REVISTA
DE ESTUDIOS DE LA JUSTICIA

NÚM. 38 (2023) • PÁGS. 1-27 • DOI 10.5354/0718-4735.2023.70292
RECIBIDO: 12/4/2023 • APROBADO: 31/5/2023 • PUBLICADO: 31/7/2023

DOCTRINA

Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Segunda parte

Computer crimes in Chile: criminal offenses, penalties and procedural rules of Law 21.459. Part two

Gonzalo Bascur
Universidad Austral de Chile

Rodrigo Peña
Universidad Autónoma de Chile

RESUMEN Este texto ofrece, como segunda parte del análisis de la Ley 21.459, un desarrollo sistemático a través de una aproximación especial a los tipos delictivos de interceptación ilícita (artículo 3), sabotaje informático (artículos 1 y 4) y falsificación informática (artículo 5), así como también sobre las reglas de sanción y de procedimiento contempladas en la normativa.

PALABRAS CLAVE Cibercrimen, delitos cibernéticos, delitos informáticos, Ley 21.459, parte especial.

ABSTRACT This text offers, as the second part of the analysis of Law No. 21.459, a systematic development through a special part approach on the criminal offenses of unlawful interception (art. 3), computer sabotage (articles 1 and 4) and computer forgery (art. 5), as well as on the rules of sanction and procedure contemplated in the regulation.

KEYWORDS Cybercrime, computer crimes, Law 21.459, special part.

1. Introducción

Este texto corresponde a la segunda parte del estudio de la normativa vigente sobre delitos informáticos contenida en la Ley 21.459 (LDI), que «establece normas sobre

delitos informáticos, deroga la Ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest» (publicada el 20 de junio de 2022), y que fuera divulgado en esta misma revista.[1] Las secciones 2 y 3 abordan los tipos delictivos de interceptación ilícita y obstrucción (artículo 3), sabotaje contra datos y sistemas informáticos (artículos 1 y 4), y falsificación informática (artículo 5); así como las reglas de sanción pertinentes. Por otra parte, en la sección 4 se analizan los aspectos más importantes de las reglas procesales contenidas tanto en el título 2 «Del procedimiento» como en el título 3 «Disposiciones finales».

2. Delitos (continuación)

2.1. Interceptación ilícita y actos de obstrucción (artículo 3)

Dado que la vida moderna se caracteriza por el uso extensivo de redes telemáticas entre las personas, se reconoce que la *confidencialidad* de dicho proceso constituye una dimensión que reclama protección jurídica (Aboso, 2017: 141-142, 154-156). En consecuencia, y tomando como base el artículo 3 del Convenio de Budapest[2] (CB), se castiga —a nuestro juicio— una conducta similar a la tipificación de lo que podría considerarse escuchas telefónicas ilegales,[3] aunque de manera conjunta en su inciso primero también se tipifican acciones de mera *obstrucción* a la señal de telecomunicación,[4] vale decir, atentados contra la *disponibilidad* de los sistemas informáticos.

La disposición castiga, en su inciso primero, 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, mientras que su inciso segundo refiere 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 aquellos.[5]

1. La primera parte corresponde a Bascur y Peña (2022). En forma ulterior, un estudio sobre esta ley fue publicado por Mayer y Vera (2022b: 280-282, 303-304), el que, en lo concerniente a lo desarrollado en la primera parte, difiere i) de los casos abarcados por la superación de barreras técnicas del tipo de (mero) acceso ilícito (artículo 2, inciso primero); y ii) ciertos aspectos de la tipicidad de la figura denominada abuso de los dispositivos (artículo 8).

2. Convenio sobre la Ciberdelincuencia celebrado en Hungría el 23 de noviembre de 2001. Finalmente promulgado por el Estado de Chile a través del Decreto Supremo número 83/2017 del Ministerio de Relaciones Exteriores y publicado el 28 de agosto de 2017.

3. En este sentido, véase Weigend (2013: 82).

4. Para los efectos interpretativos de esta diferenciación en el derecho español, véase Mata (2006: 226-227).

5. Destacan la existencia de tipos delictivos diferentes en cada inciso, Mayer y Vera (2022b: 286).

La conducta de interceptación ilícita propiamente tal se tipifica en el artículo 3, incisos primero y segundo. El hecho consiste en la acción de interceptación —ejecutada por medios técnicos— sobre información constituida por datos informáticos actualmente transmitida por un soporte no público entre dos o más sistemas y realizada indebidamente.

Como forma de atentado contra la confidencialidad de los sistemas, el artículo 3, inciso primero, castiga la acción de «interceptar» la «información» que emane de un sistema informático o que se transmita entre dos o más de aquellos. Por una parte, se trata de una acción análoga a la tipificada en el artículo 161-A del Código Penal,[6] comprendiendo dicho verbo el acceso no consentido a un proceso de transmisión de datos entre dos o más sistemas informáticos[7] —aspecto corroborado por la variante agravada de captación prevista en el inciso segundo—,[8] sin exigir su efectivo conocimiento por el autor. Por otra parte, también exhibe similitud con el hecho previsto en el 36 B literal c) de la Ley 18.168 General de Telecomunicaciones (LGT) (*Diario Oficial*: 02/10/1982),[9] circunstancia que incide, como se verá, en los aspectos concursales.

El método de ejecución consiste en el uso de «medios técnicos», vale decir, emplear dispositivos o programas informáticos idóneos para la operación (Aboso, 2017: 160) Por otra parte, el objeto de la conducta está dado por «información» en los términos ya señalados,[10] sin distinguir entre datos informáticos de orden privado o de naturaleza pública.

Ahora bien, como circunstancia de ejecución, los datos informáticos deben encontrarse siendo objeto de un proceso de transferencia, esto es, hallarse siendo transportados por el respectivo soporte de difusión desde un sistema hacia otro o más sistemas. En este aspecto se diferencia esta conducta del acceso ilícito o del espionaje, actos que, por definición, recaen sobre datos ya almacenados, pero no sobre aquellos bajo transmisión en curso,[11] circunstancia que justificaría su mayor penalidad. El proceso de transmisión de datos debe ser de carácter «no público»,[12] vale decir, reservado exclusivamente para los sistemas que intervienen en la operación, sin libre acceso ni

6. Por su parte, Mayer y Vera (2022b: 286-289) interpretan la figura como una variante de interrupción de comunicaciones más que de *intromisión* ilegal.

7. Interpretan esta conducta en sentido diverso (como evitar que los datos lleguen a su destino) Magliona y López (1999: 165), reconociendo el acceso no consentido bajo el verbo *interferencia*.

8. En esta línea, véase Moscoso (2014: 32-33). Con respecto al artículo 161-A del Código Penal, Matus y Ramírez (2021b: 418). Para ideas similares, véase Balmaceda (2021: 817).

9. La disposición sanciona la interceptación y/o captación maliciosa, o bien la grabación no autorizada de cualquier tipo de señal que se emita a través de un servicio público de telecomunicaciones.

10. Para más información, véase Bascur y Peña (2022: 7-8).

11. Detalladamente, con referencia al derecho chileno y alemán, véase Couso (2018: 54-56).

12. Como apunta Wassmer (2017: 253), no se trata del contenido de los datos, sino que del tipo de proceso de transferencia.

recepción abierta por terceros.[13] Esta circunstancia refleja la dimensión de confidencialidad informática tutelada por la norma.[14]

Como propiedad que define la ilicitud de la conducta —elemento de antinormatividad—, se requiere que sea ejecutada de manera «indebida», esto es, al margen del ordenamiento jurídico.[15] Este elemento normativo implica acreditar que la conducta no está autorizada por el derecho, de forma que, por ejemplo, diligencias en el marco de una investigación penal ajustadas a la ley procesal penal (artículo artículo 9, inciso primero, del Código Procesal Penal, CPP), o bien las acciones permitidas a los proveedores de acceso a internet (artículo 24 H de la LGT),[16] impiden la configuración de la tipicidad.

El inciso segundo del artículo 3 tipifica un supuesto calificado basado en la interceptación de datos que provienen de emisiones dentro del espectro electromagnético, paradigmáticamente, aunque no de forma exclusiva,[17] aquellas que son utilizadas por la telefonía celular y redes de conexión inalámbrica a internet, pudiendo justificarse la agravación en el carácter fundamental que despliega actualmente esta clase de interconexión en tanto condición esencial para el desarrollo de los planes de vida de los individuos (Novoa y Venegas, 2020: 62) La acción de «captación» se comprende en el sentido de la conducta de interceptación, mientras que la ausencia de la «debida autorización» se entiende de forma análoga al carácter indebido del hecho previsto en el inciso primero.

Con relación al tipo subjetivo, la figura es dolosa, incluyendo dolo eventual[18] en ambas variantes (incisos primero y segundo).

Con respecto a la sanción, la conducta base se castiga con pena privativa de libertad de 541 días a 3 años de presidio, mientras que la variante calificada del inciso segundo conlleva ampliación del marco penal previo a uno compuesto por dos grados (desde 541 días hasta 5 años de presidio).

En materia concursal, la acción de interceptación (artículo 3, inciso primero) o captación (artículo 3, inciso segundo) puede figurar como paso previo para el acceso ilícito, espionaje o divulgación, concurso que deberá solucionarse con arreglo a la teoría del concurso aparente de delitos (consunción o especialidad). Sin embargo, frente a este último caso (divulgación), potencialmente podrían realizarse los tipos

13. En este sentido, con respecto a los tipos de la LGT, Matus y Ramírez (2021b: 411).

14. De la Mata y Bariñas (2014: 77-78) destacan que la despersonalización de la información reorienta la protección hacia el método de interacción (el proceso de transmisión).

15. En relación con la normativa previa, véase Rosenblut (2008: 260-261).

16. En detalle acerca de los proveedores de internet, y las implicancias que la regulación de la LGT reviste para la confidencialidad de los datos informáticos, véase Matus y Ramírez (2021b: 412-413). En contra de lo sostenido por los autores, bajo la regulación alemana, Castillo (2017: 57).

17. Véase la fenomenología reseñada por De la Mata (2018: 736).

18. De la misma opinión, Mayer y Vera (2022b: 288).

de los artículos 161 A, inciso segundo y tercero, del Código Penal, y el tipo del artículo 36 B literal d) de la LGT.[19] Por otra parte, subsiste la posibilidad de generar un concurso entre la interceptación (inciso primero) o captación (inciso segundo) de cualquier dato en proceso de transmisión desde un sistema informático, con el tipo previsto en el artículo 36 B literal c) de dicha ley.[20]

A nivel práctico, el presupuesto para dicho concurso se basa en comprender al servicio de prestación de internet como un «servicio público de telecomunicaciones»,[21] con arreglo a la definición prevista en el artículo 3 literal b) de la LGT.[22] De admitirse lo anterior,[23] interpretación —en nuestra opinión— avalada contextualmente por las disposiciones introducidas a la Ley General de Telecomunicaciones por la Ley 20.453, la generación de un concurso ideal o aparente está condicionada por el reconocimiento o no de un bien jurídico independiente bajo los tipos de dicha ley.[24]

Por otra parte, los actos de obstrucción al proceso comunicativo tipificados en el artículo 3, inciso primero, representan atentados contra la disponibilidad de los sistemas informáticos,[25] en la medida que bajo esta disposición también se castigan las conductas de «interrupción», consistente en la obstrucción de la transmisión de datos, impidiendo su desarrollo o generando su desvío a otro destinatario, e «interferencia», comprensiva de otra clase de incidencias en sentido residual, como por ejemplo, estorbar, dificultar, retardar u obstaculizar su desarrollo.[26] Valen aquí las consideraciones efectuadas con respecto al tipo de interceptación en sentido estricto desarrolladas en el apartado previo. Si el objeto del ataque es la prestación del servicio

19. La disposición sanciona la difusión pública o privada de cualquier comunicación obtenida de la interceptación o captación maliciosa, o grabación no autorizada, desde una señal emitida por un servicio público de telecomunicaciones.

20. Una opinión similar puede verse en Mayer y Vera (2022b: 287).

21. No lo consideran abarcado por dicho concepto, Mayer y Vera (2020: 231-232).

22. La admisión del concurso no presenta contradicción entre los elementos «servicio público» y el carácter «no público» de los datos transmitidos, en la medida que la referencia del primero es el objetivo del servicio (las necesidades de comunicación de la comunidad en general), mientras que, del segundo, la posibilidad de acceso por terceros indeterminados a los datos informáticos. Una síntesis de la regulación puede hallarse en Donoso y Reusser (2021: 31-34).

23. En este sentido, véase Couso (2018: 57), Matus y Ramírez (2021b: 411).

24. Por ejemplo, Alfonsi y García, (2016: 159) proponen la correcta administración del espectro radioeléctrico, mientras que Couso (2018: 62) la inviolabilidad de los servicios públicos de telecomunicaciones, bien jurídico que contrapone a la inviolabilidad de los sistemas informáticos, empero, considerando el concurso como uno aparente, zanjado en virtud del principio de subsidiariedad tácita.

25. Sin efectuar esta distinción, para Mayer y Vera (2022b: 287) las conductas de interceptar e interrumpir serían análogas, mientras que interferir, perturbar las transmisiones.

26. En este sentido, véase Linares (2020: 139) y Oxman (2013: 236, nota número 62). Similar, bajo la anterior regulación, véase Magliona y López (1999: 164-165).

de difusión de datos, y no un proceso informático en específico, podría constituir realización del tipo previsto en el artículo 36 B literal b) de la LGT.[27]

2.2. Sabotaje contra sistemas informáticos (artículo 1) o datos informáticos (artículo 4)

Bajo la nomenclatura de «ataque contra la integridad» de datos y sistemas informáticos, los artículos 1 y 4 tipifican conductas tradicionalmente categorizadas como *sabotaje informático*,[28] vale decir, que implican destrucción o inutilización de datos o de un sistema (Mayer, 2017: 238; 2018: 166-168), de manera analógica al tipo de daños[29] y que, por lo mismo, resultan constitutivas de atentados contra la integridad informática. Sin embargo, también bajo este concepto se consideran actos de perturbación sobre el desempeño del respectivo sistema (Aboso, 2017: 355-356; Balmaceda, 2021: 816; Becker y Viollier, 2020: 81-83; De la Mata y Hernández, 2009: 313; Mayer y Vera, 2020: 171), tipificándose la paralización o neutralización de ciertas funciones que aquel desempeña a través de modificaciones no autorizadas por su titular (Castillo, 2017: 51; Mayer, 2018: 168), de modo que con ello se añade —y equipara— a la dimensión de lesividad propia de los actos de sabotaje: el injusto de los atentados contra la disponibilidad de los sistemas o datos, esto es, la mera obstaculización de su legítima utilización.[30]

El legislador ha diferenciado tipos delictivos en función del objeto de la conducta:[31] en el artículo 1 se tipifican comportamientos dirigidos en contra del funcionamiento normal de un sistema informático,[32] sea en su totalidad o en parcialidades del soporte lógico;[33] mientras que bajo el artículo 4, atentados en contra de la información

27. La disposición sanciona la interferencia, interceptación o interrupción de un servicio de telecomunicaciones (de cualquier naturaleza), ejecutada maliciosamente.

28. En esta línea, Mayer y Vera (2021: 270-271). Para el origen del concepto, asociado a un trabajador que atenta contra su empleador, véase Aboso (2017: 352-353).

29. En el contexto alemán, Mayer (2017: 238).

30. En esta línea, Aboso (2017: 354-356) y Malamud (2018: 147).

31. La Ley 19.223 que «tipifica figuras penales relativas a la informática», LTFI, publicada el 7 de junio de 1993 también distinguía entre sabotaje contra sistemas informáticos (artículo 1) y datos informáticos (artículo 3). Por otra parte, Gorjón (2021: 81) los identifica como dos clases de incidentes constitutivos de sabotaje informático.

32. Concepto definido en el artículo 15 literal b). Para más información, véase Bascur y Peña (2022: 8).

33. Reconoce la distinción, Malamud (2018: 147).

propiamente tal,[34] vale decir, ejecutados sobre datos informáticos[35] específicos que se encuentran almacenados en un sistema.[36]

Sobre la base de lo anterior, en primer lugar, el artículo 4 castiga actos de sabotaje ejecutados contra componentes específicos de un sistema informático, esto es, sobre los datos almacenados en su interior. El texto castiga a quien indebidamente los altere, dañe o suprima, siempre que con ello se cause un daño grave al titular de estos mismos.

La faz objetiva consiste en la producción de un resultado de menoscabo sobre la funcionalidad de los datos informáticos (alteración, daño o supresión) (De la Mata, 2018: 740),[37] generada indebidamente y representativa de un daño grave al titular de los datos.[38] La tipificación de este hecho zanja el problema sobre la aplicabilidad del tipo de daños al menoscabo sobre datos informáticos, específicamente debido a su naturaleza inmaterial o incorpórea.[39]

Los resultados consisten alternativamente en: producir la «alteración» de datos, lo que básicamente reside en su modificación, ocasionando una variación de su alcance o contenido inicial (Gorjón, 2021: 104),[40] sin destruirlos (Donoso y Reusser, 2021: 126); la «supresión» de datos, vale decir, su eliminación o desaparición del sistema que los alberga, sin que sea relevante la posibilidad posterior de recuperación o restauración especializada de los mismos;[41] y el «daño» a los datos, expresión residual que abarcaría toda forma de afectar la posibilidad de utilización regular de aquellos (De la Mata, 2018: 747-749).[42] Los referidos actos pueden ser ejecutados en distintas fases, vale decir, mientras los datos se hallan almacenados, o bien durante su procesamiento (por ejemplo, alterando rutinas de programa) o salida (modificando los resultados de su procesamiento) (Donoso y Reusser, 2021: 117).

34. Críticos acerca de la independencia del hecho previsto en el artículo 1 con respecto al artículo 4, Mayer y Oliver (2020: 171).

35. Concepto definido en el artículo 15 literal a). Véase Bascur y Peña (2022: 7-8).

36. Un panorama similar, bajo el derecho alemán, puede verse en Castillo (2017: 54), y en el derecho español, en De la Mata (2018: 739 y ss.).

37. Para información similar, véase Castillo (2017: 51).

38. Una fisionomía alternativa puede apreciarse en Mayer y Vera (2022b: 275-277), para quienes dichas expresiones constituirían formas de comportamiento y, en cierta forma, un tipo de mera actividad.

39. Al respecto, véase Oliver (2013: 539). En el contexto alemán, véase Castillo (2017: 51).

40. Por su parte, Magliona y López (1999: 168) consideran la introducción de datos erróneos, su transformación y desfiguración, así como también suprimir datos correctos.

41. Para más información, véase Aboso (2017: 359). Lo exponen como asunto debatido, en relación con la posibilidad de configuración de una tentativa, De la Mata (2018: 752-753) y Gorjón (2021: 105). Exigen la irreversibilidad en nuestro medio, Donoso y Reusser (2021: 126), aunque es caso de recuperabilidad aprecian la conducta de *daño*. Similar a esto último, Mayer y Vera (2022b: 276).

42. Similar, Magliona y López (1999: 168-169).

El artículo 4 constituye un tipo de resultado con medios ejecutivos no especificados, de modo que,[43] aunque por regla general el método de ejecución del delito será de naturaleza lógico-informática,[44] también —a nuestro juicio— se castigan afectaciones físico-causales realizadas sobre el *hardware*, siempre y cuando ocasionen menoscabo a la existencia o accesibilidad de los datos informáticos,[45] desplazando la aplicación del tipo de daños en virtud del artículo 488 del Código Penal.[46]

Por su parte, las acciones productoras del resultado deben ser ejecutadas «indebidamente», esto es, al margen del derecho,[47] circunstancia que comprende la falta de consentimiento del titular u otra clase de conductas autorizadas por ley.[48] Por otra parte, la tipicidad no está condicionada a la superación de mecanismos de seguridad dispuestos por el titular.

El carácter definitivo o temporal de los resultados ocasionados no tiene mayor relevancia, en la medida que genere afectación importante de la funcionalidad de los datos (De la Mata, 2018: 749), reflejada en la exigencia de «daño grave» a los intereses del titular respectivo.[49] Esta última propiedad o característica del resultado obedece a una reserva del Estado chileno frente al Convenio de Budapest, en orden a castigar exclusivamente ataques cualificados en contra de los datos.[50] Luego, en la medida que se asuma que el tipo protege un bien colectivo, nos parece que el parámetro de valoración de esta característica puede fundarse en consideraciones sobre intereses o bienes complementarios al injusto de base, pero directamente asociados a su disponibilidad (Aboso, 2017: 355-356), esto es, valores patrimoniales y extrapatrimoniales de los sujetos afectados por el acto, incluyendo la función que cumple el dato informático y que ha sido entorpecida por el hecho,[51] como también la posibilidad de recuperación del mismo.[52]

43. En contra, véase Mayer y Vera (2022b: 275).

44. Consideran solo esta modalidad de sabotaje, Donoso y Reusser (2021: 106). En relación con la fenomenología delictiva en esta materia, véase Mayer (2018: 168-171).

45. En este sentido, véase De la Mata (2018: 751), Castillo (2017: 35), Mayer y Vera (2019: 432-434), Malamud (2018: 147-150). En contra, véase Jijena (2008: 152, 157).

46. Se trata de una regla de subsidiariedad expresa de aplicación general frente a cualquier delito de mayor penalidad en materia de daños patrimoniales. En este sentido, véase Oliver (2013: 533).

47. En el mismo sentido, véase Mayer y Vera (2022b: 275).

48. Similar, en el contexto alemán, véase Castillo (2017: 51).

49. Para Mayer y Vera (2022: 276), dicha cláusula podría constituir una condición objetiva de punibilidad y no una exigencia (de lesividad) sobre el resultado típico.

50. Al respecto, véase Malamud (2018: 143-145, 153), Mayer y Vera (2022a: 278-279).

51. En tal sentido, véase Tiedemann (2010: 448-449).

52. Similar, Malamud (2018: 154-160), aunque aludiendo a principios como el de intervención mínima y subsidiariedad de la reacción penal. Asimismo, Mayer y Vera (2019: 435-436, nota número 60).

El tipo es doloso, incluyendo la imputación por dolo eventual.[53] Por otra parte, el hecho es penado como simple delito con pena privativa de libertad de 541 días a 3 años de presidio.

La ejecución de esta acción puede generar múltiples relaciones concursales con otros delitos informáticos, particularmente la alteración indebida, en la medida que puede representar, por ejemplo, la conducta de acceso ilícito (artículo 2),[54] falsificación (artículo 5), interceptación u obstrucción (artículo 3), entre otras, todos casos que deben ser zanjados como un concurso aparente de delitos por consunción o especialidad.

Luego, en segundo lugar, el artículo 1 tipifica el ataque contra la integridad de un sistema informático, el cual puede considerarse un subtipo agravado del artículo 4,[55] y castiga el ataque dirigido en contra del funcionamiento u operatividad de un sistema informático concreto (Gorjón, 2021: 81),[56] o dicho de otra forma, la afectación de la operación de tratamiento automatizado de datos ejecutada por un sistema.[57] El artículo 1 castiga al que deliberadamente obstaculice en forma grave 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.

Como se aprecia, el objeto de la conducta es el funcionamiento regular de un sistema informático específico, esto es, la función (o las funciones) que desempeña mediante el tratamiento o procesamiento automatizado de datos (Mayer y Vera, 2022b: 272).[58] Su protección se debe a que la sociedad de la información depende cada vez más del funcionamiento de redes y servicios, que son inclusive más relevantes que los propios datos que transitan por los mismos (Miró, 2012: 58). Se tutela así el correcto procesamiento de datos en tanto este funge como presupuesto de base para la ejecución de ulteriores acciones del titular.[59]

La faz objetiva representa un tipo de resultado con medio comisivo especificado, consistiendo dicho efecto en la obstaculización grave o el impedimento total o parcial del normal funcionamiento de un sistema informático, y se castiga exclusivamente su producción mediante seis métodos de ejecución.[60]

---

53. En este mismo sentido, véase Mayer y Vera (2022b: 277).

54. Mayer y Vera (2022b: 277) destacan cómo el acceso ilícito puede operar como tipo de recogida ante déficits de tipicidad por esta figura, como daños no graves sobre datos informáticos.

55. Similar, Mayer y Vera (2022b: 271). Al respecto, Moscoso (2014: 34, 73) plantea que un sistema informático está constituido por datos *funcionales*, esto es, que dan forma al soporte lógico, mientras que los ficheros (información) constituyen datos *sustantivos*. En contra de su mayor penalidad, por estimar que los datos sustantivos revisten mayor valor, véase Magliona y López (1999: 173).

56. Reconoce la distinción, Malamud (2018: 152-153). Similar, Castillo (2017: 53).

57. En este sentido, véase Wassmer (2017: 254).

58. En el derecho alemán, Castillo (2017: 53) y Tiedemann (2010: 448).

59. Con referencia al derecho alemán, véase Mayer (2017: 246-247).

60. En un sentido similar, véase Becker y Viollier (2020: 82-83).

Por una parte encontramos las tres acciones siguientes: introducción, transmisión y alteración de datos, que representan métodos para modificar los contenidos de datos informáticos, documentos o el funcionamiento de ciertos programas, todo ello en el marco de generar un desempeño irregular o anormal del sistema operativo (Aboso, 2017: 357-359).

Por otra parte están las acciones de daño, deterioro o supresión de datos, que importan la pérdida definitiva de la plataforma propiamente tal (supresión), o bien su menoscabo funcional para la generación de los resultados típicos (deterioro y/o daño) (Aboso, 2017: 359-360). En relación con estas últimas acciones, tal como se indicó en el apartado anterior, se tipifican tanto incidencias ejecutadas por medios lógicos o informáticos,[61] como también injerencias físico-materiales sobre los componentes que integran el sistema, siempre y cuando la afectación de los datos constitutivos del sistema represente alguno de los resultados típicos.[62]

Para la consumación del hecho, las conductas descritas deben producir alguno de los resultados especificados en el tipo,[63] sea la obstaculización grave del funcionamiento del sistema informático,[64] o bien el impedimento total o parcial de su normal funcionamiento,[65] ambos casos representativos de un menoscabo a la funcionalidad del sistema en relación con su desempeño, al de sus aplicaciones, programas o del acceso y gestión de sus datos informáticos (De la Mata y Hernández, 2009: 317) como por ejemplo, ralentización, dificultad o falta de operación del sistema (Magliona y López, 1999: 163), y en cualquier otro caso de privación temporal o definitiva del titular sobre su uso regular.[66]

Aquí es relevante destacar que el artículo 10, inciso segundo, establece como circunstancia agravante de efecto extraordinario —exasperación en un grado— el hecho de que la comisión de la conducta «afecte» o «interrumpa» la «provisión o prestación de servicios de utilidad pública»[67] o «el normal desenvolvimiento de los pro-

61. Detalladamente sobre los métodos informáticos usualmente empleados (la fenomenología propiamente tal), De la Mata y Hernández (2009: 312-315), Mayer (2018: 168-171).

62. En este sentido, De la Mata y Hernández (2009: 312-313).

63. Similar, Aboso (2017: 362).

64. Plantean que dicha exigencia podría comprometer la garantía de taxatividad de la ley penal, Becker y Viollier (2020: 79-80).

65. En relación con la regulación previa, véase Magliona y López (1999: 162-163). Mayer y Vera (2022b: 272) sostienen, como exigencia implícita del tipo, que la envergadura del impedimento parcial sea equiparable en gravedad (caso a caso) a su afectación total.

66. En este sentido, Aboso (2017: 361). Similar, Donoso y Reusser (2021: 120), Magliona y López (1999: 162).

67. El mismo artículo 10, inciso segundo, ejemplifica este concepto con servicios de electricidad, gas, agua, transporte, telecomunicaciones o financieros.

cesos electorales».[68] En este contexto, si el resultado típico representa alguno de los supuestos indicados, especialmente el primero (afecte o interrumpa), que se identifica con la noción —bastante extendida en el derecho comparado— de incidencia sobre infraestructura crítica,[69] cabe apreciar una agravación de la pena, sin infringir la regla del artículo 63 del Código Penal, en la medida que se pueda reconocer diversidad de fundamento en la configuración del resultado típico (integridad informática) y la incidencia sobre el correspondiente servicio de utilidad pública que justifica la agravación de la sanción (afectación colectiva de acceso a un respectivo suministro o servicio).[70]

El tipo es doloso. La redacción exige que el resultado típico sea producido «deliberadamente». No obstante, según consta en la tramitación legislativa sobre la ratificación del Convenio de Budapest, dicha expresión se mantuvo sin un fundamento claramente identificable[71] de forma que el sentido actual de la exigencia,[72] para no reconocer en ella redundancia legislativa, estaría dado por la posición que se asuma con respecto a las expresiones «malicia» o «a sabiendas»,[73] entre otras empleadas en la ley,[74] y que —cabe recalcar— varían en función del específico marco normativo en que se insertan.[75] En todo caso, de asumirse que bajo esta expresión se limitaría la imputación a dolo directo,[76] los ataques contra un sistema informático ejecutados con dolo eventual, en la medida que necesariamente constituyen alteración o daño de datos informáticos, considerados bajo la forma de un sistema operativo, software u otra clase de programa, resultarían constitutivos del tipo del artículo 4.

Se trata de un simple delito castigado con marco compuesto por dos grados, 541 días a 5 años de privación de libertad; representando, como se dijo, una variante agravada de ataque contra datos informáticos,[77] lo que desplaza su aplicación por

68. Destacan esta conexión, Mayer y Vera (2022b: 271).

69. Al respecto, véase Gorjón (2021: 83 y ss.), Mayer (2018: 163-164).

70. Consideración que resulta extensible a todos los tipos de la LDI, según la pretensión de aplicación generalizada de la circunstancia agravante prevista en el inciso tercero del artículo 10.

71. Véase el debate en Biblioteca del Congreso Nacional (2022: 4-6), donde se argumenta su necesidad solamente para mantener congruencia con el texto del CB, excluir acciones atribuibles a imprudencia (¡) o bien limitar su imputación a dolo directo.

72. Admiten dolo eventual, aunque sin mayor desarrollo, Mayer y Vera (2022b: 274).

73. Con respecto a la normativa previa, véase Magliona y López (1999: 156-157).

74. Similar, Becker y Viollier (2020: 83-84). En relación con la normativa previa, Lara, Martínez y Viollier (2014: 112-113).

75. Hernández (2011: 74) lo destaca como «una cuestión de parte especial». Crítico a la posición tradicional, en el contexto de la previa regulación, Cox (2005: 670-671). Crítico de la tesis que propone la exigencia de dolo directo, Mañalich (2011: 110).

76. En contra de esta lectura, en relación con el artículo 4 del CB (daño contra datos), Mayer y Vera (2021: 278), sosteniendo la compatibilidad del concepto con el dolo eventual.

77. En este sentido, Mayer y Oliver (2020: 171) plantean la duda de si puede haber algún caso de incidencia sobre sistemas sin injerencia en datos. También lo destacan Mayer y Vera (2022b: 271).

especialidad (concurso aparente), y puede generar relaciones concursales similares a lo dicho con respecto a esa figura.

2.3. Falsificación informática (artículo 5)

Es indudable que actualmente el tráfico comercial, bursátil y financiero depende de operaciones de intercambio e intermediación de datos, lo cual presupone necesariamente la existencia de confianza sobre su *autenticidad* y/o *veracidad*.[78] Por ello, el artículo 5, además de constituir una actualización del tipo de falsedad documental,[79] puede ser interpretado como un delito que protege la seguridad y fiabilidad de los datos informáticos,[80] ya sea que estos constituyan o no un documento en sentido estricto.[81] La 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, mientras que, en su inciso segundo, eleva la sanción si es que la conducta es cometida por empleado público abusando de su oficio.

Con respecto al tipo objetivo, en la medida que la falsificación sobre objetos (o real) consiste en modificar un determinado elemento (total o parcialmente) para engañar a terceros sobre la verdad que una o más de sus propiedades constitutivas representan,[82] en este caso los datos informáticos constituyen el objeto de la aserción o expresión falsa que se pretende comunicar a otros con la ejecución de la acción (Mayer y Vera, 2019: 267), vale decir, los datos informáticos constituyen la información que será objeto de falsedad.[83]

Se tipifican cuatro conductas realizadas sobre datos informáticos que resultan coincidentes con aquellas previstas en los delitos de sabotaje y fraude informático, esto es: alteración, daño, supresión e introducción de datos. De estas,[84] la primera (alterar) reviste el carácter de conducta genérica (Mayer y Vera, 2022b: 291) y, por ende,

78. En esta línea, véase Aboso (2017: 386-387).

79. Críticos sobre la necesidad de tipificación, Mayer y Vera (2022a: 263).

80. En este sentido, González (2013: 1083-1084). Similar, al reconocer la pluriofensividad de esta conducta bajo la regulación previa (concurso ideal), Mayer y Vera (2019: 438-446).

81. Comprendemos por *documento* un elemento normativo del tipo, consistente en un determinado soporte apto para fijar con perdurabilidad (función de perpetuación) específicos contenidos (una declaración de conocimiento o voluntad), reconducibles a su autor (función de garantía) y con incidencia en el tráfico jurídico (función probatoria o desempeño de un efecto jurídicamente reconocido). Al respecto, véase Mayer y Vera (2019: 420-426). Similar Aboso (2017: 385-386). Recientemente, Mayer y Vera (2022a: 273, 276-277).

82. Detalladamente al respecto, Mayer y Vera (2022a: 264-266).

83. En este sentido, véase Mayer y Vera (2019: 428).

84. Destacan esta circunstancia en el contexto del CB, Mayer y Vera (2019: 437), Mayer y Vera (2022a: 270-272, 277, 279-280).

comprensiva de las restantes (Mayer y Vera, 2022a: 270). Por lo mismo, la circunstancia típica que caracteriza al comportamiento como un acto de falsedad consiste en exigencias adicionales a la sola incidencia sobre datos, manifestándose en la tipificación de dos elementos subjetivos del tipo,[85] establecidos alternativamente, y que permiten diferenciar en este contexto dos clases de conductas:[86] aquellas ejecutadas sobre un documento propiamente tal (un archivo documental) y acciones realizadas sobre datos estructurados u organizados bajo otras formas diversas a un documento en sentido estricto (por ejemplo, una plataforma virtual o portal de acceso).[87]

Con mayor detalle, el primer elemento consiste en la intención de que los datos informáticos manipulados «sean tomados como auténticos», esto es, que luego de la realización de la acción, el potencial destinatario los advierta o reconozca como existentes (autenticidad propiamente tal) o adecuados en relación con su contenido (verdad como correspondencia).[88] Bajo esta exigencia se castiga la conducta ejecutada sobre datos que —bajo ciertos contextos— representan una determinada realidad virtual y que, mediante la manipulación informática, son distorsionados para dar forma a otra distinta a la auténtica (por ejemplo, en la contabilidad electrónica o en una cuenta bancaria digital), sin incidir directamente sobre un documento propiamente tal[89] (así también, por ejemplo, los casos de *phishing* y *pharming* por suplantación de un sitio web real) (Aboso, 2017: 382), en la medida que esta clase de datos se han tipificado y distinguido expresamente como objeto *alternativo* a esta última categoría (Mayer y Vera, 2019: 267). En este sentido, y por el contrario, el segundo elemento consiste en la intención de que los datos manipulados «sean utilizados para generar documentos auténticos», esto es, ejecutar la conducta para crear o producir un documento propiamente tal,[90] sea parcial o totalmente. Este documento puede ser tradi-

85. Si bien, como enfatizan Mayer y Vera (2019: 279), el Estado de Chile efectuó en este sentido una declaración con respecto al delito del artículo 7 del CB (exigencia de ánimo fraudulento orientado al perjuicio de terceros), finalmente no fue materializada en el texto de la ley.

86. En este sentido, reconociendo una eventual mayor amplitud de la figura, Mayer y Vera (2019: 273, 275-276).

87. En un sentido similar en relación con el CB, véase Mayer y Oliver (2020: 160). En contra, refiriendo al tipo exclusivamente sobre datos representativos de un documento en sentido estricto, González (2013: 1084).

88. Latamente sobre esto, Rojas (2017: 158 y ss.).

89. Al respecto, véase la discusión sobre la calificación de un *registro técnico*, por ejemplo, un electrocardiograma o una fotografía de una estación de radar, esto es, si constituyen o no un documento propiamente tal en relación con la exigencia de registro de una declaración humana, Mayer y Vera (2022a: 276-277).

90. Con respecto a la discusión sobre la calificación jurídica del *forjamiento* de un documento tradicional, esto es, su *creación* bajo la nomenclatura propia de este género delictivo, véase Mayer y Vera (2019: 448-449).

cional, electrónico o informático,[91] en la medida que existen documentos generados de manera digital pero que son rellenados posteriormente una vez impresos. Bajo esta hipótesis, a diferencia de la regulación general sobre falsedades documentales, la naturaleza pública o privada del documento es irrelevante para la sanción del hecho.[92]

Sin embargo, en la medida que el artículo 5 no castiga la conducta de utilización de documentos informáticos falsificados, a diferencia del régimen general previsto en los artículos 196 y 198 del CP, especialmente considerando que el uso es la conducta de mayor acreditación en la praxis, la naturaleza del documento falsificado no es irrelevante. En este sentido, cabe distinguir si el empleo indebido se ejecuta en el entorno virtual, caso en el cual se castiga dicha acción sobre todo dato informático, sean documentos o no, bajo el tipo de receptación informática (artículo 6: almacenamiento —o detentación— para fin ilícito) (Bascur y Peña, 2022: 27), mientras que, si la utilización se verifica en el tráfico no digital, su punibilidad se encuentra condicionada a si el intérprete considera la aplicabilidad de las normas tradicionales sobre falsedades del Código Penal en documentos (públicos o privados) electrónicos y/o informáticos,[93] castigando dicha conducta bajo los artículos 196 o 198 de dicho código.

El tipo es doloso, exigiendo la presencia de los elementos subjetivos desarrollados.[94]

La conducta base (artículo 5, inciso primero) se castiga como simple delito con privación de libertad entre 541 días y 5 años de presidio. El inciso segundo del artículo 5 establece un subtipo agravado con pena de crimen, sancionado con 3 años y un día hasta 10 años de presidio, configurado el hecho de ejecutarse por un empleado público «abusando de su oficio», esto es, en contravención a la reglamentación del cargo (por ejemplo, de documentación o gestión de una plataforma) que justifica su intervención en la gestión de los datos informáticos objeto de la conducta.

Desde la perspectiva concursal, el caso más relevante estaría dado por el *forjamiento* o *manipulación* sobre datos informáticos constitutivos de un documento, supuesto que conlleva idénticas penas que dicha falsedad ejecutada sobre un documento público, sea ejecutado por cualquier persona (artículo 194 del CP) o por funcionario público abusando de su cargo (artículo 193, inciso primero, del CP).

91. Para la distinción, véase Mayer y Vera (2019: 426-431), Rojas (2017: 76-77). Enfatizando el carácter estrictamente *probatorio* de la regulación de la Ley 19.799, véase Donoso y Reusser (2021: 137 y ss.).

92. Mayer y Vera (2019: 436) plantean que dicha circunstancia sea tomada en cuenta por el juez para la individualización exacta de la pena.

93. Afirmativamente, Mayer y Vera (2019: 425, 429-431, 438, 449-450), Mayer y Vera (2022a: 275-277), así como también Matus y Ramírez (2021b: 269-270).

94. En contra, véase Mayer y Vera (2022b: 292) sostienen que se trataría de una regulación específica del dolo y no de elementos subjetivos del tipo, en orden a su reforzamiento y consecuente restricción a dolo directo.

3. Reglas de sanción

3.1. La cooperación eficaz como circunstancia atenuante especial de efecto extraordinario (artículo 9)

En el artículo 9 se establece la circunstancia atenuante de efecto extraordinario denominada «cooperación eficaz», en términos casi idénticos que aquella prevista en el artículo 22 de la Ley 20.000 (drogas), en el artículo 33 literal c) de la Ley 19.913 (lavado de activos), en el artículo 17 C de la Ley 17.798 (control de armas), y en los artículos 260 quáter (delitos de corrupción) y 411 sexies del Código Penal (tráfico de migrantes y trata de personas), aunque en este caso se faculta al juez para rebajar la pena privativa de libertad exclusivamente en un grado,[95] pero, de cualquier modo, de forma posterior a la fijación del *quantum* inicial de pena resultante de la aplicación de los artículos 67 o 68 el Código Penal.

Las exigencias de procedencia consisten en el suministro de información con aptitud (inciso segundo: datos o información precisa, verídica y comprobable) para: a) sostener la acción penal sobre hechos constitutivos de delito de la LDI que sean actualmente investigados («esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley»); y b) para permitir identificar a uno o más imputados en los hechos investigados («permita la identificación de sus responsables»). Otra exigencia es que resulte útil para «prevenir» o «impedir» la ejecución de otros delitos de la LDI de igual o mayor gravedad.[96]

En la medida que su reconocimiento debe ser efectuado por el Ministerio Público en la formalización de la investigación o en la acusación (inciso segundo),[97] es importante destacar que, como herramienta de investigación exclusiva (o promesa de una ventaja expresamente prevista por ley: artículo 195 inciso segundo del CPP), el campo de aplicación original de la regla está destinado a supuestos de colaboración en investigaciones de crimen organizado, y no de perpetración aislada e individual de estos delitos. En este sentido, la instrucción general (del Ministerio Público) para la investigación de delitos de drogas reconoce la cooperación eficaz (para la misma investigación) para aclarar los «hechos» del mismo caso, «delitos conexos» y «sujetos responsables», exigiendo, entre algunos requisitos, que lo informado sea «inédito» y no solo una reafirmación de los (mismos) «hechos» (Fiscalía Nacional, 2017: 16-18). Como se dijo (Bascur y Peña, 2022: 25), esta circunstancia reviste im-

95. Mayer y Vera (2022b: 308) resaltan el efecto atenuado (un grado) con respecto a las restantes especies de esta circunstancia.

96. Latamente al respecto, tratándose de idéntica regla de la Ley 20.000, Figueroa y Salas (2013: 113-127).

97. En contra del texto expreso, Mayer y Vera (2022b: 307-308), quienes reconocen la posibilidad de que sea el tribunal quien podría aplicarla sin haber sido invocada por el fiscal del caso.

portancia capital en los supuestos de colaboración en un fraude informático (artículo 7, inciso segundo), en la medida que a nivel práctico suele identificarse al receptor de los fondos defraudados (mulero o intermediario electrónico).

3.2. Circunstancias agravantes especiales (artículo 10)

El artículo 10 establece dos circunstancias agravantes de responsabilidad de efecto ordinario en sus numerales 1 y 2, y una de efecto extraordinario en su inciso segundo.

La circunstancia del artículo 10, numeral 1, consiste en ejecutar 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». Se trata de una profundización del injusto (disvalor de acción) por la ejecución de la conducta desde una posición de superioridad configurada o establecida previamente por el titular de los datos afectados por el delito (si se quiere, un ataque de carácter alevoso).[98]

Por su parte, el numeral 2 del artículo 10 consiste en perpetrar el delito «abusando» de la «vulnerabilidad, confianza o desconocimiento» de «niños, niñas, adolescentes o adultos mayores». Aquí la atención no se centra en el agente, sino que en la potencial víctima (*lato sensu*) del delito informático (Mayer y Vera, 2022b: 313) Es relevante considerar las potenciales relaciones concursales entre los delitos de la LDI y los hechos constitutivos de *grooming* (artículo 366 quáter, inciso tercero, del Código Penal)[99] y de pornografía infanto-juvenil (artículo 367 quáter del mismo código).[100]

En tercer lugar, como agravación de efecto extraordinario (aumento en un grado de la pena respectiva), se contempla la «afectación» o «interrupción» de la provisión o prestación de «servicios de utilidad pública» (ejemplificados como electricidad, gas, agua, transporte, telecomunicaciones o servicios financieros), o el normal desenvolvimiento de los «procesos electorales» (regulados en la Ley 18.700), circunstancia que abarca servicios prestados tanto por entidades públicas como particulares, que constituye un listado meramente ejemplificativo y no taxativo y, como se desprende de la redacción, aplicable siempre que se constate una conexión entre el delito de la LDI y el efecto catastrófico (Mayer y Vera, 2022b: 314-316), o dicho de otro modo, que la incidencia informática ilegal sea la explicación prevalente de dicho efecto.

98. Al respecto, Biblioteca del Congreso Nacional (2022: 127-129). Para Mayer y Vera (2022b: 309-311) se trata de una especie de la circunstancia prevista en el artículo 12, numeral 7, del CP en el ámbito de la informática, esto es, la lesión de ciertas expectativas de confianza depositadas en encargados de la gestión o del cuidado de sistemas informáticos, siempre cuando se constate dicha especial vinculación.

99. Por todos, véase Scheechler (2012: 61 y ss.).

100. Esta numeración es producto de la reforma introducida por la Ley 21.522, publicada el 30 de diciembre de 2022. Con respecto a esta figura, véase Escobar (2021: 557 y ss.).

3.3. Comiso (propio) ampliado y comiso (impropio) por equivalencia (artículo 13)

El artículo 13, inciso primero, contempla como pena accesoria tanto el comiso bajo su formulación tradicional,[101] esto es, aquel que recae sobre los instrumentos y efectos del delito (artículo 31 del CP), como también en su formulación ampliada, esto es, el que recae sobre las «utilidades» que hubieren generado dichos instrumentos o efectos, cualquiera sea su naturaleza jurídica.[102] Básicamente, la regla *amplificaría* (de forma expresa) el alcance de la institución para así lograr *requisar* las ganancias patrimoniales obtenidas indebidamente con la perpetración del delito.[103]

Por otra parte, el inciso segundo, primera oración, contempla el comiso por valor equivalente (o comiso impropio) con respecto a las «especies» del inciso primero. Se trata de la requisición de valores (suma de dinero) en reemplazo de los efectos o instrumentos,[104] si por cualquier circunstancia (fáctica o legal) no es posible su enajenación forzosa entre el momento del hecho y el de la condena.[105] Esta institución es aplicable exclusivamente sobre el patrimonio de los condenados por esta clase de delitos, lo cual naturalmente se explica porque constituye la imposición de una pena conjunta (accesoria) a la pena privativa o económica principal. Finalmente, la segunda oración del inciso segundo dispone que si debido a la naturaleza de la información contenida en las especies decomisadas (piénsese en ciertas formas de *software* malicioso) ellas no pueden ser enajenadas a terceros, procede la destrucción total o parcial de los instrumentos y efectos de los cuales provengan.

4. Reglas procesales

4.1. Legitimación activa de ciertas autoridades (artículo 11)

El artículo 11 establece la posibilidad de iniciar, por parte de ciertas autoridades, estas investigaciones mediante la interposición de querellas, aunque exclusivamente en

101. Según se desprende de Mayer y Vera (2022b: 329), esta regla no se diferenciaría del artículo 31 del CP, de modo que esta última abarcaría el comiso de utilidades.

102. Como explica Hernández (2011b: 482-483), la consideración de las ganancias ilícitas o productos bajo el artículo 31 del Código Penal como «efectos» del delito, es una cuestión debatida, especialmente por la estipulación expresa del legislador en normas especiales, como, por ejemplo, bajo el inciso segundo del artículo 45 de la Ley 20.000 (drogas) y por remisión expresa a este, bajo el literal d) del artículo 33 de la Ley 19.913 (lavado de activos), como también por el artículo 13, número 2, de la Ley 20.393 (responsabilidad penal de las personas jurídicas). Por todos, véase Hasbún (2018: 425-429).

103. Roig (2016: 216). Favorables a esta institución, Matus y Ramírez (2021a: 147).

104. Gisbert (2022: 274 y ss.) da cuenta de los problemas prácticos de la institución en el derecho español. Para Mayer y Vera (2022b: 330), esta cláusula podría resultar problemática si los objetos no exhiben valor de mercado.

105. Al respecto, Ananías (2014: 164-166) y Guzmán (2008: 267). Para Mayer y Vera (2022b: 329-330) esta parte de la regla se basaría en la *inmaterialidad* de los objetos decomisados.

los casos donde la ejecución de los delitos interrumpa el normal funcionamiento de un servicio de utilidad pública, es decir, de aquellos ejemplificados en el artículo 10, inciso segundo: servicios de electricidad, gas, agua, transporte, telecomunicaciones o financieros. Se trata de un régimen de acción penal previa instancia institucional,[106] aplicable exclusivamente a las Delegaciones Presidenciales Regionales,[107] Delegaciones Presidenciales Provinciales,[108] y al Ministerio del Interior y Seguridad Pública,[109] constituyendo una manifestación de lo establecido en el artículo 111, inciso tercero, del CPP, y aplicable tanto para dar inicio al procedimiento, como para adherirse sobre aquellos que se encuentran en desarrollo.[110]

Esta regla equipara situaciones de grave conmoción pública (orden y seguridad), que tradicionalmente han estado ligadas a la legitimación activa de estos órganos, con la eventual incidencia cibernética sobre la denominada infraestructura crítica,[111] en la medida que, como indica Gorjón (2021: 83-84), la vida moderna se encuentra a merced de la intersección de una serie de sistemas informáticos que proveen servicios básicos para la población, como salud, energía e industria, entre otros.

4.2. Técnicas especiales de investigación (artículo 12)

El artículo 12, en sus incisos primero y segundo, regula las técnicas de investigación de *interceptación* telefónica u otros medios de comunicación[112] (artículo 222 a 225 del CPP), como también otros medios técnicos de investigación[113] (artículo 226 del CPP). Mientras que, en su inciso tercero, el agente encubierto en línea. En general, su previsión expresa está relacionada con la adaptación de la normativa para afrontar las nuevas circunstancias que implica la delincuencia informática, especialmente con respecto a su inmaterialidad y constante desarrollo (Mayer y Vera, 2022b: 320-321).

106. Sobre esta categoría, véase Núñez y Silva (2018: 146 y ss.).

107. La posibilidad de interponer querella se encuentra establecida en el literal h) en relación con el literal b) del artículo 2 de la Ley 19.175 Orgánica Constitucional sobre Gobierno y Administración Regional, LOCGA, contenida en el Decreto con Fuerza de Ley 1/2005 del Ministerio del Interior (*Diario Oficial*: 08/11/2005), y exclusivamente sobre hechos que comprometan el orden y tranquilidad públicas.

108. Su legitimación activa vía querella se halla establecida en el artículo 4 literal a) LOCGA, de forma idéntica que las Delegaciones Presidenciales Regionales (orden y tranquilidad públicas).

109. La legitimación activa penal para deducir querella por el ministro del Interior se encuentra prevista en el artículo 3 del Decreto con Fuerza de Ley 7.912 (Diario Oficial: 05/12/1927), específicamente, en el literal a) de su artículo 3, en los subliterales a) hasta c).

110. En este sentido, véase Mayer y Vera (2022b: 319).

111. En un sentido similar, véase Mayer y Vera (2022b: 320).

112. Como resaltan Mayer y Vera (2022b: 323-324), se trata de la captación de la información transmitida entre dispositivos (por ejemplo, mediante aplicaciones como Signal, Telegram o WhatsApp).

113. Se desprende de Mayer y Vera (2022b: 324) que una delimitación clara entre esta medida y la del artículo 222 no resulta nítida.

Como delitos objeto de estas técnicas investigativas especiales se contemplan los artículos 1 ataque a la integridad de un sistema informático, 2 acceso ilícito y espionaje informático, 3 interceptación ilícita, 4 ataque a la integridad de los datos informáticos, 5 falsificación informática y 7 fraude informático, excluyéndose la receptación informática (artículo 6) y el abuso de los dispositivos (artículo 8) básicamente en razón de su escasa penalidad comparativa (Biblioteca del Congreso Nacional, 2022: 276).[114] Dicho listado constituye un caso especial con respecto a las reglas generales al no exigirse que el hecho revista pena de crimen (artículos 222, inciso primero, y 226 del CPP),[115] considerando que la LDI tipifica exclusivamente simples delitos.

En relación con la diligencia de interceptación y a otros medios técnicos de investigación, la redacción es casi idéntica a la del artículo 226 bis, inciso primero, del Código Procesal Penal, esto es, se exige que la diligencia intrusiva sea *imprescindible*[116] y existan *fundadas sospechas* basadas en hecho determinados,[117] con la salvedad de operar tanto en casos de codelincuencia como de autoría individual, en la medida que esta se halla destinada a investigaciones donde «una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados» en la LDI;[118] además de exigir la presentación de un «informe previo detallado con respecto a los hechos y la posible participación».

En este sentido, el inciso segundo establece los requisitos que debe cumplir la orden judicial. Primero debe informar «circunstanciadamente el nombre real o alias y dirección física o electrónica del afectado por la medida»;[119] segundo, tienen que contar el tipo de diligencia autorizada; y en tercer lugar, la duración de esta. Con respecto a lo último, no existen limitaciones de tiempo prefijadas (como lo es tratándose del artículo 222, inciso cuarto, del CPP: períodos máximos de 60 días), facultando al tribunal para prorrogar el plazo concedido para lo cual deberá examinar cada vez la concurrencia de los requisitos establecidos en el inciso primero.

---

114. En un sentido similar, véase Mayer y Vera (2022b: 321).

115. Otros ejemplos de reglas excepcionales en este sentido son el artículo 226 bis, inciso primero, del CPP y el artículo 448 septies, inciso segundo, del CP. Similar, Mayer y Vera (2022b: 321).

116. Para Mayer y Vera (2022b: 321-322) dicha exigencia (imprescindible) se basaría en el principio de proporcionalidad otorgando a esta diligencia un carácter estrictamente subsidiario.

117. Mayer y Vera (2022b: 322) destacan la provisión expresa de este supuesto de hecho.

118. Por contraste, el artículo 411 octies, inciso tercero, del CP dispone que sea que se trate de una persona, un grupo de personas o de una organización delictiva. Mayer y Vera (2022b: 322-323) apuntan a que, si la actividad del autor consiste en la preparación del delito, dicha expresión (procesal) habría de tomarse en sentido de, a lo menos, tentativa, dada la excepcional tipificación de actos preparatorios y que la disposición habría prescindido del principal tipo delictivo de la LDI (abuso de los dispositivos).

119. Por largo tiempo y según el artículo 24, inciso segundo, de la Ley 20.000, y vía remisión, del artículo 33 literal a) de la Ley 19.913, dichos cuerpos legales eran los únicos que flexibilizaban la exigencia sobre la determinación de la identidad del imputado afectado por las medidas investigativas previstas en el artículo 222, inciso cuarto, en relación con el artículo 226 del CPP.

Ahora bien, el inciso tercero regula la técnica del agente encubierto (en línea). Al respecto, el artículo 25, inciso segundo, de la Ley 20.000 lo define como «el funcionario policial que oculta su identidad oficial y se involucra o introduce en las organizaciones delictuales o en meras asociaciones o agrupaciones con propósitos delictivos, con el objetivo de identificar a los participantes, reunir información y recoger antecedentes necesarios para la investigación». Luego, en la regulación de la LDI este difiere básicamente en tres aspectos:[120] no se exige como presupuesto de utilización la existencia de una asociación o agrupación delictiva, por cuanto la delincuencia cibernética se caracteriza esencialmente por la ejecución individual de comportamientos. Se requiere autorización judicial para su implementación (Mayer y Vera, 2022b: 327) y, finalmente, es aplicable en contextos virtuales y no físicos.[121]

Como requisitos para su utilización, la LDI exige (Mayer y Vera, 2022b: 327): autorización judicial previa; constatación de propósito legítimo y la existencia de una investigación.[122]

Como se sabe, un agente encubierto opera sobre una realidad delictiva preexistente y solo revela su ejecución,[123] circunstancia que explica su exención de responsabilidad por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre cuando: sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.

Así también, por igual razón las finalidades para las cuales puede intervenir están taxativamente enumeradas: i) esclarecer los hechos tipificados como delitos en la LDI; ii) establecer la identidad y participación de personas determinadas en la comisión de los mismos; iii) impedirlos; o iv) comprobarlos. Las acciones para alcanzar dichos fines se limitan a: intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido; obtener imágenes y, finalmente, grabaciones de las referidas comunicaciones.

Es importante mencionar que, en años recientes, la jurisprudencia de la Corte Suprema se ha pronunciado con respecto a la legalidad del *ciber patrullaje*, esto es, la navegación por plataformas digitales abiertas por parte de funcionarios policiales para detectar la posible comisión de delitos.[124] Sin embargo, por lo mismo, la regla en comento se refiere al despliegue del agente en «canales cerrados de comunicación» y

120. Resaltan su carácter de regulación especial, Mayer y Vera (2022b: 325).

121. El debate puede verse en Biblioteca del Congreso Nacional (2022: 133-134). Con respecto a la restricción al entorno virtual, en consonancia con el artículo 5 del CPP, Mayer y Vera (2022b: 325).

122. Con respecto a esto último, Mayer y Vera (2022b: 327) rechazan que una investigación pueda ser *iniciada* por la actuación de un agente encubierto en línea. Ahora bien, en la praxis es difícil que esto ocurra sin algún indicio previo (como un ciber-patrullaje legítimo), sin perjuicio de que, en nuestra opinión, la redacción no fuerza dicha interpretación.

123. Esto lo diferencia del denominado agente provocador, como resaltan Mayer y Vera (2022b: 328-329).

124. Esto es advertido por Mayer y Vera (2022b: 326-327).

no en fuentes plenamente accesibles al usuario medio. Por lo mismo, la autorización judicial previa es importante por cuanto el desarrollo de su función (en este contexto) implica usar una identidad falsa (perfil) e interactuar (intercambiar o enviar archivos ilícitos), nivel de intrusismo que solo puede justificarse mediando autorización judicial previa. Lo anterior se comprende sin perjuicio de autorizaciones otorgadas según el artículo 9, inciso primero, del CPP.

4.3. Preservación y custodia de antecedentes informáticos (artículo 14)

El artículo 14 dispone que los antecedentes de investigación que consistan en datos informáticos deberán ser objeto de especial custodia y preservación por el Ministerio Público, con arreglo a la normativa administrativa dictada al efecto por la Fiscalía Nacional.[125] Como se aprecia, se trata de una concreción de la regla general dispuesta en el artículo 188 del CPP, pues, tal como ocurre con respecto a las evidencias materiales o físicas, la evidencia informática recolectada durante la indagación igualmente debe ser preservada. A nuestro juicio, la regla tiene aplicación general en el sentido de que no se limita a evidencias obtenidas en la investigación de delitos informáticos, sino que sobre toda aquella incautada (bajo cualquier categoría de delito) y que corresponda al formato electrónico.

La implementación de un sistema de preservación y custodia constituye una operación compleja e incluye la adquisición de infraestructura informática específica. En este sentido, se distinguen cuatro etapas para el tratamiento de esta clase de especies: i) identificación, que tiene por objeto buscar y reconocer la evidencia digital potencialmente relevante para la investigación; ii) recolección, para incautar los dispositivos físicos en que se encuentra almacenada la información; iii) adquisición, que busca la obtención de copias o imágenes forenses íntegras de la evidencia digital, incluyendo contenido y estructura, y finalmente; iv) preservación, para la mantención de la integridad de la evidencia digital obtenida.

4.4. Preservación provisoria de datos informáticos (artículo 218 bis del Código Procesal Penal)

El artículo 18, número 1, incorporó el artículo 218 bis al CPP,[126] regla que dispone que el Ministerio Público podrá solicitar —a cualquier proveedor de servicio como dili-

125. Como afirman Mayer y Vera (2022b: 330-331), durante la tramitación legal se apuntó a que solo podría tratarse de información constitutiva de evidencia, en la medida que la regulación sobre información representativa de datos personales constituye afección de garantías fundamentales, y, por ende, requiere normativa legal (y no simplemente reglamentaria).

126. El numeral 2 suprimió del artículo 223 del CPP la expresión «telefónica», mientras que el numeral 3 reemplazó en el artículo 225 la voz «telecomunicaciones» por «comunicaciones».

gencia de investigación—[127] la conservación o protección de datos o informaciones concretas incluidas en un sistema informático bajo su disposición. Lo anterior, por un plazo de 90 días, prorrogable una sola vez y como máximo, hasta que se cumplan 180 días. Esta preservación es de carácter *provisorio* en la medida que rige mientras se desarrollan diligencias investigativas para solicitar judicialmente su entrega, especialmente tomando en cuenta las propiedades intrínsecas de esta clase de evidencia, vale decir, su volatilidad y fácil destructibilidad (Mayer y Vera, 2022b: 330-331).

Dicha institución deriva del artículo 16 del Convenio de Budapest, que impone a los Estados parte adoptar las medidas necesarias para que sus autoridades competentes ordenen u obtengan de manera similar la conservación rápida de datos informáticos específicos. Esto incluye los datos de tráfico que hayan sido almacenados mediante un sistema informático, en particular cuando existan motivos para creer que los datos son particularmente vulnerables a la pérdida o modificación, o que son y pueden ser de gran importancia en una investigación penal. De allí su interés y la relevancia de su preservación.

Es crucial la autorización judicial para la entrega de la información, en la medida que durante la tramitación se advirtió que la tenencia de metadata constituye, eventualmente, una injerencia de relevancia sobre derechos fundamentales: en muchos casos podría representar diversos aspectos de la vida privada de las personas (Biblioteca del Congreso Nacional, 2022: 69-70).

Dicha custodia implica un estricto *deber de reserva* por el proveedor. Por esto se reforzó penalmente con la tipificación en el artículo 36 B literal f) de la Ley General de Telecomunicaciones de vulnerar el deber de secreto previsto en el artículo 218 bis del CPP, mediante el acceso, el almacenamiento o la difusión de la información (simple delito: 3 años y 1 día hasta 5 años).[128]

Con respecto a la especificación de las obligaciones del proveedor una vez solicitada la preservación provisoria, el artículo segundo transitorio dispone la dictación de un reglamento. Dicho cuerpo legal definirá en detalle las obligaciones del proveedor entre el requerimiento de preservación y el requerimiento de entrega (una vez autorizado judicialmente).

127. El artículo 15 literal c) define «prestadores de servicios» como toda «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».

128. Se considera también como objeto de la conducta los antecedentes derivados de las diligencias de los artículos 219 y 222 del CPP, esto es, copias de comunicaciones provenientes de dicha clase de empresas y de la interceptación de cualquier clase de telecomunicación (abarcando, se comprende, telefónicas).

5. Otras cuestiones relevantes

El artículo primero transitorio reproduce las reglas sobre derecho intertemporal penal previstas en el artículo 18 del Código Penal. En lo que aquí interesa, su inciso quinto dispone que el delito (informático) 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». En la medida que la LDI no tipifica delitos (propios) de omisión (pura o de impedimento de un resultado) y en concordancia a lo dispuesto en el artículo (único) transitorio de la Ley 21.402 (publicada el 24 de diciembre de 2021),[129] la referencia podría servir de insumo argumentativo para la postulación de omisiones punibles en contextos regulativos ajenos a los delitos contra las personas (en concreto: delitos informáticos y delitos de incendio previstos en el CP),[130] como tradicionalmente se afronta su eventual inconstitucionalidad por infracción al principio de legalidad (a partir del inciso primero del artículo 492 de dicho código).[131]

Para finalizar, el 20 de diciembre de 2022 comenzaron a regir, según el artículo tercero transitorio, los artículos 19 y 21, esto es, la consideración de los tipos delictivos previstos en el Título 1 como ilícitos antecedentes para el tipo de lavado de activos tipificado en el artículo 27 de la Ley 19.913 y para establecer la responsabilidad penal de personas jurídicas, mediante el artículo 1 de la Ley 20.393.[132]

Referencias

Aboso, Gustavo (2017). *Derecho penal cibernético*. Buenos Aires: BdeF.

Alfonsi, Gustavo y Javier García (2016). «Radios comunitarias y su criminalización en Chile». *Anuario de Derechos Humanos*, 12: 153-171. Disponible en https://anuariocdh.uchile.cl/index.php/ADH/article/view/42747

Ananías, Rodrigo (2014). «El comiso de ganancias». *Revista de Estudios de la Justicia*, 21: 153-196. Disponible en https://rej.uchile.cl/index.php/RECEJ/article/view/36328

Balmaceda, Gustavo (2021). *Manual de derecho penal . Parte especial*. 4.ª ed. Tomo II. Santiago: Librotecnia.

129. Esta ley modificó los artículos 474, 475 y 476 del CP, vale decir, las figuras de incendio organizadas en el § IX del Título 9 del Libro II del CP («Del incendio y otros estragos»), párrafo que no contiene ningún delito de omisión.

130. En contra de esta lectura, véase Mayer y Vera (2022b: 272).

131. Para más información, véase Piña (2014: 204).

132. Se ha prescindido el tratamiento relativo a la responsabilidad penal de las personas jurídicas en relación con esta categoría de delitos. Al respecto, véase Mayer y Vera (2022b: 316-318).

Bascur, Gonzalo y Rodrigo Peña (2022). «Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Primera parte». *Revista de Estudios de la Justicia*, 37: 1-38. DOI: 10.5354/0718-4735.2022.67885.

Becker, Sebastián y Pablo Viollier (2020). «La implementación del convenio de Budapest en Chile: Un análisis a propósito del proyecto legislativo que modifica la Ley 19.223». *Revista de Derecho* (Universidad de Concepción), 248: 75-112. DOI: 10.29393/RD248-13ICSB20013.

Biblioteca del Congreso Nacional (2022). Historia de la ley 21.459. Establece normas sobre delitos informáticos, *deroga la Ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest*. Santiago: Biblioteca del Congreso Nacional. Disponible en https://bit.ly/3FmJd5h.

Castillo, Alejandra (2017). «La sistemática general de los delitos cibernéticos y los delitos cibernéticos propios en el derecho penal alemán: La necesidad de una regulación diferenciada». *Revista de Derecho Penal y Criminología*, 7: 32-62.

Couso, Jaime (2018). «Relevancia penal de la intromisión del empleador en los correos electrónicos de sus trabajadores». *Revista de Derecho* (Universidad Católica del Norte), 2: 29-76. Disponible en https://bit.ly/3uD9eqV.

Cox, Juan Pablo (2005). «Leyes penales especiales». *Revista de Derecho* (Universidad Adolfo Ibáñez), 2: 667-671.

De la Mata, Norberto (2018). «Tema 18: Delitos contra los sistemas de información». En Norberto de la Mata, Jacobo Dopico, Juan Antonio Lascuraín y Adán Nieto, *Derecho penal económico y de la empresa* (pp. 727-759). Madrid: Dykinson.

De la Mata, Norberto y Desirée Bariñas (2014). «La protección penal de la vida privada en nuestro tiempo social: ¿Necesidad de redefinir el objeto de tutela?». *Revista de Derecho Penal y Criminología*, 11: 13-92. Disponible en https://bit.ly/3Vt7yM6.

De la Mata, Norberto y Leyre Hernández (2009). «El delito de daños informáticos: Una tipificación defectuosa». *Estudios Penales y Criminológicos*, 29: 311-362. Disponible en https://bit.ly/3MY6wVm.

Donoso, Lorena y Carlos Reusser (2021). *Protección de datos personales*. Santiago: Academia Judicial de Chile. Disponible en https://bit.ly/3FkeCVY.

Escobar, Javier (2021). «Delitos de producción, distribución y almacenamiento de pornografía infanto-juvenil». En Miguel Cillero, Francisco Maldonado y Ester Valenzuela (editores), *Protección frente a la violencia contra niños, niñas y adolescentes en Chile. Aspectos jurídicos y sociales* (pp. 557-583). Santiago: Legal Publishing.

Figueroa, Renzo y Rubén Salas (2013). «La cooperación eficaz: Herramienta de política criminal y atenuante especial de la Ley 20.000». *Revista Jurídica del Ministerio Público*, 56: 113-127. Disponible en https://bit.ly/43YiEN7.

Fiscalía Nacional (2017). *Oficio FN Núm. 936/2017*. Santiago: Fiscalía Nacional de Chile.

Gisbert, Marta (2022). «Los controvertidos requisitos del decomiso ampliado: Indicios objetivos fundados del origen ilícito de los bienes». *Revista Ius et Praxis*, 3: 274-286. Disponible en https://bit.ly/3N5kJ38.

González, Patricio (2013). «Desde el delito computacional hasta el delito de alta tecnología». En Álex van Weezel (editor), *Humanizar y renovar el derecho penal: Estudios en memoria de Enrique Cury* (pp. 1073-1095). Santiago: Legal Publishing.

Gorjón, María Concepción (2021). «Sabotaje informático a infraestructuras críticas: Análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista». *Revista de Derecho Penal y Criminología*, 23: 77-124. DOI: 10.5944/rdpc.25.2021.28405.

Guzmán, José Luis (2008). *La pena y la extinción de la responsabilidad penal*. Buenos Aires: BdeF.

Hasbún, Cristóbal (2018). «El comiso penal en la legislación estadounidense como horizonte comparativo frente al Proyecto de Nuevo Código Penal». *Ius et Praxis*, 3: 421-452. DOI: 10.4067/S0718-00122018000300421.

Hernández, Héctor (2011a). «Comentario Artículo 1». En Héctor Hernández y Jaime Couso (directores), *Código Penal comentado. Parte general. Doctrina y jurisprudencia* (pp. 7-105). Santiago: Legal Publishing.

—. (2011b). «Comentario Artículo 31». En Héctor Hernández y Jaime Couso (directores), *Código Penal comentado. Parte general. Doctrina y jurisprudencia* (pp. 482-485). Santiago: Legal Publishing.

Jijena, Renato (2008). «Delitos informáticos, internet y derecho». En Luis Rodríguez (coordinador), *Delito, pena y proceso: Libro homenaje a la memoria del profesor Tito Solari Peralta* (pp. 145-162). Santiago: Jurídica de Chile.

Lara, Juan Carlos, Manuel Martínez y Pablo Viollier (2014). «Hacia una regulación de los delitos informáticos basada en la evidencia». *Revista Chilena de Derecho y Tecnología*, 1: 101-137. DOI: 10.5354/0719-2584.2014.32222.

Linares, María Belén (2020). «Delitos informáticos en el Código penal argentino». *Revista Chilena de Derecho y Ciencia Política*, 2: 122-144. Disponible en https://bit.ly/42CjRsn.

Magliona, Claudio y Macarena López (1999). *Delincuencia y fraude informático*. Santiago: Jurídica de Chile.

Malamud, Samuel (2018). «Sabotaje informático: ¿La exigencia de daño grave como elemento del injusto?». *Revista Jurídica del Ministerio Público*, 72: 143-161. Disponible en https://bit.ly/3OVciro.

Mañalich, Juan Pablo (2011). «El delito como injusto culpable: Sobre la conexión funcional entre el dolo y la consciencia de la antijuridicidad en el derecho penal chileno». *Revista de Derecho* (Universidad Austral de Chile), 1: 87-115. DOI: 10.4067/S0718-09502011000100005.

Mata, Ricardo (2006). «La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías». *Revista Penal;* 18, 217-235.

Matus, Jean Pierre y María Cecilia Ramírez (2021a). *Manual de derecho penal chileno. Parte general*. 2.ª ed. Valencia: Tirant lo Blanch.

Matus, Jean Pierre y María Cecilia Ramírez (2021b). *Manual de derecho penal chileno. Parte especial*. 4.ª ed. Valencia: Tirant lo Blanch.

Mayer, Laura (2017). «El bien jurídico protegido en los delitos informáticos». *Revista Chilena de Derecho* (Pontificia Universidad Católica de Chile), 1: 235-260. DOI: 10.4067/S0718-34372017000100011.

—. (2018). «Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos». *Ius et Praxis*, 1: 159-206. Disponible en https://bit.ly/3EXFnoT.

Mayer, Laura y Guillermo Oliver (2020). «El delito de fraude informático: Concepto y delimitación». *Revista Chilena de Derecho y Tecnología*, 1: 151-184. DOI: 10.5354/0719-2584.2020.57149.

Mayer, Laura y Jaime Vera (2019). «El documento como objeto material de las falsedades documentales y del sabotaje informático en el derecho penal chileno». *Política Criminal*, 27: 419-455. DOI: 10.4067/S0718-33992019000100419.

—. (2020). «El delito de espionaje informático: Concepto y delimitación». *Revista Chilena de Derecho y Tecnología*, 2: 221-256. DOI: 10.5354/0719-2584.2020.59236.

—. (2021). «La nueva regulación del delito de uso fraudulento de tarjetas de pago y transacciones electrónicas». *Revista de Ciencias Penales*, 2: 519-558. Disponible en https://bit.ly/3XTdbor.

—. (2022a). «La falsificación informática: ¿Un delito necesario?». *Revista Chilena de Derecho y Tecnología*, 1: 261-286. DOI: 10.5354/0719-2584.2022.65299.

—. (2022b). «La nueva ley de delitos informáticos». *Revista de Ciencias Penales*, 3: 267-336. Disponible en https://bit.ly/3XcqssA.

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

Moscoso, Romina (2014). «La Ley 19.223 en general y el delito de *hacking* en particular». *Revista Chilena de Derecho y Tecnología*, 1: 11-78. DOI: 10.5354/0719-2584.2014.32220.

Novoa, Ignacio y Leonor Venegas (2020). *Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional. Memoria para optar al grado de licenciado en Ciencias Jurídicas y Sociales*. Santiago: Universidad de Chile. Disponible en https://bit.ly/3ulog4k.

Núñez, Raúl y Manuel Silva (2018). «La acción penal regulada en el artículo 162 del Código Tributario». *Revista de Derecho* (Universidad de Valparaíso), 52: 145-172. DOI: 10.4067/S0718-68512018005000302.

Oliver, Guillermo (2013). *Delitos contra la propiedad*. Santiago: Legal Publishing.

Oxman, Nicolás (2013). «Estafas informáticas a través de internet: Acerca de la imputación penal del *phishing* y el *pharming*». *Revista de Derecho* (Pontificia Universidad Católica de Valparaíso), 41: 211-262. Disponible en https://bit.ly/3iyosKU.

Piña, Juan Ignacio (2014). *Derecho penal: Fundamentos de la responsabilidad*. 2.ª ed. Santiago: Legal Publishing.

Roig, Margarita (2016). «La regulación del comiso: El modelo alemán y la reciente reforma española». *Estudios Penales y Criminológicos,* XXXVI: 199-279. Disponible en https://bit.ly/3CsqzXb.

Rojas, Luis Emilio (2017). *Teoría funcionalista de la falsedad documental*. Madrid: Marcial Pons.

Rosenblut, Verónica (2008). «Punibilidad y tratamiento jurisprudencial de las conductas de *phishing* y fraude informático». *Revista Jurídica del Ministerio Público*, 35: 254-266. Disponible en https://bit.ly/3XPsnmL.

Scheechler, Christian (2012). «El *childgrooming* en la legislación penal chilena: Sobre los cambios al artículo 366 quáter del Código Penal introducidos por la Ley 20.526». *Revista Chilena de Derecho y Ciencia Política*, 1: 55-78. DOI: /10.7770/rchdcp-V3N1-art351.

Tiedemann, Klaus (2010). *Manual de derecho penal económico: Parte general y especial*. Trad. por Alfonso Galán Muñoz (pp. 439-450). Valencia: Tirant lo Blanch.

Wassmer, Martin (2017). «Sistemas penales comparados: Delitos informáticos *(Cybercrimes)*». *Revista Penal*, 40: 250-255.

Weigend, Thomas (2013). «Sociedad de la información y derecho penal: Relación general». *Revue Internationale de Droit Pénal*, 84: 19-47. Disponible en https://bit.ly/3VKxr9X.

Sobre los autores

Gonzalo Bascur es profesor de Derecho Penal en la Universidad Austral de Chile, sede Puerto Montt. Abogado y magíster en Derecho Penal por la Universidad de Talca y Universitat Pompeu Fabra. Su correo electrónico es gonzalo_bascur@hotmail.com.

Rodrigo Peña es profesor de Derecho en la Universidad Autónoma de Chile de Santiago. Abogado y magíster en Derecho Penal por la Universidad de Talca y Universitat Pompeu Fabra. Su correo electrónico es rodrigo.pena13@gmail.com.

REVISTA DE ESTUDIOS DE LA JUSTICIA

La *Revista de Estudios de la Justicia* es publicada, desde 2002, dos veces al año por el Centro de Estudios de la Justicia de la Facultad de Derecho de la Universidad de Chile. Su propósito es contribuir a enriquecer el debate jurídico en el plano teórico y empírico, poniendo a disposición de la comunidad científica el trabajo desarrollado tanto por los académicos de nuestra Facultad como de otras casas de estudio nacionales y extranjeras.

DIRECTOR

Álvaro Castro

(acastro@derecho.uchile.cl)

SITIO WEB

rej.uchile.cl

CORREO ELECTRÓNICO

cej@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io)