La nueva ley de delitos informáticos

Laura Mayer Lux
Pontificia Universidad Católica de Valparaíso

Jaime Vera Vega
Pontificia Universidad Católica de Valparaíso

I. Introducción

El lunes 20 de junio de 2022, se publicó en el Diario Oficial la Ley Nº 21.459, que "Establece normas sobre delitos informáticos, deroga la Ley Nº 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest". En cuanto a su estructura, dicha ley se divide en tres Títulos, a saber: un Título I, *De los delitos informáticos y sus sanciones*; un Título II, *Del procedimiento* y un Título III, denominado *Disposiciones finales*, que define los conceptos de "datos informáticos", "sistema informático" y "prestadores de servicios" (artículo 15). Este último título indica cuándo se entenderá que un sujeto cuenta con autorización para acceder a un sistema informático (ar-

tículo 16), para efectos del tipo de acceso ilícito (artículo 2º); deroga la Ley Nº 19.223 (artículo 17) y modifica diversos cuerpos legales, como el Código Procesal Penal (CPP); la Ley Nº 18.168, General de Telecomunicaciones y la Ley Nº 20.393, sobre responsabilidad penal de las personas jurídicas (artículos 18 a 21). Además, la Ley Nº 21.459 culmina con tres artículos transitorios, relativos a su aplicación desde un punto de vista temporal.

No parece exagerado afirmar que esta constituye una de las más importantes reformas a la legislación penal chilena de los últimos años, por varias razones, de las cuales es posible destacar especialmente dos. En primer lugar, porque es la primera vez que la normativa nacional, basada en buena medida en lo que establece el Convenio de Ciberdelincuencia, cuenta con un catálogo (bastante) completo de delitos informáticos, en particular si se lo compara con el listado de delitos de la Ley Nº 19.223, según veremos luego. En segundo lugar, porque la nueva ley permite perseguir responsabilidad penal tanto de personas naturales como de personas jurídicas, ampliando considerablemente el elenco de delitos que prevé el artículo 1º de la Ley Nº 20.393.

Este trabajo tiene por objeto analizar, en los términos acotados que permite un artículo, los principales aspectos sustantivos y procesales que se encuentran regulados en la Ley Nº 21.459. Para esos efectos, el texto comenzará refiriendo los antecedentes, fundamentalmente normativos, de la nueva ley de delitos informáticos, con lo cual se pretende contextualizar la reforma operada por la Ley Nº 21.459, así como expresar algunas de las razones que explican el contenido y la estructura de la nueva normativa incorporada al ordenamiento jurídico chileno. Luego, se examinarán los diversos delitos informáticos incluidos en la Ley Nº 21.459, así como las disposiciones de índole procesal relacionadas con la persecución penal de tales ilícitos; materias en las que se efectuarán constantes referencias a la Ley Nº 19.223, al Convenio de Ciberdelincuencia, así como a diversos preceptos del Código Penal (CP) y del CPP.

II. Antecedentes de la nueva ley de delitos informáticos

La nueva ley de delitos informáticos tiene dos antecedentes normativos de relevancia.

En primer lugar, cabe mencionar la Ley Nº 19.223, que *Tipifica figuras penales relativas a la informática*, publicada en el Diario Oficial el 7 de junio de 1993. Como es sabido, dicha ley se estructura sobre la base de cuatro artículos, destinados exclusivamente a regular comportamientos delictivos que se vinculan con el sabotaje informático (artículos 1º y 3º) y con el espio-

naje informático[1] (artículos 2º y 4º). Lo dicho permite destacar desde ya tres importantes diferencias entre la Ley Nº 19.223 y la Ley Nº 21.459.

La primera se relaciona con la cantidad de delitos regulados, cuestión que, si bien puede tener una dimensión meramente numérica, también da cuenta del grado de exhaustividad con que el legislador ha decidido abordar la criminalidad informática en uno y otro caso.

La segunda diferencia entre ambas leyes, que se vincula directamente con la anterior, dice relación con las categorías delictivas que en ellas se regulan. Como se dijo, dichas categorías pueden reducirse a dos, tratándose de la Ley Nº 19.223, mientras que en el caso de la Ley Nº 21.459 ellas pueden sistematizarse en seis clases distintas: tipos vinculados con el sabotaje informático (artículos 1º y 4º), delitos relacionados con el espionaje informático[2] (artículos 2º y 3º), falsificación informática (artículo 5º), receptación de datos informáticos (artículo 6º), fraude informático (artículo 7º) y abuso de los dispositivos (artículo 8º).

En fin, la tercera diferencia entre la Ley Nº 19.223 y la Ley Nº 21.459 radica en que la primera se limita a regular delitos, abarcando la segunda, en cambio, la consagración de tipos penales, de circunstancias modificatorias de la responsabilidad penal e incluso de reglas que atañen al proceso penal que se siga para la persecución de un delito informático.

En segundo lugar, constituye un importante antecedente de la nueva ley el Convenio de Ciberdelincuencia, suscrito en Budapest el 23 de noviembre de 2001. Cabe hacer presente que el 28 de agosto de 2017 se publicó el Decreto Nº 83 del Ministerio de Relaciones Exteriores, que promulgó dicho instrumento internacional en nuestro país, con lo cual el Estado chileno pasó a ser, oficialmente, parte del Convenio. Ello implicaba básicamente que la legislación penal chilena debía adecuar su contenido a los deberes surgidos del Convenio de Ci-

[1] Expresión que está siendo empleada en términos laxos, como comprensiva tanto de conductas ligadas con el acceso ilícito a datos o sistemas informáticos, como con comportamientos relacionados con su difusión. En términos análogos, tales conductas pueden sistematizarse en un tipo de "intromisión" y un tipo de "indiscreción", respectivamente. *Vid*., Aldoney, Rodrigo. "La revelación de secretos de empresa - Posibles déficits punitivos y posibilidades dogmáticas de su superación", en Van Weezel, Alex (editor). *Humanizar y renovar el Derecho penal: Estudios en memoria de Enrique Cury*. Santiago: Thomson Reuters (2013), p. 1001.

[2] Nuevamente, dicha expresión está siendo empleada de forma laxa, en el sentido de abarcar tanto el acceso ilícito como la interceptación ilícita. Esta última conducta, si bien tiene algunos puntos de contacto con el sabotaje informático, en especial cuando castiga a quien "interrumpa" o "interfiera", por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de tales sistemas, castiga, asimismo, a quien intercepte o capte (sin contar con la debida autorización) datos de un sistema informático.

berdelincuencia, cuestión que a su turno suponía actualizar y complementar la normativa nacional relativa a la criminalidad informática según lo preceptuado por dicho instrumento[3].

Tuvieron que pasar casi cinco años para que la legislación atingente a la delincuencia informática se reformara definitivamente, modificación que estuvo precedida de un arduo debate parlamentario, en el que se discutieron varios de los puntos que se desarrollarán *infra*.

III. Aspectos sustantivos de la nueva ley de delitos informáticos

Las materias sustantivas de la Ley Nº 21.459 se encuentran en su Título I, rubricado, como se dijo, *De los delitos informáticos y sus sanciones*. Dicha sección de la ley tipifica los distintos delitos informáticos, así como las circunstancias modificatorias de responsabilidad penal aplicables frente a su comisión. Por consiguiente, dividiremos el análisis de esa misma manera, para mayor claridad del lector. Además, revisaremos en este apartado la introducción de la responsabilidad penal para las personas jurídicas por la comisión de los delitos regulados en la Ley Nº 21.459.

1. Tipificación de los delitos informáticos

La nueva ley regula ocho comportamientos delictivos, que corresponden a los siguientes tipos penales: ataque a la integridad de un sistema informático (artículo 1º), acceso ilícito (artículo 2º), interceptación ilícita (artículo 3º), ataque a la integridad de los datos informáticos (artículo 4º), falsificación informática (artículo 5º), receptación de datos informáticos (artículo 6º), fraude informático (artículo 7º) y abuso de los dispositivos (artículo 8º). Como se indicó, tales ilícitos pueden sistematizarse en seis categorías delictivas, atendidos los puntos de contacto que existen entre los tipos penales de los artículos 1º y 4º (sabotaje informático), por una parte, y de los artículos 2º y 3º (espionaje informático), por otra parte.

[3] *Vid*., Becker, Sebastián y Viollier, Pablo. "La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley Nº 19.223", en *Revista de Derecho Universidad de Concepción*, vol. 88, Nº 248 (2020), p. 76.

a) Sabotaje informático

i) Ataque a la integridad de un sistema informático (artículo 1º)

Este delito, que tiene como antecedente el tipo de ataque a la integridad del sistema del artículo 5º del Convenio de Ciberdelincuencia[4], se regula en el artículo 1º de la Ley Nº 21.459, disposición que establece lo siguiente:

> "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".

Dicho supuesto corresponde al caso más grave de sabotaje informático, cuestión que se explica en atención a los efectos que tendría la conducta delictiva. En ese sentido, como veremos *infra*, el artículo 4º, que regula el otro supuesto de sabotaje informático, castiga a quien indebidamente altere, dañe o suprima datos informáticos; de modo que incluso sería posible que la comisión del delito del artículo 1º implique asimismo la realización del tipo del artículo 4º, además del impacto negativo en el funcionamiento del sistema informático de que se trate, al que nos referiremos luego.

En el plano fenomenológico, el delito en comento podría identificarse, por ejemplo, con los denominados ataques DoS, que implican "saturar el servidor del sistema logrando que el mismo se centre en la petición que realiza el atacante[,] sin que pueda atender a ninguna más"[5]. Consiguientemente, se trata de un ilícito que podría tener muy diversos impactos y afectar sistemas informáticos orientados a funciones muy distintas. Por lo mismo, la comisión del delito en comento podría hacer aplicable la nueva agravante del artículo 10 inciso final de la Ley Nº 21.459, que examinaremos *infra*.

Desde un punto de vista objetivo, el tipo se encuentra construido sobre la base de dos verbos alternativos, que corresponden a "obstaculizar" o "impedir"; por ende, basta que se verifique cualquiera de ellos para que se configure la conducta punible.

---

[4] Artículo 5 - Ataques a la integridad del sistema.

"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno 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".

[5] Miró, Fernando. *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid *et al.*: Marcial Pons (2012), p. 303.

De acuerdo con el Diccionario de la Lengua de la Real Academia Española (en adelante, DRAE), "obstaculizar" puede entenderse como dificultar o hacer más difícil, en este caso, el funcionamiento del sistema de tratamiento automatizado de la información. "Impedir", según ese mismo diccionario, implica estorbar o imposibilitar la ejecución de dicho sistema.

En ambos casos, ha de afectarse el "normal" funcionamiento del sistema informático, o sea, la manera en que él habitual u ordinariamente opera. Por consiguiente, para poder establecer si se ha incidido negativamente en el normal funcionamiento de un sistema informático, habrá que definir previamente qué funciones desempeñaba dicho sistema.

Por otra parte, se castiga tanto el comportamiento que afecta totalmente el funcionamiento del sistema informático, así como aquel que lo impacta de modo solamente parcial. Teniendo en cuenta que ambas hipótesis se encuentran conminadas con la misma pena, será necesario exigir una afectación que, siendo parcial, resulte equivalente, en cuanto a su gravedad, a los casos en que se afecta totalmente el normal funcionamiento del sistema en cuestión[6]. Por lo tanto, no cualquier impacto parcial en dicho funcionamiento será penalmente relevante.

La ley establece seis modalidades alternativas a través de las cuales es posible llevar a cabo los comportamientos consistentes en obstaculizar o impedir el normal funcionamiento del sistema informático. Todas esas modalidades implican la realización de movimientos corporales orientados a obstaculizar o impedir el funcionamiento de un sistema de tratamiento automatizado de la información, lo que permite sostener que nos encontramos ante un tipo penal de acción, cuestión que por lo demás es característica de la criminalidad informática[7]. Nuevamente, ello implica que basta con que se verifique cualquiera de esas hipótesis para que se configure la modalidad delictiva de que se trate.

---

[6] Un razonamiento análogo puede verse en Mayer, Laura y Vera, Jaime. "El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho penal chileno", en *Polítca Criminal*, vol. 14, Nº 27 (2019), pp. 435-436.

[7] Lo cual es sin perjuicio de lo que establece el inciso final del artículo primero transitorio de la Ley Nº 21.459, según el cual, para los efectos de lo dispuesto en los incisos primero y segundo de dicho precepto, "el delito se entiende perpetrado en el momento o durante el lapso en el cual se ejecuta la acción punible o se incurre en la *omisión* punible" (cursivas agregadas). A nuestro juicio, el texto transcrito no debe interpretarse como una norma habilitante para el castigo de hipótesis de omisión impropia en el ámbito de la criminalidad informática –en la línea de lo que sí permiten el artículo 11 del CP español o el § 13 del StGB–, pues para ello sería necesario que se indicaran requisitos para el castigo de la omisión impropia (*v. gr.*, la concurrencia de una posición de garante), que en la nueva ley no se señalan. Por el contrario,

Para definir los diversos comportamientos que sanciona este delito, recurriremos al DRAE. De acuerdo con él, "introducción" es la acción y efecto de introducir o introducirse, mientras que introducir equivale a meter o hacer entrar, en este caso, los datos en el sistema informático afectado.

"Transmisión", por su parte, es la acción y efecto de transmitir, verbo que puede equipararse a transferir, o bien, a traspasar, en lo que aquí interesa, datos informáticos desde un sistema de tratamiento automatizado de la información a otro.

"Daño" es el efecto de dañar, comportamiento que se identificar con causar un detrimento, perjuicio o menoscabo a dichos datos.

"Deterioro" es la acción y efecto de deteriorar, en tanto que dicha conducta supone hacer que algo, en este caso, los datos, pasen a un peor estado o condición.

"Alteración" es la acción de alterar, comportamiento que puede entenderse como cambiar o modificar[8] la configuración de los datos del sistema informático de que se trate. Más concretamente, la doctrina española entiende por alteración "toda perturbación funcional definitiva", que podría verificarse "añadiendo nuevos datos, borrando parcialmente los existentes, eliminando o modificando las relaciones entre ellos, etc."[9].

En fin, "supresión" es la acción y efecto de suprimir, conducta que puede equipararse a la de eliminar los datos en cuestión.

Considerando que cualquiera de esas modalidades podría servir a la configuración del delito del artículo 1º de la Ley Nº 21.459, resulta necesario que ellas sean interpretadas en términos equivalentes desde el punto de vista de su gravedad[10].

En cuanto a la estructura del tipo de ataque a la integridad de un sistema informático, es posible sostener que él constituye un delito de resultado, toda vez que exige que se obstaculice o impida el normal funcionamiento (resultado) a través de determinadas modalidades de comisión (medios). Por lo tanto, se requiere de una transformación del mundo externo, a través de la conducta, que se proyecta en el normal funcionamiento del sistema. Además, teniendo

---

el referido texto debe entenderse sistemáticamente, esto es, de acuerdo con el contexto en el que él se consagra, y que corresponde al de la vigencia temporal de la Ley Nº 21.459.

[8] Véase Mayer y Vera. "El documento como objeto material…", ob. cit., p. 438.

[9] Corcoy, Mirentxu. "Capítulo IX. De los daños", en Corcoy, Mirentxu y Mir, Santiago (directores), *Comentarios al Código Penal*. Valencia: Tirant lo Blanch (2015), p. 950.

[10] Mayer y Vera. "El documento como objeto material…", ob. cit., p. 438.

en cuenta que dichas modalidades son fraccionables[11], puede afirmarse que el delito admite tanto la tentativa como la frustración.

Objeto material del delito es un sistema informático, que la Ley Nº 21.459 define como "[t]odo 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" (artículo 15 b]). Resulta destacable que se aluda expresamente a un sistema "informático", lo que permite evitar los equívocos a los que podían conducir las referencias a un sistema de tratamiento de información, contenidas en la Ley Nº 19.223[12].

En el plano subjetivo, ya que el tipo penal no establece exigencia subjetiva alguna que apunte, necesariamente, a demandar dolo directo (*v. gr.*, una actuación ejecutada "maliciosamente"), basta con que el delito se perpetre con dolo eventual[13]. La modalidad culposa debe ser descartada, no sólo porque resulta muy difícil (si no imposible) concebir la realización de un "ataque" a la integridad de un sistema informático por mera imprudencia, sino porque para sancionar ese supuesto se requeriría de una cláusula en la descripción legal que claramente apuntara en esa dirección (por ejemplo, una conducta llevada a cabo con negligencia o impericia)[14].

---

[11] Por ejemplo, cuando se emplea un *malware* para la perpetración del delito, sin que todavía se haya completado la realización de la conducta respectiva. *Vid*., a propósito de dicha manera de cometer delitos informáticos, Mayer, Laura. "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", en *Ius et Praxis*, vol. 24, Nº 1 (2018), pp. 168 y ss. con referencias ulteriores.

[12] *Vid*., a propósito de la interpretación del concepto (amplio) de "sistema de información", Jijena, Renato. "Debate parlamentario en el ámbito del Derecho informático. Análisis de la Ley Nº 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, vol. XV (1993-1994), p. 351.

[13] En esa línea, no obstante que el artículo 2º CP parece equiparar los términos "dolo" y "malicia" (véase Mañalich, Juan Pablo. "Condiciones generales de la punibilidad", en *Revista de Derecho* [Universidad Adolfo Ibáñez], Nº 2 [2005], pp. 403-404), también es efectivo que el legislador sólo en determinados tipos de la Parte Especial exige obrar "maliciosamente", "a sabiendas", "de propósito", etc., lo que importa un reforzamiento de los requisitos subjetivos de tales delitos y, muy especialmente, de aquellos de reciente consagración (véase, entre otros, Hernández, Héctor. "Art. 1º", en Couso, Jaime y Hernández, Héctor [directores], *Código Penal Comentado. Parte general, Doctrina y Jurisprudencia*. Santiago: Abeledo Perrot [2011], p. 75).

[14] Ello se basa en que el ordenamiento jurídico penal chileno prevé un sistema mixto de tipificación de los delitos culposos, en el que es posible sancionar figuras imprudentes que no se encuentren entre los delitos contra las personas –como es el caso de los delitos informáticos–, en la medida en que exista una modalidad culposa aplicable. En esa línea, como

ii) Ataque a la integridad de los datos informáticos (artículo 4º)

Este delito, que tiene como antecedente el tipo de ataques a la integridad de los datos del artículo 4º del Convenio de Ciberdelincuencia[15], se encuentra regulado en el artículo 4º de la Ley Nº 21.459, precepto que establece lo siguiente:

> "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".

Desde un punto de vista objetivo, el tipo se encuentra construido sobre la base de tres comportamientos alternativos (alterar, dañar o suprimir); por ende, basta que se verifique cualquiera de ellos para que se configure la conducta punible. Todos esos comportamientos suponen la realización de acciones generadoras del grave daño para el titular de los datos, lo que permite afirmar que nos encontramos ante un tipo penal de acción. En cuanto a su sentido y alcance nos remitimos a lo sostenido respecto de tres de las modalidades típicas del ataque a la integridad de un sistema informático, por coincidir exactamente con las conductas que sanciona el tipo de ataque a la integridad de los datos informáticos.

El comportamiento típico debe llevarse a cabo "indebidamente", lo que equivale a que se realice ilícitamente. En ese sentido, de lo que se trata es de que exista una alteración, daño o supresión de datos a los que no se estaba facultado. De ello se sigue que pueden existir situaciones que tornen lícita la conducta, justamente, porque el agente se encuentra habilitado a llevar a cabo tales acciones. Así, por ejemplo, podría imaginarse la hipótesis en que el titular del sistema informático y de los datos en él contenidos le solicite al encargado de informática de la entidad en la que ambos prestan servicios que borre información almacenada en dicho sistema.

Objeto material del delito son datos informáticos, que la Ley Nº 21.459 define como "[t]oda representación de hechos, información o conceptos ex-

---

plantea Etcheberry, el castigo penal del delito culposo "requiere texto expreso". Etcheberry, Alfredo. *Derecho Penal*, *Parte General*, tomo I, reimpresión de la 3ª ed. Santiago: Editorial Jurídica de Chile (2010), p. 321.

[15] Artículo 4º - Ataques a la integridad de los datos.

"1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves".

presados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función" (artículo 15 a]).

El delito supedita la imposición del castigo al hecho de que "se cause un daño grave" al titular de los datos. La gravedad relativa del daño provocado por el sabotaje informático es una cuestión que debe analizarse caso a caso. No obstante, es posible plantear que, en principio, no implicará un daño grave aquel ataque a la integridad de datos informáticos que pueden recuperarse de forma más o menos sencilla. Por su parte, la gravedad de una destrucción meramente parcial de datos[16] dependerá del efecto que ella genere respecto de esos mismos datos o de otros datos, con los que los primeros se encuentran (funcionalmente) relacionados.

En cuanto a la naturaleza jurídica de la cláusula en comento, es posible plantear al menos las dos siguientes alternativas interpretativas:

En primer lugar, puede sostenerse que el daño grave que se causaría con la conducta delictiva sería el resultado del tipo, lo que permitiría afirmar que nos encontramos ante un delito de resultado material que, por ende, admitiría hipótesis de ejecución imperfecta de la conducta (tentativa y frustración). Ello podría sustentarse, entre otras cosas, en el hecho de que el tipo exija que se "cause" un daño grave, exigencia que evocaría la causalidad que se requiere, en los delitos de resultado, entre el comportamiento delictivo y el resultado material.

En segundo lugar, es posible plantear que el daño grave que se causaría con la conducta delictiva sería una condición objetiva de punibilidad, con lo cual no sería posible sancionar supuestos de ejecución imperfecta del delito (tentativa y frustración). En ese sentido, pese a la descripción del tipo, nos hallaríamos frente a un delito de mera actividad. Ello podrá fundarse, por ejemplo, en que el tipo parece supeditar, o sea, condicionar la imposición del castigo a la circunstancia de que se verifique aquel daño ("*siempre que* con ello se cause un daño grave"). Además, la redacción del tipo no es muy distinta a la de otras figuras delictivas, *v. gr.*, el abandono de personas desvalidas[17], en las que cláusulas similares han sido interpretadas como condiciones objetivas

16 *Vid*., respecto de dicho problema, a propósito de la destrucción parcial de un documento electrónico, Mayer y Vera. "El documento como objeto material…", ob. cit., pp. 444-445.

17 *Vid*., el artículo 352 del Código Penal, de acuerdo con el cual, "[e]l que abandonare a su cónyuge o a un ascendiente o descendiente, legítimo o ilegítimo, enfermo o imposibilitado, *si el abandonado sufriere lesiones graves o muriere a consecuencia del abandono*, será castigado con presidio mayor en su grado mínimo" (cursivas agregadas).

de punibilidad[18]. Finalmente, puede señalarse que en la discusión parlamentaria se planteó reiteradamente la necesidad de evitar el castigo de acuerdo con el delito en comento cuando la conducta no tuviera un impacto relevante en intereses de terceros[19], en coherencia con lo que dispone el artículo 4º Nº 2 del Convenio de Ciberdelincuencia[20].

En todo caso, la exclusión del castigo en virtud de dicha figura delictiva no tiene por qué implicar la impunidad del agente, considerando la amplitud de la primera hipótesis de acceso ilícito, regulada en el artículo 2º de la Ley Nº 21.459, a la que nos referiremos *infra*. En esa línea, es probable que muchos supuestos que impliquen un daño "no grave" de datos informáticos, se encuentren precedidos de la comisión del delito de acceso ilícito a un determinado sistema informático[21], en cuyo caso podrá sancionarse al agente, no por el sabotaje informático, sino por el acceso ilícito ya indicado.

En el ámbito subjetivo, el tipo penal no contempla requisito subjetivo alguno que apunte, necesariamente, a exigir dolo directo (*v. gr.*, una actuación "a sabiendas"), por lo que basta con que él se perpetre mediante dolo eventual. La modalidad culposa debe ser descartada, por las mismas razones señaladas a propósito del ataque a la integridad de un sistema informático.

b) Espionaje informático

En cuanto a las hipótesis que hemos calificado de espionaje informático (artículos 2º y 3º), cabe destacar, de acuerdo con lo señalado *supra*, que empleamos dicha expresión en términos laxos, comprensivos tanto de supuestos de acceso ilícito (de diversa índole) como de interceptación ilícita. Sin perjuicio del análisis que se efectuará luego respecto de esta última figura, es claro que el acceso ilícito ha sido el delito que más discusión ha generado a nivel doctrinal. Ello se vio reflejado en la tramitación de la Ley Nº 21.459, toda vez que buena

[18] En ese sentido, por ejemplo, Bullemore, Vivian y MacKinnon, John. *Curso de Derecho Penal*, *Parte Especial*, tomo III, 5ª ed. Santiago: Ediciones Jurídicas de Santiago (2021), p. 106; Politoff, Sergio; Matus, Jean Pierre y Ramírez, María Cecilia. *Lecciones de Derecho Penal Chileno*, *Parte Especial*, reimpresión de la 2ª ed. Santiago: Editorial Jurídica de Chile (2011), p. 170.

[19] *Vid*., en ese sentido, por ejemplo, Historia de la Ley Nº 21.459, pp. 111-112.

[20] Según el cual, "[l]as Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 [referido a los ataques a la integridad de los datos] comporten *daños graves*" (cursivas agregadas).

[21] Por lo mismo, el espionaje informático o acceso ilícito puede asumir el carácter de "delito presupuesto" de un fraude informático o de un sabotaje informático. *Vid*., Mayer y Vera. "El delito de espionaje informático…", ob. cit., p. 228.

parte del debate parlamentario se centró en el sentido y alcance que debía dársele a dicho comportamiento, actualmente regulado en el artículo 2º de la ley.

i) Acceso ilícito (artículo 2º)

Este delito, que tiene como antecedente el tipo de acceso ilícito del artículo 2º del Convenio de Ciberdelincuencia[22], se regula en el artículo 2º de la Ley Nº 21.459, disposición que establece lo siguiente:

> "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".

La norma recién transcrita debe ser complementada con lo señalado en el artículo 16 de la Ley Nº 21.459, rubricado "Autorización e Investigación Académica", de acuerdo con el cual:

> "Para efectos de lo previsto en el artículo 2º 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".

Como podrá notarse, la regulación del acceso ilícito que surge de esos preceptos cierra o al menos limita muy considerablemente la posibilidad de excluir del castigo punitivo a aquellos comportamientos que pueden englobarse dentro de la noción de *hacking* ético. Dicho concepto, cuyo significado no es del todo claro y cuya correcta precisión excedería el objeto del presente artículo, puede relacionarse, al menos provisoriamente, con las siguientes ideas.

[22] Artículo 2º - Acceso ilícito.
"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático".

Por una parte, con el hecho de que no todo *hacking* sería equivalente y que, en esa línea, las motivaciones[23] que puede tener el agente del comportamiento serían (muy) relevantes. Desde este punto de vista, podría existir un *hacking* que se realiza por una buena razón o por una buena causa[24], en contraposición con otras expresiones de esa misma conducta, caracterizadas por llevarse a cabo con una finalidad ilegítima, que se identifica, genéricamente, con la provocación de un daño a terceros[25].

Por otra parte, el concepto de *hacking* ético parece estar indisolublemente asociado con ciertos avances en el ámbito de la informática, en el sentido de que quienes lo practican serían sujetos cuya labor es esencial para identificar vulnerabilidades o brechas de seguridad. En ese sentido, el *hacker* ético no se limitaría a ingresar al sistema informático de que se trate y a evaluar sus niveles de amenaza, sino que informaría a su titular qué riesgos advirtió y cómo es posible solucionarlos[26].

Ahora bien, dicha aproximación al problema, que divide al mundo del *hacking* entre "buenos" y "malos", así como entre sujetos cuyo aporte es "decisivo" o no para el desarrollo de la informática, a ratos oculta una realidad bastante más plausible, a saber, que muchas conductas se encuentran en una zona gris[27], en la que no es evidente la bondad de las motivaciones del agente ni la importancia que tiene su comportamiento para el avance de aquella disciplina. Como sea, la exclusión del *hacking* ético de los supuestos penalmente relevantes no logró concitar acuerdo parlamentario, imponiéndose la idea de que el *hacking*, en cualquiera de sus expresiones, no se encontrará permitido en la legislación penal chilena.

Si tenemos en cuenta lo que dispone el artículo 2º de la Ley Nº 21.459, se advertirá que en él se regulan cuatro tipos penales, todos los cuales están consagrados como delitos de acción.

---

[23] *Vid*., respecto de dicho problema, Owen, Ken y Head, Milena. "Motivation and Demotivation of Hackers in Selecting a Hacking Task", en *Journal of Computer Information Systems* (2022).

[24] En términos similares Maurushat, Alana. *Ethical Hacking*. S.l.: University of Ottawa Press (2019), p. 1.

[25] En este contexto, es común que se abandone el concepto de *hacking* y se lo reemplace por el de *cracking*. *Vid*., Mayer. "Elementos criminológicos…", ob. cit., p. 167, n. 72 con referencias ulteriores; Miró. *El cibercrimen*…, ob. cit., p. 302.

[26] *Vid*., Callejas Espinoza, Gustavo. "*Ethical Hacking*: Conciencia de Seguridad", en *Revista PGI*, Nº 7 (2021), p. 43.

[27] En ese sentido, Jaquet-Chiffelle, David-Olivier y Loi, Michele. "Chapter 9: Ethical and Unethical Hacking", en Christen, Markus; Gordijn, Bert y Loi, Michele (editores). *The Ethics of Cybersecurity*. Cham: Springer Open (2020), pp. 179 y ss.

En primer lugar, se prevé un tipo penal que podríamos catalogar de mero acceso ilícito[28], que castiga "[a]l que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático" (inciso primero). Comparativamente, dicho ilícito tiene asignada una pena baja, que puede ser presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales; de modo tal que el castigo de dicho supuesto podría ser exclusivamente pecuniario.

En segundo lugar, el artículo 2º establece una figura que podríamos calificar de espionaje informático[29], que debe aplicarse "[s]i el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático" (inciso segundo, primera parte). En dicho evento, la pena a imponer será la de presidio menor en sus grados mínimo a medio.

En tercer lugar, se castiga, también con la pena recién señalada, "a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste" (inciso segundo, segunda parte); mientras que, en cuarto lugar, se establece que, "[e]n 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" (inciso tercero).

Por lo tanto, en el artículo 2º de la Ley Nº 21.459 se regulan tanto hipótesis de "intromisión" como de "indiscreción"[30].

En cuanto al tipo penal de mero acceso ilícito, del artículo 2º inciso primero de la ley, es posible destacar tres cuestiones que se desprenden de su sola lectura.

La primera tiene que ver con un asunto que podríamos calificar de técnico-legislativo, en el sentido de lo superflua que sería la alusión a "exceder la autorización que se posea", situación que perfectamente podría subsumirse en la referencia a la falta total de autorización para acceder al sistema, que se prevé en la primera parte del precepto. Ello es así, pues si, por ejemplo, un sujeto tiene autorización para acceder a un sistema informático, con la sola finalidad de visualizar datos que en él se contienen, es claro que no tendría autorización para, *v. gr.*, modificar o almacenar esos datos en un dispositivo

[28] En el que probablemente serán subsumidos los casos de *hacking* ético, a los que hicimos referencia, así como otros supuestos de *hacking* de menor gravedad en comparación con las restantes hipótesis del artículo 2º de la ley.

[29] En la medida en que se asuma que él "involucra tanto un acceso a los datos como un conocimiento de ellos (en ambos casos, indebido)" (Mayer, Laura y Vera, Jaime. "El delito de espionaje informático: concepto y delimitación", en *Revista Chilena de Derecho y Tecnología*, vol. 9, Nº 2 [2020], p. 226).

[30] *Vid.*, *supra*, nota 1.

distinto de aquel en el cual ellos están registrados. En ese caso, quien excede la autorización que posee, en realidad, obra sin autorización. No obstante, todo indica que el legislador prefirió, a fin de evitar eventuales discusiones a este respecto, incluir ambas alternativas, aunque ello involucrara la incorporación de una cláusula redundante.

La segunda cuestión destacable se relaciona con la idea de "superar" barreras técnicas o medidas tecnológicas de seguridad, que debe concurrir junto con la exigencia de falta de autorización para el ingreso (sea que no se contaba con autorización alguna, sea que se hubiere excedido la que se tenía). De acuerdo con el DRAE, superar implica vencer un obstáculo o una dificultad, en este caso, de índole informática, lo que podría vincularse, por ejemplo, con el hecho de que el sistema exija una clave de autenticación para ingresar a él. En ese sentido, si el agente cuenta con dicha clave, *v. gr.*, porque el titular del sistema se la ha proporcionado para que acceda sólo a una parte de una determinada base de datos, el ingreso no autorizado a otros datos, en rigor, no implicaría "superar" una barrera técnica o una medida tecnológica de seguridad. Ello podría provocar que en supuestos como ese la exigencia en orden a "exceder la autorización que se posea" no cumpla la función de abarcar un número mayor de supuestos penalmente relevantes, justamente, porque no se verificaría, copulativamente, la superación antes referida.

La tercera cuestión que merece la pena destacar, que se vincula con la anterior, concierne a la exigencia de que quien acceda a un sistema informático lo haga "superando barreras técnicas o medidas tecnológicas de seguridad", a continuación del requisito de que se obre "sin autorización o excediendo la autorización que posea". En esta materia, como se trata de dos exigencias típicas diferenciables, contenidas en el artículo 2º inciso primero de la Ley Nº 21.459, no sería posible sostener que el acceso es no autorizado si se verifica una superación de tales barreras o medidas[31], pues ello importaría confundir esos dos requisitos legales. Por lo tanto, será indispensable darle a cada uno de ellos un sentido independiente o autónomo. Volveremos sobre esta cuestión *infra*.

"Acceder", según el DRAE, significa entrar en un lugar, en este caso, al sistema informático al que no se está autorizado a ingresar. Consiguientemente, para llevar a cabo ese comportamiento el agente debe estar, en algún sentido, fuera del sistema informático referido. Ello se ve confirmado por la exigencia

[31] *Vid*., con referencias a la legislación alemana, así como analizando la exigencia de un acceso "no autorizado", por una parte, en el que ha habido "superación de mecanismos técnicos de protección", por la otra, Medina, Gonzalo. "Estructura típica del delito de intromisión informática", en *Revista Chilena de Derecho y Tecnología*, vol. 3, Nº 1 (2014), p. 86.

indicada, en orden a que dicho sujeto ha de "superar" barreras técnicas o medidas tecnológicas de seguridad, que deben ser vencidas para concretar el acceso. Esta conclusión, nuevamente, podría provocar que la cláusula "exceder la autorización que se posea" no cumpla la función de comprender un número mayor de supuestos penalmente relevantes, precisamente, porque no se verificaría la superación antes indicada.

El acceso debe ser llevado a cabo por un sujeto que no cuenta en absoluto con autorización para ingresar al sistema informático de que se trate, o bien, que cuenta con autorización, pero no respecto de la parte, del ámbito o de las funciones del sistema informático al cual está accediendo. La primera hipótesis importa actuar sin autorización, mientras que la segunda implica exceder la autorización que se posee. Como se adelantó, el artículo 16 de la nueva ley de delitos informáticos acota considerablemente el modo en el que puede otorgarse dicha autorización, así como las finalidades para las cuales ella puede prestarse. En efecto, sólo es admisible una autorización expresa del titular del sistema informático, lo que excluye la posibilidad de entregarla tácitamente o a través de comportamientos concluyentes. Además, esa autorización puede otorgarse "en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática", cuestión que a nuestro juicio no se opone a que existan autorizaciones con otras finalidades, cuyo efecto tendría que someterse a las reglas generales.

En lo que concierne a la naturaleza jurídica de la exigencia, según la cual, debe actuarse sin autorización, es posible plantear al menos dos vías interpretativas.

En primer lugar, puede sostenerse que la cláusula en comento se asemeja al requisito, establecido en otros delitos informáticos, en orden a que la conducta debe llevarse a cabo "indebidamente"[32]. En ese sentido, ambas exigencias se relacionarían con la idea de ilicitud[33], así como con el hecho de que el agente no se encuentre facultado para llevar a cabo el comportamiento que realiza. Por lo mismo, podrían existir hipótesis que tornen lícita la conducta, precisamente, porque el sujeto activo se encuentra habilitado para realizarla.

En segundo lugar, puede afirmarse que dicha exigencia equivale a la cláusula contenida expresa o tácitamente en otros delitos de la Parte Especial, que

[32] Por ejemplo, en el tipo de interceptación ilícita, del artículo 3º o de ataque a la integridad de los datos informáticos, del artículo 4º.

[33] Véase, a propósito del vínculo entre ausencia de autorización y antijuridicidad, Medina. "Estructura típica del delito de intromisión informática…", ob. cit., p. 86 con referencias ulteriores.

requieren actuar sin la voluntad de la víctima. Así ocurre, por ejemplo, en la violación de morada o en el hurto, delitos en que la concurrencia de la voluntad del titular del bien jurídico opera excluyendo la tipicidad[34] de la conducta y, por ende, el delito.

En cuanto a la exigencia en orden a superar "barreras técnicas o medidas tecnológicas de seguridad", ya hemos señalado que ella se relaciona con la idea de vencer un obstáculo de índole informática, que se encuentra establecido para dificultar que cualquier sujeto pueda ingresar al sistema de que se trate. Se ha señalado que tales mecanismos "no pueden consistir en meras medidas organizativas o autorizaciones de acceso", y que "pese a la diversidad de mecanismos, el más habitual es el uso de contraseñas"[35].

En lo que respecta a la estructura del tipo de acceso ilícito, es posible sostener que las cuatro hipótesis alternativas que él regula constituyen delitos de mera actividad, pues basta con que se acceda ilícitamente a un sistema informático, o bien, que (además) se (obtenga y) divulgue la información a la que se ha accedido, para que se configure el tipo penal. Por lo tanto, debe excluirse el castigo de la frustración. En cambio, considerando que dichas modalidades son fraccionables[36], es posible afirmar que cabe la sanción penal de la tentativa.

Objeto material de la conducta es un sistema informático; por ende, este delito recae sobre el mismo objeto que otros delitos informáticos, *v. gr.*, el ataque a la integridad de un sistema informático (artículo 1º), de modo que nos remitimos a lo dicho respecto de este último ilícito.

En el plano subjetivo, ya que el tipo penal no establece exigencia subjetiva alguna que apunte, necesariamente, a demandar dolo directo (*v. gr.*, una actuación "maliciosamente"), basta con que el delito se perpetre con dolo eventual. Además, tampoco se requiere la presencia de un elemento subjetivo del tipo o del injusto, cuestión que resulta relevante si se compara esta figura con la del artículo 2º inciso segundo de la Ley Nº 21.459, que sí establece una exigencia de esa índole, como veremos luego. La modalidad culposa de mero

[34] En ese sentido, a propósito del tipo penal de violación, Rodríguez, Luis. "Capítulo VIII: Delitos contra la indemnidad sexual", en Rodríguez, Luis (director). *Derecho Penal*, *Parte Especial*, vol. II. Valencia: Tirant lo Blanch (2022), p. 91.

[35] Véase Medina. "Estructura típica del delito de intromisión informática…", ob. cit., p. 86 con referencias ulteriores.

[36] *V. gr.*, si se utiliza un programa malicioso para la comisión del delito, sin que todavía se haya completado la realización del comportamiento respectivo. *Vid.*, a propósito de dicha forma de perpetrar delitos informáticos, Mayer. "Elementos criminológicos…", ob. cit., pp. 168 y ss. con referencias ulteriores.

acceso ilícito debe ser descartada, por las razones señaladas a propósito de los supuestos de sabotaje informático.

Por otra parte, el tipo de espionaje informático, del artículo 2º inciso segundo, primera hipótesis de la ley, establece básicamente las mismas exigencias objetivas que el tipo de mero acceso ilícito, de modo que será necesario que el agente, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático; requisitos que deben ser interpretados en iguales términos que respecto del tipo del artículo 2º inciso primero de la ley. En ese orden de ideas, las diferencias entre ambas figuras, y que son las que explican la mayor penalidad del tipo del artículo 2º inciso segundo, primera hipótesis de la Ley Nº 21.459 (presidio menor en sus grados mínimo a medio), se ubican fundamentalmente en el plano subjetivo.

Desde este último punto de vista, resulta destacable que el tipo en comento consagre un elemento subjetivo del tipo o del injusto parecido al que se establecía en el antiguo delito de espionaje informático de la Ley Nº 19.223. En efecto, en este último ilícito debía concurrir "ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma", exigencia que podía resultar problemática en casos de mero *hacking* o acceso ilícito (como los del artículo 2º inciso primero de la Ley Nº 21.459), en los que no era posible acreditar la presencia de semejante ánimo.

Llama la atención que el tipo de la nueva ley de delitos informáticos sólo aluda al "ánimo de apoderarse o usar la información", excluyendo una referencia al ánimo de conocerla. Dicha circunstancia admite diversas interpretaciones, entre las que pueden mencionarse al menos dos.

Primero, es posible afirmar que al legislador no le habría parecido relevante o conveniente exigir la verificación de un ánimo de conocer la información, por ejemplo, en atención a los problemas probatorios que implicaría su acreditación, en la línea de lo ya señalado; y que, por consiguiente, tal conocimiento no se demandaría ni como parte del dolo (del mero acceso ilícito o del espionaje informático) ni como parte de un elemento subjetivo distinto de aquel (en el tipo de espionaje).

Segundo, es posible sostener que la exigencia de conocimiento de la información del sistema informático forma parte del dolo del tipo de espionaje informático, de suerte que ella tendría que verificarse para poder imponer la sanción asociada a dicho delito. En cambio, mucho más discutible sería plantear que también al tipo de mero acceso ilícito subyace una exigencia implícita de conocimiento de la información, pues, como señalamos, ese delito se centra en el solo acceso al sistema informático. En ese sentido, es posible que se ingrese

indebidamente a un sistema informático sin que exista un conocimiento de la información en él contenida, en cuyo caso sería perfectamente aplicable el tipo del artículo 2º inciso primero de la ley.

Ahora bien, en relación con dicha exigencia subjetiva ("ánimo de apoderarse o usar la información"), como es propio de los delitos cuya descripción requiere la presencia de un ánimo especial, basta con que este se presente en el momento en que se realiza el comportamiento típico; en cambio, no es necesario que el agente efectivamente logre su propósito de apoderarse o de usar la información respectiva.

Tratándose del delito regulado en el artículo 2º inciso segundo, segunda hipótesis de la Ley Nº 21.459, él castiga con la misma pena del espionaje informático ya comentado (presidio menor en sus grados mínimo a medio), a quien divulgue la información a la cual se accedió de manera ilícita, en caso de que no haya sido obtenida por el agente. Por ende, nos hallamos nuevamente ante un supuesto más grave que el de mero acceso ilícito del artículo 2º inciso primero.

En el ámbito objetivo, el delito exige que el agente "divulgue" determinada información, conducta que de acuerdo con el DRAE puede interpretarse como extenderla, publicarla o, análogamente, ponerla al alcance del público. En términos similares, es posible equiparar dicho comportamiento con la conducta consistente en dar a conocer a terceros la información contenida en el sistema de tratamiento automatizado de la misma.

Junto con ello, el delito presupone que se ha verificado un acceso ilícito a un sistema informático, conceptos que pueden entenderse de la misma forma señalada en relación con los tipos de mero acceso ilícito y de espionaje informático.

Finalmente, el tipo hace aplicable su pena, en la medida en que quien divulgue la información no sea la misma persona (natural) que accedió previamente al sistema informático en cuestión y haya obtenido la información; acceso y obtención que tienen que haberse verificado indebidamente. "Obtener", según el DRAE, puede interpretarse como conseguir la información que se pretende. De forma similar, es posible entender dicha conducta como equivalente a la de apoderarse de la información a través de cualquier medio idóneo para ello.

En el plano subjetivo, el tipo penal no contempla requisito subjetivo alguno que apunte, necesariamente, a exigir dolo directo (*v. gr.*, una actuación "a sabiendas"), por lo que basta con que él se perpetre con dolo eventual. La modalidad culposa debe ser descartada, por las mismas razones señaladas a propósito de otros delitos informáticos.

Por último, el artículo 2º inciso tercero de la Ley Nº 21.459 castiga con la pena más alta prevista en dicho precepto (presidio menor en sus grados medio

a máximo) aquel supuesto en que una misma persona obtiene y divulga la información. Consiguientemente, tendrá que ser idéntico sujeto quien obtenga, o sea, consiga o se apodere de la información, y quien la divulgue, esto es, quien la ponga al alcance de terceros o la dé a conocer a estos.

El tipo exige, copulativamente, la realización de dos conductas: obtener y divulgar información. Por la manera como se encuentra redactado, es posible afirmar que también esta figura presupone la concurrencia de un acceso ilícito a un sistema informático, al que le sigue una obtención indebida de información en él contenida y una divulgación de dicha información.

En el ámbito subjetivo, ya que el tipo penal no establece exigencia subjetiva alguna que apunte, necesariamente, a demandar dolo directo (*v. gr.*, una actuación "maliciosamente"), basta con que el delito se perpetre con dolo eventual. Asimismo, la modalidad culposa ha de ser descartada, por las razones a las que ya hemos hecho referencia respecto de otros delitos informáticos.

ii) Interceptación ilícita (artículo 3º)

Este delito, que tiene como antecedente el tipo de interceptación ilícita del artículo 3º del Convenio de Ciberdelincuencia[37], se encuentra regulado en el artículo 3º de la Ley Nº 21.459, precepto que establece lo siguiente:

> "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".

Si consideramos lo dispuesto en el artículo 3º de la ley, se advertirá que en él se regulan dos tipos penales distintos, que se encuentran consagrados como delitos de acción.

[37] Artículo 3º - Interceptación ilícita.
"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno 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. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático".

En primer lugar, se castiga a quien 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. De acuerdo con el DRAE, "interceptar" es apoderarse, en este caso, de la transmisión señalada, antes de que llegue a su destino; o bien, detenerla, interrumpirla u obstruirla. "Interrumpir" es un comportamiento análogo al de interceptar, al punto que, como se dijo, ambos pueden ser interpretados como sinónimos. Asimismo, es posible entender que interrumpir implica, según el DRAE, cortar la continuidad, en este caso, de la transmisión referida; mientras que "interferir" puede definirse como el hecho de que una señal se introduzca en la recepción de otra y la perturbe.

En tanto se exige una actuación indebida, es preciso que ella sea ilícita, de lo que se sigue que podrían existir interceptaciones, interrupciones o interferencias lícitas, llevadas a cabo por un sujeto que se encuentra facultado o habilitado para ello.

Aunque se trate de una obviedad, el legislador ha preferido explicitar que el delito debe llevarse a cabo "por medios técnicos". En ese sentido, la interceptación ilícita que se ejecute por medios materiales debe castigarse a través de otras figuras delictivas, *v. gr.*, recurriendo al tipo penal de daños.

En cuanto a la estructura de la primera modalidad de interceptación ilícita, es posible sostener que ella corresponde a un delito de mera actividad, pues sólo se exige la interceptación, interrupción o interferencia de una transmisión, sin que se demande un resultado material espacio-temporalmente separado de tales conductas. Considerando que esas acciones son fraccionables[38], puede afirmarse que cabe el castigo de la tentativa.

Objeto material de este tipo es información de un sistema informático, término que puede entenderse como equivalente al de datos, a su vez, definido en el artículo 15 a) de la Ley Nº 21.459, al que ya nos hemos referido en diversas oportunidades. Este objeto material permite diferenciar al delito en comento de otros ilícitos penales, por ejemplo, los regulados en el artículo 36 B letras b) y c) de la Ley Nº 18.168, General de Telecomunicaciones[39].

[38] Por ejemplo, cuando se emplea un *malware* para la perpetración del delito, sin que todavía se haya completado la realización de la conducta respectiva. *Vid.*, a propósito de dicha manera de cometer delitos informáticos, Mayer. "Elementos criminológicos…", ob. cit., pp. 168 y ss. con referencias ulteriores.

[39] En efecto, el primero de dichos delitos castiga "[a]l que maliciosamente interfiera, intercepte o interrumpa un *servicio de telecomunicaciones*", mientras que el segundo sanciona "[a]l que intercepte o capte maliciosamente o grabe sin la debida autorización, cualquier tipo de señal que se emita a través de un *servicio público de telecomunicaciones*" (cursivas agregadas).

En el ámbito subjetivo, el tipo penal no contempla requisito subjetivo alguno que apunte, necesariamente, a exigir dolo directo (*v. gr.*, una actuación "a sabiendas"), por lo que basta con que él se perpetre con dolo eventual. La modalidad culposa debe ser descartada, por las mismas razones señaladas a propósito de otros delitos informáticos.

En segundo lugar, se sanciona a quien, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos.

La ley exige que el agente "capte"[40] datos, verbo que de acuerdo con el DRAE puede entenderse como recibirlos, recogerlos o capturarlos.

La conducta delictiva ha de realizarse sin la debida autorización, concepto que puede interpretarse según su sentido natural y obvio como el acto (paradigmáticamente de una autoridad) "por el cual se permite a alguien una actuación en otro caso prohibida" (DRAE, 2ª acepción del término «autorización»). A nuestro juicio, ya que este delito no exige, para efectos de descartar la sanción de la conducta, que exista una autorización "expresa" del titular del sistema informático, estimamos que podría admitirse una autorización tácita o concluyente de su parte.

Nuevamente, el legislador ha preferido indicar que el delito ha de realizarse "por medios técnicos". La verdad es que cuesta imaginar cómo puede llevarse a cabo una captación de datos a través de medios que no sean técnicos, por ejemplo, recurriendo a mecanismos de carácter material. No obstante, de ser ello posible, no podría aplicarse la figura en comento, por no verificarse la exigencia típica referida.

En lo que respecta a la estructura de la segunda modalidad de interceptación ilícita, puede afirmarse que ella constituye un delito de mera actividad, pues sólo exige una captación de datos, sin que se requiera un resultado material. Teniendo en cuenta que ese comportamiento es fraccionable[41], es posible sostener que cabe el castigo de la tentativa.

El objeto material de la conducta son datos informáticos, noción respecto de la cual nos remitimos a lo señalado *supra*.

---

[40] En cambio, si se interpreta la idea de "captar" como sinónimo de "leer" los datos, podría generarse una confusión entre este delito y el tipo de acceso ilícito.

[41] *V. gr.*, si se utiliza un programa malicioso para la comisión del delito, sin que todavía se haya completado la realización del comportamiento respectivo. *Vid.*, a propósito de dicha forma de perpetrar delitos informáticos, Mayer. "Elementos criminológicos…", ob. cit., pp. 168 y ss. con referencias ulteriores.

Desde un punto de vista subjetivo, el tipo penal no contempla requisito subjetivo alguno que apunte, forzosamente, a demandar dolo directo (por ejemplo, una actuación realizada "maliciosamente"), de modo que basta con que él se cometa con dolo eventual. La modalidad culposa debe ser descartada, por las mismas razones indicadas respecto de otros delitos informáticos.

c) Falsificación informática (artículo 5º)

Este delito tiene como antecedente el tipo de falsificación informática del artículo 7º del Convenio de Ciberdelincuencia[42] y se tipifica en el artículo 5º de la Ley Nº 21.459, disposición que establece lo siguiente:

> "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 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".

Ya que el tipo penal regula un supuesto de "falsificación o, lo que es lo mismo, de falsedad", es posible definir la conducta delictiva como "una alteración de la verdad"[43]. Sabido es que, entre las clasificaciones más importantes que se han desarrollado respecto de las conductas falsarias, está la que diferencia entre falsedades reales y personales: mientras que las falsedades reales "se caracterizan porque la alteración de la verdad recae sobre un objeto (…), que puede ser una moneda, un sello, un documento", etc., "las falsedades personales recaen sobre la calidad o condición de una persona (…), como ocurre en el ejercicio ilegal de la profesión, la usurpación de nombre, el falso testimonio, entre otros"[44]. También se sabe que para que una falsedad sea penalmente relevante es necesario que el objeto falseado "tenga vocación de entrada en

[42] Artículo 7º - Falsificación informática.
"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal".

[43] Mayer, Laura y Vera, Jaime. "La falsificación informática: ¿Un delito necesario?", en *Revista Chilena de Derecho y Tecnología*, vol. 11, Nº 1 (2022), p. 264 con referencias ulteriores.

[44] *Idem*.

el tráfico jurídico, esto es, que trascienda la esfera íntima del individuo" que incurre en la falsedad[45]. Por ello, no constituye una falsedad, en el sentido señalado, el hecho de alterar un documento que el agente luego conserva en un armario al que ningún otro sujeto tiene acceso.

Ahora bien, una de las falsedades que mayor relevancia teórica y práctica tiene es la que se extiende a documentos, objeto respecto del cual surge la distinción entre falsedades materiales e ideológicas[46], siendo las primeras aquellas que "se proyectan sobre el soporte documental o sobre los signos lingüísticos que contiene, modificando con ello la relación de correspondencia entre el enunciado y el fragmento de la realidad que se pretende mostrar"; y las segundas, aquellas en que "no existen modificaciones o alteraciones sobre el soporte o sobre los signos lingüísticos que él contiene, sino que estos últimos son organizados en el documento de una manera tal que el soporte formula enunciados o aserciones sin correspondencia con la realidad"[47].

Todos los comportamientos que se regulan en el tipo penal de falsificación informática del artículo 5º ya fueron analizados a propósito de la hipótesis de sabotaje informático del artículo 1º de la Ley Nº 21.459. Recordemos que, según el DRAE, "introducir" puede entenderse como meter o hacer entrar, en este caso, datos informáticos; así como que "alterar" implica cambiar la configuración de los datos, o bien, perturbar definitivamente sus funciones[48]. De acuerdo con ese mismo diccionario, "dañar" equivale a causar un detrimento, perjuicio o menoscabo a dichos datos, mientras que "suprimir" puede interpretarse como eliminar los datos de que se trate.

Según podrá notarse, el delito se encuentra estructurado como un tipo de hipótesis alternativas, de modo que basta con que se verifique cualquiera de ellas para que se configure una falsificación informática. Además, todos esos verbos implican la realización de acciones, no existiendo una modalidad omisiva que resulte punible.

---

[45] *Idem*.

[46] Véase, por ejemplo, Armenteros, Miguel. *Los delitos de falsedad documental*. Granada: Comares (2011), pp. 179 y ss.

[47] Mayer y Vera. "La falsificación informática…", ob. cit., p. 265, indicando como ejemplo de falsedad material el caso en que "se altera el signo lingüístico relativo a la fecha de expedición o se hacen raspaduras en la parte del papel que lo contiene"; y como ejemplo de falsedad ideológica el caso en que "en el documento se da cuenta de una operación jurídica jamás realizada" o en que "los suscribientes declaran vender un objeto que en realidad no se está enajenando".

[48] En ese sentido Corcoy. "Capítulo IX. De los daños…", ob. cit., p. 950, a propósito del sabotaje informático.

En especial el comportamiento consistente en "alterar" datos informáticos se vincula con el sentido que tradicionalmente se ha atribuido a las falsedades; conductas que, como se dijo, implican una alteración de la verdad, plasmada en alguna clase de soporte. Además, es posible afirmar que dicho verbo constituye "algo así como una conducta genérica, dentro de la cual pueden englobarse las de introducir, dañar o suprimir", toda vez que "cuando se introducen, dañan o suprimen datos, también se produce una 'alteración', en este caso, de datos o programas de sistemas informáticos"[49]. No obstante, debe reconocerse que los comportamientos que importan dañar o suprimir datos más bien se acercan a las denominadas falsedades impropias o asimiladas a las falsedades *stricto sensu*[50]; o bien, al delito de sabotaje informático, cuyos vínculos con el tipo en comento, en virtud de la exigencia consistente en "alterar" datos, ya han sido destacados[51].

La conducta delictiva debe llevarse a cabo "indebidamente", lo que implica que se realice ilícitamente. En ese orden de ideas, ha de existir una introducción, una alteración, un daño o una supresión de datos a los que no se estaba facultado. De ello se colige que pueden existir situaciones que tornen lícito el comportamiento, precisamente, porque el agente se encuentra habilitado a llevar a cabo tales acciones. Así, por ejemplo, podría imaginarse la hipótesis en que el titular de los datos solicita a un asistente que introduzca, en un documento electrónico en el que se contiene un contrato, una cláusula inicialmente no prevista en él.

En cuanto a la estructura del tipo, puede afirmarse que la falsificación informática constituye un delito de mera actividad, toda vez que basta con que se lleve a cabo una introducción, una alteración, un daño o una supresión de datos para que se configure el tipo penal. Consiguientemente, ha de excluirse el castigo penal de la frustración; mientras que, como dichos comportamientos son fraccionables[52], cabe sostener que la tentativa sí es punible, tesis que podría ser objeto de reparos, si se parte de la base de que nos encontramos ante actos preparatorios que se han elevado a la categoría de delito autónomo.

---

[49] Mayer y Vera. "La falsificación informática…", ob. cit., p. 270.

[50] En esa línea, por ejemplo, Garrido, Mario. *Derecho Penal*, *Parte Especial*, tomo IV, reimpresión de la 4ª ed. Santiago: Editorial Jurídica de Chile (2011), p. 66, en relación con la falsedad por uso y por ocultación.

[51] Véase Mayer y Vera. "El documento como objeto material…", ob. cit., p. 437.

[52] Por ejemplo, cuando se emplea un *malware* para la perpetración del delito, sin que todavía se haya completado la realización de la conducta respectiva. *Vid*., a propósito de dicha manera de cometer delitos informáticos, Mayer. "Elementos criminológicos…", ob. cit., pp. 168 y ss. con referencias ulteriores.

El objeto material de la conducta son datos, término respecto del cual nos remitimos a lo indicado *supra*. Que esos datos informáticos puedan identificarse con el concepto de documento (electrónico o informático) dependerá de la amplitud con la que se defina dicho concepto[53].

En el ámbito subjetivo, el tipo penal exige que se actúe con la intención de que los datos introducidos, alterados, dañados o suprimidos sean tomados como auténticos o utilizados para generar documentos auténticos. A nuestro juicio, esa forma de regular el dolo, en especial por la exigencia en orden a que se actúe "para" generar documentos auténticos, puede entenderse como un reforzamiento del elemento subjetivo, que equivale a una exigencia de dolo directo.

Finalmente, cabe destacar que todo lo señalado es aplicable a lo que podríamos denominar la hipótesis básica de falsificación informática que regula la Ley Nº 21.459, prevista en el artículo 5º inciso primero, en oposición a la modalidad agravada de ese mismo delito, que se regula en el inciso segundo de dicho precepto. De acuerdo con este último, cuando la conducta descrita en el inciso primero "sea cometida por empleado público, abusando de su oficio", en lugar de imponerse la pena de presidio menor en sus grados medio a máximo, será aplicable la de presidio menor en su grado máximo a presidio mayor en su grado mínimo.

En la línea de la regulación de las falsedades documentales, se establece una agravación respecto de la figura básica en atención a que quien lleva a cabo el delito es un sujeto calificado, concretamente, un empleado o funcionario público –conceptos que podemos utilizar como sinónimos–, que abusa de su oficio, o sea, que aprovecha la especial posición que tiene como tal para cometer la conducta incriminada.

Empleado o funcionario público, de acuerdo con el artículo 260 CP, es "todo el que desempeñe un cargo o función pública, sea en la Administración Central o en instituciones o empresas semifiscales, municipales, autónomas u organismos creados por el Estado o dependientes de él, aunque no sean de nombramiento del Jefe de la República ni reciban sueldo del Estado", con independencia de que el cargo sea o no de elección popular. A nuestro juicio, a pesar de que el propio artículo 260 CP se encarga de señalar que esa definición es aplicable "[p]ara los efectos de este Título y del Párrafo IV del Título III", su carácter general permite recurrir a ella también en el contexto específico

[53] Véase, respecto de dicho problema, Mayer y Vera. "La falsificación informática…", ob. cit., pp. 273 y ss.

de la criminalidad informática, en especial a falta de una definición de dicho concepto en la Ley Nº 21.459.

d) Receptación de datos informáticos (artículo 6º)

El delito de receptación informática es una figura delictiva que no tiene antecedentes directos en el Convenio de Ciberdelincuencia y que, en ese sentido, constituye un tipo penal original. No obstante tratarse de una figura inédita en el contexto de la criminalidad informática, la receptación como ilícito ya se encuentra regulada en la legislación penal chilena, *v. gr.*, en el ámbito de los delitos contra la propiedad (artículo 456 bis A CP[54]) o a través de la receptación aduanera (artículo 182 incisos primero y segundo

[54] Artículo 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, Nº 1º, 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.

Para la determinación de la pena aplicable el tribunal tendrá especialmente en cuenta el valor de las especies, así como la gravedad del delito en que se obtuvieron, si éste era conocido por el autor.

Cuando el objeto de la receptación sean vehículos motorizados o cosas que forman parte de redes de suministro de servicios públicos o domiciliarios, tales como electricidad, gas, agua, alcantarillado, colectores de aguas lluvia o telefonía, se impondrá la pena de presidio menor en su grado máximo y multa equivalente al valor de la tasación fiscal del vehículo o la pena de presidio menor en su grado máximo, y multa de cinco a veinte unidades tributarias mensuales, respectivamente. La sentencia condenatoria por delitos de este inciso dispondrá el comiso de los instrumentos, herramientas o medios empleados para cometerlos o para transformar o transportar los elementos sustraídos. Si dichos elementos son almacenados, ocultados o transformados en algún establecimiento de comercio con conocimiento del dueño o administrador, se podrá decretar, además, la clausura definitiva de dicho establecimiento, oficiándose a la autoridad competente.

Sin perjuicio de lo dispuesto en el inciso anterior, se aplicará el máximum de la pena privativa de libertad allí señalada y multa equivalente al doble de la tasación fiscal, al autor de receptación de vehículos motorizados que conociere o no pudiere menos que conocer que en la apropiación de éste se ejerció sobre su legítimo tenedor alguna de las conductas descritas en el artículo 439. Lo dispuesto en este inciso no será aplicable a quien, por el mismo hecho, le correspondiere participación responsable por cualquiera de las hipótesis del delito de robo previstas en el artículo 433 y en el inciso primero del artículo 436.

Se impondrá el grado máximo de la pena establecida en el inciso primero, cuando el autor haya incurrido en reiteración de esos hechos o sea reincidente en ellos. En los casos de reiteración o reincidencia en la receptación de los objetos señalados en el inciso tercero, se aplicará la pena privativa de libertad allí establecida, aumentada en un grado.

de la Ordenanza de Aduanas[55]). Con todo, la inmaterialidad del objeto en el que recae el delito, que es característica de la criminalidad informática, en parte explica que se haya decidido tipificar, autónomamente, un supuesto de receptación informática.

El artículo 6º de la Ley Nº 21.459, que lo tipifica, dispone lo siguiente:

> "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 2º, 3º y 5º, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado".

El tipo está estructurado en torno a tres comportamientos alternativos, de modo que basta con que concurra cualquiera de ellos para que se verifique el ilícito en comento. Todos ellos constituyen acciones, de modo que debe descartarse la receptación omisiva de datos informáticos.

Según el DRAE, "comercializar" implica dar a un producto condiciones y vías de distribución para su venta, o bien, poner a la venta un producto. En este caso, lo que tendría que comercializarse son datos informáticos que, como veremos, constituyen el objeto material del delito.

De acuerdo con ese mismo diccionario, "transferir" supone pasar o llevar algo, en este caso, datos informáticos, desde un lugar a otro. Dicha conducta puede equipararse con la de transmitir, que ya analizamos a propósito del delito de ataque a la integridad de un sistema informático, del artículo 1º de la Ley Nº 21.459. En definitiva, de lo que se trata es de traspasar datos informáticos desde un sistema de tratamiento automatizado de la información a otro.

También, según el DRAE, "almacenar" involucra reunir, guardar o registrar, en lo que aquí interesa, datos informáticos.

Tratándose del delito de abigeato la multa establecida en el inciso primero será de setenta y cinco a cien unidades tributarias mensuales y el juez podrá disponer la clausura definitiva del establecimiento.

Si el valor de lo receptado excediere de cuatrocientas unidades tributarias mensuales, se impondrá el grado máximo de la pena o el máximum de la pena que corresponda en cada caso" (subsanados los errores de transcripción).

[55] Artículo 182 incisos primero y segundo:

"Las penas establecidas por los delitos de contrabando o fraude se aplicarán también a las personas que adquieran, reciban o escondan mercancías, sabiendo o debiendo presumir que han sido o son objeto de los delitos a que se refiere este Título.

Se presumirá dicho conocimiento de parte de las personas mencionadas por el solo hecho de encontrarse en su poder las mercancías objeto del fraude o contrabando".

Las conductas indicadas pueden realizarse "a cualquier título", lo que permite evitar discusiones en torno a las razones o contextos a partir de los cuales el agente realiza el comportamiento delictivo.

Además, el tipo exige que los datos informáticos, que se comercializan, transfieren o almacenan, provengan de determinados delitos, a saber, acceso ilícito (artículo 2º), interceptación ilícita (artículo 3º) o falsificación informática (artículo 5º). Por lo tanto, si los datos informáticos provienen de algún otro delito, ya sea informático (*v. gr.*, fraude informático del artículo 7º de la Ley Nº 21.459), o bien, de otra índole (por ejemplo, los regulados en los artículos 161-A[56] o 161-C[57] CP), no será posible aplicar la figura en comento.

En lo que respecta a la estructura del tipo, la receptación de datos informáticos corresponde a un delito de mera actividad, pues sólo exige que se comercialicen, transfieran o almacenen datos, concurriendo ciertos requisitos, sin que se exija un resultado material. Teniendo en cuenta que ese

---

[56] Artículo 161-A:

"Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 Unidades Tributarias Mensuales al que, en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado; sustraiga, fotografíe, fotocopie o reproduzca documentos o instrumentos de carácter privado; o capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público.

Igual pena se aplicará a quien difunda las conversaciones, comunicaciones, documentos, instrumentos, imágenes y hechos a que se refiere el inciso anterior.

En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a ésta las penas de reclusión menor en su grado máximo y multa de 100 a 500 Unidades Tributarias Mensuales.

Esta disposición no es aplicable a aquellas personas que, en virtud de ley o de autorización judicial, estén o sean autorizadas para ejecutar las acciones descritas".

[57] Artículo 161-C:

"Se castigará con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, al que en lugares públicos o de libre acceso público y que por cualquier medio capte, grabe, filme o fotografíe imágenes, videos o cualquier registro audiovisual, de los genitales u otra parte íntima del cuerpo de otra persona con fines de significación sexual y sin su consentimiento.

Se impondrá la misma pena de presidio menor en su grado mínimo y multa de diez a veinte unidades tributarias mensuales, al que difunda dichas imágenes, videos o registro audiovisual a que se refiere el inciso anterior.

En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a ésta, la pena de presidio menor en su grado mínimo a medio y multa de veinte a treinta unidades tributarias mensuales".

comportamiento es fraccionable[58], es posible sostener que cabe el castigo de la tentativa.

Pese a la redacción confusa de la norma, que exige realizar el comportamiento "con el mismo objeto u otro fin ilícito", resulta relevante que la nueva ley de delitos informáticos establezca este requisito, a fin de evitar una aplicación desmesurada del tipo penal. En ese sentido, el agente, desde un punto de vista subjetivo, debe actuar con dolo, al menos eventual, respecto de la procedencia de los datos; pero, además, ha de llevar a cabo las conductas consistentes en comercializarlos, transferirlos o almacenarlos con una finalidad ilícita, o sea, antijurídica.

En efecto, el tipo penal puede cometerse "conociendo" el origen de los datos, cláusula que equivale a una exigencia de dolo directo; o "no pudiendo menos que conocerlo", exigencia que puede identificarse con el dolo eventual[59]. De ello se sigue que se excluye el castigo de la receptación de datos informáticos si sólo concurre culpa en el agente del comportamiento incriminado.

Resulta destacable que el legislador haya decidido sancionar la receptación de datos informáticos con "la pena asignada a los respectivos delitos, rebajada en un grado". De ello se sigue que se le ha atribuido una gravedad menor a la de los delitos desde los cuales pueden provenir los datos, gravedad que va a depender concretamente del castigo con el que se encuentran conminados los tipos de acceso ilícito, de interceptación ilícita y de falsificación informática[60].

---

[58] *V. gr.*, si se utiliza un programa malicioso para la comisión del delito, sin que todavía se haya completado la realización del comportamiento respectivo. *Vid*., a propósito de dicha forma de perpetrar delitos informáticos, Mayer, "Elementos criminológicos…", ob. cit., pp. 168 y ss. con referencias ulteriores.

[59] Véase, en relación con el artículo 456 bis A CP, Oliver, Guillermo. "Capítulo IX: Delitos contra la propiedad", en Rodríguez, Luis (director), *Derecho Penal*, *Parte Especial*, vol. II. Valencia: Tirant lo Blanch (2022), pp. 350-351, efectuando sin embargo una distinción entre el conocimiento respecto de la conducta y el conocimiento relativo al origen de las especies.

[60] Esta regla se asemeja a la del artículo 456 bis A CP que, en materia de delitos contra la propiedad, indica que para la determinación de la pena aplicable a la receptación "el tribunal tendrá especialmente en cuenta el valor de las especies, así como la gravedad del delito en que se obtuvieron, si éste era conocido por el autor".

e) Fraude informático (artículo 7º)

Este delito, que tiene como antecedente el tipo de fraude informático del artículo 8º del Convenio de Ciberdelincuencia[61], se encuentra regulado en el artículo 7º de la Ley Nº 21.459, precepto que establece lo siguiente:

> "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".

El delito de fraude informático era uno de los más esperados a nivel doctrinal, por varias razones. Por una parte, sabido es que la Ley Nº 19.223 no contemplaba una hipótesis particular de fraude informático, situación que, si bien no implicaba forzosamente la impunidad de los comportamientos que podían calificarse de tales, de todos modos, suponía grandes dificultades para el castigo penal de dicho ilícito, que sólo podía sancionarse por vías indirec-

[61] Artículo 8º - Fraude informático:
"Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los 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 o para otra persona".

tas[62]. Por otra parte, y vinculado con lo anterior, la ausencia de una figura específica de fraude informático en la legislación penal chilena resultaba especialmente problemática, considerando que, entre los delitos informáticos, aquel es el de mayor frecuencia práctica[63] y el que más impacto provoca en el sistema económico. Justamente, esta última circunstancia, ha llevado a que muchos autores entiendan que el fraude informático integra la criminalidad económica[64].

El tipo penal referido se encuentra consagrado como una figura paralela a la estafa y, en especial, al fraude del artículo 467[65] CP, norma que establece la regla general en cuanto al castigo aplicable a los delitos que se prevén en el Párrafo 8º del Título IX del Libro II de dicho cuerpo normativo, denominado "*Estafas y otros engaños*". De ello se sigue que, si bien el fraude informático es una figura de naturaleza distinta a la estafa, en especial en lo que dice relación con la conducta delictiva[66], ambos constituyen ilícitos penales que el legislador considera equivalentes desde el punto de vista de su gravedad,

---

62 Véase Hernández, Héctor. "Tratamiento de la criminalidad informática en el derecho penal chileno: Diagnóstico y propuestas", *Informe solicitado por la División Jurídica del Ministerio de Justicia*, *Inédito* (2001), p. 18, en relación con la posibilidad de subsumir conductas constitutivas de fraude informático en el tipo penal del artículo 2º o del artículo 3º de la Ley Nº 19.223.

63 Véase, con algunos matices, Miró, Fernando. "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del *phishing*", en *Revista Electrónica de Ciencia Penal y Criminología*, Nº 15-12 (2013), pp. 3-5.

64 En ese sentido, Tiedemann, Klaus. *Wirtschaftsstrafrecht Besonderer Teil*, 3ª ed. München: Vahlen (2011), pp. 287 y ss.

65 Artículo 467:

"El que defraudare a otro en la sustancia, cantidad o calidad de las cosas que le entregare en virtud de un título obligatorio, será penado:

1º Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si la defraudación excediera de cuarenta unidades tributarias mensuales.

2º Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

3º Con presidio menor en su grado mínimo y multa de cinco unidades tributarias mensuales, si excediere de una unidad tributaria mensual y no pasare de cuatro unidades tributarias mensuales.

Si el valor de la cosa defraudada 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".

66 Véase, con referencia a la idea, bastante extendida entre la doctrina, de que no es posible engañar a una máquina, Choclán, José Antonio. "Capítulo 3: Infracciones patrimoniales en los procesos de transferencia de datos", en Romeo, Carlos (coordinador). *El cibercrimen: nuevos retos jurídico-penales*, *nuevas respuestas político-criminales*. Granada: Comares (2006), p. 72.

lo que justifica que compartan varias exigencias típicas. Además, en tanto uno y otra hacen depender la pena aplicable del monto del perjuicio causado, es posible sostener que esos dos delitos inciden negativamente en intereses patrimoniales ajenos[67].

De la lectura del artículo 7º de la Ley Nº 21.459 fluye que el fraude informático se encuentra regulado sobre la base de dos tipos penales, consagrados en el inciso primero y en el inciso segundo de dicho artículo, respectivamente.

La hipótesis contemplada en el artículo 7º inciso primero de la ley regula algo así como un supuesto tradicional de fraude informático, que cumple con la idea referida, de constituir un tipo penal paralelo al delito de estafa.

La conducta delictiva corresponde a manipular un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de dicho sistema.

De acuerdo con el DRAE, "manipular" puede entenderse como intervenir, en este caso, los datos informáticos, distorsionando su configuración. En la misma línea, es común que se afirme que manipular equivale a alterar datos informáticos[68].

Dicha manipulación puede verificarse a través de cinco modalidades alternativas. Por ende, basta con que concurra cualquiera de ellas para que se configure el delito de fraude informático del artículo 7º inciso primero de la Ley Nº 21.459. Todas ellas implican la realización de acciones que constituyen la causa del perjuicio patrimonial ajeno, lo que permite sostener que nos encontramos ante un tipo penal de acción.

En primer lugar, es posible manipular el sistema informático de que se trate mediante una introducción, una alteración, un daño o una supresión de datos informáticos. En cuanto al sentido y alcance de dichos conceptos, nos remitimos a lo sostenido respecto de cuatro de las modalidades típicas del ataque a la integridad de un sistema informático, por coincidir exactamente con las referidas modalidades del tipo de fraude informático.

En segundo lugar, es posible manipular dicho sistema informático a través de cualquier interferencia en su funcionamiento. En el contexto que ahora analizamos, "interferir" puede interpretarse como perturbar o alterar el normal

---

67 Véase, en relación con la estafa, así como aludiendo al sentido económico del perjuicio, Mayer, Laura. "Capítulo X: Delitos contra intereses patrimoniales", en Rodríguez, Luis (director). *Derecho Penal*, *Parte Especial*, vol. *II*. Valencia: Tirant lo Blanch (2022), p. 423 y *passim*.

68 En ese sentido Mayer, Laura y Oliver, Guillermo. "El delito de fraude informático: Concepto y delimitación", en *Revista Chilena de Derecho y Tecnología*, vol. 9, Nº 1 (2020), p. 152 y *passim*.

funcionamiento del sistema de tratamiento automatizado de la información, mediante el cual se perpetra el delito. En tanto puede llevarse a cabo "cualquier" clase de interferencia, claramente nos encontramos ante una cláusula abierta, cuya consagración –no sin riesgo de vulnerar el principio de taxatividad penal– apunta a evitar vacíos de punición.

En lo que atañe a la estructura del tipo de fraude informático, es posible sostener que él constituye un delito de resultado, toda vez que exige que se cause un perjuicio (resultado) a través de determinadas modalidades de comisión (medios). Teniendo en cuenta que dichas modalidades son fraccionables[69], puede afirmarse que el delito que analizamos admite tanto la tentativa como la frustración.

El objeto material de la conducta son datos informáticos, noción respecto de la cual nos remitimos a lo señalado *supra*.

Como la penalidad aplicable depende del monto al que asciende el perjuicio ocasionado, según se indicó *supra*, es claro que ha de tratarse de una merma de carácter económico, cuestión que es coherente con la regulación de las estafas en la regulación penal chilena, figuras que paradigmáticamente demandan un perjuicio de carácter económico[70].

En el plano subjetivo, a pesar de que la descripción del fraude informático requiere que se actúe con una determinada finalidad, exigencia que podría entenderse como una demanda de dolo, ella en realidad corresponde a un elemento del tipo o del injusto, concretamente, al ánimo de lucro. En efecto, en el ámbito de los delitos contra intereses patrimoniales, actúa con ánimo de lucro el sujeto que busca obtener una utilidad o ventaja económica[71] a través del comportamiento incriminado, idea que en nada difiere de la exigencia establecida en el artículo 7º inciso primero de la nueva ley de delitos informáticos.

Además, resulta destacable que el legislador haya establecido expresamente que puede perseguirse un lucro para sí (o sea, para el propio agente) o para un tercero. Gracias a ello, es posible evitar las discusiones que surgen respecto

---

[69] Por ejemplo, cuando se emplea un *malware* para la perpetración del delito, sin que todavía se haya completado la realización de la conducta respectiva. *Vid*., a propósito de dicha manera de cometer delitos informáticos, Mayer. "Elementos criminológicos…", ob. cit., pp. 168 y ss. con referencias ulteriores.

[70] Asimismo, vinculan el carácter del perjuicio con el modo de determinar la penalidad aplicable, en relación con el tipo penal de estafa, Bullemore, Vivian y MacKinnon, John. *Curso de Derecho Penal*, *Parte Especial*, tomo IV, 5ª ed. Santiago: Ediciones Jurídicas de Santiago (2021), p. 110.

[71] Por todos Politoff; Matus y Ramírez. *Lecciones de Derecho Penal chileno*…, ob. cit., p. 306.

de delitos como el hurto o el robo, a propósito de los cuales la ley exige un ánimo de *lucrarse*[72].

Por último, en relación con dicha exigencia subjetiva, como es propio de los delitos cuya descripción requiere la presencia de un ánimo especial, basta con que este concurra en el momento en que se realiza el comportamiento típico; en cambio, no es necesario que el agente efectivamente logre su propósito de obtener, para sí o para un tercero, una ventaja económica[73].

La hipótesis prevista en el artículo 7º inciso segundo de la ley regula, como tipo penal autónomo, un supuesto de participación en un fraude informático, que ha sido elevado a la categoría de autoría. Ello se ve confirmado porque a él resulta aplicable la misma pena que prevé la figura del inciso primero, así como porque también *se considera* que es autor (de un fraude informático) a quien realiza la conducta en él descrita.

En el plano objetivo, el tipo exige facilitar los medios con que se comete un fraude informático. De acuerdo con el DRAE, "facilitar" implica hacer posible la ejecución de algo, en este caso, de un fraude informático, o bien, proporcionar o entregar, en lo que aquí interesa, los medios para perpetrarlo. Ese mismo diccionario indica que un "medio" es una cosa que puede servir para un determinado fin, en este supuesto, la realización de dicho fraude. Por ende, se incluyen dentro de dicha cláusula todos aquellos comportamientos que resulten idóneos para su perpetración, por ejemplo, proporcionar un *malware* o información relevante[74] para su ejecución; facilitar una cuenta bancaria a la que se transfieran los fondos provenientes de un fraude[75]; etc.

En el ámbito subjetivo, el tipo regula una exigencia análoga a la contenida en la receptación informática, toda vez que demanda que el agente conozca o no pueda menos que conocer la ilicitud de la conducta constitutiva de fraude informático, que se regula en el inciso primero del artículo 7º de la nueva ley de delitos informáticos. En ese sentido, es posible que el agente conozca esa

---

[72] Véase, a propósito de dicha discusión, Oliver. "Capítulo IX: Delitos contra la propiedad…", ob. cit., pp. 227-228.

[73] Así, en relación con el tipo penal de estafa, Politoff; Matus y Ramírez. *Lecciones de Derecho Penal Chileno…*, ob. cit., p. 306.

[74] *V. gr.*, nombre de usuario, contraseña, claves que genera un dispositivo de seguridad o que se requieren para realizar transferencias electrónicas, etc.

[75] Supuesto que involucra la intervención de los denominados (ciber-)muleros. *Vid.*, a propósito de dicha hipótesis, más en detalle, Miró. "La respuesta penal al ciberfraude…", ob. cit., pp. 1 y ss.

ilicitud, en cuyo caso obrará con dolo directo, o bien, que no pueda menos que conocerla, situación en la que actuará con dolo eventual[76].

f) Abuso de los dispositivos (artículo 8º)

Este delito, que tiene como antecedente el tipo de abuso de los dispositivos del artículo 6º del Convenio de Ciberdelincuencia[77], se regula en el artículo 8º de la Ley Nº 21.459, disposición que establece lo siguiente:

> "El que para la perpetración de los delitos previstos en los artículos 1º a 4º de esta ley o de las conductas señaladas en el artículo 7º de la ley Nº 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".

---

76 Véase *supra* el punto III.1.d).

77 Artículo 6º - Abuso de los dispositivos:

"1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2º a 5º del presente Convenio;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2º a 5º; y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2º a 5º. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2º a 5º del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1º a) ii) del presente artículo".

Con la regulación de este tipo penal el legislador ha elevado a la categoría de delito autónomo lo que en realidad constituyen actos preparatorios de otros delitos informáticos. En ese orden de ideas, su inclusión en el catálogo de delitos informáticos implica un adelantamiento de las barreras de protección de los intereses subyacentes a la criminalidad informática, que de no haberse establecido habría determinado la impunidad de las conductas que en él se describen. Ello es así, pues, en el Derecho penal chileno, los actos preparatorios sólo excepcionalmente se castigan, no existiendo una norma general que permita su sanción punitiva en el ámbito de la criminalidad informática[78].

Como se desprende del texto transcrito, el tipo penal tiene un ámbito de aplicación acotado a la comisión de determinados delitos informáticos, a saber, ataque a la integridad de un sistema informático (artículo 1º), acceso ilícito (artículo 2º), interceptación ilícita (artículo 3º) y ataque a la integridad de los datos informáticos (artículo 4º), además de los regulados en el artículo 7º de la Ley Nº 20.009[79]. En esa línea, resulta llamativo que no se incluya al fraude

[78] En esa misma línea, a propósito de la normativa española, Romeo, Carlos, "Capítulo 1: De los delitos informáticos al cibercrimen: Una aproximación conceptual y político-criminal", en Romeo, Carlos (coordinador). *El cibercrimen: nuevos retos jurídico-penales*, *nuevas respuestas político-criminales*. Granada: Comares (2006), p. 14.

[79] Artículo 7º:

"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:

a) Falsificar tarjetas de pago.

b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.

c) Negociar, en cualquier forma, tarjetas de pago falsificadas o sustraídas.

d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.

e) Negociar, en cualquier forma, con los datos, el número de tarjetas de pago y claves o demás credenciales de seguridad o autenticación para efectuar pagos o transacciones electrónicas, con el fin de realizar las operaciones señaladas en el literal anterior.

f) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, bloqueadas, en cualquiera de las formas señaladas en las letras precedentes.

g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado, según corresponda, para obtener la autorización que sea requerida para realizar transacciones.

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.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de

informático entre los delitos para cuya perpetración puede llevarse a cabo el comportamiento del artículo 8º de la Ley Nº 21.459, no sólo por la importancia teórica y práctica de dicha figura, sino porque el tipo de abuso de los dispositivos sí se aplica en relación con el delito de uso fraudulento de tarjetas de pago y transacciones electrónicas, que también constituye un fraude en el que, de alguna forma, se emplean medios tecnológicos[80]. No obstante, es posible que el vacío de punición que ello genera se vea colmado por la regulación, como tipo penal autónomo de fraude informático, de la conducta consistente en facilitar los medios para la ejecución de dicho ilícito (artículo 7º inciso segundo).

Desde un punto de vista objetivo, el agente debe entregar u obtener para su utilización, importar, difundir o realizar otra forma de puesta a disposición de uno o más objetos, a los que nos referiremos *infra*, creados o adaptados principalmente para la perpetración de los delitos de ataque a la integridad de un sistema informático (artículo 1º), acceso ilícito (artículo 2º), interceptación ilícita (artículo 3º) o ataque a la integridad de los datos informáticos (artículo 4º), además de los regulados en el artículo 7º de la Ley Nº 20.009.

De acuerdo con el DRAE, "entregar" es dar una cosa a alguien o hacer que pase a tenerla, en este caso, alguno de los objetos que indica el artículo 8º de la Ley Nº 21.459. "Obtener" (para su utilización) puede entenderse como lograr o conseguir alguno de dichos objetos; en tanto que "importar" implica introducirlo al país desde el exterior. "Difundir", por su parte, puede interpretarse como sinónimo de divulgar, por ejemplo, informaciones o datos que permitan la perpetración de alguno de los delitos señalados en el artículo 8º. En fin, "poner a disposición" supone colocar alguno de los posibles objetos materiales del delito de forma tal que se encuentre apto y listo para un determinado fin, concretamente, como medio para la ejecución de alguno de los ilícitos penales indicados *supra*.

Como podrá notarse, el tipo penal regulado en el artículo 8º de la Ley Nº 21.459 es de hipótesis alternativas, por lo que basta con que concurra cualquiera de ellas para que él se verifique. Además, todas ellas implican la realización de movimientos corporales, lo que permite sostener que nos encontramos ante un delito de acción.

---

una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas".

80 *Vid*., respecto de dicho delito, Mayer, Laura y Vera, Jaime. "La nueva regulación del delito de uso fraudulento de tarjetas de pago y transacciones electrónicas", en *Revista de Ciencias Penales*, Sexta Época, vol. XLVII (2021), pp. 519 y ss.

En cuanto a la estructura del tipo, puede afirmarse que el delito de abuso de los dispositivos constituye un tipo de mera actividad, pues sólo exige que se lleve a cabo una entrega, una obtención (para su utilización), una importación, una difusión o una puesta a disposición para que se configure el tipo penal. Consiguientemente, ha de excluirse el castigo penal de la frustración; mientras que, como dichos comportamientos son fraccionables[81], cabe sostener que la tentativa sí es punible.

Objeto material del delito pueden ser 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 alguno de los delitos que indica el legislador. En ese sentido, a pesar de que se trata de un listado que, al menos formalmente, está redactado en términos taxativos, se trata de objetos de tal amplitud (por ejemplo, por la referencia a "dispositivos" o a "datos"), que prácticamente permiten incluir cualquier cosa que sea idónea para la comisión de aquellos ilícitos.

Dichos objetos deben haber sido creados o adaptados principalmente para la perpetración de alguno de los delitos que establece la ley. Según el DRAE, "crear" implica producir; mientras que "adaptar" supone acomodar o ajustar, en este caso, alguno de los objetos que se indican en el artículo 8º, para cometer los delitos de ataque a la integridad de un sistema informático (artículo 1º), acceso ilícito (artículo 2º), interceptación ilícita (artículo 3º), ataque a la integridad de los datos informáticos (artículo 4º), o bien, alguno de los regulados en el artículo 7º de la Ley Nº 20.009. Como se exige que tales objetos sean creados o adaptados "principalmente" con dicha finalidad, se disipan las dudas en torno a la calidad de objeto material del delito de aquellos dispositivos que solo parcialmente se orientan a la comisión de los ilícitos indicados, con la sola limitación de que ellos deben ser creados o adaptados, *en mayor medida* o *especialmente* (mas no exclusivamente), con el fin aludido.

En el plano subjetivo, el tipo penal exige que los comportamientos delictivos se lleven a cabo *para* la perpetración de los delitos que establece el legislador, exigencia que implica demandar dolo directo en el agente de la conducta típica. En ese sentido, el comportamiento que se lleva a cabo, y que opera como medio, debe tener como finalidad la perpetración de alguno de los delitos que especifica la ley, exigencia que no se satisface si sólo concurre dolo eventual.

[81] Por ejemplo, cuando se proporciona parte de los datos requeridos para la comisión del delito, sin que todavía se complete su entrega total.

2. Circunstancias modificatorias de responsabilidad penal aplicables en materia de delitos informáticos

En este ámbito, el legislador se preocupó de establecer circunstancias modificatorias que se relacionan, al menos en parte, con el injusto específico de la criminalidad informática, o bien, con la investigación de dichos ilícitos. En este contexto, se regula una atenuante de responsabilidad penal, de cooperación eficaz, así como tres supuestos en los que se agrava la responsabilidad penal del agente, que podemos denominar agravantes de abuso de confianza, de abuso de vulnerabilidad y de infraestructura crítica.

a) Circunstancia atenuante

Como se dijo, la Ley Nº 21.459 regula expresamente la atenuante de cooperación eficaz, ampliando con ello el grupo de delitos que la contemplan expresamente (*v. gr.*, en la Ley Nº 20.000 o en el Título V del Libro II CP). En efecto, según el artículo 9º de la ley, "[s]erá circunstancia atenuante especial de responsabilidad penal (…) la cooperación eficaz que conduzca 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". Además, la nueva ley de delitos informáticos define explícitamente qué debe entenderse por cooperación eficaz, a saber, "el suministro de datos o informaciones precisas, verídicas y comprobables, que contribuyan necesariamente a los fines señalados [anteriormente]".

La circunstancia modificatoria de cooperación eficaz se relaciona especialmente con las atenuantes generales, consagradas en los numerales 8º y 9º del artículo 11 CP. Como es sabido, la primera de ellas opera si el agente, "pudiendo eludir la acción de la justicia por medio de la fuga u ocultándose, se ha denunciado y confesado el delito"; mientras que la segunda se aplica si dicho sujeto "ha colaborado sustancialmente al esclarecimiento de los hechos".

Desde el punto de vista de sus fundamentos, la cooperación eficaz integra aquel grupo de circunstancias modificatorias que apuntan a favorecer el esclarecimiento de los hechos investigados, otorgando un incentivo penológico al imputado. En esa línea, es posible sostener que el fundamento de la circunstancia atenuante en comento se encuentra en razones de política criminal vinculadas, justamente, con la finalidad de comprobar que ha existido un he-

cho constitutivo de delito y quiénes han tenido una intervención penalmente relevante en él[82].

Tratándose de la atenuante que se regula en la Ley Nº 21.459, es posible llevar a cabo una cooperación eficaz a través de diversos medios, toda vez que el legislador no establece mecanismos específicos para el esclarecimiento de los hechos. Por ende, será posible proporcionar informaciones orientadas a esa finalidad mediante declaraciones verbales; documentos, incluidos los electrónicos; archivos de audio o video; programas computacionales; etcétera.

Además, la información suministrada por alguna de las vías señaladas u otras que sean idóneas ha de ser precisa, verídica y comprobable. La precisión excluye datos ambiguos o vagos, que no permitan a los persecutores el desarrollo de líneas investigativas para el esclarecimiento de delitos de igual o mayor gravedad. Que la información sea verídica significa que los datos proporcionados deben corresponderse con la realidad, por lo tanto, resulta necesario que efectivamente existan otros hechos y otros partícipes en delitos informáticos. Finalmente, el carácter comprobable ha sido interpretado en el sentido de que el desarrollo de la investigación, por parte del Ministerio Público y de las Policías, a partir de la información proporcionada, permita efectivamente descubrir otros hechos constitutivos de delito y establecer la participación de sus responsables[83].

La ley exige que el Ministerio Público reconozca esta circunstancia expresándola al momento de formalizar la investigación o en el escrito de acusación. En relación con la misma atenuante, regulada en la Ley Nº 20.000, la doctrina ha entendido dicha referencia en el sentido de que es el órgano persecutor penal quien determina la concurrencia de la aminorante, razón por la cual ella sólo sería aplicable si así lo establece el Ministerio Público[84]. El problema, sin embargo, radica en determinar cuál es el efecto que tiene tal reconocimiento, o bien, la falta del mismo, sobre todo en los casos en que ha existido un intento

[82] En términos similares, pero respecto de la circunstancia atenuante del artículo 11 Nº 8 CP, Matus, Jean Pierre. "§ 3. De las circunstancias que atenúan la responsabilidad criminal: Artículo 11", en Politoff, Sergio y Ortiz, Luis (directores). *Texto y comentario del Código Penal chileno*, tomo I, *Libro Primero - Parte General*, reimpresión de la 1ª ed. Santiago: Editorial Jurídica de Chile (2010), p. 182.

[83] En esa línea, a propósito de la Ley Nº 20.000, CA de Copiapó, de 23 de junio de 2015, rol Nº 109-2015, considerando 5º.

[84] En ese orden de ideas Silva Silva, Hernán. "La cooperación eficaz de la ley de drogas", en *Revista de Derecho y Ciencias Penales*, Nº 17 (2011), p. 223.

de cooperación y el fiscal respectivo no ha invocado la circunstancia en las oportunidades anotadas.

En nuestra opinión, el pronunciamiento final en torno a la concurrencia de esta circunstancia debe quedar entregado a los tribunales de justicia, incluso en el evento en que no sea reconocida por el Ministerio Público, por cuanto la apreciación de circunstancias modificatorias integra la fase de juzgamiento penal, función que no corresponde en caso alguno al órgano persecutor, por disponerlo expresamente el artículo 83 inciso primero de la Constitución (CPR). En ese orden de ideas si, por ejemplo, el imputado presta declaración, aportando datos que cumplen con todos los requisitos establecidos en la ley y el Ministerio Público no reconoce la atenuante, por entender que la información no es comprobable, el abogado defensor podría, en cualquier caso, intentar su demostración en el respectivo procedimiento o juicio.

En cuanto a su efecto penológico, la Ley Nº 21.459 indica que la cooperación eficaz "permitirá rebajar la pena hasta en un grado", así como que la reducción señalada "se determinará con posterioridad a la individualización de la sanción penal según las circunstancias atenuantes o agravantes comunes que concurran; o de su compensación, de acuerdo con las reglas generales". Como podrá advertirse, desde el punto de vista de sus efectos, el legislador ha innovado respecto de regulaciones análogas existentes en otros cuerpos normativos, que establecen un efecto atenuatorio más intenso, como es el caso de la cooperación eficaz aplicable a la malversación de caudales públicos, a los fraudes y exacciones ilegales, así como al cohecho, que permite al tribunal reducir la pena hasta en dos grados (artículo 260 quáter CP); o de la cooperación eficaz regulada en la ley sobre tráfico ilícito de estupefacientes y sustancias psicotrópicas, que faculta a una rebaja de hasta dos o incluso tres grados (artículo 22 de la Ley Nº 20.000)[85].

Además, el legislador se encargó de precisar que la consideración de la atenuante tendrá lugar de manera independiente a la ponderación de circunstancias comunes. De ello se colige, que la ponderación de esta atenuante no integra la fase de compensación racional a la que normalmente se someten todas las circunstancias modificatorias en el proceso de individualización de la pena[86]. Por

[85] Es probable que la razón subyacente a tales diferencias obedezca a que, en la ley sobre tráfico ilícito de estupefacientes y sustancias psicotrópicas, el reconocimiento de esta circunstancia para rebajar dos o tres grados implique el esclarecimiento de delitos graves, o bien, el desbaratamiento de una organización criminal.

[86] Esta idea, que se encuentra implícita en la nueva ley de delitos informáticos, ha sido expresamente reconocida en el artículo 269 quáter CP, norma que regula la atenuante de

lo mismo, ello puede redundar en un efecto atenuatorio que resulte aplicable *en todo caso*.

Por último, en lo que atañe a la compatibilidad entre la cooperación eficaz y la colaboración sustancial al esclarecimiento de los hechos del artículo 11 Nº 9 CP, la doctrina y la jurisprudencia[87] se han pronunciado negativamente respecto de su aplicación conjunta cuando se basan en los mismos antecedentes[88]. Esta solución se sustenta en la semejanza que se atribuye al fundamento de ambas circunstancias modificatorias. Por consiguiente, de seguirse ese razonamiento, ellas no serían incompatibles si los hechos en que se fundan son diversos, por ejemplo, una confesión respecto de la participación propia y la entrega de información precisa, verídica y comprobable de otros sujetos en relación con delitos informáticos de igual o mayor gravedad.

b) Circunstancias agravantes

De acuerdo con lo señalado *supra*, la nueva ley de delitos informáticos regula tres situaciones que determinan un aumento de la penalidad aplicable, que hemos denominado agravantes de abuso de confianza, de vulnerabilidad y de infraestructura crítica.

En cuanto a la primera de dichas agravantes, el artículo 10 Nº 1) de la Ley Nº 21.459 establece que constituye circunstancia agravante de los delitos de que trata la ley el hecho de cometerlo "abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función".

Llama la atención que se haya consagrado expresamente dicha circunstancia modificatoria, toda vez que el artículo 12 Nº 7 CP ya regula la agravante genérica de abuso de confianza. En ese sentido, esta última circunstancia no es más que el género del cual la modificatoria contemplada en la nueva ley de delitos informáticos constituye una especie, que sólo precisa un supuesto concreto en el cual el abuso de confianza tendría que verificarse.

---

cooperación eficaz aplicable a diversos delitos funcionarios, a saber, la malversación de caudales públicos, los fraudes y exacciones ilegales, y el cohecho. En efecto, según el inciso cuarto del precepto aludido, "[l]a reducción de pena se determinará con posterioridad a la individualización de la sanción penal según las circunstancias atenuantes o agravantes comunes que concurran; *o de su compensación*, de acuerdo con las reglas generales" (cursivas agregadas).

87 Así, CA de Antofagasta, 13 de mayo de 2008, rol Nº 82-2008, considerando sexto.

88 Véase Matus, Jean Pierre y Ramírez, María Cecilia. *Manual de Derecho Penal Chileno, Parte Especial*, 4ª ed. Valencia: Tirant lo Blanch (2021), p. 486.

Más allá de la redundancia indicada respecto de la consagración expresa de la agravante del artículo 10 Nº 1) de la Ley Nº 21.459, el fundamento de la agravante de abuso de confianza "se identifica con la creación, el incremento o el aprovechamiento del estado de indefensión del ofendido, o sea, un mayor injusto o una mayor afectación de los bienes jurídicos involucrados"[89].

En cuanto al sentido y alcance de la agravante de abuso de confianza, ella se compone de dos partes, a saber, la idea de confianza y el abuso que se llevaría a cabo en relación con aquella.

De acuerdo con su sentido natural y obvio, la expresión "confianza" se vincula con la familiaridad o intimidad[90] que se tiene respecto de otra persona. En términos análogos, ella se relaciona con la existencia de un especial vínculo, que nace de la fe que un sujeto ha depositado en otro[91], el cual puede originarse en diversas circunstancias, *v. gr.*, la cercanía que existe entre ambos, la opinión que el primero tiene del segundo, etc.[92]. Por lo tanto, no tiene que tratarse, necesariamente, de una confianza de carácter personal, pudiendo extenderse, por el contrario, a un vínculo más o menos impersonal, que surge de las relaciones jurídicas propias de la vida moderna[93].

Que un individuo espere que otro le guarde fidelidad[94] o lealtad[95] implica tener ciertas expectativas respecto de la conducta de aquel en quien se confía[96]. Así, por ejemplo, en el ámbito de la informática, podría ocurrir que el primero confíe que el segundo mantendrá en reserva ciertos datos que no deben trascender[97], o bien, que los conservará a través de respaldos idóneos.

---

89 Mayer, Laura y Vera, Jaime. "Agravante de abuso de confianza", en González Jara, Manuel Ángel (coordinador). *Circunstancias atenuantes y agravantes en el Código Penal chileno*. Santiago: Ediciones Jurídicas de Santiago (2020), p. 219.

90 Véase Etcheberry, Alfredo. *Derecho Penal Parte General*, tomo II, reimpresión de la 3ª ed. Santiago: Editorial Jurídica de Chile (2010), p. 30 y Garrido, Mario. *Derecho Penal*, *Parte General*, tomo I, reimpresión de la 2ª ed. Santiago: Editorial Jurídica de Chile (2018), p. 222.

91 Así, Cury, Enrique. *Derecho Penal*, *Parte General*, 10ª ed. Santiago: Ediciones UC (2011), p. 501.

92 Mayer y Vera. "Agravante de abuso de confianza…", ob. cit., p. 215.

93 Así, en relación con los tipos de apropiación indebida del artículo 470 Nº 1 y de administración desleal del artículo 470 Nº 11 CP, Mayer. "Capítulo X: Delitos contra intereses patrimoniales…", ob. cit., pp. 476 y 507 con referencias ulteriores.

94 Así, Garrido. *Derecho Penal*, *Parte General*, tomo I, ob. cit., p. 222.

95 Véase Cury. *Derecho Penal*…, ob. cit., p. 501.

96 Mayer y Vera. "Agravante de abuso de confianza…", ob. cit., p. 215.

97 Desde un punto de vista más general, Mayer y Vera. "Agravante de abuso de confianza…", ob. cit., p. 215.

Por su parte, el hecho de exigir un "abuso" de la confianza depositada en otro sujeto implica, de acuerdo con el DRAE, que aquel hace un uso excesivo, injusto o indebido de dicha confianza. De forma similar, es posible sostener que la agravante en comento involucra un aprovechamiento de la posición en la que se encuentra el agente que quebranta la confianza de otro, sujeto que, según los casos, podrá incluso resultar instrumentalizado por aquel en quien confía.

La agravante de abuso de confianza regulada en la Ley Nº 21.459 resulta aplicable a dos supuestos específicos: a quien administra un sistema informático y a quien es custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función. De acuerdo con su sentido natural y obvio, que puede consultarse en el DRAE, "administrar" un sistema informático implica estar encargado de su gestión, labor que puede suponer actuaciones organizativas o incluso de dirección, dependiendo del nivel de facultades que tenga el sujeto que administra. Por su parte, el "custodio" de los datos informáticos es quien está a cargo de guardarlos, idea que en el ámbito de la informática involucra almacenarlos con cuidado, a fin de que ellos no resulten afectados por la actuación de terceros.

En el contexto de la delincuencia informática, es común que se refiera la actuación de "*insiders*", que corresponden a "trabajadores o prestadores de servicios de la empresa o establecimiento afectado", que se encuentran en una posición especialmente ventajosa para la comisión de la conducta delictiva, derivada de su vínculo con la víctima[98]. Tal forma de operar se opone a los ataques informáticos que provienen, por así decirlo, externamente, por parte de un sujeto que carece de la relación indicada.

En términos generales, los encargados de informática de una empresa u organización podrían tener una posición de confianza, en la línea de lo señalado. Sin embargo, ella no es inherente a su labor, por lo que será necesario analizar caso a caso en qué hipótesis se encuentra dicho sujeto. Así, por ejemplo, no se hallará en ese supuesto quien simplemente preste apoyo técnico, instale programas, solucione posibles fallas, etc. En cambio, sí podría encontrarse en la posición de confianza referida aquel sujeto que tiene a su cargo una base de datos con información sensible, de carácter reservado.

Por otra parte, cabe destacar que los delitos informáticos de mayor relevancia teórica y práctica se verifican a través de internet[99], por parte de un individuo que carece de vínculos con su potencial víctima, de modo que

[98] Mayer. "Elementos criminológicos…", ob. cit., p. 187 con referencias ulteriores.

[99] En esa línea Miró. "La respuesta penal al ciberfraude…", ob. cit., p. 3.

respecto de ellos el abuso de confianza no será inherente a la comisión del ilícito en cuestión. Consiguientemente, en esos supuestos será posible aplicar la agravante en comento, siempre que, al perpetrar el hecho, el agente se hubiere aprovechado de la confianza que en él depositó el ofendido.

Atendida la relación de género a especie que hemos afirmado entre la agravante genérica de abuso de confianza (artículo 12 Nº 7 CP) y la agravante específica de abuso de confianza de la nueva ley de delitos informáticos (artículo 10 Nº 1], Ley Nº 21.459), no es posible aplicarlas conjuntamente. Hacerlo implicaría una vulneración flagrante al principio *non bis in idem*. Esta idea se ve confirmada por el hecho de que la agravante de abuso de confianza de la nueva ley de delitos informáticos no establece un régimen especial aplicable a sus efectos, de modo que se sujeta a las reglas generales en materia de ponderación de circunstancias modificatorias de la responsabilidad penal.

En cuanto a la agravante de vulnerabilidad, la nueva ley de delitos informáticos establece, en su artículo 10 Nº 2), que constituye circunstancia agravante de la responsabilidad penal el hecho de "[c]ometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores".

La regulación de esta agravante puede entenderse como expresión de una tendencia en orden a ampliar la aplicación de la circunstancia modificatoria de alevosía a ámbitos distintos de los delitos contra las personas. Recordemos que esta última agravante, regulada en el artículo 12 Nº 1 CP, establece explícitamente que constituye una circunstancia que determina una agravación del castigo, el hecho de "[c]ometer el delito *contra las personas* con alevosía, entendiéndose que la hay cuando se obra a traición o sobre seguro" (cursivas agregadas). En ese sentido, el legislador ha ido extendiendo el ámbito de procedencia de dicha agravante, por ejemplo, a algunos de los delitos sexuales[100], cuestión que ha requerido de reformas legales expresas, por tratarse de contextos en los que la agravante genérica no resultaría aplicable.

De acuerdo con su sentido natural y obvio, la alevosía equivale a la "[c]autela para asegurar la comisión de un delito contra las personas, sin riesgo para el delincuente" (DRAE). En ese orden de ideas, ella corresponde a un modo de ejecución del comportamiento delictivo, que se caracteriza por "el mayor desvalor que la ley le atribuye al estado de indefensión que

[100] *Vid*., el artículo 368 bis Nº 1 CP, que hace aplicable la agravante de alevosía a los delitos del Párrafo 5º (*De la violación*) y 6º (*Del estupro y otros delitos sexuales*) del Título VII del Libro II CP.

inexorablemente afecta a la víctima"[101]; por ende, su fundamento radica en el mayor injusto subyacente a la conducta, que es llevada a cabo en "condiciones especialmente riesgosas" para el ofendido y para los bienes jurídicos de que él es titular[102].

Como podrá notarse, dichas ideas se vinculan directamente con la noción de vulnerabilidad. En ese orden de cosas, de acuerdo con el DRAE, un sujeto es vulnerable si "puede ser herido o recibir lesión, física o moralmente". Por lo tanto, de lo que se trata es de que la potencial víctima se encuentre en una posición de riesgo, que haga más probable que el agente pueda consumar el hecho delictivo, por ejemplo, porque no puede recurrir a terceros que actúen en su defensa; idea que tiene bastantes puntos de contacto con el obrar "sobre seguro", que integra la agravante de alevosía, a la cual nos referimos *supra*.

No cabe confundir vulnerabilidad con desconocimiento (*v. gr.*, del funcionamiento de los sistemas de tratamiento de la información), pues la ley prevé expresamente al desconocimiento de niños, niñas, adolescentes o adultos mayores como un supuesto distinto al de la vulnerabilidad, de modo que el intérprete debe dotar de un contenido diferenciado a ambas hipótesis. En esa línea, desconocer implica no comprender o no dominar ciertas operaciones que pueden realizarse a través de sistemas de tratamiento automatizado de la información, o bien, no captar el sentido y alcance que ellas podrían tener. En este caso, la víctima se encuentra en una posición de ignorancia, que posibilita un cierto nivel de instrumentalización en su contra por parte del agente del comportamiento delictivo.

Además, el artículo 10 Nº 2) de la nueva ley de delitos informáticos contempla el abuso de la confianza de niños, niñas, adolescentes o adultos mayores como un supuesto de agravación de la responsabilidad penal. Esta situación se diferencia de la agravante de abuso de confianza del artículo 10 Nº 1), que no se centra en la potencial víctima de la conducta (niño, niña, adolescente o adulto mayor), sino que en el agente de aquella (quien tiene una posición de confianza "en la administración del sistema informático" o por el hecho de ser "custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función").

---

101 Rodríguez, Luis y Mayer, Laura. "Alevosía genérica y alevosía específica", en Acevedo, Nicolás; Collado, Rafael y Mañalich, Juan Pablo (coordinadores). *La justicia como legalidad. Estudios en homenaje a Luis Ortiz Quiroga*. Santiago: Thomson Reuters (2020), p. 695.

102 *Ibid.*, p. 701.

No obstante, todo lo dicho respecto del carácter redundante de la agravante de abuso de confianza del artículo 10 Nº 1) de la Ley Nº 21.459 es perfectamente aplicable al supuesto específico de abuso de confianza de niños, niñas, adolescentes o adultos mayores, de modo que nos remitimos a las críticas efectuadas *supra*, en especial, a las relativas a la posibilidad de recurrir a la agravante genérica de abuso de confianza del artículo 12 Nº 7 CP para lograr el mismo efecto agravatorio. Por lo ya señalado, no cabe aplicar conjuntamente esta última agravante con la contemplada en el artículo 10 Nº 2) de la nueva ley de delitos informáticos, pues ello importaría una vulneración del principio *non bis in idem*.

Finalmente, la nueva ley contempla la agravante de infraestructura crítica, según la cual, "si como resultado de la comisión de las conductas contempladas en (…) el Título [I], 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, la pena correspondiente se aumentará en un grado".

El fundamento de la agravante en comento radica en el mayor injusto implicado en conductas que impactan negativamente en infraestructura crítica. Por ende, lo que está en juego es una posible afectación, de gran entidad y particularmente intensa, de los bienes jurídicos asociados a la infraestructura que resulta impactada a través de la comisión de delitos informáticos.

Si bien a nivel doctrinal pueden advertirse matices en torno a la definición del concepto de infraestructura crítica, cuyo examen desbordaría los márgenes del presente trabajo, podemos sostener que ella está integrada por servicios de suministro básico e instalaciones de carácter técnico y estratégico, que son de enorme importancia para la economía, la sociedad y el Estado; los cuales se extienden a ámbitos como los servicios ya mencionados de electricidad, gas, agua, transporte, telecomunicaciones o financieros; a los que pueden añadirse los servicios hospitalarios, de provisión de alimentos, de bomberos, de policías, entre otros[103].

Pues bien, probablemente para evitar posibles discusiones en torno a qué implica, exactamente, la infraestructura crítica, es que el legislador optó por hacer una referencia, no a dicho concepto, sino que a un listado de servicios que pueden incluirse dentro de aquel. Se trata de una enunciación no taxativa,

[103] Así, Kochheim, Dieter. *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik*. München: Beck (2015), p. 609.

como se deduce de la expresión "tales como" que la precede. Particularmente significativa a este respecto es la mención que se efectúa a los procesos electorales, que pese a poder englobarse en el concepto de infraestructura crítica, atendida su relevancia para el sistema democrático, suele no constituir un ejemplo clásico de esa clase de infraestructura a nivel doctrinal.

La agravante en comento contempla dos situaciones que pueden diferenciarse: por una parte, es posible que se afecte o interrumpa la provisión o prestación de servicios de utilidad pública, o bien, el normal desenvolvimiento de los procesos electorales que se regulan en la Ley Nº 18.700. "Afectar" implica, en este contexto, incidir negativamente en alguno de los servicios indicados; mientras que "interrumpir", según lo señalado a propósito del delito de interceptación ilícita (artículo 3º de la Ley Nº 21.459), supone cortar la continuidad, en este caso, de un servicio de utilidad pública. Como se trata de un listado no taxativo, estimamos que sería posible afectar o interrumpir procesos electorales regidos por normas distintas de la Ley Nº 18.700, en la medida en que ellos puedan equiparase, por su relevancia, a las otras hipótesis que prevé la agravante.

La nueva ley de delitos informáticos establece expresamente que la agravante de infraestructura crítica es aplicable "si como resultado de la comisión de las conductas" se producen algunos de los efectos que hemos señalados. Por lo tanto, es necesario que exista y se acredite un vínculo causal entre la perpetración de alguno de los delitos informáticos que regula la Ley Nº 21.459 y la afectación o interrupción de la provisión o prestación de servicios de utilidad pública o del normal funcionamiento de los procesos electorales indicados.

La agravante de infraestructura crítica puede relacionarse con la circunstancia genérica, regulada en el artículo 12 Nº 3 CP, según la cual, constituirá una agravante el hecho de "[e]jecutar el delito por medio de inundación, incendio, veneno u otro artificio que pueda ocasionar grandes estragos o dañar a otras personas". Por lo tanto, se trata de una agravante que se relaciona con los resultados que ciertos hechos generan en la naturaleza o en la sociedad, con impactos muy negativos para la vida de las personas. De ahí que la doctrina entienda que su fundamento radica en el empleo de medios catastróficos para la comisión del delito[104]. En ese sentido, ella tiene importantes puntos de contacto con la agravante de infraestructura crítica, razón por la cual su aplicación conjunta constituiría una vulneración del principio *non bis in idem*.

[104] Así, Künsemüller, Carlos. "§ 4. De las circunstancias que agravan la responsabilidad criminal: Artículos 12 y 13", en Politoff, Sergio y Ortiz, Luis (directores). *Texto y comentario del Código Penal chileno*, tomo *I*, *Libro Primero - Parte General*, *reimpresión de la 1ª ed*. Santiago: Editorial Jurídica de Chile (2010), p. 193.

Desde el punto de vista de sus efectos penológicos, esta agravante tiene una consecuencia más gravosa que las otras dos agravantes específicas que hemos comentado, pues se escapa de las reglas generales y establece que la pena correspondiente se aumente en un grado. Cabe recordar que de acuerdo con las disposiciones relativas a la determinación de la pena que se prevén en el CP, es posible que la existencia de una agravante no implique un aumento de la penalidad aplicable, *v. gr.*, por la clase de pena impuesta al delito o por la existencia de una compensación (racional) entre agravantes y atenuantes. En cambio, la agravante de infraestructura crítica obliga a aumentar la pena en un grado, *en todo caso*.

3. Responsabilidad penal de las personas jurídicas por delitos informáticos

La nueva ley de delitos informáticos, junto con establecer diversas figuras delictivas que pueden ser cometidas por personas naturales, regula expresamente la posibilidad de que una persona jurídica responda penalmente por su comisión, en la medida en que se verifiquen los requisitos de imputación que se consagran en la Ley Nº 20.393[105]. Dicha responsabilidad tiene como antecedente lo dispuesto en el artículo 12 del Convenio de Ciberdelincuencia, norma que, sin embargo, plantea que la responsabilidad de las personas jurídicas no tiene que ser necesariamente penal, pudiendo también ser civil o administrativa.

Como sea, la nueva ley de delitos informáticos ha implicado una ampliación considerable del catálogo de delitos a los que puede extenderse la responsabilidad penal de las personas jurídicas, previsto en el artículo 1º de la Ley Nº 20.393. En concreto, la Ley Nº 21.459 ha dispuesto que todos los delitos regulados en su Título I pueden acarrear responsabilidad penal para una persona jurídica (artículo 21 Nº 1] de la Ley Nº 21.459), de modo que esta puede referirse a cualquiera de los ilícitos penales ya examinados (ataque a la integridad de un sistema informático, ataque a la integridad de los datos informáticos, acceso ilícito, interceptación ilícita, falsificación informática, receptación de datos informáticos, fraude informático y abuso de los dispositivos).

[105] Y que básicamente implican que el delito sea cometido por una persona natural perteneciente a un determinado círculo, directa e inmediatamente en interés o para provecho de la persona jurídica, y como consecuencia del incumplimiento, por parte de la persona jurídica, de sus deberes de dirección y supervisión (artículo 3º de la Ley Nº 20.393). Véase, respecto de tales exigencias, por ejemplo, Rojas, Luciano. "Capítulo I. Responsabilidad penal de las personas jurídicas. Consideraciones generales", en Artaza, Osvaldo (director). *Compliance penal: Sistemas de prevención de la corrupción*. Santiago: DER (2019), pp. 11-16.

Ciertamente, esta es una de las modificaciones más relevantes que ha introducido la nueva ley de delitos informáticos, por varias razones, de las que podemos mencionar al menos dos.

Por una parte, ya que el contexto comisivo de los delitos informáticos es, por así decirlo, un espacio en el que conviven permanentemente toda clase de personas jurídicas, la criminalidad informática constituye un ámbito que puede afectarlas en diversos sentidos. En ese orden de ideas, es posible imaginar situaciones en las que la persona jurídica sea víctima de un delito informático, o bien, hipótesis en las que ella sea utilizada para la comisión de alguno de los delitos regulados en la Ley Nº 21.459.

En el plano de la responsabilidad penal de las personas jurídicas es este último supuesto el que resultará de especial interés, lo que es sin perjuicio de que pueda controvertirse, *v. gr.*, si la persona jurídica en cuestión realmente ha sido víctima de un determinado delito o si ella, más bien, posibilitó o incluso facilitó su perpetración.

Igualmente, podría discutirse si acaso los requisitos de imputación de responsabilidad penal para la persona jurídica deberían interpretarse considerando las particularidades de comisión de los delitos informáticos. Así, por ejemplo, es posible cuestionar qué implica, en ese especial ámbito de la criminalidad, que el delito sea cometido directa e inmediatamente en interés o para provecho de la persona jurídica, así como qué supone, en materia de delitos informáticos, infringir deberes de dirección y supervisión. Asimismo, podría debatirse qué clase de sujetos más plausiblemente llevarán a cabo delitos informáticos (*v. gr.*, prestadores de servicios[106]; encargados de informática que se identifican con

[106] El artículo 15 c) de la nueva ley de delitos informáticos define a los prestadores de servicios como "[t]oda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo". Por lo tanto, ellos pueden corresponder a personas naturales, subsumibles en algunas de las categorías indicadas en el artículo 3º de la Ley Nº 20.393, o bien, a personas jurídicas. Esta última es la hipótesis más probable, pues los prestadores de servicios informáticos suelen corresponder a empresas, incluso de gran envergadura y carácter trasnacional, cuya persecución penal plantea problemas clásicos, como si y en qué medida es posible aplicarles la legislación chilena, qué mecanismos investigativos pueden utilizarse a su respecto, etc. Como sea, en este contexto resulta de especial interés el problema relativo a si tales prestadores pueden ser responsabilizados en caso de que incorporen contenidos ilícitos, particularmente si ellos provienen de terceros. *Vid.*, respecto de este problema, Riquert, Marcelo. "La responsabilidad penal de las personas jurídicas en Argentina y el 'Ciberconvenio' de Budapest", en Dupuy, Daniela (directora). *Cibercrimen II*. Montevideo-Buenos Aires: B de f (2020), pp. 447 y ss., pp. 454 y ss.

alguna de las categorías de sujetos que se refieren en el artículo 3º de la Ley Nº 20.393; etc.).

Esta última cuestión se vincula con el segundo aspecto que da cuenta de la importancia de la reforma introducida en materia de responsabilidad penal de las personas jurídicas, y que tiene que ver con los desafíos que implica para los programas de *compliance* la introducción de los delitos informáticos en el catálogo de ilícitos que pueden hacer surgir esa clase de responsabilidad. En ese orden de ideas, y en relación con lo señalado *supra*, mientras que ilícitos como el financiamiento del terrorismo, hoy contenido en dicho catálogo, pueden involucrar riesgos menores para muchas personas jurídicas, debido a las bajas probabilidades que tiene su perpetración, no puede decirse lo mismo de los delitos regulados en la Ley Nº 21.459.

En efecto, prácticamente no existe persona (natural o jurídica) que no recurra a los sistemas informáticos y a internet para desarrollar diversas actividades de frecuente verificación. En el caso específico de las personas jurídicas, ello las expone a sufrir la comisión de delitos informáticos, pero también a ser potenciales autoras de los diversos comportamientos que se regulan en la Ley Nº 21.459. Ahora bien, pese a que dichos riesgos se presentan a propósito de todos los delitos informáticos, es claro que hay algunos cuya perpetración parece más probable.

En este contexto, especial mención merece el tipo penal de receptación informática del artículo 6º de la nueva ley, sobre todo en lo que atañe a la posibilidad de castigar a quien almacene datos informáticos provenientes de delitos como el acceso ilícito. A este respecto, si bien se establecen ciertas exigencias adicionales, que pueden hacer más difícil la imputación (por ejemplo, que se acredite la existencia de dolo o la finalidad ilícita en el agente), de todos modos, el almacenamiento de datos de origen incierto puede constituir un foco de riesgos, que los modelos de *compliance*, a partir de la publicación de la Ley Nº 21.459, tendrán que afrontar.

IV. Aspectos procesales de la nueva ley de delitos informáticos

Los aspectos procesales de la Ley Nº 21.459 se encuentran en su Título II, rubricado, como se dijo, *Del Procedimiento*. Dicha sección de la ley tipifica la legitimación activa para presentar querella, las técnicas especiales de investigación, el comiso y el tratamiento de los antecedentes de la investigación contenidos en formato electrónico. Consiguientemente, dividiremos el análisis de esa misma forma, para mayor claridad del lector.

1. Legitimación activa para presentar querella en materia de delitos informáticos (artículo 11)

El artículo 11 de la Ley Nº 21.459 prevé una norma especial, relativa a la legitimidad activa del Ministerio del Interior y Seguridad Pública, de los Delegados Regionales y de los Delegados Presidenciales Provinciales, quienes pueden dar inicio al proceso penal mediante la interposición de una querella. Dicho precepto debe ser relacionado con el artículo 111 inciso tercero CPP, según el cual, la intervención como querellantes por parte de órganos y servicios públicos queda circunscrita sólo a aquellos casos en que la ley expresamente lo establece, como ocurre con el referido artículo 11.

En el caso del Ministerio del Interior y Seguridad Pública, dicha norma se suma a otras dispersas en el ordenamiento jurídico, que posibilitan su intervención como querellante en procesos penales, como ocurre en el caso de los delitos tipificados en la Ley Nº 18.314, de 17 de mayo de 1984, sobre conductas terroristas (artículo 10); o en el D.F.L. Nº 7.912, de 5 de diciembre de 1927, en lo relativo a los delitos contra el orden y la seguridad públicos.

Llama la atención que el artículo 11 de la nueva ley de delitos informáticos posibilite la interposición de una querella a los organismos antes referidos para dar inicio al proceso penal, lo que provoca que puedan surgir dudas en torno a la facultad de interponer dicha querella cuando el proceso penal se ha iniciado de otra manera, como podría ser la formulación de una denuncia o de oficio por el Ministerio Público. En relación con este punto, cabe considerar que la querella no siempre es la forma de inicio del procedimiento, pudiendo interponerse hasta el cierre de la investigación (artículo 112 CPP). Por ello, de acuerdo con una interpretación restrictiva del artículo 11, los organismos públicos por él legitimados, sólo podrían interponer una querella para dar inicio al respectivo proceso. No obstante, teniendo en cuenta que la intervención de dichos sujetos apunta a la salvaguarda del normal funcionamiento de servicios de utilidad pública, según veremos a continuación, resulta conveniente favorecer una interpretación amplia de la norma, que posibilite la intervención de esos organismos, como querellantes, independientemente si con el escrito respectivo se da inicio o no al proceso.

De acuerdo con lo que señalábamos, la intervención como querellante de dichos órganos se encuentra subordinada a que el o los delitos informáticos que se investigan "interrumpieren el normal funcionamiento de un servicio de utilidad pública". En nuestra opinión, corresponderá a tales organismos esgrimir las razones por las cuales nos encontraríamos ante dicho supuesto, debiendo el Juez de Garantía, al pronunciarse sobre la admisibilidad de la que-

rella, examinar si concurre tal afectación. De todas maneras, considerando que podríamos encontrarnos en una etapa preliminar del proceso, no se requerirá una demostración equivalente a la que se exige en la etapa de juicio, sino que bastará la existencia de ciertos indicios que den cuenta de la interrupción del normal funcionamiento de un servicio de utilidad pública.

Teniendo en cuenta que la norma no alude a un servicio público, sino que a uno de "utilidad pública", sería posible incluir a actividades prestacionales que apuntan a la satisfacción de necesidades colectivas no obstante ser llevadas a cabo por privados (*v. gr.*, servicios de suministro eléctrico o de agua potable). Asimismo, la alusión a un servicio de utilidad pública parece más amplia que la idea de "infraestructura crítica"; no obstante, existiendo una relación de género a especie entre ambas nociones, la norma de legitimación activa que comentamos ciertamente será aplicable cuando lo que se interrumpa sea un servicio integrante de tal infraestructura crítica.

2. Técnicas especiales de investigación en materia de delitos informáticos (artículo 12)

a) Cuestiones generales relativas a la investigación de delitos informáticos

La nueva ley de delitos informáticos, como fluye del análisis realizado *supra*, apunta a una modernización de dicho sector de la criminalidad, en el sentido de adaptar las descripciones de los diferentes delitos que la integran a los desarrollos que ha experimentado la informática en los últimos años. Ahora bien, dicho propósito quedaría inconcluso, si tales reformas no fueran acompañadas de una modernización de las disposiciones procesales tendientes a investigar esos delitos, posibilitando una persecución penal más eficiente y eficaz de este sector de la criminalidad.

Por otra parte, la delincuencia informática se caracteriza por incidir en objetos inmateriales, lo que la distingue de otros ilícitos, por ejemplo, aquellos que afectan a la vida o a la salud de las personas. Tal inmaterialidad hace necesario enfrentar la investigación delictiva a través de mecanismos y de medidas idóneos, muchos de los cuales también implicarán el recurso a las tecnologías[107].

[107] Véase, con referencia al empleo de programas computacionales y de técnicas de inteligencia artificial, Zaragoza, Javier. "Ciberpatrullaje e investigación tecnológica en la red: Una aproximación a la inteligencia artificial desde el punto de vista de la investigación y represión de hechos ilícitos", en Dupuy, Daniela y Corvalán, Juan (directores). *Cibercrimen III*. Montevideo-Buenos Aires: B de f (2020), pp. 212 y ss.

En esa línea, así como considerando las dificultades existentes para la investigación de los delitos informáticos, la ley destinó un título particular (II), en el que se regulan ciertas técnicas especiales para la indagación de tales ilícitos. Nos referimos a las medidas de interceptación de comunicaciones privadas, a otros medios técnicos de investigación y al establecimiento de agentes encubiertos, a las que podría agregarse la cooperación eficaz, que ya fue analizada en el presente trabajo a propósito de las circunstancias modificatorias de responsabilidad penal.

b) Interceptación de comunicaciones y otros medios técnicos de investigación

La posibilidad de utilizar dichas técnicas se aplica a determinados delitos informáticos, que corresponden a los ilícitos más graves que regula la nueva ley, a saber, ataque a la integridad de un sistema informático (artículo 1º), acceso ilícito (artículo 2º), interceptación ilícita (artículo 3º), ataque a la integridad de los datos informáticos (artículo 4º), falsificación informática (artículo 5º) y fraude informático (artículo 7º).

Dicha norma hace excepción a la regla general contenida en el CPP, según la cual, las dos primeras diligencias intrusivas señaladas (interceptación de comunicaciones y otros medios técnicos de investigación) sólo proceden respecto de hechos que merezcan la pena de crimen. No obstante, todos los delitos informáticos de la Ley Nº 21.459 están regulados como simples delitos, lo que en parte explica que el legislador haya decidido restringir el ámbito de aplicación de las técnicas en comento únicamente a los ilícitos penales más graves. A nuestro juicio, la introducción de una excepción a las reglas generales se relaciona especialmente con lo compleja que resulta la investigación penal por la comisión de delitos informáticos, por ejemplo, en lo que respecta a la identificación de su autor o a la acreditación del elemento subjetivo.

A pesar de que el legislador efectúa un reenvío a los artículos 222 a 226 CPP, reguló de manera expresa las condiciones de procedencia de la interceptación de comunicaciones y de otros medios técnicos de investigación. En efecto, se requiere que la investigación de los respectivos delitos haga "imprescindible" la utilización de estas medidas, idea que derivaría del principio de prohibición de exceso[108]. En nuestra opinión, tal referencia del legislador alude a una de las proyecciones del principio de proporcionalidad, a saber, la de necesidad

[108] *Cfr*. Horvitz, María Inés y López, Julián. *Derecho Procesal Penal Chileno*, tomo I, reimpresión de la 1ª ed. Santiago: Editorial Jurídica de Chile (2017), p. 529 con referencias ulteriores.

de la medida. En ese sentido, el uso de tales diligencias intrusivas no puede constituir el primer recurso a ser empleado para la indagación del delito informático. Por ello, existiendo la alternativa de otras diligencias que no afecten o que afecten en menor medida derechos fundamentales, ellas deben preferirse por sobre la interceptación de comunicaciones y la utilización de otros medios técnicos de investigación.

Tratándose de una diligencia intrusiva de investigación, resulta destacable que el legislador haya establecido de manera expresa el presupuesto material para su procedencia, a saber, que "existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en [los artículos 1º, 2º, 3º, 4º, 5º y 7º de la ley]". Esta exigencia supone que el Ministerio Público, previo a la solicitud que formule ante el Juez de Garantía, a fin de obtener la autorización judicial respectiva, cuente con antecedentes relativos a la existencia de un delito informático y a la intervención en dicho delito, de un modo penalmente relevante, de uno o más imputados. Desde luego, el estándar requerido en la demostración del hecho punible y de la participación de quien corresponda no es equivalente al que se demanda para condenar; antes bien, basta con la concurrencia de indicios que permitan dar por establecida la existencia del hecho y de la intervención indicados.

Por otra parte, resulta criticable que el legislador, al regular el presupuesto de aplicación de tales diligencias intrusivas, aluda tanto a la comisión como a la preparación del hecho, por cuanto ello podría habilitar a la autorización de esas diligencias cuando los delitos informáticos respectivos se encuentren en la etapa de los actos preparatorios, *v. gr.*, proposición o conspiración. Sin embargo, la interpretación señalada no resulta admisible en atención a que el legislador, tratándose de los delitos informáticos, no sanciona los actos preparatorios, ajustándose la no punición de estos a las reglas generales. A mayor abundamiento, cabe destacar que el legislador excluyó expresamente de la procedencia de estas técnicas especiales de investigación al delito previsto en el artículo 8º (abuso de los dispositivos), que es el único que sanciona formas de preparación de delitos informáticos como tipo penal autónomo. En consecuencia, a pesar de la referencia a la preparación que prevé la norma en comento, el Juez de Garantía sólo podrá acceder a la solicitud del Ministerio Público en el evento de que este demuestre que el hecho investigado se encuentra a lo menos en fase de tentativa[109]. Finalmente, incluir a los actos

[109] En términos similares, Horvitz y López. *Derecho Procesal Penal Chileno*…, ob. cit., p. 528.

preparatorios en el presupuesto de aplicación de dichas diligencias iría en abierta contradicción de la proporcionalidad que subyace a la exigencia, según la cual, la investigación de los respectivos delitos ha de hacer "imprescindible" la utilización de tales técnicas.

En otro orden de cosas, el artículo 12 inciso segundo de la Ley Nº 21.459 establece algunos requisitos formales aplicables a las diligencias en comento. En ese sentido, la orden que las disponga "deberá indicar circunstanciadamente el nombre real o alias y dirección física o electrónica del afectado por la medida y señalar el tipo y la duración de la misma". Además, se dispone que el Juez de Garantía podrá prorrogar la duración de la orden impartida, en cuyo caso "deberá examinar cada vez la concurrencia de los requisitos [ya señalados]".

"Interceptar" (una comunicación), según el sentido natural y obvio de dicha expresión, contenido en el DRAE, puede entenderse como apoderarse de las señales que están siendo transmitidas desde un dispositivo a otro. De forma análoga, es posible interpretar dicho concepto como equivalente al de captar, por medios técnicos, informaciones que se intercambian entre tales dispositivos.

En relación con dicha medida, una de las primeras cuestiones que puede plantearse es el significado que cabe atribuir a la cláusula "interceptación y grabación de (…) comunicaciones telefónicas o de *otras formas de telecomunicación*" (cursivas agregadas). Una "telecomunicación", según el DRAE, es un "[s]istema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos". El término "telecomunicación" se encuentra asimismo definido en el artículo 1º de la Ley Nº 18.168, General de Telecomunicaciones, de acuerdo con el cual, para los efectos de dicha ley, "se entenderá por telecomunicación toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos e informaciones de cualquier naturaleza, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos". A nuestro juicio, pese a que la norma circunscribe expresamente su ámbito de aplicación, la definición de telecomunicación que indica perfectamente puede aplicarse al contexto que nos ocupa, a partir de una interpretación sistemática de las normas que rigen las materias en comento.

En ese orden de ideas, es posible subsumir en dicha cláusula tanto las transmisiones que se emiten por radio, por televisión y, especialmente, a través de internet, que constituye uno de los ámbitos más propicios para la perpetración de delitos informáticos. Tanto es así, que muchos autores identifican a la criminalidad informática con aquella que se lleva a cabo a través de internet, en cuyo caso suele emplearse el concepto de cibercriminalidad para

aludir a esa clase de ilícitos[110]. Pero, incluso de no aceptarse tal identificación, es evidente que internet constituye un contexto paradigmático de comisión de dichas figuras delictivas y, en ese sentido, el ámbito de mayor incidencia práctica de los delitos informáticos[111].

Desde un punto de vista más específico, es posible sostener que se incluyen en el concepto de telecomunicación, a través de internet, toda clase de mensajes de texto, audio, imagen o video que se intercambien por redes sociales como Instagram, Facebook, LinkedIn, TikTok, o bien, mediante aplicaciones para teléfonos móviles como WhatsApp, Telegram, Signal, entre otros.

En lo que respecta al recurso de otros medios técnicos de investigación, ante el silencio de la Ley Nº 21.459, debemos entender que dicha medida se refiere a aquella regulada en el artículo 226 CPP, disposición que posibilita que el Juez de Garantía ordene, a petición del Ministerio Público, "la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos". El juez también "podrá disponer la grabación de comunicaciones entre personas presentes".

Como se indicó *supra*, esta diligencia, en el ámbito de la criminalidad informática, presenta la particularidad de que no tiene que utilizarse, necesariamente, frente a la comisión de un hecho que merezca la pena de crimen, a diferencia de lo que establece el artículo 226 CPP como regla general. Ello es así, pues si bien la nueva ley efectúa una remisión a los artículos 222, 223, 224, 225 y 226 CPP, también indica que tales diligencias podrán aplicarse, genéricamente, frente a la comisión de los delitos informáticos más graves que regula la Ley Nº 21.459.

Por otra parte, dado que el ámbito de realización de esta técnica de investigación no aparece precisado por el legislador, será posible emplearla tanto en términos físicos como digitales. Así, por ejemplo, sería posible grabar una conversación que dos sujetos mantienen a través de una videollamada que se realiza mediante una red social, sea que se efectúe porque existe un micrófono o cámara ocultos en el lugar en que se entabla la conversación, sea que se acceda al sistema informático desde el cual ella se verifica.

---

110 Véase, en ese sentido, por ejemplo, Cárdenas, Claudia. "El lugar de comisión de los denominados ciberdelitos", en *Revista Política Criminal*, Nº 6 (2008), pp. 2 y ss.; y Romeo, Carlos. "Capítulo 1: De los delitos informáticos al cibercrimen…", ob. cit., pp. 9-10.

111 Circunstancia que ha llevado a muchos autores a preferir el concepto de "cibercrimen" por sobre el de "delito informático", precisamente, por el papel que internet juega en la comisión de la primera categoría delictiva referida. *Vid*., respecto de la evolución terminológica en esta materia, como consecuencia de la evolución del fenómeno criminal que subyace a ella, Miró. *El cibercrimen*…, ob. cit., pp. 34 y ss.

c) Agentes encubiertos

El agente encubierto constituye una figura regulada en diversos cuerpos legales, por ejemplo, en la Ley Nº 20.000, sobre tráfico ilícito de estupefacientes y sustancias psicotrópicas. En términos generales, un agente encubierto es un funcionario policial que simula su identidad oficial y se infiltra en organizaciones criminales o meras agrupaciones con propósitos delictivos[112], "con el objetivo de identificar a los participantes, reunir información y recoger antecedentes necesarios para la investigación"[113].

No obstante, la Ley Nº 21.459 establece una regulación particular del agente encubierto, que considera las características propias de la criminalidad informática. En efecto, el artículo 12 inciso tercero de dicha ley posibilita a los funcionarios policiales que actúan en esa calidad, a actuar bajo identidad supuesta, en comunicaciones mantenidas en canales cerrados de comunicación. De acuerdo con lo señalado, la ley regula un "agente encubierto cibernético" o un "ciber-agente encubierto", que el legislador también denomina "agente encubierto en línea" (artículo 12 inciso tercero), sujeto cuyas actuaciones se concretarán a través de sistemas informáticos y muy, especialmente, mediante internet. En ese sentido, debe destacarse que la regulación no se haya limitado a reproducir aquella que se contiene en otros cuerpos legales de índole penal.

Ahora bien, a pesar de que es imaginable que un agente encubierto se introduzca "físicamente" en una organización delictual, orientada a la comisión de delitos informáticos, la ley regula al agente encubierto del ámbito informático en otros términos, los que deben interpretarse restrictivamente, toda vez que nos encontramos ante diligencias limitativas de derechos fundamentales que, de acuerdo con el artículo 5º CPP, no pueden aplicarse de forma analógica[114]. Por lo tanto, se excluye la intervención del ciber-agente encubierto en términos físicos. Del mismo modo, atendida la inexistencia de otras normas que amplíen la intervención policial en la investigación de delitos informáticos, el referido sería el acotado ámbito en el que tendría reconocimiento legal expreso el agente encubierto cibernético.

---

112 Véase Riquelme, Eduardo. "El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo", en *Polítca Criminal*, Nº 2 (2006), p. 8.

113 Artículo 25 inciso segundo, Ley Nº 20.000.

114 En ese sentido, a apropósito de las medidas cautelares, Marín, Juan Carlos. "Las medidas cautelares personales en el nuevo Código procesal penal chileno", en *Revista de Estudios de la Justicia*, Nº 1 (2002), p. 19.

Se puede vincular con el ciber-agente encubierto el denominado "ciber-patrullaje", supuesto que comprende, de acuerdo con Martín Ríos, a un "conjunto de técnicas" que apuntan a "detectar actividad ilegal en la red y descubrir a los delincuentes", además "de prevenir la perpetración de delitos"[115]. Según dicha autora, el ciber-patrullaje "no se limita al monitoreo de las redes, sino que también comprende la obtención y recolección de información", así como el "almacenamiento y análisis del contenido que existe en ellas"[116].

De acuerdo con la definición indicada, el ciber-patrullaje podría implicar dos órdenes de comportamientos que es preciso diferenciar. Por una parte, es posible que él se limite, por ejemplo, a un rastreo realizado en redes abiertas, que supone vigilar la actividad de sujetos en fuentes "plenamente accesibles para el usuario medio (chats […] [o] foros de carácter abierto, redes sociales, plataformas digitales, etc.)"[117]. Por otra parte, es posible que el ciber-patrullaje implique un acceso a sistemas informáticos que no se encuentran abiertos al público y que están protegidos por alguna clase de barrera técnica, situación que normalmente se va a verificar en el contexto de la investigación de un eventual delito.

A nuestro juicio, el primer supuesto de ciber-patrullaje, que podemos denominar preventivo, no resulta problemático y se enmarca en las labores de los organismos que colaboran en la prevención y persecución de comportamientos ilícitos, que no requieren autorización del Juez de Garantía. En cambio, el segundo caso de ciber-patrullaje, que podemos catalogar de intrusivo, sí genera dificultades relacionadas con el respeto a diversos derechos fundamentales que podrían resultar afectados.

En principio, en nuestro sistema jurídico, la única manera en que podría recabarse válidamente información para efectos de indagar la comisión de un delito informático, en el marco de un ciber-patrullaje intrusivo, es a través de la figura del agente encubierto. Por lo tanto, la información proveniente de un ciber-patrullaje realizado fuera de los márgenes del ciber-agente encubierto podría dar lugar a un supuesto de prueba ilícita. Así ocurriría en el caso en que el ciber-patrullaje implique el ingreso a un sistema informático con fines

115 Martín Ríos, Pilar. "Empleo de *big data* y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras", en *Revista de Internet, Derecho y Política*, Nº 36 (2022), p. 3.

116 *Idem*.

117 Zaragoza. "Ciberpatrullaje e investigación tecnológica en la red…", ob. cit., p. 211.

de mero control o vigilancia, sin que aún exista un ilícito conocido y un procedimiento penal iniciado.

No obstante, dicha idea podría ser matizada a partir de lo establecido en el artículo 9º CPP, que da cabida en forma amplia a diligencias investigativas limitativas de derechos, siempre que el organismo persecutor actúe previamente autorizado por el Juez de Garantía. Consiguientemente, y entendiendo que el artículo 9º es aplicable supletoriamente para la investigación de delitos informáticos, en tanto norma de carácter general, sería posible sostener que el ciber-patrullaje, que se realiza en el marco de un proceso penal ya iniciado, podría quedar incluido en dicha norma de carácter general.

Además de lo señalado respecto de su ámbito de aplicación, el agente encubierto en línea debe cumplir con las restantes condiciones que establece el artículo 12 inciso tercero de la nueva ley de delitos informáticos, a saber: autorización judicial previa, existencia de una investigación penal en curso y propósito legítimo.

En lo que respecta a la exigencia de autorización judicial, el ciber-agente encubierto se diferencia de lo previsto en otros contextos en que se regula la figura en comento, en los que basta únicamente autorización del Ministerio Público. Así ocurre tratándose del agente encubierto en la investigación de los delitos tipificados en la Ley Nº 20.000. En virtud de la exigencia prevista en la Ley Nº 21.459, no queda duda alguna de que el ciber-agente encubierto constituye un supuesto de diligencia intrusiva o limitativa de derechos fundamentales que sí requiere autorización judicial previa. Ella se rige por lo dispuesto en el artículo 9º, norma según la cual la autorización, por regla general, debe ser otorgada por escrito y sólo en casos urgentes puede obtenerse por otros medios, como teléfono, correo electrónico, etc.

La necesidad de que exista una investigación en curso se infiere de lo dispuesto en la última parte del artículo 12 inciso tercero de la nueva ley de delitos informáticos que, a la hora de establecer la exención de responsabilidad del agente, por los delitos en que debe incurrir o que no haya podido impedir, prevé que ellos sean una consecuencia necesaria del desarrollo de la "investigación". Esto supone, además, que la investigación no podría iniciarse a través de la técnica del ciber-agente encubierto; tampoco sería posible que la responsabilidad penal se funde exclusivamente en el empleo de esta técnica especial, pues tendrían que haber habido otros antecedentes, cuya fuente sea distinta a la del agente encubierto en línea.

La exigencia de un propósito legítimo se encuentra explicitada por el legislador, al señalar que el ciber-agente encubierto debe actuar para "esclarecer los hechos tipificados como delitos" en la ley, "establecer la identidad y par-

ticipación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos". Por lo tanto, cualquier otra finalidad para la cual se emplee esta figura quedará fuera de los márgenes de la ley como técnica de investigación, así como para los efectos de una eventual exención de responsabilidad del agente, de acuerdo con lo que se señalará *infra*.

El incumplimiento de los requisitos señalados, *v. gr.*, la falta de autorización judicial previa dará lugar a un supuesto de prueba ilícita que, por ende, no podrá utilizarse en juicio en contra de los presuntos responsables del delito informático de que se trate, quienes por esa vía quedarán exentos de castigo. Ahora bien, el incumplimiento de los requisitos referidos podría dar origen a la responsabilidad penal del propio agente, en especial, cuando falte un propósito legítimo para emplear la medida. Sin embargo, no puede descartarse la posibilidad de que el ciber-agente encubierto no actúe en términos penalmente relevantes, por ejemplo, en caso de existir un error de prohibición o una causal de inexigibilidad de otra conducta. Con todo, para que el agente quede exento de responsabilidad penal también deberá darse cumplimiento a lo que establece el artículo 12 inciso tercero parte final, de acuerdo con el cual, "[e]l agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma". En este caso, los terceros que actúen bajo el influjo del ciber-agente encubierto sí responderán por el o los delitos que se les atribuyan.

Finalmente, no debe confundirse al agente encubierto en línea con la figura del agente provocador. El primero, como se puede colegir de lo señalado *supra*, ejerce su función respecto de una realidad delictiva preexistente, la que queda en evidencia a partir de la información que este logra recabar. En cambio, el agente provocador, de un modo equivalente al de un instigador, crea en otros un propósito criminal, el cual se materializa en la perpetración de uno o más delitos en el plano de la realidad (delitos provocados). No obstante, dicho sujeto es un agente policial que normalmente actúa a través de un engaño[118] (*v. gr.*, que está interesado en adquirir droga), originando "de un modo artificial una infracción penal que antes no existía"[119]. A nuestro juicio, una figura como el agente provocador no resulta admisible en el marco de un Estado democrático

[118] Véase, matizando el sentido peyorativo del empleo de engaño en este contexto, Sánchez, Raúl. "El agente encubierto informático", en *La ley penal*, N° 118 (2016), apartado II.

[119] Joshi, Ujala. *Los delitos de tráfico de drogas I. Un estudio analítico del art. 368 CP.* Barcelona: Bosch (1999), p. 288.

de derecho, modelo que no es compatible con que los agentes estatales inciten a la perpetración de delitos.

d) Reglas relativas al comiso (artículo 13)

La nueva ley de delitos informáticos contempla normas especiales en materia de comiso. En efecto, el artículo 13 de la Ley Nº 21.459, establece lo siguiente:

> "Sin perjuicio de las reglas generales, caerán especialmente en comiso los instrumentos de los delitos penados en esta ley, los efectos que de ellos provengan y las utilidades que hubieren originado, cualquiera que sea su naturaleza jurídica.
> Cuando por cualquier circunstancia no sea posible decomisar estas especies, se podrá aplicar el comiso a una suma de dinero equivalente a su valor, respecto de los responsables del delito. Si por la naturaleza de la información contenida en las especies, éstas no pueden ser enajenadas a terceros, se podrá ordenar la destrucción total o parcial de los instrumentos del delito y los efectos que de ellos provengan".

Pese a que esta norma se encuentra entre las disposiciones relativas al "Procedimiento", que se contienen en la Ley Nº 21.459, el comiso no constituye una materia de índole procesal, toda vez que corresponde a una de las penas aplicables a los delitos. Por lo tanto, ella debió ubicarse en otra sección de la nueva ley de delitos informáticos.

Como podrá notarse, la norma contenida en el inciso primero del artículo 13 resulta superflua, toda vez que no establece una regulación que realmente se aparte de lo que indica el CP. Efectivamente, el artículo 31 de dicho cuerpo legal dispone que "[t]oda pena que se imponga por un crimen o simple delito, lleva consigo la pérdida de los efectos que de él provengan y de los instrumentos con que se ejecutó, a menos que pertenezcan a un tercero no responsable del crimen o simple delito"; mientras que el artículo 21, del mismo Código, indica que constituye una pena común a los crímenes, simples delitos y faltas la "[p]érdida o comiso de los instrumentos o efectos del delito".

Distinta es la situación de lo dispuesto en el inciso segundo del artículo 13 de la nueva ley. Dicha norma se hace cargo de la inmaterialidad del objeto sobre el que recaen los delitos informáticos, o sea, datos; así como de la eventual inmaterialidad de los instrumentos o efectos de esa clase de ilícitos. Además, como se trata, entre otras cosas, de objetos cuya ubicación no siempre es fácil de precisar o cuyo acceso puede ser complejo para el órgano persecutor penal, la ley establece, haciendo excepción a las reglas generales, la posibilidad

de aplicar el comiso "de valor"[120], por una suma equivalente al valor de los instrumentos, efectos o utilidades.

Esta última cláusula podría ofrecer problemas cuando los instrumentos o efectos del delito no tengan un valor de mercado. Por ejemplo, si se tratara de una falsedad informática que recae sobre una autorización administrativa, el documento electrónico adulterado podría calificarse como efecto del delito, sin embargo, no es claro cómo podría establecerse su valor pecuniario[121].

e) Tratamiento de los antecedentes de la investigación contenidos en formato electrónico (artículo 14)

De acuerdo con el artículo 14 de la Ley Nº 21.459,

> "[s]in perjuicio de las reglas generales, los antecedentes de investigación que se encuentren en formato electrónico y estén contenidos en documentos electrónicos o sistemas informáticos o que correspondan a datos informáticos, serán tratados en conformidad a los estándares definidos para su preservación o custodia en el procedimiento respectivo, de acuerdo a las instrucciones generales que al efecto dicte el Fiscal Nacional".

Según la Historia de la Ley Nº 21.459, esta norma se sustenta en brindar un tratamiento especial a los antecedentes investigativos relacionados con los delitos informáticos, que consistan en datos informáticos, atendido su "carácter volátil" y su "fácil destructibilidad"[122].

Durante la tramitación legislativa, a propósito del control de constitucionalidad, el Tribunal Constitucional hizo presente que lo dispuesto en el artículo 14 de la nueva ley de delitos informáticos se reduce exclusivamente a la preservación o custodia de los datos en el marco de una investigación penal. Ello es así, puesto que la protección de los datos personales fuera de ese ámbito requiere –conforme con el artículo 19 Nº 4 CPR– una regulación de rango legal, exigencia que no satisface la normativa proveniente del Fiscal

[120] Véase, desde un punto de vista más general, Hernández, Héctor. "Art. 31", en Couso, Jaime y Hernández, Héctor (directores). *Código Penal Comentado. Parte general, Doctrina y Jurisprudencia*. Santiago: Abeledo Perrot (2011), p. 484 con referencias ulteriores.

[121] A nuestro juicio, en tanto estamos analizando un supuesto de comiso de valor, que alude expresamente a "una suma de dinero" equivalente al valor de los instrumentos, efectos o ganancias, no podrían entrar en consideración otra clase de valores, *v. gr.*, el valor de afección.

[122] Historia de la Ley Nº 21.459, p. 7.

Nacional, de acuerdo con el artículo 91 CPR, a la luz del cual, sus oficios pueden calificarse como un reglamento en sentido laxo[123].

El artículo 14 de la Ley Nº 21.459 se relaciona con una modificación legal introducida al CPP, al que se agregó un artículo 218 bis[124], titulado "Preservación provisoria de datos informáticos", del siguiente tenor:

> "El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquier proveedor de servicio, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un periodo de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia".

La norma transcrita permite que el Ministerio Público directamente, o sea, sin intervención del Juez de Garantía, requiera a proveedores de servicios la conservación o protección de datos informáticos que puedan ser relevantes para la investigación de alguno de los delitos tipificados en la Ley Nº 21.459, hasta la obtención de la autorización judicial respectiva.

Como es sabido, la entrega de dichos datos constituye una diligencia intrusiva, que podría afectar, entre otros, el derecho fundamental a la protección de la vida privada, razón por la que su práctica requiere de autorización judicial.

Al mismo tiempo, ya que la obtención de dicha autorización supone que el Ministerio Público desarrolle una mínima actividad investigativa, para justificar su solicitud, es que se hace necesario establecer una norma como la indicada, que permita que tales datos no desaparezcan mientras se obtiene la referida autorización. Efectivamente, durante el periodo que media entre el inicio de la investigación y la obtención de la autorización por parte del Juez de Garantía, los datos en cuestión podrían desaparecer, atendido su carácter volátil y fácilmente destructible, razón que justifica la consagración expresa de la regla en comento.

---

123 *Vid*., Historia de la Ley Nº 21.459, p. 423.

124 Cabe destacar que según el artículo segundo transitorio de la Ley Nº 21.459, su artículo 18, que es el que establece las modificaciones al CPP –y, entre ellas, introduce el artículo 218 bis– "comenzará a regir transcurridos seis meses desde la publicación en el Diario Oficial de un reglamento dictado por el Ministerio de Transportes y Telecomunicaciones, suscrito además por el Ministro del Interior y Seguridad Pública". El precepto indicado establece asimismo que dicho reglamento "deberá dictarse dentro del plazo de seis meses, contado desde la publicación de la presente ley en el Diario Oficial".

Esta disposición también se explica por los tiempos involucrados en el recurso a los mecanismos tradicionales de cooperación internacional[125], factor que igualmente podría poner en riesgo el éxito de la persecución penal por delitos informáticos.

Bibliografía

Aldoney, Rodrigo. "La revelación de secretos de empresa - Posibles déficits punitivos y posibilidades dogmáticas de su superación", en Van Weezel, Alex (editor). *Humanizar y renovar el Derecho penal: Estudios en memoria de Enrique Cury*. Santiago: Thomson Reuters (2013), pp. 977-1015.

Armenteros, Miguel. *Los delitos de falsedad documental*. Granada: Comares (2011).

Bullemore, Vivian y MacKinnon, John. *Curso de Derecho Penal*, *Parte Especial*, tomo III, 5ª ed. Santiago: Ediciones Jurídicas de Santiago (2021).

_____. *Curso de Derecho Penal*, *Parte Especial*, tomo IV, 5ª ed. Santiago: Ediciones Jurídicas de Santiago (2021).

Becker, Sebastián y Viollier, Pablo. "La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley Nº 19.223", en *Revista de Derecho Universidad de Concepción*, vol. 88, Nº 248 (2020), pp. 75-112.

Callejas Espinoza, Gustavo. "*Ethical Hacking*: Conciencia de Seguridad", en *Revista PGI*, Nº 7 (2021), pp. 43-46.

Cárdenas, Claudia. "El lugar de comisión de los denominados ciberdelitos", en Revista *Política Criminal*, Nº 6 (2008), pp. 1-14.

Choclán, José Antonio. "Capítulo 3: Infracciones patrimoniales en los procesos de transferencia de datos", en Romeo, Carlos (coordinador). *El cibercrimen: nuevos retos jurídico-penales*, *nuevas respuestas político-criminales*. Granada: Comares (2006), pp. 69-95.

Corcoy, Mirentxu. "Capítulo IX. De los daños", en Corcoy, Mirentxu y Mir, Santiago (directores), *Comentarios al Código Penal*. Valencia: Tirant lo Blanch (2015), pp. 943-959.

Cury, Enrique. *Derecho Penal*, *Parte General*, 10ª ed. Santiago: Ediciones UC (2011).

[125] Véase Dupuy, Daniela y Kiefer, Mariana. "Datos e innovación tecnológica", en Dupuy, Daniela y Corvalán, Juan (directores). *Cibercrimen III*. Montevideo-Buenos Aires: B de f (2020), p. 355.

Dupuy, Daniela y Kiefer, Mariana. "Datos e innovación tecnológica", en Dupuy, Daniela y Corvalán, Juan (directores), *Cibercrimen III*. Montevideo-Buenos Aires: B de f (2020), pp. 353-396.

Etcheberry, Alfredo. *Derecho Penal*, *Parte General*, tomo I, reimpresión de la 3ª ed. Santiago: Editorial Jurídica de Chile (2010).

_____. *Derecho Penal*, *Parte General*, tomo II, reimpresión de la 3ª ed. Santiago: Editorial Jurídica de Chile (2010).

Garrido, Mario. *Derecho Penal*, *Parte General*, tomo I, reimpresión de la 2ª ed. Santiago: Editorial Jurídica de Chile (2018).

_____. *Derecho Penal*, *Parte Especial*, tomo IV, reimpresión de la 4ª ed. Santiago: Editorial Jurídica de Chile (2011).

Hernández, Héctor. "Art. 1º", en Couso, Jaime y Hernández, Héctor (directores). *Código Penal Comentado*. *Parte general*, *Doctrina y Jurisprudencia*. Santiago: Abeledo Perrot (2011), pp. 7-105.

_____. "Art. 31", en Couso, Jaime y Hernández, Héctor (directores). *Código Penal Comentado*. *Parte general*, *Doctrina y Jurisprudencia*. Santiago: Abeledo Perrot (2011), pp. 482-485.

_____. "Tratamiento de la criminalidad informática en el derecho penal chileno: Diagnóstico y propuestas", *Informe solicitado por la División Jurídica del Ministerio de Justicia*, *Inédito* (2001), pp. 1-26.

Horvitz, María Inés y López, Julián. *Derecho Procesal Penal Chileno*, tomo I, reimpresión de la 1ª ed. Santiago: Editorial Jurídica de Chile (2017).

Jaquet-Chiffelle, David-Olivier y Loi, Michele. "Chapter 9: Ethical and Unethical Hacking", en Christen, Markus; Gordijn, Bert y Loi, Michele (editores). *The Ethics of Cybersecurity*. Cham: Springer Open (2020), pp. 179-204. Disponible en: https://library.oapen.org/bitstream/handle/20.500.12657/22489/1007696.pdf.

Jijena, Renato. "Debate parlamentario en el ámbito del Derecho informático. Análisis de la Ley Nº 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, vol. XV (1993-1994), pp. 347-401.

Joshi, Ujala, *Los delitos de tráfico de drogas I. Un estudio analítico del art. 368 CP*. Barcelona: Bosch (1999).

Kochheim, Dieter. *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik*. München: Beck (2015).

Künsemüller, Carlos. "§ 4. De las circunstancias que agravan la responsabilidad criminal: Artículos 12 y 13", en Politoff, Sergio y Ortiz, Luis (directores).

Texto y comentario del Código Penal chileno, tomo I, Libro Primero - Parte General, reimpresión de la 1ª ed. Santiago: Editorial Jurídica de Chile (2010), pp. 187-227.

Mañalich, Juan Pablo. "Condiciones generales de la punibilidad", en *Revista de Derecho* (Universidad Adolfo Ibáñez), Nº 2 (2005), pp. 396-405.

Marín, Juan Carlos. "Las medidas cautelares personales en el nuevo Código procesal penal chileno", en *Revista de Estudios de la Justicia*, Nº 1 (2002), pp. 9-54.

Martín Ríos, Pilar. "Empleo de *big data* y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras", en *Revista de Internet*, *Derecho y Política*, Nº 36 (2022), pp. 1-13.

Matus, Jean Pierre. "§ 3. De las circunstancias que atenúan la responsabilidad criminal: Artículo 11", en Politoff, Sergio y Ortiz, Luis (directores). *Texto y comentario del Código Penal chileno*, *tomo I*, *Libro Primero - Parte General*, *reimpresión de la 1ª ed*. Santiago: Editorial Jurídica de Chile (2010), pp. 165-186.

Matus, Jean Pierre y Ramírez, María Cecilia. *Manual de Derecho Penal Chileno*, *Parte Especial*, 4ª ed. Valencia: Tirant lo Blanch (2021).

Maurushat, Alana. *Ethical Hacking*. S.l.: University of Ottawa Press (2019).

Mayer, Laura. "Capítulo X: Delitos contra intereses patrimoniales", en Rodríguez, Luis (director). *Derecho Penal*, *Parte Especial*, *Vol. II*. Valencia: Tirant lo Blanch (2022), pp. 391-571.

_____. "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", en *Ius et Praxis*, vol. 24, Nº 1 (2018), pp. 159-206.

Mayer, Laura y Oliver, Guillermo. "El delito de fraude informático: Concepto y delimitación", en *Revista Chilena de Derecho y Tecnología*, vol. 9, Nº 1 (2020), pp. 151-184.

Mayer, Laura y Vera, Jaime. "Agravante de abuso de confianza", en González Jara, Manuel Ángel (coordinador). *Circunstancias atenuantes y agravantes en el Código Penal chileno*. Santiago: Ediciones Jurídicas de Santiago (2020), pp. 213-237.

_____. "El delito de espionaje informático: concepto y delimitación", en *Revista Chilena de Derecho y Tecnología*, vol. 9, Nº 2 (2020), pp. 221-256.

_____. "El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho penal chileno", en *Política Criminal*, vol. 14, Nº 27 (2019), pp. 419-455.

_____. "La falsificación informática: ¿Un delito necesario?", en *Revista Chilena de Derecho y Tecnología*, vol. 11, Nº 1 (2022), pp. 261-286.

_____. "La nueva regulación del delito de uso fraudulento de tarjetas de pago y transacciones electrónicas", en *Revista de Ciencias Penales*, Sexta Época, vol. XLVII (2021), pp. 519-558.

Medina, Gonzalo. "Estructura típica del delito de intromisión informática", en *Revista Chilena de Derecho y Tecnología*, vol. 3, Nº 1 (2014), pp. 79-99.

Miró, Fernando. *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid *et al.*: Marcial Pons (2012).

_____. "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del *phishing*", en *Revista Electrónica de Ciencia Penal y Criminología*, Nº 15-12 (2013), pp. 1-56.

Oliver, Guillermo. "Capítulo IX: Delitos contra la propiedad", en Rodríguez, Luis (director). *Derecho Penal*, *Parte Especial*, vol. II. Valencia: Tirant lo Blanch (2022), pp. 213-389.

Owen, Ken y Head, Milena. "Motivation and Demotivation of Hackers in Selecting a Hacking Task", en *Journal of Computer Information Systems* (2022), DOI: 10.1080/08874417.2022.2081883 (artículo aceptado para publicación).

Politoff, Sergio; Matus, Jean Pierre y Ramírez, María Cecilia. *Lecciones de Derecho Penal Chileno*, *Parte Especial*, reimpresión de la 2ª ed. Santiago: Editorial Jurídica de Chile (2011).

Riquelme, Eduardo. "El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo", en *Política Criminal*, Nº 2 (2006), pp. 1-17.

Riquert, Marcelo. "La responsabilidad penal de las personas jurídicas en Argentina y el 'Ciberconvenio' de Budapest", en Dupuy, Daniela (directora), *Cibercrimen II*. Montevideo-Buenos Aires: B de f (2020), pp. 443-482.

Rodríguez, Luis. "Capítulo VIII: Delitos contra la indemnidad sexual", en Rodríguez, Luis (director), *Derecho Penal*, *Parte Especial*, vol. II. Valencia: Tirant lo Blanch (2022), pp. 79-210.

Rodríguez, Luis y Mayer, Laura. "Alevosía genérica y alevosía específica", en Acevedo, Nicolás; Collado, Rafael y Mañalich, Juan Pablo (coordinadores). *La justicia como legalidad. Estudios en homenaje a Luis Ortiz Quiroga*. Santiago: Thomson Reuters (2020), pp. 693-720.

Rojas, Luciano. "Capítulo I. Responsabilidad penal de las personas jurídicas. Consideraciones generales", en Artaza, Osvaldo (director). Compliance *penal: Sistemas de prevención de la corrupción*. Santiago: DER (2019), pp. 7-34.

Romeo, Carlos. "Capítulo 1: De los delitos informáticos al cibercrimen: Una aproximación conceptual y político-criminal", en Romeo, Carlos (coordinador). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Comares (2006), pp. 1-42.

Sánchez, Raúl. "El agente encubierto informático", en *La ley penal*, Nº 118 (2016).

Silva Silva, Hernán. "La cooperación eficaz de la ley de drogas", en *Revista de Derecho y Ciencias Penales*, Nº 17 (2011), pp. 211-223.

Tiedemann, Klaus. *Wirtschaftsstrafrecht Besonderer Teil*, 3ª ed. München: Vahlen (2011).

Zaragoza, Javier. "Ciberpatrullaje e investigación tecnológica en la red: Una aproximación a la inteligencia artificial desde el punto de vista de la investigación y represión de hechos ilícitos", en Dupuy, Daniela y Corvalán, Juan (directores), *Cibercrimen III*. Montevideo-Buenos Aires: B de f (2020), pp. 209-240.

Jurisprudencia

CA de Antofagasta, 13 de mayo de 2008, rol Nº 82-2008.

CA de Copiapó, de 23 de junio de 2015, rol Nº 109-2015.