Realidad actual de los delitos informáticos: un estudio de la Ley Nº 21.459 a la luz del Convenio de Budapest y la Ley Nº Nº 19.223.

FRANCISCO PINOCHET CANTWELL
Doctor en Derecho
Universidad Nacional de Rosario, Argentina

LORENA LEMUNAO AGUILAR
Directora Área de Derecho Civil
Asociación Regional de Magistrados
Región de Los Lagos

1. Introducción

Con el objetivo de poder cumplir con los compromisos asumidos por el Estado de Chile en contexto de la adopción del Convenio sobre Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest, con la promulgación del decreto N° 83 del Ministerio de Relaciones Exteriores en abril del año 2017, el congreso de embarcó en una ardua labor legislativa que finalmente se sustanció en la Ley Nº 21.549 "establece normas sobre delitos informáticos, deroga la Ley Nº N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest", publicada el 20 de junio del 2022.

Esta ley, que viene a pagar la deuda de 5 años de legislar para adecuarse a aquel estándar internacional, establece definiciones de conceptos relativos a las tecnologías de la información y tipifica una serie de delitos que solamente podían intuirse en la prosa de la Ley Nº 19.223.

En este sentido, el mensaje de la Ley Nº 21.549 señala que *"Lo anterior tiene lugar en un mundo globalizado, en el cual Chile no se encuentra ajeno a este fenómeno criminal, unido al aumento del acceso a Internet y otros dispositivos*

electrónicos, de modo que resulta indispensable una actualización a nuestra legislación en esta materia"[1].

Así, el interés del legislador se radicó en poder adaptar el ordenamiento interno a una realidad para la cual las herramientas legales disponibles no daban abasto, situación que debía remediarse para salvaguardar la situación del estado en un mundo globalizado, interconectado, y en el cual la esfera de relaciones jurídicas se vuelve cada vez más digital.

2. Convenio de Budapest.

El Convenio sobre Ciberdelincuencia del Consejo de Europa del 23 de noviembre del 2001, en la ciudad de Budapest, según lo establece su preámbulo, busca establecer "*una política común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular, mediante la adopción de una legislación adecuada y a la mejora de la cooperación internacional*" y "*prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción* (…)"[2]

En este instrumento, se da una batería de definiciones necesarias para los fines que propone regular, las que se advierten en términos generales para asegurar su aplicabilidad más allá de las tecnologías existentes al momento previendo potenciales avances.

Además, establece 9 situaciones que el Convenio mandata a los estados que lo suscriben tipificar como delitos, y que dicha labor legislativa se realice en el marco

[1] Biblioteca del Congreso Nacional, *Historia de la Ley Nº 21.459,* Mensaje, pág. 4.
[2] Consejo Europeo, *Convenio sobre la ciberdelincuencia*, Budapest, 2001, pág. 1.

de los parámetros y términos que el mismo Convenio determine, de los cuales cabe mencionar 7 de ellos por su vinculación al contenido de la Ley Nº 21.459

3. Delitos del convenio de Budapest.

Acceso ilícito: El Convenio define en su artículo 2° el acceso ilícito como el *"acceso deliberado e ilegítimo a todo o parte de un sistema informático"*, permitiendo a los estados exigir o no que se realice infringiendo medidas de seguridad, con la intención de obtener datos informáticos u con otro objetivo delictual, o respecto a un sistema informático conectado a otro sistema informático.

Interceptación ilícita: El Convenio define en el artículo 3° este delito como la *"interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos"*. Da libertad a los estados partes de exigir o no que se cometa con intención delictual, o que se cometa respecto a un sistema informático conectado a otro.

Ataques a la integridad de los datos: El Convenio busca, mediante lo señalado en el artículo 4°, que se castigue *"todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos*", permitiendo a los estado establecer o no la exigencia de que estos actos reporten daños graves para su punibilidad.

Ataques a la integridad del sistema: Importa el Convenio, al tenor de su artículo 5°, que los estados parte tipifiquen como delito *"la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos*". En este caso, el Convenio no establece otros elementos a considerar para la tipificación.

Abuso de los dispositivos: Dispone el Convenio en el artículo 6° que se debe tipificar la comisión deliberada e ilegítima de dos supuestos:

El primero de ellos, *"la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de: cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos en los artículos 2 a 5 del presente Convenio; de una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de ser utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5"*.

El segundo caso, se refiere a la posesión de alguno de los elementos mencionados en el primer caso, con la intención de ser utilizados para cometer los delitos señalados en los artículos 2 a 5 del Convenio, a saber, el Acceso ilícito, interceptación ilícita, ataques a la integridad de los datos o a la integridad de los sistemas.

Al respecto, señala el Convenio que no debe de interponerse responsabilidad penal cuando no haya intencionalidad de cometer alguno de los delitos mencionados anteriormente, como en el caso de pruebas autorizadas de seguridad.

Finalmente, dispone que autoriza a los estados a no penalizar la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de: cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos señalados anteriormente, siempre que no afecte la penalización de las mismas actitudes para con las contraseñas, códigos de acceso o similares que permitan acceso a los sistemas.

Falsificación informática: Define el Convenio en el artículo 7° la falsificación informática como *"la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención que sean tomados o utilizados a efectos legales como auténticos"*. Al respecto, permite

a los estados el exigir o no, para su sanción, que exista intención dolosa o delictiva similar.

Fraude informático: Determina el Convenio en su artículo 8° que los estados parte deben tipificar como delito "*actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático; con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo u otra persona*". En este caso, el Convenio no se refiere a otros elementos a considerar por los estados parte.

4. Ley Nº Nº 19.233.

La antigua Ley Nº 19.233 que tipifica figuras penales relativas a la informática del 28 de mayo de 1993 establecía 4 delitos relativos a la, entonces, nueva y creciente esfera de los sistemas de información. La penetración de estas tecnologías en los diversos ámbitos de la vida pública y empresarial hizo necesario establecer tipos penales que pudieran regular y dar cierta seguridad a su utilización.

Señalaba el mensaje de esta ley que esta *"tiene por finalidad proteger este nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. Aquella, por el actual desarrollo tecnológico de la sociedad, merece ser protegida mediante la creación de figuras delictuales nuevas, que pongan de relieve su importancia"*[3].

Contempló esta concentradísima ley, 4 artículos en los que se tipificaron los delitos de sabotaje de sistemas informáticos, espionaje informático, revelación

[3] Biblioteca del Congreso Nacional, *Historia de la Ley Nº 19.223*, Mensaje, Pág. 4.

indebida de información y el daño o alteración maliciosa de datos informáticos, del siguiente modo:

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

Como se puede observar, la extensión de la ley y la forma en la cual se expresaron los tipos penales dista mucho de una visión comprehensiva de los fenómenos delictuales en ambientes digitales, mas cumplió una función de cubrir una necesidad imperiosa de regulación de la que adolecía nuestro ordenamiento jurídico. En este sentido, el primer informe de la comisión de constitución es transparente en el carácter de *primeros auxilios* del proyecto, señalando que los tipos que comprende están *"referidos exclusivamente al delito informático y no a otras ideas afines, que va a permitir sancionarlos por las graves consecuencias económicas y sociales que acarrean. Ha optado por este camino, menos*

pretencioso pero más realista, como única manera de permitir su aprobación en el plazo más breve posible."[4]

5. Críticas a la Ley Nº 19.223.

Derivado de las bajas pretensiones regulatorias de la Ley Nº 19.223, la doctrina nacional pudo identificar una serie de falencias. Las principales críticas de la doctrina nacional a este cuerpo normativo, podemos sintetizarlas en las siguientes:

1. Para algunos autores, la ley en comento, no hace una diferenciación doctrinaria, entre los delitos computacionales y los delitos informáticos, produciéndose una confusión en estos conceptos.

En este sentido, el profesor Herrera Bravo, señala que "al respecto, la Ley Nº Nº 19.223 confunde esta distinción y trata como delito informático a algunos delitos computacionales. Esto tiene como consecuencia, que, en esos casos, en vez de actualizar el tipo tradicional contenido en el Código Penal, –que habría sido lo correcto– crea una supuesta nueva figura. El problema que produce es comparable con la situación de considerar como delitos distintos el robo de una lámpara y el de una impresora, pese a que se trata de un mismo delito"[216].

2. En cuanto al bien protegido por la legislación sobre delitos informáticos, se sostiene por la doctrina, la existencia de otra confusión jurídica. Según los legisladores que aprobaron la ley, el bien protegido es la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan.

Sin embargo, la doctrina considera que se trata de varios bienes jurídicos, otorgándole a los ciberdelitos el carácter de "pluriofensivos".

[4] Biblioteca del Congreso Nacional. *Historia de la Ley Nº 19.223,* primer informe de Comisión de Constitución, pág. 7.

En esta línea, el profesor Herrera Bravo, sostiene que *"como los delitos informáticos atentan contra programas computacionales y ciertos datos, es ahí donde se debe buscar el bien jurídico. En el caso de los datos digitalizados, no todos merecen protección penal, sólo aquellos que sean relevantes o importantes. Ese grado de importancia puede ser dado por la naturaleza de la información, por ejemplo, nominativa, estratégica o económica. Por lo tanto, los delitos informáticos son pluriofensivos, afectan la intimidad, el patrimonio, la propiedad intelectual, la seguridad, etc."*[217].

En este mismo sentido, el autor Claudio Magliona, adhiere a la tesis de que los ciberdelitos son pluriofensivos, ya que *"protegen otros bienes jurídicos como la propiedad, la privacidad y la confianza en el correcto funcionamiento de los sistemas y redes computacionales"*[218].

3. Referente a las sanciones establecidas en estos delitos, se ha considerado que las penas privativas de libertad son muy altas, y que un mejor castigo, sería la aplicación de multas en U.T.M., a beneficio fiscal y del afectado.

Por ejemplo, según el artículo 1, si alguien destruye dolosamente un computador, puede ser sancionado con la pena de presidio menor en su grado medio a máximo, es decir, puede tener desde 541 días hasta 5 años de cárcel[219].

4. Otra crítica que compartimos, es la ubicación del texto normativo fuera del Código Penal. Ello es considerado como una desafortunada técnica legislativa, debido a que debilita a la legislación codificada.

En tal sentido, la solución a este problema, es el fortalecimiento de dicho Código y no seguir creando legislaciones penales particulares y especiales, que dispersan aún más la normativa penal existente, situación que dificulta la labor del juez y la defensa de los imputados.

5. Se señala también que la Ley Nº 19.223, no contemplaba las figuras delictuales de:

a) Hacking directo.

b) Fraude informático.

c) Copia ilegal de programas o piratería informática. Debemos señalar que este delito sí está contemplado en la Ley Nº 17.336 “sobre Propiedad Intelectual”, que analizamos en el numeral 10.2.3.4., de este trabajo.

d) La creación y distribución de programas computacionales dañinos y virus.

e) La falsificación de documentos electrónicos.

En general, la doctrina mayoritaria, consideraba que la Ley Nº 19.223 tipificaba, solamente, los delitos de sabotaje informático (artículos 1 y 3), y de espionaje informático (artículos 2 y 4), no lográndose un tratamiento adecuado del tema221.

Sin embargo, otros autores entre ellos Magliona, consideraron que el artículo 3, sancionaba el denominado “delito de alteración de datos”, consistente en *“alterar (introducción de datos erróneos, transformación y desfiguración de datos, y el suprimir datos correctos), dañar (borrado parcial de datos o oscurecimiento de datos) o destruir (borrado de datos, que los hace desaparecer de modo completo e irrecuperable) los datos contenidos en un sistema de tratamiento de información”*[222].

De esta manera, para el autor mencionado, la Ley Nº 19.223 distinguía entre los delitos de sabotaje informático y de alteración de datos, señalando que *“el sabotaje informático hace referencia a las acciones contra el sistema de tratamiento de información o contra su funcionamiento. En cambio, el delito de alteración de datos se refiere a las acciones contra los datos”*[223].

Por otro lado, el ya referido autor, consideró que el artículo 4 sancionaba la “revelación o difusión de datos contenidos en un sistema de tratamiento de información”. En tal sentido, explica que *“cuando se ocupa el verbo revelar, el dato debe ser secreto. Si se ocupa el verbo difundir, no es necesario que el dato sea secreto, pero creemos que sólo deberían protegerse por este artículo aquellos datos*

que realmente sean de interés para el sujeto pasivo. El inciso segundo del artículo 4, contempla una agravante de responsabilidad, cuando el que incurre en las acciones de revelación y difusión es el responsable del sistema de tratamiento de información. Este es el único caso en que la ley exigía la concurrencia de un sujeto calificado"[224].

Por el contrario, según el mencionado autor, sólo el artículo 2 de la Ley Nº 19.223, contemplaba el delito de espionaje informático.

En este caso, compartimos la opinión del autor Claudio Magliona, en el sentido de que la sanción de estos ilícitos resultaba dificultosa, mediante los tipos penales de sabotaje informático y de alteración de datos, debido a que la distribución del virus, no siempre proviene de su creador, sino que del computador de alguien conocido, quien muchas veces desconoce que su computador ha sido infectado, y que él mismo está infectando a otros.

Así, el mencionado autor concluye, *"que la sanción de la creación y distribución de programas destinados a dañar los sistemas de tratamiento de la información y las redes debe ser cubierta a través de un nuevo tipo, y no a través de las figuras de sabotaje informático y alteración de datos, las que no fueron creadas para reprimir esta nueva clase de conductas ilícitas, que producen daños a nivel mundial"*[226].

6. Ley Nº 21.459.

Como respuesta a las falencias observadas en la Ley Nº 19.223 y como medio de cumplir las obligaciones contraídas por el estado de Chile en la suscripción del Convenio de Budapest, la Ley Nº 21.459 tipifica de manera distinta los delitos relacionados a la esfera digital.

En cuanto al bien jurídico tutelado, la doctrina se muestra bastante conteste en que se trata del orden público económico, dentro del cual podemos encontrar

intereses como la fiabilidad del sistema financiero y la seguridad del tráfico económico.[5] Esta situación se encuentra en armonía del Convenio, por cuanto este cita entre sus referencias recomendaciones del Comité de Ministros relativas a medidas para luchar contra la piratería en materias de propiedad intelectual y derechos afines, protección de datos personales en servicios de telecomunicaciones y delincuencia informática.[6]

Además, es de relevancia destacar que los artículos 15 y 16 establecen un apartado con definiciones de utilidad para la correcta inteligencia del contenido de la ley. A continuación, se transcribirán las letras a) y b) del artículo 15, imprescindibles a efecto de comprender la tipificación:

> *a) Datos informáticos: Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.*
>
> *b) Sistema informático: Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.*

Al respecto, se puede observar una tipificación más fiel a los términos señalados en el Convenio, reconociendo los 7 delitos ya mencionados anteriormente en dicho instrumento y agregando una figura especial de receptación de datos informáticos.

---

[5] Radonich, Estefani (30-12-2022), Renzo Gandolfi Díaz, abogado, especialista en derecho de la empresa, regulación, ciberseguridad y tecnologías: "Con la entrada en vigor de la Ley Nº 21.459, hemos dado un salto de calidad muy necesario en nuestra legislación, que nos coloca en un pie de cumplimiento con el Convenio de Budapest», *Diario Constitucional*, https://www.diarioconstitucional.cl/entrevistas/renzo-gandolfi-diaz-abogado-especialista-en-derecho-de-la-empresa-regulacion-ciberseguridad-y-tecnologias-con-la-entrada-en-vigor-de-la-Ley Nº-21-459-hemos-dado-un-salto-de-calidad-muy-nec/

[6] Consejo Europeo, *Convenio sobre la ciberdelincuencia*, Budapest, 2001, pág. 2.

6.1 Ataque a la integridad de un sistema informático

El artículo 1° de la Ley Nº 21.459 tipifica el delito de ataque a la integridad de un sistema informático como *"El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo."*

Aquí se reconoce el delito señalado en el artículo 5° del Convenio de Budapest, manteniendo el verbo rector *obstaculizar*, manteniendo los mismos medios de comisión, salvo el borrado de información que podría subsumirse dentro del deterioro de la misma. Además, se aprecia que el legislador prescinde de la necesidad de gravedad de la afectación al sistema informático.

6.2 Acceso ilícito y divulgación de información obtenida de manera ilícita.

El artículo 2° tipifica el delito de acceso ilícito disponiendo que "*El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo."*

Este artículo recoge las ideas vertidas en el artículo 2° del Convenio, tomando la recomendación del mismo en cuanto exige el infringir medios de seguridad para su sanción, pero prescindiendo de exigir el ánimo de apoderamiento de la información como elemento subjetivo del tipo, reconociéndolo, en cambio, como una

agravante especial. Así, se observa el delito de acceso ilícito como uno de mera actividad, por cuanto no se requiere un resultado determinado, sino que basta con el sólo hecho de acceder a un sistema sin mantener las autorizaciones necesarias para que se configure el delito.

Al respecto, es menester referirse la regla contenida en el artículo 16° de la ley, la que dispone que "*Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo"*. Se colige del artículo que el consentimiento expreso del titular del sistema oficia como un justificante, estableciéndolo como causal de atipicidad del comportamiento. Reconoce aquí el legislador que la actividad de seguridad informática tiende a utilizar las mismas herramientas a las que podría tener acceso un pirata informático a efectos de probar la resistencia de un sistema a las entradas no autorizadas

También reconoce un segundo delito en la forma de la divulgación de información que haya sido obtenida por medios ilícitos, aunque no sea el mismo sujeto quien la extrae del sistema, igualando en su penalidad al delito de acceso ilícito. Y, con todo, se establece una forma agravada de este delito cuando sea una misma persona quien obtiene la información por medios ilícitos y luego la divulga.

En esta última figura no se exige el conocimiento de la ilicitud del origen de la información que se divulga, permitiendo así su configuración vía dolo eventual o culpa. Será importante, al caso, atender a la calidad de aquellos datos para vislumbrar qué tan evidente resulta su carácter ilícito para los efectos de esta última distinción.

Es claro el interés del legislador en salvaguardar la información contenida en los sistemas informáticos por sus repercusiones altamente nocivas para gran cantidad de personas, situación reconocida incluso en la génesis de la Ley Nº

19.223 alertando ante potenciales filtraciones de datos de Administradoras de Fondos previsionales con fines ilícitos de lucro, y reconociendo el tratamiento de *delitos masivos* por su afectación a indeterminados números de clientes.[7]

6.3 Interceptación ilícita.

El artículo 3° de la Ley Nº 21.459 dispone que comete el delito de interceptación ilícita: *"El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio. El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo."*

En este caso, la ley distingue dos supuestos. El primero de ellos, la intercepción, interrupción o interferencia por medios técnicos de una transmisión entre 2 o más sistemas, hace referencia a la técnica de piratería informática conocida como de interceptación de paquetes o *sniffing*, la que consiste en utilizar un programa o aparato para monitorear, capturar y analizar las transmisiones que se dan entre dos o más equipos.

El segundo supuesto es el de captura de datos contenidos en emisiones electromagnéticas, el que contempla situaciones como el valerse de elementos tecnológicos para captar señales de televisión de pago o de internet inalámbrico de manera ilegítima.

Al igual que el artículo homónimo del Convenio, la ley mantiene el verbo rector *interceptar* en el primer caso, pero agrega los medios de comisión mediante interrupción e interferencia al tipo.

[7] Biblioteca del Congreso Nacional. *Historia de la Ley Nº 19.223,* Mensaje, pág. 4.

En ambos casos, se observa que el legislador no requiere para su sanción un fin malicioso, situación que se encuentra permitida en el articulado del Convenio. Además, hace referencia a medios técnicos como único medio de comisión, dejando de lado otras posibilidades como, por ejemplo, las derivadas de la llamada *ingeniería social*, las que corresponden a *"técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados"*[8].

6.4 Ataque a la integridad de datos informáticos.

El artículo 4° de la Ley Nº 21.459 tipifica el delito de ataque a la integridad de datos informáticos, disponiendo que *"El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos"*.

En este caso, el legislador hace uso de la posibilidad del número 2 del artículo 4° del Convenio por cuando exige gravedad en el daño provocado en los datos como requisito objetivo de punibilidad, alejándose de una figura de delito de mera actividad. Además, en el requisito de punibilidad se reconocen los elementos no conservados de *daño* y *deterioro* a los que hace mención el Convenio como medios de comisión.

6.5 Falsificación informática.

El artículo 5° de la ley regula el delito de falsificación informática como *"El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo. Cuando la conducta descrita en el inciso anterior sea*

[8]Ingeniería social: Definición, página web de Kaspersky, consultada el día 27-08-2023, https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo."

Mantiene prácticamente en su totalidad las actitudes sancionadas señaladas en el Convenio, solamente cambiando la expresión *borre* por *dañe*, esta última con una rango de aplicación mayor por cuanto permite distintos niveles de afectación que no alcancen a la destrucción del dato.

Exige la ley una intencionalidad de engaño para establecer la punibilidad, por lo que parece excluir la posibilidad de una comisión culposa. Además, establece como agravante la circunstancia de que el actor sea empleado público y que haya abusado de su posición de tal para cometer el delito. Lo anterior explicado entendiendo el especial rol de salvaguardar la fe pública que conlleva el actual de quienes ejercen roles públicos.

6.6. Receptación de datos informáticos.

Dispone el artículo 6° de la Ley Nº 21.459, respecto de receptación de datos informáticos, que *"El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado"*.

A priori, identificamos que el legislador utiliza la misma estructura y el mismo elemento subjetivo del tipo que en el inciso primero del artículo 456 bis A del Código Penal[9], el cual tipifica el delito de receptación. Se puede vislumbrar, además, idéntico objetivo en la penalización: atacar la reducción en el mercado de los bienes

[9] Art. 456 bis A.- El que conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, a cualquier título, especies hurtadas, robadas u objeto de abigeato, de receptación o de apropiación indebida del artículo 470, número 1°, las transporte, compre, venda, transforme o comercialice en cualquier forma, aun cuando ya hubiese dispuesto de ellas, sufrirá la pena de presidio menor en cualquiera de sus grados y multa de cinco a cien unidades tributarias mensuales.

provenientes de hechos delictuales, al caso, el mercado secundario de datos personales obtenidos de forma ilícita y dar posibilidades de punibilidad ante el hallazgo casual de elementos de origen ilícito vinculados a otros delitos.

Este delito se entiende como el correlato práctico al de abuso de dispositivos contenido en el artículo 8° de ley, por cuanto este último, como se verá a continuación, exige cierto elemento de intencionalidad para su verificación. En cambio, al bastar que conozca o no pudiera menos que conocer el origen ilícito de la información las posibilidades de punibilidad son mayores.

Es posible argüir que este tipo tiene su correlato en el contenido en la letra b del número 1 del artículo 6° del Convenio, la cual requiere la penalización de la posesión de dispositivos, programas informáticos, contraseñas, códigos de acceso u otros datos similares que permitan acceso a todo o parte de un sistema, con el objeto de la perpetración de los delitos de acceso ilícito, interceptación ilícita y ataques a la integridad de los datos o sistemas.

Si bien comparte con la receptación de datos informáticos la punibilidad derivada solamente de tener su poder ciertos elementos, la situación del Convenio se refiere a elementos para la perpetración de los delitos, en cuanto la receptación se refiere a elementos obtenidos mediante los delitos. Así, la figura de la letra b número 1 del artículo 6° del Convenio es, más bien, identificable con la posesión de elementos conocidamente utilizados para cometer el delito de robo del artículo 445 del Código Penal[10].

[10] Artículo 445 del Código Penal: "*El que fabricare, expendiere o tuviere en su poder llaves falsas, ganzúas u otros instrumentos destinados conocidamente para efectuar el delito de robo y no diere descargo suficiente sobre su fabricación, expendición, adquisición o conservación, será castigado con presidio menor en su grado mínimo.*"

6.7 Abuso de los dispositivos.

Tal como se adelantó en el punto anterior, el artículo 8° de la Ley Nº 21.459 contempla el delito de abuso de los dispositivos en los siguientes términos: *"El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta Ley Nº o de las conductas señaladas en el artículo 7° de la Ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales."*

Además de los delitos de ataque a la integridad de sistemas y datos informáticos, acceso ilícito e interceptación ilícita, se remite la ley al delito de uso fraudulento de tarjetas de pago y transacciones electrónicas contenidas en el artículo 7° de la Ley Nº 20.009 que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude[11]. Así, este tipo incluye tanto la información que se utilizará como los medios de *software* y *hardware* necesarios para la perpetración de los delitos.

Se reconoce en el presente tipo solamente una comisión dolosa derivada de la necesidad del elemento subjetivo del tipo correspondiente a la intención de perpetrar, con aquellos medios tecnológicos, los delitos señalados anteriormente.

[11] Artículo 7° Ley Nº 20.009: "*Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado: f) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, bloqueadas, para realizar pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de ellas; h) Obtener maliciosamente, para sí o para un tercero, el pago total o parcial indebido, sea simulando la existencia de operaciones no autorizadas, provocándolo intencionalmente, o presentándolo ante el emisor como ocurrido por causas o en circunstancias distintas a las verdaderas.*" Las letras a, b, c, d, e y g se encuentran derogadas.

De este modo, sigue la Ley Nº 21.459 los lineamientos del Convenio en cuanto el número 2 de su artículo 6° indica que no debe imponer responsabilidad penal cuando no tenga aquella intencionalidad. A modo ejemplar, considerar las pruebas autorizadas u otros procedimientos propios de la seguridad informática, los que tienden a valerse de idénticas o muy similares herramientas.

6.8 Fraude informático.

El delito de fraude informático se encuentra contenido en el artículo 7° de la Ley Nº 21.459, tipificándose del siguiente modo:

> *"Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:*
>
> *1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales.*
>
> *2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.*
>
> *3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales.*
>
> *Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.*

Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito."

De la prosa del artículo anterior se observa un apego fiel del legislador chileno a los lineamientos del Convenio, manteniendo tanto los verbos rectores (salvo la modificación de *borrado* por *daño*, de forma símil a al caso del delito de falsificación informática), la necesidad de un perjuicio y el requisito de un elemento subjetivo de pretender un beneficio económico sea propio o para un tercero.

Además, salta a la vista que la estructura en la cual se expresa el tipo, e incluso la forma en la cual se establecen rangos de penalidad conforme a la cuantía del perjuicio, es reminiscente de los delitos de estafa contenidos en los artículos 467 y siguientes del Código Penal. En este mismo sentido, la extensión de punibilidad en los mismos términos que el autor a quien adquiera o ponga a disposición los medios informáticos para cometer el delito también se la encuentra en el inciso tercero del artículo 468 del Código Penal[12], el que se incorporó por medio de modificación legal derivada de la Ley Nº 21.595 de delitos económicos.

Así, es posible entender la figura del artículo 7° de la ley como una forma de estafa diferenciada por una forma de comisión especialmente ligada a la esfera informática.

Ahora bien, es menester destacar una importante diferencia en el núcleo del comportamiento reprochado en la ley y en la figura de estafa del Código Penal derivada del rol del sujeto pasivo o víctima del delito. En el caso del artículo 467, requiere que mediante engaño se produzca un error que induzca a la víctima una actitud que signifique un detrimento en su patrimonio y un correspondiente beneficio

[12] Artículo 468 inciso 3° del Código Penal: "Sin perjuicio de las penas que correspondan conforme al inciso anterior, sufrirá la pena de presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales el que obtenga indebidamente los datos codificados en una tarjeta de pago que la identifiquen y habiliten como medio de pago. La misma pena sufrirá el que los adquiera o ponga a disposición de otro a cualquier título."

al del actor del delito. En cambio, en la figura del artículo 7° el núcleo de la acción radica completamente en el actor del delito. Lo anterior se explica por cuanto, en este último caso, es el sistema informático el que provoca el detrimento de un patrimonio en beneficio de otro en razón de la introducción, alteración, daño o supresión de datos. Como no es posible reconocerle voluntad al sistema, el núcleo del acto debe necesariamente de descansar en el delincuente.

En este sentido, el mensaje de la Ley Nº 21.459 que "*figura conocida como "fraude informático", a juicio de algunos puede considerarse incluida dentro del tipo penal de estafa, pero en "aquellos ámbitos donde se han automatizado procesos de trabajo que antes desarrollaban personas físicas, al punto que en muchos casos la actividad autónoma de un sistema informático no sólo sirve de apoyo para la toma de decisiones, sino que dentro de determinado marco es el encargado de tales "decisiones". En este contexto, la manipulación informática puede ciertamente dar lugar a resultados perjudiciales para el patrimonio de determinadas personas, pero sin que resulte clara la concurrencia de un engaño ni del error correlativo."*[13]

Por ende, es posible concluir que la divergencia observada obedece a las particularidades de las tecnologías de la información y no a una pretensión de distinguirse necesariamente de las figuras de estafa.

7. **Atenuantes y agravantes especiales**.

Además de los delitos ya mencionados, la Ley Nº 21.459 establece circunstancias atenuantes y agravantes especiales, contenidas en sus artículos 9° y 10°.

8. Cooperación eficaz.

Dispone el artículo 9° la circunstancia atenuante de la cooperación eficaz en la investigación. Define este tipo de cooperación, en sus incisos primero y segundo, como *el suministro de datos o informaciones precisas, verídicas y comprobables,*

[13] Biblioteca del Congreso Nacional, *Historia de la Ley Nº 21.459,* Mensaje, pág. 7.

que contribuyan necesariamente al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en esta ley.

Esta clase de atenuante se encuentran cada vez más presentes en los cuerpos legales que tratan los tipos relacionados con estructuras delictivas o asociaciones ilícitas, como, por ejemplo, en el artículo 260 quáter del Código Penal respecto a delitos funcionarios, en el artículo 33 de la Ley Nº 20.000 sobre tráfico ilícito de estupefacientes o en el artículo 64 de la ley de delitos económicos. Obedece esta figura a una decisión estratégica de política criminal, con la que se opta por reducir el nivel de reproche al actor que permita desbaratar la estructura delictual de la cual es parte, y respecto a la cual muchas veces es imposible llegar sin información de alguien en su interior.

Esta circunstancia es recogida en su importancia investigativa durante la primera discusión en sala en el senado de la Ley Nº 21.459, pero advirtiendo un peligro consistente en establecer un sistema, en la práctica, de negociación de penas sobre el cual nuestro sistema procesal penal no fue construido[14], aunque podamos reconocer una apertura hacia dicho modelo de la mano de las negociaciones penológicas con la defensa en miras de un procedimiento abreviado.

9. Circunstancias agravantes.

El artículo 10 de la Ley Nº 21.459 reconoce 2 agravantes genéricas y una agravante especial que implica necesariamente un aumento de grado de penalidad.

El Número 1) de este artículo indica como agravante el *"cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio*

[14] Biblioteca del Congreso Nacional, *Historia de la Ley Nº 21.459,* Primer trámite constitucional: senado, discusión en sala, pág. 10.

de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función." En este caso, se observa un reconocimiento al elemento fiduciario que tiende a permear la labor de administración de bases de datos o sistemas informáticos, aumentando el reproche cuando esta relación de confianza es traicionada.

El número 2) indica que constituye una agravante el *"Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores."* Obedece este supuesto a la necesidad especial de cuidado que requieren estos sujetos especialmente vulnerables, y las dificultades de alfabetización digital que pueden existir en alguno de ellos considerado los conocimientos técnicos y específicos que implica la esfera informática.

El inciso segundo del artículo 10 dispone que se aumentará la pena en un grado cuando, *"como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la Ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios."*

Aquí lo que se salvaguarda especialmente son los sistemas informáticos utilizados para el control y administración de las grandes redes de suministros y estructuras organizacionales a nivel de gobierno y administración pública, en atención a las repercusiones dañinas potenciales para con un número indeterminado de personas que dependen del uso de estos sistemas, o para el normal funcionamiento de las instituciones.

10. Críticas a la Ley Nº 21.459.

Es posible replicar la crítica, realizada en su momento en contexto de la Ley Nº 19.223, consistente en que la actual Ley Nº 21.459 también se encuentra fuera del Código Penal.

El mantener una técnica legislativa de este tipo conlleva a que, paulatinamente, se le quite fuerza y cohesión a la norma codificada. Especialmente en materia penal, en el entendido de los importantes bienes jurídicos que salvaguarda, debería el legislador fortalecer la figura del Código Penal, tanto para fomentar una correcta aplicación del derecho al reducir la dispersión normativa, como para lograr de mejor manera los fines de prevención general que supone todo cuerpo normativo publicado que contemple penas.

En esta misma línea de pensamiento, el autor Meneses Díaz, sostiene que resulta oportuno *"fomentar la realización (de) una reforma al derecho penal sustantivo, que tenga como uno de sus pilares la existencia de un Código Penal como único cuerpo normativo que regule esta materia. En este mismo sentido, se debe señalar que en el derecho penal español estas figuras delictivas han sido incorporadas en su Código Penal (artículo 248 que trata de la estafa informática; artículo 264 que regula el delito de daño informático o sabotaje y el artículo 278 que trata el espionaje informático)"*[220].

Creemos que la correcta técnica legislativa debiera ser incorporar un nuevo título acerca de los "delitos informáticos", a continuación del último párrafo de los delitos contra la propiedad.

11. Conclusiones.

La Ley Nº 21.459, como respuesta del ordenamiento jurídico chileno a la necesidad de adaptarse a las exigencias del Convenio de Budapest, es una norma efectiva que, no solo cumple con los estándares que supone dicho instrumento internacional, sino que supone un enorme avance regulatorio en comparación a la anterior ley regulatoria de delitos informáticos, la 19.223.

Esta mejora se explica tanto por un mejor entendimiento de la doctrina acerca de los delitos informáticos que supone el paso del tiempo adaptación a las nuevas tecnologías, sino también por elegir una técnica legislativa más efectiva centrada en los bienes jurídicos tutelados.

Tipifica la ley, en concordancia con el señalado Convenio, un catálogo de derechos mucho más robusto que el anterior y con un mayor nivel de detalle sin ser restrictivo en sus verbos rectores, lo que facilita su aplicación en circunstancias de tecnología actual como, se espera, futura.

Sin perjuicio de lo anterior, se detecta una falencia en la técnica legislativa de la Ley Nº 21.459 correspondiente a haberse sustanciado como una ley extra código, debilitando la codificación de leyes penales y estableciendo barreras a la hora de una correcta aplicación del derecho mediante la dispersión normativa.

Con todo, esta ley está recién nacida, por lo que hay espacio presente para que tanto la doctrina como la jurisprudencia puedan observar el desarrollo de su aplicación y proponer mejoras que puedan extraerse de la experiencia. Ya que, más allá de la pretensión regulatoria de largo tiempo que implica el legislar, por el vertiginoso avance de las tecnologías de la información no sería extraño que nuevamente nos veamos ante un proceso legislativo en estas materias.