, no se encuentran protegidos de forma especial por el sujeto quien lo posee legítimamente.

c) Actos preparatorios de espionaje de datos y Phishing

El artículo 202.c[62] dispone:

"(1) El que prepara la comisión de un delito bajo la sección 202 o la sección 202.b por producir, adquirir para sí o para otro, la venta, el suministro a otro, difusión o cualquier otra forma accesible.

Primero contraseñas u otros códigos de seguridad que permiten el acceso a los datos (sección 202a (2)), o Segundo software para el propósito de la comisión de dicho delito, será castigado con pena de prisión no superior a un año o multa. (2) Sección 149 (2) y (3) se aplicarán mutatis mutandis".

Esta norma sanciona el acto en grado de tentativa, ya que el acto de sustracción de información o difusión de esta no requiere que se encuentre consumado, bastando para el tipo penal con la sola preparación de éste.

El objeto sobre el cual recae el delito es "contraseñas u otros códigos de seguridad que permiten el acceso a los datos", por ello el objeto no es propiamente el dato o contenido de la información, que se encuentra en el sistema de tratamiento de la información, sino que el acceso a ella, es decir las contraseñas o códigos de acceso a la información, ya sea para beneficio propio o de terceros por cualquier medio, y como también lo señala la norma con la creación de un software para la comisión del presente tipo penal, marcando con esto la gran diferencia entre la sección 202.b.

---

aus der elektromagnetischen Ausstrahlung einer Datenverarbeitungsanlage, so ist die Strafe Freiheitsstrafe von nicht mehr als zwei Jahren oder Geldstrafe, wenn die Tat verursacht eine schwere Strafe unter den sonstigen Rückstellungen". Citado por Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto, Op. Cit.

[62] "Abschnitt 202.c: "(1) Wer bereitet die Begehung einer Straftat nach § 202a oder § 202b durch die Herstellung, den Erwerb für sich selbst oder anderen, Verkauf, die Lieferung in ein anderes, Verbreitung oder machen sonst zugänglich
Ein. Passwörter oder andere Sicherheitscodes den Zugang zu Daten (202a (2)), oder
2. Software zum Zwecke der Begehung einer solchen Straftat,
Wird mit Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe.
(2) § 149 (2) und (3) gelten sinngemäß". Citado por Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto, Op. Cit.

d) Estafa mediante ordenador o Fraude informático.

El artículo 263.a[63]. dispone:

"(1) Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medio de una errónea configuración del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso, será castigado con pena de privación de libertad de hasta cinco años o con multa.
(2) Sección 263 (2) a (7) se aplicarán mutatis mutandis.
(3) El que prepara un delito en virtud del inciso (1) anterior escribiendo programas informáticos con la finalidad de que está tratando de comprometerse a actuar, o adquiera para sí o para otro, ofrece a la venta, o la posesión o los entrega a otro será sancionado con prisión de hasta tres años o una multa.
(4) En los casos previstos en el inciso (3) anterior sección 149 (2) y (3) se aplicarán mutatis mutandis. En primer lugar para comenzar con el análisis de los elementos que dilucidarán la estructura del presente apartado, resulta necesario tener presente los elementos que componen la figura típica de la estafa, por ello se analizará conforme a dicho tipo penal.
El legislador alemán consagra la sanción a los actos preparatorios al señalar "El que prepara un delito en virtud del inciso (1)".

La norma incorpora los elementos básicos de la estafa, el engaño a una persona, el error, el acto de disposición patrimonial lesivo, y los elementos subjetivos, ya que, tanto el engaño como el error y el acto de disposición patrimonial lesivo no son necesarios para que la conducta sea típica.

Establece además una agravante del tipo (privación de libertad de uno a 10 años) por la expresa remisión que efectúa al párrafo 263 (2) a (7).

[63] "Abschnitt 263.a: "(1) Wer in der Absicht, den Erhalt für sich selbst oder eine dritte Person eine rechtswidrige materiellen Vorteil schädigt das Eigentum eines anderen durch Beeinflussung des Ergebnisses einer Datenverarbeitung Betrieb durch falsche Konfiguration eines Programms, fehlerhafte oder unvollständige Daten zu verwenden, unbefugte Nutzung Daten oder anderen unerlaubten Einfluss auf den Verlauf der Verarbeitung haftet Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.
(2) § 263 (2) bis (7) gelten sinngemäß.
(3) Wer bereitet eine Straftat nach Absatz (1) oben, indem er Computerprogramme, dessen Zweck darin, eine solche Tat zu begehen, oder beschafft sie für sich selbst oder anderen bietet sie zum Verkauf oder hält oder führt sie zu einem anderen gelten mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.
(4) In den Fällen des Absatzes (3) über § 149 (2) und (3) gelten sinngemäß". Citado por Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto, Op. Cit.

e) Alteración de datos

El artículo 303.a[64]. dispone:

"(1) Quien borre, elimine, inutilice o altere ilícitamente datos (202.a, apartado 2) será castigado con pena de privación de libertad de hasta dos años o con multa. (2). La tentativa será punible".

La disposición protege al que almacena los datos y a la persona afectada por el contenido de éstos; los datos que son protegidos son de aquellos que no son de inmediata percepción, además se tipifican cuatro acciones señaladas expresamente por el legislador:

- El borrado de datos, ya sea de forma completa o parcial, con lo cual el destruir el soporte lógico de un dispositivo de tratamiento de la información, o borrar los elementos necesarios para establecer una conexión o acceso a determinados sistemas, se enmarcaría en dicho tipo.
- La inutilización de los datos.
- La alteración es una perturbación de carácter funcional, relativa a la transformación de su valor informático, por ello los datos poseen un nuevo contenido producto de la alteración efectuada.
- Como consecuencia de lo señalado anteriormente, todas las conductas identificadas produciría el efecto del ocultamiento de los datos para la persona que posee el acceso legítimo a ellas.

f) Sabotaje informático

El artículo 303.b[65] dispone:

" (1) El que interfiere con las operaciones de procesamiento de datos que son de importancia sustancial a otro por: 1. Comisión de un delito tipificado en sección303a (1), o 2. Entrar a la transmisión de datos (sección 202a (2)) con la

[64] "Abschnitt 303.a: " (1) Wer rechtswidrig löscht, unterdrückt, unbrauchbar macht oder verändert Daten (§ 202ª (2)) haftet Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.
(2) Der Versuch ist strafbar". Citado por Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto, Op. Cit.

[65] "Abschnitt 303.b: " (1) Wer stört Datenverarbeitungen, die von wesentlicher Bedeutung sind, um anderen durch 1. Begehung einer Straftat unter section303a (1) oder 2. Eingabe oder Übertragung von Daten (§ 202a (2)) mit der Absicht, einen Schaden zu verursachen, um eine andere, oder 3. zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert eine Datenverarbeitungsanlage oder einen Datenträger, wird mit Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe. (2) Wenn die Datenverarbeitungs-Operation ist von wesentlicher Bedeutung für ein anderes Geschäft, Unternehmen oder einer Behörde, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. (3) Der Versuch ist strafbar. (4) In besonders schweren Fällen des Absatzes (2) über die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren.Ein besonders schwerer Fall tritt in der Regel, wenn der Täter 1. verursacht große finanzielle Verluste, 2. wirkt auf kommerzieller Basis oder als Mitglied einer Bande, deren Zweck die fortgesetzten Begehung von Computersabotage oder 3. durch die Straftat gefährdet Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die nationale Sicherheit der Bundesrepublik Deutschland.". Citado por Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto, Op. Cit.

intención de causar daños a otro; o 3. destruir, dañar, inutilizar, supresión o alteración de un sistema de procesamiento de datos o en un soporte de datos, será sancionado con prisión de hasta tres años o con multa.(2) Si la operación de procesamiento de datos es de importancia sustancial para el negocio de la empresa o de otra autoridad pública, la pena será de prisión de hasta cinco años o con multa.(3) La tentativa será castigada.(4) En los casos especialmente graves en virtud del inciso (2) por encima de la pena será de prisión de seis meses a diez años. Un caso especialmente grave ocurre normalmente si el delincuente1. Provoca importantes pérdidas financieras, 2. Actúa sobre una base comercial o como miembro de una banda cuyo objetivo es la comisión permanente de sabotaje informático, o 3. por la transgresión pone en riesgo el suministro de la población con bienes o servicios esenciales o la seguridad nacional de la República Federal de Alemania.(5) Sección 202c se aplicará mutatis mutandis a los actos preparatorios de un delito previsto en el apartado (1) anterior.".

El Código Penal alemán tipifica la vulneración de importancia sustancial, excluyendo vulneraciones irrelevantes o de poca importancia para el sujeto que sufre la transgresión del bien jurídico protegido. Por ello abarca una serie de circunstancias, desde la alteración de datos (sección 303a.), espionaje informático (sección 202a (2)) hasta la alteración y destrucción de la información contenida en un sistema de tratamiento de la información, relativo a los datos propios de esta como los datos los cuales se encuentran almacenados en ella.

El numeral (2) de este artículo contiene una agravante a la conducta anteriormente descrita, en atención al sujeto pasivo sobre el cual recae la conducta típica, que pueden ser empresas privadas o públicas. Así, se considera la gravedad y las circunstancias perniciosas que se podrían derivar al vulnerar y alterar datos de entidades de carácter público; lo mismo sucede con las entidades de carácter privado.

También se sanciona la tentativa.

También, la norma sistematiza el alcance que se debe tener presente cuando se señala aquellas conductas especialmente graves, aumentado la pena base contenida en el tipo, con lo cual se establece una agravante, las que van desde provocar importantes pérdidas financieras, actuar sobre una base comercial o como miembro de una banda cuyo objetivo es la comisión permanente de sabotaje informático, hasta la transgresión que pone en riesgo el suministro de la población con bienes o servicios esenciales o la seguridad nacional.

Se sancionan las conductas tipificadas relativas a la alteración de datos (sección 303a.), espionaje informático (sección 202a (2)), alteración y destrucción de la información contenida en un sistema de tratamiento de la información, por los actos preparatorios de estas, aplicándose mutatis mutandis al tipo penal señalado.

4. Argentina

La Ley N° 26.388[66] de Delitos Informáticos, de Junio de 2008, contempla delitos informáticos, regulando este tipo de delitos en un cuerpo normativo separado del Código Penal, no con figuras propias y específicas, sino que modifica, sustituye e incorpora figuras típicas a diversos artículos del Código Penal.

A lo largo de su articulado tipifica, entre otros, los siguientes delitos informáticos, y cometidos por medios informáticos:

- Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP);
- Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP);
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP);
- Acceso a un sistema o dato informático (artículo 153 bis CP);
- Publicación de una comunicación electrónica (artículo 155 CP);
- Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP);
- Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP);
- Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data);
- Fraude informático (artículo 173, inciso 16 CP);
- Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP).

Las penas establecidas son: a) prisión; b) inhabilitación (cuando el delito lo comete un funcionario público o el depositario de objetos destinados a servir de prueba); c) multa (ej. art. 155).

- Delito concreto de daño informático

El artículo 10 de la ley dispone: Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:

"En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

El artículo 183 antes vigente, que tipificaba el delito de daño en general, sólo era aplicable cuando la acción dañosa recaía sobre un bien tangible, no sobre un bien intangible, y tanto los datos como el *software* (programas) corresponden a esta última categoría.

[66] Disponible en: http://bcn.cl/1tr7b (Diciembre, 2015).

5. Francia

En 1988 entra en vigencia la Ley 88-19, sobre modificación del Código Penal (artículos 323-1 a 323-7, que tipifican los atentados contra los sistemas de tratamiento automatizado de datos, y 441-1) en materia de delincuencia vinculada con las nuevas tecnologías de la información, o "*Ley Godfrain*". Esta norma fue modificada sustancialmente por la Ley 2004-575.

El Código Penal Francés en su Libro III, Título II, Capítulo III: De los atentados contra los sistemas de tratamiento automatizado de datos, contiene el tratamiento relativo a los delitos informáticos, principalmente entre los artículos 323-1 a 323-7.

Según Gutiérrez Francés[67], en esta ley el legislador francés optó por el sistema de reconducir a un único bloque o cuerpo legal toda la nueva realidad criminal compleja vinculada a las nuevas tecnologías de información, recogiéndolas en un nuevo capítulo del Código Penal de 1994.

Si bien los tipos penales de Ley 88-19 suponen, en algunos casos, el manejo fraudulento de datos, ello no implica que correspondan a la figura tradicional de las defraudaciones patrimoniales (estafa), que siguen siendo contempladas por el tradicional artículo 313-1 del Código Penal de 1994[68].

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

- Artículo 323-3[69]: Sanciona la introducción, supresión o modificación de datos de manera fraudulenta en un sistema de tratamiento automatizado.
- Artículo 323-2[70]: Sanciona la obstaculización o alteración del funcionamiento de un sistema de tratamiento automatizado de datos.

---

[67] Gutiérrez Francés, María. Delincuencia económica e informática en el nuevo Código Penal. Séptima ponencia en el curso Ámbito jurídico de las tecnologías de la información. Cuadernos de Derecho Judicial. Escuela Judicial. Madrid. 1996. Citado por Rovira del Canto, Op. Cit., p. 389.

[68] Rovira del Canto, Op. Cit., pp. 390 y 391. El autor utiliza como argumento decisiones o jurisprudencia de la Corte de Casación Francesa y de los Tribunales de Apelaciones franceses.
El Artículo 313-1 del Código Penal francés dispone: Es estafa el hecho de engañar a una persona física o jurídica, bien mediante el uso de un nombre falso o de una falsa calidad, bien mediante el abuso de una calidad verdadera, o bien mediante el empleo de maniobras fraudulentas, determinándola así, en perjuicio propio o de tercero, a entregar fondos, valores o cualquier bien, a prestar un servicio o a consentir un acto que le imponga una obligación o aceptar una descarga.
La estafa será castigada con cinco años de prisión y multa de 2.75.000 euros.".

[69] "Article 323-3. "Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende". Citado por Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto, Op. Cit.

[70] "Article 323-2. "Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende".

- Artículo 323-1[71]: Se sanciona el hecho de acceder de manera fraudulenta a la totalidad o a parte de un sistema de tratamiento automatizado de datos, o de mantenerse en él fraudulentamente. Constituye agravante de esta conducta: si a consecuencia de las acciones enunciadas se produce la supresión o la modificación de datos contenidos en el sistema, o una alteración del funcionamiento del mismo. Esta norma impone sanciones de dos años de prisión y 30.000 euros de multa. Si el resultado fuere la supresión o modificación de datos contenidos en el sistema, o una alteración del funcionamiento del mismo, la pena es de tres años de prisión y 45.000 euros de multa.

Normas comunes a los artículos precedentes son:

- Artículo 323-3-1[72]: Este tipo sanciona a quien, sin motivo legítimo, importa, tiene, ofrece, cede o pone a disposición equipamiento, instrumento, programa informático o cualquier dato concebidos o especialmente adaptados para cometer una o varias de las infracciones previstas por los artículos anteriores.
- Artículo 323-4[73]: Sanciona a los grupos organizados para la comisión de todos los delitos antes indicados.
- Artículo 323-6[74]: Sanciona a las personas jurídicas, salvo al Estado, por las infracciones cometidas por sus órganos o representantes. Cabe hacer presente que la responsabilidad penal de las personas jurídicas no excluirá la de las personas físicas autoras o cómplices de los mismos hechos
- Artículo 323-7[75]**:** La tentativa de los delitos previstos por los artículos 323-1 a 323-3-1 será castigada con las mismas penas asignadas a ellos.

---

[71] "Article 323-1: "Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende".

[72] "Article 323-3-1: "Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est punides peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".

[73] "Article 323-4. "La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".

[74] "Article 323-6: "Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.
L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise".

[75] "Article 323-7: "La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines". Citado por Bustos Bobadilla, Álvaro Francisco, y Zúñiga Sánchez, Carlos Alberto, Op. Cit.

6. Gran Bretaña

Se sanciona como delito el simple acceso a la totalidad o a una parte (datos o programa) de un sistema informático, en el *Computer Misuse Act* de 1990, en la Sección 1 (1), donde se señala: "una persona es culpable de un delito si: a) hace que un computador ejecute una función con la intención de asegurarse un acceso a cualquier programa o a los datos almacenados en cualquier computador; b) el acceso que pretende asegurarse no está autorizado; y c) conoce en el momento que ejecuta dicha función en el computador que tal acceso no está autorizado" [76].

7. Portugal

Se ha optado por una incriminación del acceso ilícito a sistemas informáticos acompañado de exigencias posteriores, ya sean una determinada finalidad o una vulneración de medidas de seguridad[77].

La Ley 109/91 sobre criminalidad informática tipifica en el artículo 7 el delito de acceso ilícito a un sistema o a una red informáticos: "1. Quien acceda de cualquier modo, no estando autorizado y con la intención de obtener, para sí o para otro, un beneficio o ventaja ilegítimos, a un sistema o red informáticos será castigado con la pena de prisión, de hasta un año o con la pena de multa, de hasta 120 días. 2. La pena será de prisión de hasta tres años o multa si el acceso se consigue con la infracción de medidas de seguridad. 3. La pena será de prisión de uno a cinco años cuando: a) a través del acceso, el sujeto haya tenido conocimiento de un secreto comercial o industrial de datos comercial o industrial o de datos confidenciales, protegidos por ley; b) el beneficio o ventaja patrimonial obtenidos sean de valor considerablemente elevado. 4. Se castiga la tentativa. 5. En los casos previstos en los números 1, 2 y 4 el procedimiento penal depende de querella"[78].

8. Suiza

El Libro II del Código Penal suizo, en el Título II, relativo a las "Infracciones contra el patrimonio", establece en su artículo 143 bis, que "quien se introduzca ilícitamente, sin la intención de enriquecerse, a través de un sistema de transmisión de datos, en un sistema informático ajeno y especialmente protegido contra cualquier acceso, será castigado, según la petición, con una pena privativa de libertad de hasta tres años o pena de multa." [79].

[76] Fuente y traducción: Rueda Martín, María Ángeles, Op. Cit., pp. 161 y ss.
[77] Rueda Martín, María Ángeles, Op. Cit., p. 162.
[78] Ibídem.
[79] Ibídem.

X. Conclusiones

1. En relación al ordenamiento interno y la legislación extranjera

La sistematización de los artículos de la Ley N° 19.223 parece dificultar la comprensión de su sentido y alcance. Por ejemplo, el artículo 1 incorpora los atentados contra un sistema de tratamiento de información, destruyéndolo o inutilizándolo mediante atentados a las partes o componentes físicos de dicho sistema. Esta conducta coincide con el delito común de daños, confundiéndose el delito informático propiamente tal con los delitos de daños a la propiedad. Además, el mismo artículo penaliza conjuntamente los atentados contra el funcionamiento del sistema y contra la destrucción delmismo, conductas que en la legislación extranjera analizada se trata por separado.

La ley no contempla una gran variedad de hechos ilícitos, como el *phishing*, *hacking*, fraude informático, asociación para cometer delitos informáticos, actos preparatorios (incluyendo la tentativa).

La hipótesis de acceso no autorizado a información contenida en sistemas computacionales (*hacking*) ofrece problemas, al exigir la concurrencia de un elemento subjetivo adicional (ánimo de apropiación, uso o conocimiento).

La ley no trata especialmente a las personas jurídicas y naturales como sujetos, tanto activos como pasivos del delito, ni incluye agravantes cuando se efectúan dichas conductas en circunstancias que el legislador considere graves o que afecten sustancialmente los sistemas de tratamiento de información y los datos contenidos en ellos.

En cuanto al alcance de la norma se puede apreciar, que los artículos 1, 3 y 4 de la Ley N° 19.223 exigen dolo, lo que limita la punibilidad de la mayoría de los actos señalados en los tipos penales correspondientes. La legislación comparada analizada no exige dolo o ánimo especial alguno para la comisión del hecho típico como regla general, facilitando de este modo la aplicabilidad de la norma relativa a los delitos informáticos.

El legislador nacional trata esta materia en una ley especial, mientras que la corriente mayoritaria en el tratamiento de este tipo de delitos lo hace en sus Códigos Penales correspondientes, lo que puede tener algunas ventajas, tales como proporcionar un mayor entendimiento y alcance de la naturaleza del delito, ya que necesariamente se tendrá que enmarcar en algún título, sección o capítulo, lo cual ayudaría significativamente a solucionar dicha interrogante, además, con ello se evitaría crear una confusión innecesaria en el tratamiento sistemático de la norma, ya que al poseer un tratamiento único en un solo cuerpo legal, disminuiría considerablemente la difusión de normas relativas al mismo tema en el ordenamiento jurídico correspondiente, y evitaría discusiones sobre la procedencia de remisiones a normas generales del ordenamiento penal.

La Ley N° 19.223, se promulgó en un momento en que no existía la actual conectividad y concepto de redes, por lo que la actual tipificación del delito informático no protegería adecuadamente las diversas formas de transacción comercial, financiera y cultural que hoy son posibles y cotidianas gracias a la "red".

Es cuestionable que las disposiciones de la ley sean también aplicables a la afectación del *hardware* y de datos no informáticos, pues con ello el legislador abandonaría el propósito inicial de enfrentar los desafíos de las nuevas tecnologías, alterando sin fundamento claro, ámbitos abarcados por la legislación anterior.

En cuanto a la competencia relativa, en materia de delitos informáticos, cabe considerar que la distancia produce problemas en cuanto a la legislación aplicable y la jurisdicción o competencia de los tribunales. Ello se debe a que el artículo 157 del Código Orgánico de Tribunales señala en su inciso primero que "será competente para conocer de un delito el tribunal en cuyo territorio se hubiere cometido el hecho que da motivo al proceso", mientras que su inciso final agrega: "el delito se considerará cometido en el lugar donde se dio comienzo a su ejecución". Por lo tanto el lugar donde el sujeto activo, prevalido de un computador, cometa la conducta típica a distancia, será el elemento determinante, pues es desde ese punto donde el sujeto tiene el control sobre las acciones tendientes a la realización del ataque informático. Lo anterior es aplicable al ámbito nacional e internacional. Por lo tanto, si el autor es un chileno ubicado en el extranjero, y comete el delito en contra de víctimas ubicadas en Chile, los tribunales chilenos no tienen competencia para conocer de tales delitos.

Pese a no ser exigible para Chile, la legislación nacional se adapta a las recomendaciones internacionales de incriminación de estas conductas, formuladas por el Consejo de Europa y la Unión Europea, aunque de modo insatisfactorio, pues en Chile no se incrimina el simple acceso no autorizado a un computador o sus datos por medios informáticos.

2. Proyecto de Ley que tipifica y sanciona los delios informáticos y deroga la Ley N° 19.223

El proyecto de ley antes descrito, modifica los delitos informáticos, introduce modificaciones en materia procesal penal para facilitar la persecución de éstos delitos, y deroga la Ley N° 19.223.

El proyecto el delito de destrucción o inutilización de sistema informático de tratamiento computacional de datos, y crea delitos nuevos, tales como: el delito de acceder o usar, sin derecho, información contenida en un sistema informático de tratamiento de datos; el delito de impedir a otro por vía informática, acceder a sus datos personales u otros de su propiedad intelectual; el delito de alterar, dañar o destruir los datos contenidos en un sistema informático de tratamiento de datos, sancionado con presidio menor en su grado medio; el delito de tenencia, posesión, producción, venta, difusión, o cualquier otra forma de puesta a disposición de dispositivos, programas informáticos, aplicaciones, claves, códigos de acceso u otro tipo de elemento informático que permitan o faciliten la comisión de delitos; y el

delito de exacción patrimonial; consistente en: "El que sin la voluntad de su dueño y con ánimo de lucrar, transfiriere u obtuviere la transferencia de cualquier activo patrimonial de un tercero empleando medios informáticos", sancionado con presidio mayor en sus grados mínimo a medio.

También se crea una agravante especial consistente en que si quien incurriere en las conductas descritas en los artículos anteriores fuere responsable del sistema de información, la pena se aumentará en un grado, y se crea una nueva circunstancia agravante, genérica, en el artículo 12, circunstancia 22ª en el Código Penal, consistente en emplear medios informáticos para ejecutar el delito.

Se sancionan la tentativa y la frustración de los delitos contemplados en esta ley.

También se modifica el Código Procesal Penal para introducir normas procesales penales que fortalecen al Ministerio Público y a las Policías.

La mayoría de los delitos previstos exigen dolo directo, contrariamente a lo observado en las legislaciones extranjeras analizadas.