Comentario a 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

Valeria Jélvez Gallegos*

I. Introducción

La reciente dictación de 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 sobre la Ciberdelincuencia del Consejo de Europa ("Convenio" o "Convenio de Budapest") supone un cambio importante en la regulación de la ciberdelincuencia y de los delitos informáticos en general, los cuales han cobrado cada vez más protagonismo, convirtiéndose en un fenómeno delictual con mucha presencia a nivel nacional y mundial, fomentado no sólo por la constante evolución de sus medios de comisión, sino que incluso potenciado por la reciente pandemia[1].

Pese a recaer sobre un fenómeno de crecimiento exponencial en los últimos años, y a la obligación asumida por Chile de adecuar nuestra legislación al

* Abogada, Universidad de Chile. Magíster en Derecho Penal, Universidad de Talca y Universidad Pompeu Fabra. Abogada Asesora de la Unidad Especializada en Lavado de Activos, Delitos Económicos, Medioambientales y Crimen Organizado, Fiscalía Nacional.

[1] Ilustrativo del impacto de la pandemia por COVID-19 en la ciberdelincuencia es el Informe "Ciberdelincuencia: Efectos de la COVID-19", confeccionado por Interpol, en agosto de 2020, en el cual destacan entre sus conclusiones que "[l]os ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica a escala mundial… al mismo tiempo, las medidas de confinamiento impuestas en el mundo han propiciado una mayor dependencia de la conectividad y las infraestructuras digitales, lo que aumenta las oportunidades de llevar a cabo intrusiones o ataques cibernéticos." En: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19. En sentido similar, se grafica la importancia de este fenómeno delictual en el "Informe Resumido sobre las tendencias de la delincuencia a escala mundial", confeccionado por Interpol, en octubre de 2022, disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/Los-delitos-financieros-y-los-cometidos-por-Internet-son-los-que-mas-preocupan-a-la-policia-de-todo-el-mundo-segun-un-nuevo-informe-de-INTERPOL.

Convenio de Budapest, la mencionada ley no fue de fácil tramitación, tardando casi cuatro años desde el ingreso del proyecto hasta su publicación. En esta tramitación participaron activamente no sólo parlamentarios y el Ejecutivo, sino que también diversas instituciones públicas, como el Ministerio Público, y actores de la sociedad civil, como distintas organizaciones especializadas en la materia. Todo este interés supuso que las discusiones fueran arduas y los consensos difíciles de lograr, pero la ley ya se encuentra publicada, correspondiendo ahora el análisis y aplicación de los preceptos que finalmente quedaron plasmados.

Sin duda su análisis y aplicación dará lugar a diversas discusiones que este trabajo no pretender abarcar a cabalidad, sino que más bien tiene por objeto esbozar un panorama general sobre esta nueva regulación, refiriendo el contexto y marco general de su promulgación tenido presente para su concepción, sus fundamentos, el análisis de algunos conceptos generales que son relevantes de tener a la vista y una revisión preliminar de las distintas disposiciones que contiene a nivel sustantivo. Todo ello con la finalidad de anunciar algunos lineamientos iniciales tanto para el estudio como para la aplicación de esta nueva normativa.

II. Contexto

Como lo señala el propio Mensaje, la Ley Nº 21.459 encuentra su fundamento en la necesidad de (i) resguardar "nuevos riesgos y ataques contra bienes jurídicos social y penalmente relevantes, algunos de los cuales no se encuentran protegidos desde la óptica penal"[2]; (ii) dar cumplimiento al contenido y compromisos internacionales adquiridos mediante el Decreto Nº 83 del Ministerio de Relaciones Exteriores, de fecha 27 de abril de 2017, que promulgó en nuestro país el Convenio de Budapest[3]; y (iii) actualizar la legislación vigente en Chile, plasmada en la Ley Nº 19.223, que tipifica figuras penales relativas a la informática ("Ley Nº 19.223") y las herramientas de persecución penal que han resultado insuficientes para una adecuada investigación de este tipo de delitos[4].

[2] Historia de 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, p. 3.

[3] Historia de la Ley Nº 21.450, ob. cit., p. 3.

[4] Historia de la Ley Nº 21.450, ob. cit., p. 4.

Si bien estos tres ejes tienen matices distintos, lo cierto es que se trata de una legislación detrás de la cual se encuentra la necesidad de actualizar la legislación vigente a esa fecha[5], contenida en la Ley Nº 19.223, la cual habiéndose publicado en el año 1993 no había sufrido modificación alguna pese a la constante evolución de los fenómenos delictuales que subyacen a la ciberdelincuencia en general. Esto había dado lugar a críticas tanto operativas como dogmáticas, tales como, "la existencia de problemas prácticos respecto de la aplicación de la ley, tratándose de normas de compleja aplicación y cuya cobertura resultó mayor a la que se propuso al momento de su dictación"[6], las dificultades técnicas en la investigación de algunos de estos hechos lo que tenía como consecuencia el desincentivo de su persecución[7], el constante debate sobre la inexistencia de un delito de fraude informático[8], entre otras, que urgían una modificación en la materia.

Sumado a lo anterior, la urgencia y punto de partida de esta actualización se reforzó al promulgarse el Convenio de Budapest, en el año 2017, a través del cual Chile se obligó a modificar su legislación vigente con el objeto de adecuarla a dicho instrumento. Ahora bien, la importancia del Convenio no es sólo haber servido como motor para la modificación legal, sino que, como veremos, sirvió de marco para las disposiciones específicamente contempladas en la ley, y por ello, en lo que sigue, resultará relevante referirnos a su objetivo y contenido, que posiblemente más de alguna herramienta interpretativa nos entregará. En este sentido recurriremos especialmente al Informe Explicativo del mismo convenio, el que puede facilitar la aplicación

[5] El proyecto de ley fue presentado con fecha 7 de noviembre de 2018.

[6] Lara, Juan Carlos; Martínez, Manuel; Viollier, Pablo. "Hacia una regulación de los delitos informáticos basada en la evidencia", en *Revista Chilena de derecho y Tecnología*, vol. 3, Nº 1 (2014), p. 102.

[7] Mayer, Laura. "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", en revista *Ius et Praxis*, Nº 1 (2018), p. 185.

[8] Si bien con discusiones relativas a esta afirmación. En el extremo, "… actualmente en nuestro Derecho penal, el acceso ilegítimo a cuentas corrientes de terceros, a través de la plataforma de Internet de una entidad bancaria con la finalidad de transferir los dineros depositados o los créditos contenidos en ellas, resulta increíblemente para los tiempos que corren atípico, sin que sea posible recurrir a ninguna figura alternativa…". Oxman, Nicolás. "Estafas informáticas a través de internet: acerca de la imputación penal del 'phishing' y el 'pharming'", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, vol. XLI (2013), p. 257. En el mismo sentido, Muñoz, Fernando. "Epistemología de la techne: a propósito del fraude informático", en *Revista Chilena de derecho y tecnología*, vol. 2, Nº 2 (2013), pp. 248-249.

de sus disposiciones[9], así como también a legislaciones comparadas que han adecuado su legislación al Convenio con anterioridad, como ocurre especialmente con España.

El Informe Explicativo del Convenio de Budapest señala expresamente que este tiene como finalidad primordial:

> "1) armonizar los elementos de los delitos de conformidad con el derecho sustantivo penal de cada país y las disposiciones conexas en materia de ciberdelincuencia; 2) establecer, de conformidad con el derecho procesal penal de cada país, los poderes necesarios de investigación y procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico; y 3) establecer un régimen rápido y eficaz de cooperación internacional"[10].

Los objetivos de este convenio fueron refrendados en el Mensaje del proyecto de ley que, como ya se señaló, tenía por objeto adecuar la normativa y reforzar las herramientas de persecución penal, haciéndose cargo de la naturaleza trasnacional de este tipo de fenómenos delictuales.

Cabe hacer presente que, pese a este interés plasmado en el Mensaje del proyecto de ley, este no abarcó todas las materias contempladas en el Convenio. Así, por ejemplo, el Convenio se refiere a (i) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; (ii) delitos informáticos; (iii) delitos relacionados con el contenido; (iv) delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines. La Ley Nº 21.459 incluyó solo aquellos mencionados en los numerales (i) y (ii), modificando figuras ya existentes e incorporando otras nuevas (dejando fuera los delitos relacionados con el contenido (vinculados a pornografía infantil), así como las infracciones a la propiedad intelectual y derechos afines), adoptó los conceptos de datos informáticos, sistemas informáticos y proveedor de servicios contemplados en el Convenio, consagró la responsabilidad penal de la persona jurídica y, con algunos temores, incorporó medidas procesales tendientes a facilitar la persecución penal. A todo esto nos referiremos en las páginas que siguen.

III. Algunos conceptos generales

Lo cierto es que los conceptos de ciberdelincuencia y delitos informáticos que hasta ahora se han utilizado sin precisión de su contenido, no son de fácil

[9] Informe explicativo del Convenio sobre la Ciberdelincuencia, coe.int/cybercrime, p. 55.

[10] Informe explicativo, ob. cit., pp. 63 y 64.

definición. En efecto, se trata de conceptos cuyo alcance ha sido discutido, lo cual puede generar equívocos en su utilización[11].

Respecto a estos conceptos, el Convenio, por una parte, entre las categorías de delitos refiere algunos que califica como delitos informáticos propiamente tales (como la falsificación y el fraude informático)[12], y por otra, en su Informe Explicativo, señala que las disposiciones relativas a los delitos y otras disposiciones conexas de la Sección 1 del Capítulo II, sobre Derecho penal sustantivo, se refieren al ámbito de la ciberdelincuencia de los delitos relacionados con el empleo de ordenadores[13].

La Organización de las Naciones Unidas[14], por su parte, propone una distinción entre delito cibernético en sentido estricto o delito informático y delito cibernético en sentido lato o delito relacionado con computadores[15]. El primero referido a "todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos" y el segundo, relativo a "todo comportamiento ilícito realizado por medio de un sistema o red informático, o en relación a ellos…"[16]; *i. e.*, realizando una distinción entre delitos "contra medios informáticos" y delitos cometidos "con medios informáticos"[17].

Esta distinción parecía plasmarse en la Ley Nº 19.223, respecto de la cual, aún sin definir los conceptos, por su contenido e historia, es posible concluir que "el propósito de la misma es el resguardo de los datos informáticos y de los sistemas que los contienen"[18]. En ese sentido, el concepto estricto de delito informático sería aquello protegido por la ley, entendiendo por tal la "criminalidad cometida 'respecto de' o 'contra' sistemas informáticos… (*v. gr.* Sabotaje

---

[11] Mayer, Laura. "El bien jurídico protegido en los delitos informáticos", en *Revista Chilena de Derecho*, vol. 44, Nº 1 (2017), p. 237. En sentido similar, 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 Universidad Católica de Valparaíso*, vol. XV, (1993-1994).

[12] Convenio sobre la Ciberdelincuencia, Título II, sección 1, Capítulo II, coe.int/cybercrime.

[13] Informe explicativo, ob. cit., p. 64.

[14] Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, Viena, 10 a 17 de abril de 2000.

[15] Lara; Martínez; Viollier, ob. cit., p. 104.

[16] Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, ob. cit., p. 5.

[17] Jijena, Renato. "La criminalidad informática: situación de lege data y lege ferenda en Chile", en *Informática y derecho: Revista iberoamericana de derecho informático*, Nº 3 (1992).

[18] Lara; Martínez; Viollier, ob. cit., p. 108.

o espionaje informático)"[19], es decir, "ha de tratarse de comportamientos que incidan en el software o soporte lógico, esto es, en los programas, instrucciones y reglas informáticas que permiten el procesamiento de datos"[20].

La nueva ley reorganiza e incorpora nuevas figuras a los delitos informáticos que se encontraban regulados en la antigua ley, adoptando los tipos penales en términos muy similares al Convenio, contemplando los delitos (i) de sabotaje informático, distinguiendo entre ataque a un sistema o a datos informáticos, (ii) de espionaje informático, (iii) de fraude informático, (iv) de falsificación informática, (v) abuso de dispositivos, e incorporando como novedad el delito de (vi) receptación de datos informáticos.

Adicionalmente, es útil advertir que la Ley Nº 21.459 adopta también las definiciones de conceptos relevantes para el análisis de los tipos penales recién anunciados. En efecto, se definen los conceptos de "datos informáticos", "sistema informático" y "proveedor de servicio", especialmente relevantes para estos efectos y tomados de casi idéntica forma desde el artículo 1 del Convenio de Budapest.

El artículo 15 de la nueva ley define como datos informáticos, "[t]oda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute su función". Esta definición, tomada desde el Convenio, supone afirmar que los datos informáticos que se procesan automáticamente pueden ser objeto de los delitos contemplado en el Convenio (y ahora en la ley que se analiza). Para esto, el Informe Explicativo explicita que por dato debe entender todo dato "en formato electrónico u otro formato que se preste a tratamiento informático directamente"[21], y a su vez, entendiendo la frase "que permita el tratamiento informático", como que los datos "están en un formato tal que pueden ser procesados directamente por un sistema informático"[22].

En el mismo artículo 15, se define el concepto sistema informático, 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". En esta línea, el Convenio entiende por sistema informático, un dispositivo con hardware y software, que tiene por función el tratamiento automatizado de datos, lo cual implica

[19] Mayer, "El bien jurídico protegido en los delitos informáticos", ob. cit., p. 237.

[20] Mayer, "El bien jurídico protegido en los delitos informáticos", ob. cit., p. 237.

[21] Informe explicativo, ob. cit., p. 67.

[22] Informe explicativo, ob. cit., p. 67.

que no existe intervención directa del ser humano, mediante la ejecución de un programa informático. A su vez, programa informático es un conjunto de instrucciones destinadas a obtener el resultado deseado. Finalmente, una interconexión es una red entre dos o más sistemas informáticos[23].

Por último, el artículo 15 define al proveedor 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". Sobre este concepto, cabe señalar que la intención del Convenio era abarcar una categoría amplia de personas que desempeñan un papel respecto a la comunicación o tratamientos de datos a través de sistemas informáticos, siendo irrelevante si se trata de usuarios de grupos cerrados o abiertos al público, si es gratuito o pagado. Además, se incluye dentro del concepto a personas que procesen o almacenen datos en nombre de las personas mencionadas en la primera parte de la definición, así como a los servicios que proporcionan *hosting* y a los que ponen copias de los contenidos de los sitios web en dispositivos de almacenamiento temporal (*caching*) y también a los que proveen la conexión de red. Quedarían fuera los meros proveedores de contenidos[24], si es que no ofrecen servicios de comunicaciones o relacionados al tratamiento de datos[25].

La estructura y los conceptos recién expuestos son transversales a las disposiciones de la ley, que a continuación se analizan.

IV. Delitos en la nueva ley

1. Nueva regulación del sabotaje informático

El sabotaje informático, que suele identificarse con aquellas conductas que implican la destrucción o la inutilización de datos o programas de sistemas informáticos[26], ya se encontraba regulado en los artículos 1º y 3º de la derogada Ley Nº 19.223. En ese sentido, la Ley Nº 21.459 modifica tales figuras, adecuándolas a la normativa contemplada en el Convenio de Budapest, específicamente en los artículos 1º y 4º de esta nueva ley.

---

23 Informe explicativo, ob. cit., pp. 66-67.

24 "… tal como la persona que firma un contrato con una empresa de hospedaje de dominios (*web hosting*)". Informe explicativo, ob. cit., p. 69.

25 Informe explicativo, ob. cit., p. 69.

26 Mayer, "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", ob. cit., pp. 166-167.

Por una parte, *el artículo 1º contempla el ataque a la integridad de un sistema informático*, sancionando al 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" con la pena de presidio menor en su grado medio a máximo. Y por otra, *el artículo 4º sanciona el ataque a la integridad de los datos informáticos,* disponiendo que "[e]l 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".

Si bien las redacciones no son exactamente iguales a las contenidas en los artículos 4 y 5 del Convenio, en su esencia apuntan a lo mismo, razón por la cual es pertinente señalar que, de acuerdo con el Convenio, la conducta sancionada en nuestro artículo 1º encontraría su justificación en la protección de los intereses jurídicos "de los operadores y usuarios de los sistemas informáticos o de telecomunicaciones en su funcionamiento correcto"[27], mientras que la conducta sancionada en el artículo 4º encontraría su justificación en la protección de "la integridad y el correcto funcionamiento o utilización de los datos almacenados o de los programas informáticos"[28]. Así, detrás de estas figuras se encuentra la idea de proteger la integridad y la disponibilidad de los datos informáticos. Ahora bien, nuestro legislador ha regulado este delito sin referencia alguna al patrimonio ni a la causación de un perjuicio patrimonial, como lo hace la legislación española que los regula a propósito de ese tipo de ilícitos[29]. Y, además, se optó por la eliminación en el caso del ataque a la integridad de los sistemas informáticos, de la referencia que el antiguo artículo 1º de la Ley Nº 19.223, realizaba a las "*partes o componentes* [de un sistema de información]", que apuntaba a incluir dentro de ese delito la afectación del *hardware* o soporte físico de un sistema informático. En efecto, la eliminación de esta referencia es más coherente y apunta a una postura que ya venía adoptando nuestra doctrina al entender que tales afectaciones corresponden sean sancionadas a través de los delitos patrimoniales clásicos, en particular el delito de daños común[30], y no como una hipótesis especial de delito informático.

[27] Informe explicativo, ob. cit., p. 85.

[28] Informe explicativo, ob. cit., p. 83.

[29] Artículos 264 y 264 bis, Capítulo IX De los daños, Título XIII Delitos contra el patrimonio y contra el orden socioeconómico del Código Penal español.

[30] Mayer, "El bien jurídico protegido en los delitos informáticos", ob. cit., p. 237.

a) Respecto del ataque a la integridad de un sistema informático

Como se señaló, esta figura sanciona a quien 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.

Se trata, entonces, de un delito común pues puede ser cometido por cualquier sujeto y la conducta debe consistir en la "introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos", sea cualquiera la forma en que ello ocurra y bastando que concurra una de ellas para la realización del tipo.

Ahora bien, a su vez, es necesario que tal conducta "obstaculice o impida", total o parcialmente, el normal funcionamiento del sistema. La delimitación de uno y otro concepto no es tan evidente. En efecto, la Real Academia Española ("RAE") define obstaculizar como el "impedir o dificultar la consecución de un propósito", e impedir como el "[e]storbar o imposibilitar la ejecución de algo". Es decir, puede ocurrir que ambos conceptos se refieran a lo mismo, sin embargo, lo cierto es que basta cualquiera de los dos para que la conducta se entienda configurada (es decir, se trataría de un delito de tipicidad reforzada), siempre que afecten el "normal funcionamiento" del sistema, debiendo entonces apreciarse en consideración a una definición previa de cuál sería ese normal funcionamiento que se ve obstaculizado o impedido,

Cabe hacer presente que esta hipótesis no establece un requisito de gravedad, como sí se contempla en otras legislaciones como la española y como sí lo hace el artículo 4 relativo al ataque a la integridad de datos informáticos. Ahora bien, el requisito de gravedad si bien apunta a distinguir aquellas circunstancias que sí merecen protección penal dada su entidad, de aquellas que no, no deja de ser un concepto indeterminado. De hecho, esa indeterminación se evidenció y advirtió en España, señalándose que "al hallarnos ante un término jurídicamente indeterminado, el problema surgirá en discernir en qué supuestos se entenderá obstaculizado o interrumpido el funcionamiento del sistema informático ajeno de manera grave y cuando no…"[31]. Una alternativa es señalar que la omisión de tal requisito, desde una interpretación literal del precepto, podría apuntar a la impertinencia de discutir sobre la concurrencia

[31] Contreras, Beatriz; Garrós, Imma. "Los principales delitos cibernéticos cuyos sujetos pasivos pueden ser los particulares, las personas jurídicas o la administración pública", en *Revista Aranzadi de Derecho y Proceso Penal*, Nº 48 (2017), p. 9.

de un requisito no explícitamente exigido, en términos de la decisión del legislador de no distinguir respecto de la gravedad, sin embargo, tampoco se puede pecar de ingenuidad pensando que la discusión relativa a que la conducta en el caso concreto de determinada manera afecta al bien jurídico para que se pueda afirmar la necesidad de protección a través del derecho penal.

b) Respecto del ataque a la integridad de los datos informáticos

Esta figura sanciona al que indebidamente altere, dañe o suprima datos informáticos, causando un daño grave al titular de estos mismos. Nuevamente, se trata de un delito común pues puede ser cometido por cualquier persona, siempre que no sea el titular de los datos informáticos de que se trate.

La conducta sancionada se configura –alternativamente– si se alteran, dañan o suprimen datos informáticos. Sobre qué debe entenderse por estos conceptos, y sin perjuicio al recurso disponible en la RAE, es útil precisar que el Informe Explicativo del Convenio, en cuanto señala que, por *alteración*, se entiende la modificación de los datos existentes; por *daño*, se entiende una alteración negativa de la integridad o del contenido de la información de los datos y programas; y, por *supresión*, "cualquier acción que impida o ponga fin a la disponibilidad de los datos para la persona que tiene acceso al computador o al soporte en que se encuentran almacenados"[32]. Ahora bien, la disposición no exige que las conductas se realicen por algún medio en particular, por lo que pueden realizarse por cualquier medio.

Lo que sí exige el legislador es que el ataque a la integridad de los datos informáticos sea realizado indebidamente y que cause un daño grave, requisitos no exigidos para el ataque a la integridad de un sistema informático. Estos dos elementos del tipo penal contemplados para el sabotaje relativo a datos informáticos podrán generar discusión y deberán ir limitándose jurisprudencialmente, sin perjuicio a continuación se intentan entregar algunas herramientas para su interpretación.

Respecto a la exigencia de un actuar indebido puede resultar útil referirnos a la exigencia de ilegitimidad que contempla el Convenio y que no se traspasó de forma textual a nuestro ordenamiento. Al respecto el Convenio entiende que la exigencia de actuar ilegítimo permite afirmar que son atípicas aquellas actividades comunes inherentes al diseño de las redes, o las prácticas comerciales y de operación comunes[33] que se efectúan de forma

[32] Informe explicativo, ob. cit., pp. 83-84.

[33] Informe explicativo, ob. cit., p. 86.

legítima. Sumado a lo cual, en este mismo sentido, en la tramitación de la ley se señaló que "[l]o que debe sancionarse es la perturbación o ataque sin autorización o sin derecho, esto es, 'indebidamente'"[34]. Así, se podría tratar de un requisito que apunta al "actuar sin autorización" que contempla la legislación española en el artículo 264 del Código Penal. Este actuar sin autorización, como sí se señala en el delito de acceso ilícito, aunque de forma redundante, igualmente incluye a quien no tiene autorización alguna, como a aquel que excede la autorización que posee[35].

En lo que respecta a la exigencia de que con la conducta desplegada se ocasione un daño grave, como ya se refirió, provoca indefinición y ambigüedad[36] en el precepto. En efecto, la gravedad no se encuentra definida en el Convenio ni en su Informe Explicativo, pues el objetivo era que cada país determinara los criterios que hacen al ataque merecedor de sanción penal[37], sin embargo, la Ley Nº 21.459 tampoco adoptó una definición, lo cual forzará a la determinación jurisprudencial del concepto. Ahora bien, un criterio que puede resultar útil, sin perjuicio de que se trata de un aspecto que deberá determinarse caso a caso, viene dado por el Tribunal Supremo español[38] que ha señalado que:

> "En todo caso, la tipicidad exige además que la disfunción electrónica genere un resultado realmente gravoso para el titular de los instrumentos digitales. Nuestra sentencia anteriormente citada, atendiendo a que el supuesto que resolvíamos consistió en la eliminación de unos datos después recuperados de la 'papelera de reciclaje' y compartiendo la posición sustentada en la Circular de la Fiscalía General del Estado Nº 3/2017 (ARP 2017, 1680), proclamaba que la gravedad típica se alcanza cuando es imposible recuperar la operatividad del sistema o cuando su recomposición es difícilmente reversible sin notables esfuerzos de dedicación técnica y económica"[39].

---

[34] Historia de la Ley Nº 21.459, p. 93.

[35] Así también se interpreta, por ejemplo, en la legislación española en relación con este mismo ilícito contemplado en el artículo 264 del Código Penal. Corcoy, Mirentxu. "Arts. 263-267", en Corcoy, Mirentxu; Mir, Santiago (coords.), *Comentarios al Código Penal, Reforma LO 1/2015 y LO 2/2015*. Valencia: Editorial Tirant lo Blanch, 2015, p. 950.

[36] Becker; Viollier, "La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley Nº 19.223", ob. cit., p. 80.

[37] Informe explicativo, ob. cit., p. 86.

[38] Debe advertirse que en España este tipo penal exige gravedad de la conducta y del resultado.

[39] Tribunal Supremo español, de 7 de febrero de 2022, Recurso de casación 322/2020, considerando 5º.

c) Algunas consideraciones comunes a ambos tipos

Es relevante advertir que, en ambas figuras, se eliminó el requisito de que la afectación sea realizada maliciosamente que se exigía en los artículos 1º y 3º de la antigua ley. Esta exigencia subjetiva que ha sido interpretada como "una voluntad consciente y determinada no solo de realizar una conducta típica y antijurídica, sino que, además, el agente se encuentra animado a lograr la producción del hecho punible y, su plasmación en la realidad mediante la consecución de sus resultados"[40] (es decir, como una exigencia de dolo directo), generó más de una dificultad en la aplicación de estos preceptos y otros tantos que la contemplan. De esta manera, la eliminación de este requisito mejora la técnica legislativa, pues se elimina una carga probatoria adicional y deja de generar la discusión sobre la posibilidad de que la conducta fuese realizada con dolo eventual[41], lo cual ahora pareciera admisible.

Adicionalmente, es posible que ambas figuras concurran conjuntamente cuando el ataque a la integridad del sistema informático se produzca por la alteración, daño o supresión de datos informáticos, lo cual deberá resolverse en sede concursal dependiendo del caso concreto. Lo mismo ocurrirá en relación con los restantes ilícitos contemplados en esta ley.

2. Nueva regulación del espionaje informático

Al igual que en el caso anterior, el espionaje informático vinculado al "acceso u obtención indebidos de datos o programas de sistemas informáticos"[42] ya se encontraba regulado a través de la Ley Nº 19.223, en sus artículos 2º y 4º, por lo que la nueva ley supone una modificación en la materia.

El artículo 2º, que se refiere al *acceso ilícito*, sanciona a quien:

> "… 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.

[40] Cavada, ob. cit., p. 18.

[41] Becker, Sebastián; 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*, Nº 248 (2020), p. 83. En el mismo sentido, Cavada, Juan Pablo. "Delitos Informáticos. Chile y legislación extranjera", en *Biblioteca del Congreso Nacional* (2015), p. 18.

[42] Mayer, "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", ob. cit., p. 167.

> 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".

Por su parte, el artículo 3º de la nueva ley sanciona la *interceptación ilícita*, señalando:

> "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".

Esta nueva normativa supone una reformulación de aquello que se encontraba sancionado en la Ley Nº 19.223, toda vez que no solo reorganiza las hipótesis, sino que realiza algunas modificaciones que conviene advertir.

a) Respecto al delito de acceso ilícito

El inciso primero del artículo 2º sanciona un acceso ilícito que no requiere de más requisitos que el actuar sin autorización o excediendo la que se tiene, y superando barreras técnicas. Esto podría resultar similar a lo que antes se sancionaba como "conocer indebido", pero la técnica legislativa y los requisitos son distintos. Sólo en el inciso segundo se contempla la hipótesis que sancionaba la antigua ley con la exigencia de que la conducta tenga por objeto apoderarse o usar la información a la que se accede. Y, por su parte, el inciso tercero sanciona a quien obtiene y, además, divulga la información referida.

Este tipo penal puede apreciarse como "la puerta de entrada" a la mayoría de los demás ilícitos contenidos en la ley. En efecto, una vez que se accede ilícitamente a un sistema informático, pueden tener lugar las restantes conductas sancionadas en la ley, lo cual podrá generar discusiones en sede concursal. Así el acceso ilícito se refiere al "delito básico que constituyen las amenazas peligrosas y los ataques a la seguridad (es decir, contra la confidencialidad, la integridad y la disponibilidad) de los sistemas y datos informáticos[43], sin

[43] Informe explicativo, ob. cit., p. 76.

necesidad de daño o perjuicio en la información[44], sino más bien en la línea de una afectación de una legítima pretensión de exclusión de terceros al acceso de un determinado contenido"[45].

Así, se sigue tratando de un delito de mera actividad[46], pues no requiere de resultado alguno para su ejecución, siendo irrelevante "si se produce o no un resultado dañoso sobre la información o los datos, es penalmente irrelevante para la consumación del delito"[47]. Es más, basta con que el acceso sea al sistema informático, sin necesidad de que se acceda a datos en particular[48]. El acceso podrá ser directo o remoto, pues el precepto no hace distinción al respecto. Por directo se entiende aquel que se produce al acceder físicamente a un sistema ajeno y, por remoto, aquel que se produce por medio de una red informática de un sistema informático a otro, sea de carácter público o privado[49].

Ahora bien, el tipo penal exige que la conducta se realice *sin autorización o excediendo la autorización que posea el sujeto activo*. Como ya advertimos, esta doble referencia puede resultar redundante toda vez que, en realidad, si se excede la autorización que se poseía, no se tenía autorización para acceder en los términos en los que el sujeto activo accede. Esta mención podría entenderse como el reemplazo de las cláusulas 'deliberado' e 'ilegítimo' que contempla el Convenio. El concepto 'deliberado' no hace referencia a una especificación del elemento subjetivo (como lo era la exigencia de malicia, y, por tanto, admitiría dolo eventual), sino que, desde la óptica del Convenio tiende a evitar la sanción de quienes acceden "a un sistema por error o bajo percepción errada de que se cuenta con las credenciales necesarias"[50] (es decir, de aquellos que se encuentran en un error de tipo). La exigencia de ilegitimidad tendría por objeto limitar la conducta a quien no tiene acceso autorizado, es decir, no se trata del propietario u otro tenedor legítimo del sistema o de parte del mismo, y por

---

44 Becker; Viollier. "La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley Nº 19.223", ob. cit., p. 90.

45 Medina, Gonzalo. "Estructura típica del delito de intromisión informática", en *Revista chilena de derecho y tecnología*, vol. 3, Nº 1, p. 89.

46 Moscoso, Romina. "Ley Nº 19.223 en general y el delito de hacking en particular", en *Revista chilena de derecho y tecnología*, vol. 3, Nº 1 (2014), p. 47.

47 Moscoso, ob. cit., p. 47.

48 Mismo sentido legislación española. Bolea, Carolina. "Arts. 197-216", en Corcoy, Mirentxu; Mir, Santiago (coords.), Comentarios al Código Penal, *op. cit.*, p. 759.

49 Bolea, ob. cit., p. 759.

50 Becker; Viollier. "La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley Nº 19.223", ob. cit., p. 92.

cierto, no constituiría delito acceder a un sistema informático que permita el acceso libre y abierto al público[51].

A este respecto, el artículo 16 de la Ley Nº 21.459 establece expresamente que, cuentan con autorización para el acceso a un sistema informático, quienes 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. Si bien esta norma fue de aquellas que mayor discusión generó durante la tramitación de la ley, quedó finalmente restringida a la concurrencia de dos elementos que provocarían la atipicidad de la conducta de acceso, esto es, (i) contar con autorización expresa del titular, (ii) en el marco e investigaciones de vulnerabilidad o para mejorar la seguridad informática. Esto tiene impacto directo sobre la posibilidad de aceptar hipótesis distintas o clásicas de *hacking* ético.

Adicionalmente, este tipo penal exige que se superen barreras técnicas o medidas tecnológicas de seguridad, lo cual tiene por objeto asegurar que el delito "sea cometido a través de medios técnicos o informáticos, y evitar conductas como el mero incumplimiento contractual o de términos y condiciones del sistema"[52]. Este requisito "aporta un criterio objetivo para la delimitación del comportamiento penalmente relevante y confiere mayor certeza a la interpretación de la figura"[53]. Para su interpretación podemos recurrir a algunas consideraciones que se han tenido a la vista en la legislación alemana y española que ya contemplaban este requisito en términos similares. En ese sentido, en Alemania este requisito se ha interpretado apuntando "a la entidad de la conducta criminal y que excluye la protección frente a conductas negligentes del titular de datos… [siendo lo] relevante… la superación de mecanismos técnicos…"[54]. Así mismo, en España se ha señalado que, con este requisito, "no se exige una naturaleza especial de los datos, esto es, que sean secretos o reservados, pues basta con la exigencia de la barrera de ingreso al sistema"[55]. Sobre la entidad de la medida de seguridad en España, se ha señalado que la medida de seguridad puede ser cualquiera que se establezca para impedir el

[51] Informe explicativo, ob. cit., p. 78.

[52] Becker; Viollier. "La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley Nº 19.223", ob. cit., p. 93.

[53] Mayer, Laura; Vera, Jaime. "El delito de espionaje informático: Concepto y delimitación", en *Revista chilena de derecho y tecnología*, vol. 9, Nº 2 (2020), p. 245.

[54] Medina, ob. cit., p. 86.

[55] Medina, ob. cit., p. 88.

acceso al sistema, con independencia de que la misma sea más o menos sólida, compleja o robusta[56], y se incluyen claves de acceso al sistema informático de que se trate, el *firewall* o medidas de bloqueo del equipo[57].

El inciso segundo del artículo 2, en su primera parte, sanciona una conducta que ya se encontraba tipificada en la antigua ley; esto es, el acceso con el ánimo de apoderarse o usar la información contenida en el sistema informático. Esto seguirá produciendo conflictos a la hora de evaluar el elemento subjetivo de este tipo penal, toda vez que no se encuentra justificado "si se considera que lo decisivo en el espionaje informático es actuar con el dolo de acceder a y conocer indebidamente la información del sistema"[58]. Ahora bien, pese a que este problema se mantiene, lo cierto es que, a diferencia de lo que ocurría en la legislación anterior, en caso de duda se podrá recurrir a la figura básica contemplada en el inciso primero que no lo requiere.

Luego, en la segunda parte, se sanciona a quien divulgue la información a la cual accedió ilícitamente, lo cual, sumado a la agravación de la pena que se contempla en el inciso final del artículo 2º, confirma algo que no se señalaba expresamente en la antigua legislación, pero cuya interpretación lo hacía posible. Esto es, que "para ser sancionado no es necesario que quien revela los datos haya sido la misma persona que accedió ilícitamente a ellos"[59].

b) Respecto al delito de interceptación ilícita

Este delito sanciona al 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", con la pena de presidio menor en su grado medio. Y, en su inciso segundo, al 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", "con la pena de presidio menor en sus grados medio a máximo".

Se trata de un delito común que puede cometer cualquier persona. Los verbos 'interceptar' e 'interferir' que antes se encontraban contemplados en

---

56 Torres, Adriá; Torres, Antoni; Contreras, Beatriz; Garrós, Imma. "El 'hacking' desde una perspectiva legal, criminológica y técnica, en *Revista Aranzadi Doctrinal*, Nº 6/2021, p. 28.

57 Torres; Torres; Contreras; Garrós, ob. cit., p. 28.

58 Mayer; Vera, ob. cit., p. 244.

59 Couso, Jaime. "Relevancia penal de la intromisión del empleador en los correos electrónicos de sus trabajadores", en *Revista de Derecho Universidad Católica del Norte*, Nº 2 (2018), en relación con fallo de Corte Suprema de 20 de marzo de 2013, rol Nº 3951-2012, p. 61.

el artículo 2º de la Ley Nº 19.223, ahora sumados al verbo 'interrumpir' y se consagran en el artículo 3º de la nueva ley, a lo cual se agrega en el inciso segundo, el verbo 'captar'.

Si bien habrá que evaluar la necesidad de hacer referencia a tantos verbos rectores, algunos de los cuales hasta podrían tener la misma significación y aun cuando el Convenio solo refiere la interceptación ilícita para la configuración de esta conducta, podemos señalar que igualmente esta disposición "tiene como finalidad proteger el derecho a la privacidad de las comunicaciones de datos"[60] y que incluye "a todas las formas de transferencia electrónica de datos, ya sea por teléfono, fax, correo electrónico o transferencia de archivos"[61].

Por su parte, si los conceptos 'medios técnicos' y 'transmisión no pública' que fueron utilizados en el artículo 3º, son una réplica del contenido del Convenio, también podremos recurrir a él, como criterio para su interpretación. Así, 'medios técnicos' es definido como "escuchar, supervisar o vigilar el contenido de las comunicaciones, a adquirir los contenidos de datos, ya sea de forma directa, mediante el acceso y uso del sistema informático, o en forma indirecta, mediante el uso de dispositivos electrónicos para escuchar en forma secreta o de dispositivos para intervenir conversaciones"[62], incluyendo grabación.

Por su parte, el concepto de 'transmisiones no públicas' se refiere al proceso de transmisión y no a la naturaleza de los datos transmitidos. En ese sentido, "[l]os datos comunicados pueden ser información que esté accesible al público, pero que las Partes quieren comunicar de forma confidencial… Por lo tanto, el término 'no pública' no excluye *per se* las comunicaciones que se realizan a través de las redes públicas"[63].

En el mismo sentido que ya hemos señalado, la exigencia de que la interceptación sea indebida podrá dar lugar a más de alguna discusión pese a las referencias que ya se han hecho a su alcance.

3. Nuevo delito de falsificación informática

Una novedad legislativa para nuestro ordenamiento es la consagración de la figura de falsificación informática que se sanciona en el artículo 5º de la Ley

[60] Informe explicativo, ob. cit., p. 80.

[61] Informe explicativo, ob. cit., p. 80.

[62] Informe explicativo, ob. cit., p. 80.

[63] Informe explicativo, ob. cit., p. 81.

Nº 21.459. Esta disposición sanciona al que "indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos", con la pena de presidio menor en sus grados medio a máximo.

Agrega el artículo que "[c]uando 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".

Esa figura también fue adoptada desde el Convenio, el cual la regula con el objeto de "establecer un delito al de falsificación de documentos tangibles"[64], intentando protegerse el interés jurídico de "la seguridad y la fiabilidad de los datos electrónicos, que pueden tener consecuencias para las relaciones legales"[65].

La necesidad de esta nueva figura delictiva, como lo plantea el Convenio, puede ser puesto en duda en nuestro ordenamiento si seguimos el análisis realizado por la profesora Mayer[66], quien sugiriendo la adopción de un concepto amplio de documento, no limitado necesariamente a un (papel) escrito, permitiría la inclusión de los documentos electrónicos como objeto material de los delitos de falsedades electrónicas, lo cual implicaría que su resguardo se puede hacer a través de las normas comunes a este delito[67], y en ese caso, la incorporación de esta figura no sería necesaria. De hecho, así ocurre, por ejemplo, en España, donde se ha incluido jurisprudencialmente en el concepto penal de documento, que hace referencia a soportes materiales, los documentos electrónicos[68], sin necesidad de incorporar un tipo penal específico para este tipo de documentos.

---

64 Informe explicativo, ob. cit., p. 92.

65 Informe explicativo, ob. cit., p. 92.

66 Mayer, Laura y Vera, Jaime. "El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho Penal Chileno", en revista *Política Criminal*, vol. 14, Nº 27 (2019).

67 Mayer; Vera. "El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho Penal Chileno", ob. cit., p. 450.

68 "En efecto, un documento electrónico es información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. Su reconocimiento a efectos penales es admisible dada la amplia fórmula establecida en el artículo 26 del Código Penal (RCL 1995, 3170 y RCL 1996, 777) que define a efectos penales el documento como todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otra relevancia jurídica… Cualquier sistema que permita incorporar ideas, declaraciones, informes o datos

Ahora bien, el concepto de documento no es unánime en Chile. Ese concepto amplio recién citado se contrapone al concepto restringido que adoptan algunos autores, y que consiste en la "manifestación de voluntad o consignación de hechos (…) escrita y más o menos permanente, realizada por una persona, que puede tener consecuencias jurídicas"[69].

En ese sentido, la regulación de esta figura podría suponer una decisión legislativa de que los documentos electrónicos deben ser excluidos del concepto de documento regulado en el Código Penal o bien puede dar lugar a problemáticas de tipo concursal que deberán irse resolviendo ahora que la norma se encuentra vigente.

En principio se trata de un delito común que puede ser cometido por cualquier persona, pero se contempla en el inciso segundo una sanción agravada para los casos en que la conducta es realizada por un funcionario público, abusando de su oficio. Por su parte, la exigencia de que la conducta sea realizada con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos puede implicar una exigencia de dolo directo. Pese a que se exige que el documento sea falsificado para "ser tomado o utilizado" como auténtico, no se sanciona su uso.

4. Nuevo delito de receptación de datos informáticos

Esta disposición es una novedad no solo para nuestro ordenamiento, sino también a nivel comparado e incluso para el Convenio de Budapest. El artículo 6 de la nueva ley sanciona al 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

susceptibles de ser reproducidos en su momento, suple con ventajas al tradicional documento escrito, siempre que existan instrumentos técnicos que permitan acreditar la fiabilidad y seguridad de los impresos en el soporte magnético. Se trata de una realidad social que el derecho no puede desconocer. El documento electrónico imprime en las neuronas tecnológicas, de forma indeleble, aquello que se ha querido transmitir por el que maneja los hilos que transmiten las ideas, pensamientos o realidades de los que se quiere que quede constancia. Su autenticidad es tan firme que supera la realidad que puede visualizarse en un documento escrito. El documento electrónico adquiere, según sus formas de materializarse, la posibilidad de adquirir las categorías tradicionales de documentos privados, oficiales o públicos, según los elementos técnicos que se incorporen para su uso y materialización". Tribunal Supremo español, 15 de enero de 2020, Recurso de Casación Nº 672/2019, considerando 4º.

[69] Mayer; Vera. "El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho Penal Chileno", ob. cit., p. 424.

de las conductas descritas en los artículos 2º, 3º y 5º", con la pena asignada a los respectivos delitos, pero rebajada en un grado.

Se trata de una norma en la línea del delito de receptación contemplado en el artículo 456 bis A del Código Penal que tendría por objeto sancionar la conducta de quien comercialice, transfiera o almacene datos informáticos, sin necesidad de acreditar que dicha persona es quien obtuvo ilícitamente la información, es decir, se sanciona "el uso posterior de los datos obtenidos"[70], con la finalidad de prohibir la conducta de los sujetos que compran datos informáticos obtenidos mediante alguno de ellos delitos regulados en la misma ley, y a quienes de otra manera no sería posible sancionar recurriendo a delitos comunes[71].

Los datos informáticos sobre los que recae este delito deben provenir de las conductas correspondientes a acceso ilícito, interceptación ilícita y falsificación informática, sin perjuicio de que en la discusión legislativa se mencionaba también que estos datos pudieran provenir del fraude informático[72], el cual finalmente no fue incluido sin que queden claras las razones de tal decisión.

Finalmente, este tipo penal que, como se señaló, se encuentra formulado en clave de receptación, incorpora el mismo elemento subjetivo que allí se contempla (conociendo su origen o no pudiendo menos que conocerlo) pero incorpora un elemento adicional relativo a que la comercialización, transferencia o almacenamiento sea con el mismo objeto u otro fin ilícito. Esto pareciera decir relación con el objeto del ilícito que da origen a la obtención de los datos, dejando la puerta abierta a otros fines ilícitos que no sean posible de prever taxativamente. También se separa de la receptación en tanto la pena se gradúa rebajando la pena en un grado según sea el delito que permitió la obtención de los datos informáticos, lo cual puede tener relación con este vínculo relacionado con el mismo objeto que se exige.

5. Delito de fraude informático

Esta figura es probablemente una de las más relevantes de la nueva ley, pues resuelve una permanente discusión sobre si este tipo de conductas podía sancionarse a través de figuras comunes o si, en realidad, nos en-

[70] Historia de la Ley Nº 21.459, ob. cit., p. 114.

[71] Historia de la Ley Nº 21.459, ob. cit., p. 116.

[72] Historia de la Ley Nº 21.459, ob. cit., p. 114.

contrábamos frente a una conducta atípica[73]. Esta discusión fue recogida en el Mensaje[74].

El artículo 7 sanciona al 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", estableciendo una graduación de la pena según el perjuicio que la conducta provoque, en la línea de la estafa del Código Penal. Adicionalmente, establece que "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".

Detrás de esta regulación, se encontraba la necesidad de agregar un delito específico que consistiera en la defraudación a otro utilizando la información contenida en un sistema informático al que se hubieren introducido ilegítimamente datos informáticos o aprovechando la alteración, daño o supresión de documentos electrónicos, datos transmitidos o contenido del sistema informático[75].

Esta disposición es muy similar a lo dispuesto en el artículo 8 del Convenio que se refiere al fraude informático. Al respecto, y según se desprende de su tenor literal, se trata entonces, de un delito de resultado que exige una lesión patrimonial. Así, este delito puede ser entendido como "un delito en que el perjuicio patrimonial de otro es ocasionado a través de determinados medios 'informáticos'"[76] y al tratarse de un delito de resultado, sigue la estructura típica de estos delitos, a saber: "la ejecución de un comportamiento delictivo,

---

[73] Ver, por ejemplo, Oxman, ob. cit., y 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).

[74] "Tal como se explicaba latamente en el Mensaje Nº 13-348, enviado durante el Gobierno del ex presidente Lagos, la figura conocida como 'fraude informático', a juicio de algunos puede considerarse incluida dentro del tipo penal de estafa, pero en 'aquellos ámbitos donde se ha automatizado procesos de trabajo que antes desarrollaban personas físicas, al punto que en muchos casos la actividad autónoma de un sistema informático no sólo sirve de apoyo para la toma de decisiones, sino dentro de un determinado marco es el encargado de tales 'decisiones'". En este contexto, la manipulación informática puede ciertamente dar lugar a resultados perjudiciales para el patrimonio de determinadas personas, pero sin que resulte clara la concurrencia de un engaño ni del error correlativo ni, consecuentemente, de una disposición patrimonial fundada en un error, tal como requiere el tipo penal de estafa". Historia de la Ley Nº 21.459, p. 6.

[75] Historia de la Ley Nº 21.459, p. 6.

[76] Mayer; Oliver, ob. cit., p. 170.

la provocación de un resultado típico y la existencia de un vínculo causal entre ese comportamiento y el resultado"[77].

La conducta sancionada en esta disposición es la manipulación de un sistema informático que debe realizarse a través de la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema. En ese sentido, conviene señalar que esta descripción típica corresponde a una noción más estricta del concepto. En efecto, cuando "la noción de fraude informático se vincula con la producción de un perjuicio patrimonial mediante la manipulación o alteración de datos o programas de sistemas informáticos", estamos frente a una noción estricta del concepto. En oposición a nociones más amplias en que es usual que "en el concepto de fraude informático se incluyan conductas que no necesariamente son la causa (directa) del perjuicio patrimonial de la víctima, sino que corresponden a mecanismos orientados a, por ejemplo, conseguir datos indispensables para generarlo"[78].

La adopción de este concepto de fraude vinculado al perjuicio patrimonial ocasionado por la manipulación de un sistema informático podría implicar dejar fuera del ámbito de aplicación de este tipo penal las conductas conocidas como *phishing* y *pharming*, que podrían ser concebidas como actos preparatorios de este delito[79], y para cuya sanción se deberá recurrir a otras figuras típicas. En efecto, sin que sea necesario entrar en detalle, cabe señalar que "mientras en el 'phishing' no se utiliza otra cosa que el correo electrónico como soporte material para reconducir a la víctima a un sitio 'web' falso, en el 'pharming' lo que se introduce es un *malware* o un gusano en el servidor de Internet del usuario para reconducirlo mediante la manipulación del 'Domain Name Server' (DNS) a una página 'web' falsa"[80], lo que implica que se trata de conductas alejadas aún de la producción del perjuicio patrimonial que exige el tipo penal.

Ahora bien, el tipo penal regulado en la nueva ley exige un elemento subjetivo cuya descripción adopta directamente desde el Convenio, esto es, la finalidad de obtener un beneficio económico para sí o para un tercero. Este elemento alude a lo que, en nuestro ordenamiento, tratamos como ánimo de lucro. La exigencia de este elemento es de suma relevancia en este tipo penal

[77] Mayer; Oliver, ob. cit., pp. 170-171.

[78] Mayer; Oliver, ob. cit., p. 156.

[79] Mayer; Oliver, ob. cit., pp. 159-160.

[80] Oxman, ob. cit., p. 216.

porque es "el que le imprime un carácter particular al fraude informático y cuya ausencia impide su configuración, lo que es sin perjuicio de que se verifique algún otro delito informático, en especial, el ya mencionado sabotaje informático (en caso de que, por ejemplo, hubiere habido una alteración de datos con un consiguiente daño patrimonial) o un espionaje informático (por ejemplo, si hubiere habido un acceso a y conocimiento indebido de datos).

Respecto a esta exigencia subjetiva conviene también apuntar al beneficio económico para el autor o para un tercero y que, a diferencia de lo que ocurre en el Convenio, se exige para todas las hipótesis reguladas en este tipo penal y no solo para la interferencia en el funcionamiento de un sistema informático, distinción que, en todo caso, no aparece como justificada.

Por último, también es relevante hacer una mención explícita a la conducta sancionada en el inciso final del artículo 7º, que prevé la sanción en calidad de 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". Esta incorporación tuvo por objeto resolver un problema que se generaba en la persecución de este tipo de delitos, en tanto, por su naturaleza muchas veces ocurre que la única persona identificada es aquella que recibe los fondos en su cuenta bancaria, sin que se obtenga información sobre la persona que realizó la manipulación propiamente, por lo que, se generaban dificultades para acreditar un concierto previo que permitiera sanción a la persona identificada conforme con el artículo 15 Nº 3 del Código Penal[81].

Ahora bien, como parte del incentivo a esta sanción, es lograr identificar a la persona que realiza la manipulación, junto con la sanción a la conducta de quien recibe (siempre que lo haga conociendo o no pudiendo menos que conocer), se contempló una circunstancia atenuante especial de cooperación eficaz en el artículo 9º, que permitirá rebajar la pena en un grado, cuando la cooperación permita la identificación de los responsables, entre otras cuestiones que veremos más adelante.

81 "La norma sugerida, explicó [abogado Rodrigo Peña, del Ministerio Público], permitirá perseguir penalmente a quien facilite su cuenta bancaria para que se deposite el dinero que ha sido sustraído ilícitamente a la víctima. La idea es considerarlo como autor al encontrarse dentro del curso causal del delito (quedaría excluida a su respecto la figura de la receptación). Lo medular, agregó, es que no se puede realizar ningún tipo de fraude informático si previamente no hay una persona a quien depositarle el dinero que será sustraído ilícitamente. Lo anterior, porque el sujeto que hace la transacción debe ingresar los datos de la cuenta a la cual se destina el dinero. Actualmente no es posible sancionar a la persona que facilita una cuenta bancaria con arreglo a las normas de participación del artículo 15, Nº 3, del CP, dado que no se puede acreditar el concierto previo". Historia de la Ley Nº 21.450, ob. cit., p. 120.

6. Nuevo delito de abuso de los dispositivos

Finalmente, la nueva Ley sanciona en su artículo 8º, el abuso de dispositivos, señalando que "[e]l 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", con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales. Los ilícitos vinculados son el ataque a la integridad de un sistema informático, el acceso ilícito, la interceptación ilícita, y el ataque a la integridad de los datos informáticos, además del ilícito contemplado en el artículo 7º de la Ley Nº 20.009.

Detrás de esta disposición, extraída del Convenio, pero no en idénticos términos, tiene por objeto reconocer que la comisión de estos delitos habitualmente requiere de la posesión de medios de acceso (herramientas de piratería) u otras herramientas, existiendo un fuerte incentivo de adquirirlas con fines ilícitos, lo que incluso puede derivar en una especie de mercado negro para su producción y distribución, lo cual debe prohibirse[82].

V. Otras disposiciones

Adicionalmente a la reestructuración de los tipos penales ya revisados, la nueva ley contempla algunas disposiciones especiales.

En relación con el artículo 9º que contempla la circunstancia atenuante especial que ya se enunció, supone el reconocimiento de una cooperación eficaz si es que el suministro de datos e informaciones precisas, verídicas y comprobables, conducen al esclarecimiento de los hechos investigados que sean constitutivos de delitos contemplados en la misma ley, permite la identificación de los responsables o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad a los contemplados en esta ley. Esta cooperación eficaz deberá ser expresada por el Ministerio Público, en la formalización de la investigación o en el escrito de acusación y supondrá una rebaja en un grado de la pena (lo cual deberá determinarse con posterioridad a la sanción penal según las circunstancias atenuantes o agravantes comunes o de su compensación).

[82] Informe explicativo, ob. cit., p. 88.

El artículo 10, por su parte, incorpora dos agravantes vinculadas específicamente a los delitos contemplados en esta ley. Primero, aquella consistente en "cometer el delito 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", lo cual tiene especial relevancia en este tipo de delitos, en los cuales los conflictos laborales, comerciales o de confianza en muchos casos potencian o fomentan la actuación del sujeto activo que pertenece a la organización que administra el sistema informático o custodia los datos se aprovecha de dicha circunstancia. Segundo, aquella consistente en "cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores", lo cual puede en casos de fraude informático, por ejemplo, tener bastante aplicación práctica.

Pero, adicionalmente, se contempla la agravación en un grado de la pena, si como resultados de los delitos contemplados en la ley, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública (electricidad, agua, gas, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la Ley Nº 18.700). Esta agravación de la pena sería, en rigor, aplicable a cualquiera de los delitos contemplados en esta ley, sin embargo, dada la naturaleza del resultado que se prevé para su procedencia, es presumible que su aplicación práctica se concentre en las hipótesis de sabotaje informático y, especialmente –aunque no exclusivamente–, en los ataques a la integridad de los sistemas informáticos dados los riesgos asociados a las conductas que allí se sancionan. De hecho, así ocurre en la legislación española en la cual se contempla una hipótesis agravada cuando se afecte infraestructura crítica, entendiendo por tal aquellas esenciales para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población[83].

De conformidad con lo dispuesto en el Convenio, la nueva ley en su artículo 21, modificó la Ley Nº 20.393, consagrando la responsabilidad penal de las personas jurídicas por los delitos contemplados en esta ley.

Finalmente, en su artículo 19 modificó el artículo 27 de la Ley Nº 19.913, incorporándose estos delitos como delitos base de lavado de activos e incorporó un nuevo delito en el inciso primero del artículo 36 B de la Ley Nº 18.168, General de Telecomunicaciones.

[83] Artículo 264.4 Código Penal español.

VI. Conclusiones

Revisada la nueva normativa plasmada en la Ley Nº 21.459 resulta visible que las modificaciones no son menores en relación con lo que teníamos previamente consagrado en la Ley Nº 19.223, en el Código Penal y en el Código Procesal Penal.

En efecto, como se observa, se realizaron modificaciones a los delitos de sabotaje y espionaje informático, se incorporaron nuevas figuras penales, tales como la falsificación informativa, la receptación de datos informáticos y de abuso de dispositivos y la penalización específica de un delito de fraude informático. Todas estas modificaciones supondrán, sin duda, discusiones sobre el alcance de protección y de las conductas sancionadas, resultando en un desafío relevante a nivel doctrinario y jurisprudencial por la importancia de este tipo de delincuencia a nivel nacional e internacional. Es por eso que en estas páginas se intentan dar algunas luces sobre los recursos que tenemos disponibles para una correcta y coherente interpretación de estos nuevos preceptos aprovechando que se trata de figuras que ya tienen una consagración a nivel internacional y han tenido aplicación práctica en otros países. En ese sentido, es importante recordar que la presente normativa tenía por finalidad adecuar la legislación al Convenio de Budapest y, por tanto, su aplicación e interpretación debiese intentar mantener tal coherencia.

Bibliografía

Becker, Sebastián; 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*, Nº 248 (2020).

Bolea, Carolina. "Arts. 197-216", en Corcoy, Mirentxu; Mir, Santiago (coords.), *Comentarios al Código Penal, Reforma LO 1/2015 y LO 2/2015*, Valencia: Tirant lo Blanch, 2015.

Cavada, Juan Pablo. "Delitos Informáticos. Chile y legislación extranjera", en *Biblioteca del Congreso Nacional* (2015).

Corcoy, Mirentxu. "Arts. 263-267", en Corcoy, Mirentxu; Mir, Santiago (coords.), *Comentarios al Código Penal, Reforma LO 1/2015 y LO 2/2015*, Valencia: Tirant lo Blanch, 2015.

Couso, Jaime. "Relevancia penal de la intromisión del empleador en los correos electrónicos de sus trabajadores", en *Revista de Derecho Universidad Católica*

del Norte, Nº 2 (2018), con relación a fallo de Corte Suprema de 20 de marzo de 2013, rol Nº 3951-2012.

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 Universidad Católica de Valparaíso,* vol. XV (1993-1994).

_____. "La criminalidad informática: situación de lege data y lege ferenda en Chile", en *Informática y derecho: Revista iberoamericana de derecho informático*, Nº 3 (1992).

Lara, Juan Carlos; Martínez, Manuel; Viollier, Pablo. "Hacia una regulación de los delitos informáticos basada en la evidencia", en *Revista Chilena de Derecho y Tecnología,* vol. 3, Nº 1 (2014).

Mayer, Laura. "Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos", en revista *Ius et Praxis*, Nº 1 (2018).

_____. "El bien jurídico protegido en los delitos informáticos", en *Revista Chilena de Derecho*, vol. 44, Nº 1 (2017).

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).

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. 245.

_____. "El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho Penal Chileno", en revista *Política Criminal,* vol. 14, Nº 27 (2019).

Medina, Gonzalo. "Estructura típica del delito de intromisión informática", en *Revista chilena de derecho y tecnología*, vol. 3, Nº 1 (2014).

Moscoso, Romina. "Ley Nº 19.223 en general y el delito de hacking en particular", en *Revista chilena de derecho y tecnología*, vol. 3, Nº 1 (2014).

Muñoz, Fernando. "Epistemología de la techne: a propósito del fraude informático", en *Revista Chilena de derecho y tecnología*, vol. 2, Nº 2 (2013).

Oxman, Nicolás. "Estafas informáticas a través de internet: acerca de la imputación penal del 'phishing' y el 'pharming'", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, vol. XLI (2013).

Torres, Adriá; Torres, Antoni; Contreras, Beatriz; Garrós, Imma. "El 'hacking' desde una perspectiva legal, criminológica y técnica", en *Revista Aranzadi Doctrinal*, Nº 6/2021.

Documentos citados

Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, Viena, 10 a 17 de abril de 2000.

Historia de 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.

Informe explicativo del Convenio sobre la Ciberdelincuencia, coe.int/cybercrime.

Informe "Ciberdelincuencia: Efectos de la COVID-19", confeccionado por INTERPOL, en agosto de 2020, en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19.

Informe Resumido sobre las tendencias de la delincuencia a escala mundial", confeccionado por INTERPOL, en octubre de 2022, disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/Los-delitos-financieros-y-los-cometidos-por-Internet-son-los-que-mas-preocupan-a-la-policia-de-todo-el-mundo-segun-un-nuevo-informe-de-INTERPOL.