REVISTA
DE ESTUDIOS DE LA JUSTICIA

NÚM. 37 (2022) • PÁGS. 1-38 • DOI 10.5354/0718-4735.2022.67885
RECIBIDO: 29/7/2022 • APROBADO: 28/9/2022 • PUBLICADO: 31/12/2022

DOCTRINA

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

Computer crimes in Chile: criminal offenses, penalties and procedural rules of Law No. 21.459. Part one

Gonzalo Bascur
Universidad Austral de Chile

Rodrigo Peña
Universidad Autónoma de Chile

RESUMEN Con la publicación de la Ley 21.459 el Estado de Chile actualizó la normativa relativa a los delitos informáticos y estableció nuevos tipos penales, reglas de sanción y procesales. Este texto ofrece, como primera parte del análisis de la regulación, una introducción sobre el contenido de ilicitud de esta clase de infracciones y un desarrollo sistemático a través de una aproximación a los tipos delictivos de acceso ilícito (artículo 2), fraude informático (artículo 7), receptación informática (artículo 6) y abuso de los dispositivos (artículo 8).

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

ABSTRACT With the publication of Law 21,459, the State of Chile updated the regulations on computer crimes, establishing new types of offenses, specif rules of punishment and procedural rules. This text offers, as a first part of the analysis of the regulation, an introduction on the illegal content of this kind of offenses and a systematic development through a special part approach on the offenses of illicit access (art. 2), computer fraud (art. 7), computer theft (art. 6) and abuse of devices (art. 8).

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

1. Introducción

El 20 de junio de 2022 se publicó en el *Diario Oficial* la Ley 21.459 o Ley de Delitos Informáticos (LDI),[1] que reemplaza a la Ley 19.223 que «tipifica figuras penales relativas a la informática» (LTFI),[2] publicada el 7 de junio de 1993. El antecedente inmediato de esta nueva regulación es la normativa prevista en el Convenio sobre la Ciberdelincuencia,[3] coloquialmente denominado Convenio de Budapest, celebrado en Hungría el 23 de noviembre de 2001, y finalmente promulgado por el Estado de Chile a través del Decreto Supremo número 83/2017 del Ministerio de Relaciones Exteriores,[4] y publicado el 28 de agosto de 2017.[5]

El título 1 de la normativa, «De los delitos informáticos y sus sanciones», establece tipos delictivos propiamente tales (artículos 1 a 8), así como también circunstancias modificatorias de efecto ordinario (artículo 10, número 1 y 2) y extraordinario (artículo 9 y artículo 10 inciso segundo); el título 2, «Del procedimiento», contempla reglas sobre legitimación activa institucional (artículo 11), técnicas especiales de investigación (artículo 12), comiso (artículo 13) y tratamiento de evidencia (artículo 14); y finalmente, el título 3, «Disposiciones finales», aglutina diversas clases de reglas, entre otras, definiciones legales específicas (artículo 15), explicitación del elemento normativo «autorización» previsto en el tipo del artículo 2 (artículo 16), derogación y reenvío de las referencias a la Ley 19.223 hacia la presente regulación (artículo 17), modificaciones al Código Procesal Penal (artículo 18), establecimiento de los delitos previstos en el título 1 como ilícitos antecedentes para el delito de lavado de activos (artículo 19) y la configuración de responsabilidad penal de las personas jurídicas (artículo 21), tipificación de un nuevo delito (artículo 21) en el literal f) del artículo 36 b) de la Ley 18.168,[6] y tres artículos transitorios.[7] Inexplicablemente, no se consagró

1. 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».

2. Una revisión puede hallarse en Donoso y Reusser (2021: 115-127), Magliona y López (1999: 119-178) y Jijena (2008: 157-160). Para antecedentes y estadísticas relevantes de su aplicación práctica, véase Lara y otros (2014: 101 y ss.).

3. Lo destacan, Mayer (2017: 244-246), Mayer y Oliver (2020: 169-170). Crítico al respecto, Cortés (2017: 186-189). Un resumen en Donoso y Reusser (2021: 108-114), así como un juicio crítico en Balmaceda (2009: 91-94).

4. Una exposición detallada puede consultarse en Novoa y Venegas (2020: 51 y ss.).

5. Véase, por todos, Becker y Viollier (2020: 79-81), Novoa y Venegas (2020: 57-58).

6. Ley General de Telecomunicaciones, LGT, publicada en el *Diario Oficial* el 2 de octubre de 1982.

7. Desde la perspectiva sustantiva, destaca el inciso quinto del artículo 1, que incorpora bajo la definición de «perpetración» cuando «se incurre en la omisión punible», lo cual abre espacio al debate sobre la posibilidad de reconocer omisiones (impropias) bajo el texto legal, de forma similar a la Ley 21.402 (publicada el 24 de diciembre de 2021) en el inciso quinto de su artículo (único) transitorio, con relación a los delitos de incendio.

ninguna regla especial para abordar el problema de la territorialidad en esta clase de delitos.[8]

Se trata de una regulación exhaustiva sobre diversos aspectos que involucra la delincuencia informática, razón por la cual su estudio será dividido en dos partes, las que serán publicadas en forma sucesiva. El presente texto versa exclusivamente sobre el desarrollo de las cuestiones sustantivas generales y los tipos delictivos de acceso ilícito (artículo 2), receptación de datos informáticos (artículo 6), fraude informático (artículo 7) y abuso de los dispositivos (artículo 8), reservándose el segundo para el tratamiento de los demás aspectos de fondo y procedimentales.[9]

1.1 El injusto informático

Actualmente, por *tecnologías de la información y comunicación* se designan todos los modos de sistematización y transmisión de información (por ejemplo, la banca y comercio electrónico, redes sociales, etcétera),[10] y que, debido a su relevancia social han sido objeto de regulación penal desde la época de la codificación.[11] En este contexto, las computadoras, entendidas como sistemas de almacenamiento, procesamiento y transferencia directa de datos[12] (o tratamiento automatizado de datos),[13] revisten una importancia capital, tornándose asimismo relevantes los conceptos de delito informático o cibernético en sentido *propio* (o *estricto)*.[14]

Inicialmente, la protección penal estuvo focalizada en los datos informáticos almacenados en los respectivos terminales, en la medida que estos representaban, digitalmente, específicos bienes jurídicos tradicionales. Sin embargo, tanto el carácter inmaterial de los datos informáticos, [15] consistentes en simples flujos o impulsos

8. Destacan esta dificultad, Aboso (2016: 77-88) y Castillo (2017: 38). Esto resulta llamativo, considerando la regla especial del artículo 374 ter del Código Penal.

9. Esto es, los tipos previstos en los artículos 1, 3, 4, 5, las reglas de sanción de los artículos 9, 10 y 13, y las normas procesales de los artículos 11, 12, 14 y el artículo 218 bis del Código Procesal Penal

10. En este sentido, Aboso (2017: 1-3), Cortés (2017: 176-179), Malamud (2018: 143), Mayer (2017: 248-251; 2018a: 163-164), Medina (2014: 96-97) y Miró (2012: 25).

11. Los primeros sistemas de comunicación interpersonal tutelados consistieron en la correspondencia epistolar o postal (artículos 155 y 156, Código Penal) y la correspondencia telegráfica, entendida como la remisión codificada de mensajes escritos a través de señales eléctricas (artículos 156, 195, 333, 334, 335, 337, 338 y 339, Código Penal). La tutela penal de un tercer sistema de comunicación se produce recién en 1982 con la promulgación de la LGT.

12. Véase Mayer (2017: 248-249), Mayer y Vera (2020: 224), y Weigend (2013: 80-81).

13. Véase Arocena (2012: 951).

14. Lo desarrolla Castillo (2017: 34-35, 40 y ss.). Véase González (2013: 1073-1092). Un panorama resumido puede apreciarse en Donoso y Reusser (2021: 95-107).

15. Circunstancia resaltada por Castillo (2017: 35-36), Gorjón (2021: 103) y Jijena (2008: 150, 152). Se manifiesta en contra, Moscoso (2014: 18-19, 24).

electromagnéticos,[16] como también la importancia que han adquirido y por ende, revisten en sí mismos los procesos de transmisión y tratamiento de estos,[17] incluyendo el funcionamiento de las redes telemáticas y la prestación de cruciales servicios de utilidad pública, explican la razón por la cual puede considerarse, a partir del derecho vigente, el surgimiento de un bien jurídico autónomo consistente en la integridad, confidencialidad y disponibilidad de los sistemas informáticos,[18] y de los datos contenidos en ellos.[19] En este sentido, los datos y sistemas informáticos se han transformado en una plataforma vital para el desarrollo de intereses individuales (intimidad, gestión de activos patrimoniales, libertad de expresión) y para el mantenimiento de objetivos macrosociales e institucionales (seguridad nacional, la estructura de servicios masivos, economía),[20] en la medida que casi ninguna actividad de la vida se halla desconectada del tratamiento automatizado de datos a través de sistemas insertos en redes computacionales y telemáticas.[21]

Sobre la base de lo anterior, ciertos hitos de la Ley de Delitos Informáticos,[22] y considerando al Convenido de Budapest,[23] nos parece que los tipos delictivos pre-

16. Propiedad que generaba dificultades para la interpretación analógica de actos computacionales respecto de conductas típicas preexistentes (por ejemplo, violación de morada, hurto o estafa). Así Castillo (2017: 55) y Tiedemann (2010: 440-441). Similar, Mayer y Vera (2022: 269). Un resumen del problema (la naturaleza incorpórea) puede revisarse en Mata (2003: 76-78).

17. Aspecto destacado por Miró (2012: 37-39, 58).

18. En contra, a partir de la regulación previa, Alvarado (2022: 523-524), para quien los delitos de intromisión e indiscreción de la LTFI protegerían la intimidad.

19. En tal sentido, Castillo (2017: 41) y Rueda (2020: 203 y ss.). Similar, De la Mata (2018: 732-733, 742-744). Por otra parte, crítica sobre la consideración copulativa de tales propiedades, pero no de la idea central (autonomía del bien jurídico), Mayer (2017: 245-246). Con relación a los antecedentes de producción de regulación previa, véase Winter (2013: 280-281). Una opinión contraria en nuestro medio, en Donoso y Reusser (2021: 98-100, 116-117), y con relación a los proyectos de ley de inicios de siglo, en Londoño (2004: 171 y ss.). En derecho comparado, el debate consiste en si se trata de un contenido de injusto independiente, o tan solo la reformulación virtual de ataques contra bienes jurídicos tradicionales. Para el contexto español, véase Castiñeira y Estrada (2021: 168-170) y Rueda (2020: 200-204). Según indica Mayer (2017: 246-248), la segunda posición sería dominante en Alemania como afirma Tiedemann (2010: 440-441). Otra opinión al respecto en Castillo (2017: 41).

20. Véase Castillo (2017: 33-34), Mayer (2018a: 163-164) y Rueda (2020: 207-208, 210-211). Lo restringe a ciertas materias, Jijena (2008: 148) destacando la subsidiariedad que debería exhibir la herramienta penal en esta materia (155-156).

21. Con referencia al surgimiento de nuevos intereses de tutela (por ejemplo identidad digital), véase Solari (2022: 126 y ss.).

22. Algunos hitos de la regulación nacional, la cláusula concursal prevista en el artículo 9 de la Ley 20.009 y la irrelevancia de la clase de dato informático objeto de alguno de los comportamientos de intrusismo para rellenar la tipicidad, como apunta Alvarado (2022: 526), entre otros.

23. Instrumento que constituye el esfuerzo regulatorio más relevante en la unificación de las tipologías delictivas asociadas a la realidad informática, como indica Castillo (2017: 33, número 4). De *lex ferenda*, lo aprueban con matices, Lara y otros (2014: 119-120).

vistos en dicha ley constituyen, como expresamos más arriba, delitos informáticos o cibernéticos en sentido *propio* (o *estricto*), esto es, conductas que tienen como objeto de ataque los componentes lógicos de un sistema informático,[24] tanto los datos específicamente considerados como el funcionamiento de un sistema concreto (o en estricto rigor, el tratamiento de datos informáticos efectuado por este),[25] cuya ejecución incide perjudicialmente sobre alguna de sus tres condiciones básicas de operación:[26] integridad, confidencialidad y disponibilidad de datos o de un sistema, propiedades que, conjunta o individualmente consideradas, representan un contenido de antijuridicidad autónomo,[27] expresivo del menoscabo de un bien jurídico de carácter colectivo o supraindividual.[28]

1.2 Sistemática de la Ley 21.459

Aunque se puede reconocer una confusión entre fenomenología y derecho en el tratamiento dogmático de estos delitos,[29] ocasionado por la superposición de fenómenos criminológicos y categorías jurídicas (*DoS*, *hacking*, *phishing*, etcétera),[30] nos parece que el contenido de injusto previamente desarrollado permite sistematizar, desde una aproximación jurídica basada en la fisonomía de los comportamientos, gran parte de los tipos delictivos previstos en la Ley de Delitos Informáticos.

Así, las figuras pueden ser ordenadas a través de las siguientes clasificaciones: i) atentados contra la integridad (artículos 1 y 4), ii) contra la disponibilidad (artículo 3 inciso primero) y iii) contra la confidencialidad de los datos informáticos o sistemas

24. Véase, González (2013: 1081-1083), Lara y otros (2014: 108-109, 112), Mayer (2018a: 160-161), Mayer y Vera (2022: 267), Moscoso (2014: 13-14) y Rosenblut (2008: 257). Similar, añadiendo la relevancia de los involucrados, Jijena (2008: 148, 150-152). En general, para la evolución de esta conceptualización, véase González (2013: 1072-1085), Magliona y López (1999: 33-63).

25. Crítica de este triple enfoque, Mayer (2017: 237, 248-255), Mayer (2018a: 163-166), Mayer y Vera (2019: 433-434, número 37; 2020: 277), Mayer y Oliver (2020: 154-155, 174) sosteniendo que lo protegido es la funcionalidad informática, concepto que abarca el desenvolvimiento o funcionalidad regular de los procesos automatizados sobre datos que ejecutan los sistemas informáticos, específicamente, con el almacenamiento, tratamiento y transferencia de información, en tanto dichos procesos representan un presupuesto esencial para realización de múltiples intereses socialmente valorados (individuales y colectivos). En la misma línea, Malamud (2018: 149-150-151). Por su parte, Magliona y López (1999: 65, 132, 138, 254) proponen el carácter pluriofensivo, incluyendo bienes informáticos propiamente tales.

26. Malamud (2018: 144), González (2013: 1088-1089, 1094) y Rueda (2020: 209). Lo describen críticamente, Balmaceda (2021: 813-815), Mayer (2017: 245-246, 251) y Weigend (2013: 81 y ss.).

27. Véase Miró (2012: 34) y Rueda (2020: 204 y ss.).

28. En el mismo sentido, González (2016: 62, 65 y 68), Mayer (2017: 252-253), Mayer y Oliver (2020: 175), Malamud (2018: 151) y Rueda (2020: 205 y ss.).

29. Véase González (2013: 1095) y Londoño (2004: 171-175). Crítico, Balmaceda (2009: 63-68).

30. Véase Cortés (2017: 183 y ss.) y González (2013: 1081, 1087-1088).

informáticos (artículos 2 y 3), así como también ciertas iv) conductas instrumentales (artículo 8) o de aprovechamiento (artículo 6) y finalmente, v) tipos de naturaleza mixta (artículos 5 y 7).

Por atentados contra la integridad de datos y sistemas informáticos se comprende la dimensión que abarca su existencia o incolumidad y que se manifiesta en actos de modificación, alteración y eliminación no autorizada de los mismos. Se emplea tradicionalmente la expresión *sabotaje* informático para designar conductas de destrucción e inutilización,[31] mientras que *fraude* informático para actos de manipulación o alteración.[32] En este sentido, la Ley 21.459 establece como figuras de sabotaje, pero incluyendo también acciones propias de *fraude*, a los tipos delictivos de ataque contra la integridad de un sistema informático del artículo 1 y de ataque contra datos del artículo 4.

Los ii) atentados contra la disponibilidad de los datos o sistemas se refieren a la mantención permanente de estos para su empleo a voluntad por el titular,[33] garantizando así la ausencia de incidencias o perturbaciones no consentidas que obstaculicen su utilización. En esta línea, el artículo 3 inciso primero castiga las acciones de interferencia o interrupción sobre la transmisión de datos.

Se comprenden como iii) atentados contra la confidencialidad de los sistemas o datos informáticos, actos que violentan la expectativa de exclusión que ostenta el usuario-titular de un sistema en la gestión de los datos almacenados en su interior, protegiéndose la restricción o limitación de acceso y conocimiento de estos frente a terceros.[34] Las figuras pertinentes corresponden a: a) tipo de acceso ilícito, previsto en el artículo 2 inciso primero; b) espionaje informático, que opera como subtipo calificado del anterior, establecido en el inciso segundo, primera oración; c) divulgación de datos obtenidos ilegalmente, tipificado en el artículo 2 inciso segundo, segunda oración, y en el inciso tercero[35] y, finalmente, d) tipo de interceptación ilícita previsto en el artículo 3.

Por otra parte, iv) es posible reconocer dos delitos que no obedecen con nitidez a las categorías previas, bien por resultar instrumentales o funcionales para la ejecución de las figuras anteriores,[36] o porque constituyen actos posteriores o subsecuentes

31. Véase Alvarado (2022: 532), Cortés (2017: 183-184), Donoso y Reusser (2021: 105-106), Jijena (2008: 149), Mayer (2017: 238, 253; 2018a: 161, 166-167) y Moscoso (2014: 13-14). Similar, Lara y otros (2014: 110).

32. Véase Alvarado (2022: 531), Donoso y Reusser (2021: 103), González (2013: 1077, número 10), Jijena (2008: 148-149), Mayer (2017: 238, 253; 2018a: 161, 166-167), Mayer y Vera, (2020: 223) y Mayer y Oliver (2020: 154).

33. Véase Mayer (2017: 245).

34. Véase Jijena (2008: 149), Donoso y Reusser (2021: 106-107).

35. Véase sección 2.

36. Véase Aboso (2017: 340-341), Castillo (2017: 43 y 50), Mayer (2018a: 167) y Weigend (2013: 87-89).

de aprovechamiento. Así, el artículo 8 tipifica el abuso de los dispositivos,[37] hecho relativo a la gestión o intermediación de elementos (incluyendo datos informáticos) necesarios para la ejecución de ciertos delitos taxativamente enumerados. Y el artículo 6 tipifica la denominada receptación informática,[38] conducta consistente tanto en actos de disfrute de los efectos de datos provenientes de un catálogo cerrado de delitos informáticos, como de preparación.

Finalmente, v) existen dos tipos delictivos cuya lesividad es compleja de establecer, porque se puede reconocer en ellos la naturaleza de delitos informáticos o cibernéticos en sentido impropio (o delitos computacionales), en la medida que representan un delito jurídicamente preexistente perpetrado por medios informáticos.[39] Y porque exhiben propiedades de delitos informáticos en sentido estricto al comprometer la integridad informática. Nos referimos al *fraude informático*, del artículo 7,[40] asociado a la fenomenología denominada como *estafa informática*,[41] y a la *falsificación informática*, establecido en el artículo 5.

Ahora bien, el debate de si estos delitos constituyen figuras de lesión o de peligro (abstracto) en contra del bien jurídico informático propiamente tal (o contra los bienes jurídicos tradicionales involucrados en el injusto),[42] y cómo la adopción de una u otra posición incide en la operación de subsunción (función dogmático-interpretativa del bien jurídico), es una cuestión que no será desarrollada en el presente trabajo, ya que su objetivo reside solo en la exposición de los elementos esenciales de la tipicidad y el régimen de sanción de la nueva regulación.

1.3 Definiciones legales expresas

El artículo 15 contempla conceptos legales claves para la interpretación de los tipos penales.[43] El literal a) define *datos informáticos* como «toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento

37. Véase sección 5.

38. Véase sección 4.

39. Aboso (2017: 153), Castillo (2017: 39-40), González (2013: 1078-1080), Lara y otros (2014: 113), Mayer (2017: 237, 248), Mayer (2018a: 160-161), Miró (2012: 48), Moscoso (2014: 12-13) y Suazo (2013: 149-152). Muestra del derecho chileno es Donoso y Reusser (2021: 128-133).

40. Puede ser analizado como un supuesto particular de ataque contra la integridad de datos y sistema propio de la fenomenología asociada a la defraudación informática. Similar, destacando la superposición de métodos ejecutivos y el parecido de familia, Mayer y Oliver (2020: 171, 173, 176-177).

41. Véase sección 3.

42. Aceptan la consideración de lesión como forma de menoscabo sobre esta clase de bienes jurídicos (colectivos), respecto de los tipos de la Ley 20.009, Mayer y Vera (2021: 530-531, 554) y respecto a los delitos informáticos en sentido estricto (bajo estructuras pluriofensivas), Mayer y Oliver (2020: 155).

43. El artículo 15 literal c) define «prestadores de servicios», concepto relevante para la aplicación del nuevo artículo 218 bis del Código Procesal Penal, introducido por el artículo 18 numeral 1.

informático, incluidos los *programas* diseñados para que un sistema informático ejecute una función», vale decir, comprendiéndolos como unidades básicas de información bajo la forma de impulsos electromagnéticos procesados.[44] Aquí es importante destacar, por una parte, que los datos constituyen el objeto de la acción de prácticamente todos los delitos tipificados en la Ley de Delitos Informáticos,[45] y por otro, no se realizan referencia hacia la Ley 19.628,[46] vale decir, no se plantean efectos jurídicos especiales si es que los datos objeto de las conductas constituyen «datos personales»,[47] lo cual no obsta a su eventual utilidad interpretativa, como por ejemplo, para la individualización exacta de la pena (artículo 69, Código Penal).

Por otra parte, el literal b) define *sistema informático* como «todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa», esto es, se considera sistema a todo elemento destinado a la creación, envío, recepción, procesamiento y almacenamiento de datos, a partir de secuencias lógicas de instrucciones o indicaciones para la realización de tareas y obtención de resultados informáticos, conforme a las reglas predeterminadas por el usuario-titular.[48] Concepto amplio que comprende, además de los computadores tradicionales, aparatos cuyo funcionamiento depende en parte de un sistema, pero contemplando también elementos no electrónicos (por ejemplo, máquinas expendedoras).[49]

A continuación, se ofrece un desarrollo especial sobre los tipos de: acceso ilícito (artículo 2),[50] fraude informático (artículo 7),[51] receptación informática (artículo 6),[52] y finalmente, abuso de los dispositivos (artículo 8),[53] con énfasis en los aspectos que se estiman más relevantes en su aplicación.

---

44. Véase De la Mata (2018: 744-745). Una fina distinción sobre clases de datos informáticos y sus derivados puede verse en Balmaceda (2009: 110-111).

45. Véase Mayer y Vera (2022: 268).

46. Ley 19.628 sobre protección de la vida privada, publicada en el *Diario Oficial* el 28 de agosto de 1999..

47. Definidos en el artículo 2 literal f) de la Ley de Datos Personales. No se olvide que la Ley 21.096 (publicada el 16 de junio de 2018) incorporó dichos datos como garantía constitucional en el artículo 19 número 24 de la Constitución Política de la República.

48. Arocena (2012: 950-951), Balmaceda (2012: 110, número 14), De la Mata (2018: 745-746) y Weigend (2013: 80-81). Respecto al carácter automatizado de los sistemas informáticos, véase Jijena (2008: 150-151). Acerca del funcionamiento informático, Mayer (2017: 250-252).

49. En este sentido, Aboso (2017: 323) y Galán (2005: 573-574).

50. Véase sección 2.

51. Véase sección 3.

52. Véase sección 4.

53. Véase sección 5.

2. El delito de acceso ilícito (artículo 2)

Bajo la nomenclatura «acceso ilícito» el artículo 2 contempla tres clases de atentados contra la *confidencialidad* informática,[54] sancionando hechos análogos a un allanamiento de morada electrónico (inciso primero) y a la violación de correspondencia epistolar y de las comunicaciones privadas (inciso segundo, primera oración)[55] incluyendo el acto de divulgación de la información (inciso segundo, segunda oración e inciso tercero).

Es importante destacar que descartamos la expresión *hacking* para designar estos comportamientos,[56] básicamente por su ambigüedad y polivalencia,[57] siendo más acertada la denominación, con matices, de actos de *intrusismo*, *intromisión* o *espionaje informático*.[58]

2.1 Acceso ilícito propiamente tal (artículo 2 inciso primero)

El tipo previsto en el artículo 2 inciso primero sanciona actos de *intrusismo* o *intromisión* informática en sentido estricto,[59] esto es, un contenido de injusto consistente en violentar la expectativa de exclusión de terceros que se reconoce al titular de un sistema informático.[60]

El artículo 2 inciso primero castiga la simple entrada o penetración de un sistema protegido sin autorización,[61] con prescindencia de la obtención —ni la intención de obtener— los datos ahí almacenados,[62] circunstancia prevista solo para la tipicidad de la figura del inciso segundo, primera oración (*espionaje* en sentido estricto).

54. Véase sección 1.3. Al respecto, Becker y Viollier (2020: 88-89) y Couso (2018: 54-55). Similar, Aboso (2017: 181). Lo plantea como bien jurídico basal en estos delitos, Moscoso (2014: 16-18, 30-31).

55. Lo resaltan Castillo (2017: 42), Mayer y Vera (2020: 225, 249) y Tiedemann (2010: 449).

56. Otra opinión, Castillo (2017: 41-42) y Escalona (2004: 149).

57. Por todos, Mayer y Vera (2020: 225-226).

58. Emplean el primer término, Aboso (2017: 177) y Winter (2013: 278 y ss.), mientras que el segundo, Medina (2014: 80 y ss.) y, finalmente, el tercero, Mayer y Vera (2020: 222 y ss.).

59. Respecto a esta clase de conductas, Aboso (2017: 181), De la Mata (2016: 75 y ss.), Escalona (2004: 155), Miró (2012: 54), Rodríguez (2003: 142-143).

60. Expresamente, Mayer y Vera (2020: 244, número 46). Recalca la lesividad de este hecho por sí solo, Moscoso (2014: 42-43). Lo destaca como asunto debatido (ofensividad), Medina (2014: 81, 87-89) y expone las principales razones de criminalización, Escalona (2004: 155-157). En tal sentido, con matices, Oxman (2013: 232-233), mientras que crítico al respecto, Jijena (2008: 153).

61. Como indica Castillo (2017: 43) y Weigend (2013: 81) se trata de un hecho punible de común tipificación en el derecho comparado. También Medina (2014: 89). Expone los argumentos contra su tipificación, Escalona (2004: 157-162).

62. A diferencia de la regulación previa (artículo 2 LTFI), como explica Winter (2013: 279).

El tipo objetivo está constituido por i) la conducta de «acceso» a un sistema, mediante ii) la «superación» de «barreras técnicas» o «medidas tecnológicas de seguridad», ejecutada iii) «sin autorización» del titular o «excediendo» aquella concedida.

De esta descripción, como también por lo dispuesto en el artículo 16, se desprende que necesariamente el sistema de referencia debe ser total o parcialmente *ajeno*, vale decir, encontrarse adscrito a la esfera de gestión y acceso de una persona distinta del autor,[63] sea esta propietaria o no del software o hardware que lo soporta (por ejemplo, la casilla electrónica de un trabajador subordinado).[64]

La i) acción típica de «acceso» consiste en entrar, llegar, penetrar o ingresar a un sistema ajeno por cualquier método o procedimiento imaginable (modalidades y adelantos técnicos), con independencia de si este es directo o remoto[65] (*hacking*, programas *spyware*, *keyloggers*, etcétera), o de si el autor permanece o no al interior del sistema,[66] constituyendo así un tipo de medio comisivo abierto o inespecífico.[67] Si por cualquier razón el ingreso resulta denegado (o rechazado) la conducta ejecutada queda en grado de tentativa.[68] Por otra parte, es importante destacar que el objeto de la conducta es un sistema informático en sí considerado y no específicamente los datos que este contiene,[69] lo cual permite castigar, por ejemplo, la vulneración de la seguridad de un sistema para la subida (o carga) de ciertos datos al mismo, incluso sin haber accedido los datos previamente almacenados.[70]

Adicionalmente, se exige una propiedad objetiva de la acción típica cuya función es caracterizar objetivamente su ilicitud,[71] esto es, que aquella represente ii) la «superación» de «barreras técnicas» o «medidas tecnológicas de seguridad»,[72] circunstancia que cumple el rol de acreditar el interés inequívoco del titular en orden a mantener el secreto (o libertad de exclusión) sobre sus datos.[73] Esto requiere del establecimiento previo, por parte del titular del sistema, de mecanismos destinados a neutralizar el posible ingreso por terceros. Por ende, se descartan las limitaciones puramente

63. También Moscoso (2014: 35-36).

64. Con arreglo a la normativa previa, véase Couso (2018: 61-62) y respecto al debate en el medio español, De la Mata (2018: 734-735).

65. Lo sostiene, respecto al derecho español, De la Mata (2018: 734). En nuestro medio, Alvarado (2022: 527) recoge la distinción entre acceder (genérica) y accesar (ingresar desde un dispositivo periférico).

66. Esto es planteado, con relación a la regulación previa, por Medina (2014: 90).

67. Así como en el texto, González (2013: 1090).

68. Destacado por Aboso (2017: 185).

69. Lo resaltan Magliona y López (1999: 164). Crítica al respecto, Moscoso (2014: 34).

70. Alude como una falencia del tipo previsto en el derecho alemán, Castillo (2017: 50).

71. En este sentido, Mayer y Vera (2020: 223, 226, 246-247, 249), como también, con matices, Becker y Viollier (2020: 90-91).

72. Donoso y Reusser (2021: 107) consideran este hecho como tipología delictiva (intrusión ilegítima).

73. Esta idea es compartida por Balmaceda (2021: 817), Mayer y Vera (2020: 240) y Tiedemann (2010: 447).

contractuales o convencionales de acceso, en la medida que no reflejan una voluntad intensa de exclusión.[74] Los mecanismos referidos consisten en toda condición de acceso dispuesta para restringir o limitar la posibilidad de ingreso,[75] de modo que no se limitan solo a la vulneración de sistemas de seguridad (por ejemplo, antivirus, cortafuegos, encriptados, etcétera), abarcando también el simple acceder con la propia clave del titular, obtenida ilícitamente.[76] Por *superación* se comprende toda clase de transgresión, tanto la *anulación* como la *evitación* de los referidos mecanismos.[77]

Esta exigencia típica corresponde a una opción del Estado de Chile de restringir la tipificación de la conducta de *acceso* prevista en el artículo 2 del Convenio de Budapest.[78] Se resuelve la tensión entre la libertad de acceso a datos reconocida en el ciberespacio y la voluntad de exclusión de esta por parte de los titulares de un sistema,[79] optándose por castigar exclusivamente una forma *cualificada* de ingreso ilícito y no cualquier acto de ingreso ilegal.[80]

Ahora bien, con relación a iii) los elementos normativos de carácter alternativo «sin autorización del titular» y «excediendo la autorización que se posea», estos reflejan con nitidez que los datos o el sistema informático no se encuentra destinado al autor de la intromisión.[81] Bajo la expresión «sin autorización», se castiga a los denominados *outsiders* (o *extraneus*) del sistema, mientras que mediante la segunda redacción, «excediendo la autorización que se posea», a los *insiders* (o *intraneus*).[82] Estas exigencias constituyen elementos de *antinormatividad*,[83] vale decir, elementos normativos que expresan la contrariedad a derecho de la conducta de acceso,[84] o según la nomenclatura más difundida, que determinan si el ingreso pertenece o no a la esfera de un riesgo permitido.[85]

---

74. Expresamente Medina (2014: 93).

75. De la Mata (2018: 735) y Medina (2014: 85, 93-95).

76. En el medio comparado, Aboso (2017: 156, 184-185), Castiñeira y Estrada (2021: 170) y De la Mata (2018: 735).

77. De la Mata (2018: 735) y Castiñeira y Estrada (2021: 170).

78. Véase Becker y Viollier (2020: 93-94) y Mayer y Vera (2020: 240, 244-245). Con relación al derecho comparado, véase Aboso (2017: 177-180).

79. Mayer y Vera (2020: 240).

80. Véase Medina (2014: 93-95, 97). Por su parte, le atribuye una función político-criminal a esta exigencia, Rueda (2020: 210).

81. Medina (2014: 85-86), refiriéndose al derecho alemán.

82. Respecto a la normativa previa, Winter (2013: 279-280).

83. Esta definición es acuñada en Chile por De la Fuente (2016: 11 y ss.).

84. Véase Medina (2014: 92) y González (2013: 1090). Se limitan a describirlos como elementos representativos de la voluntad del titular con incidencia en la tipicidad, Mayer y Vera (2020: 247) y en el contexto de la regulación previa, véase Winter (2013: 281).

85. Para Becker y Viollier (2020: 92) la exclusión del carácter «ilegítimo» del acceso en la Ley, tal como se consagra en el Convenio de Budapest, resultaría problemática, pues no se exigiría comprobar que la

Consecuencia de los elementos ii) y iii), si el ingreso inicial a un sistema informático se realiza de manera autorizada y regular, pero luego se accede lesionando mecanismos de protección a fragmentos internos de este, igualmente se verifica el injusto (por ejemplo, casillas de correo y carpetas).[86] Sin embargo, existiendo un acceso previo ajustado a derecho, la sola mantención no autorizada no resulta típica, de manera similar a la tipificación de la violación de morada.[87]

Esto obliga a aludir a la figura del *hacking* ético, blanco o puro. En el debate dogmático se denomina a los actos de acceso ilícito ejecutados para la detección de vulnerabilidades en sistemas informáticos, realizada de buena fe por el autor y con la intención de reportarlo posteriormente al respectivo titular, pero ejecutado sin autorización o consentimiento de este.[88]

Con arreglo a lo dispuesto en el artículo 2 inciso primero, se trata de un hecho delictivo al faltar la circunstancia típica de autorización para el ingreso.[89] Respalda lo anterior lo señalado en el artículo 16 que exige autorización expresa del titular del mismo.

Se advierte una toma de posición del legislador para castigar el denominado *hacking ético*,[90] habiéndose zanjado la ponderación entre libertad de acceso a la información en el ciberespacio y los intereses de terceros a favor de lo último.[91] El intrusismo con fines de reportar vulnerabilidades (¿auditor independiente?)[92] solo resulta atípico si es que existe una autorización del titular del sistema informático, que debe ser *expresa* y no *tácita* o *presunta*.[93] O dicho de otra forma, la normativa vigente no reconoce la licitud de los actos denominados *hacking ético*,[94] con la sola excepción de la posible construcción dogmática del artículo 10, número 10 del CP.

Finalmente, el artículo 16 refuerza que el injusto del acceso ilícito se verifica por

---

entrada ha sido efectuada de manera injustificada (ejercicio de un derecho) o amparada por una causal de exculpación. Nos parece que la sola relación general entre normas prohibitivas, permisivas y excusas permite descartar dicha observación.

86. Medina (2014: 91), respecto a la normativa previa.

87. Medina (2014: 91) y Oxman (2013: 235).

88. Así lo describen Becker y Viollier (2020: 89), Mayer (2018a: 167, n. 72), y Mayer y Vera (2020: 248-249), mientras que Escalona (2004:155) lo denomina *hacking* directo.

89. Similar, Escalona (2004: 155).

90. Sobre la discusión inicial del proyecto de ley, Becker y Viollier (2020: 94-97). A favor de su punibilidad, Rueda (2020: 209-210). Como indican Mayer y Vera (2020: 249) no es labor del Derecho Penal contribuir al desarrollo de actividades sociales como la ciberseguridad.

91. Véase Mayer y Vera (2020: 248-249). A favor de priorizar la libertad de información, Escalona (2004: 164-167). Similar, acerca de la regulación previa, Moscoso (2004: 39-42).

92. Becker y Viollier (2020: 97).

93. Mayer y Vera (2020: 249).

94. Esto fue discutido durante la tramitación del proyecto, según consta en Biblioteca del Congreso Nacional (2022: 395-396) imponiéndose finalmente la prohibición penal.

la sola incidencia sobre la confidencialidad de los sistemas,[95] con independencia de los motivos del autor.[96] De ahí que no resulta convincente una reducción teleológica del campo de aplicación del tipo-base (o interpretación restrictiva).[97] El legislador chileno ha optado por castigar todo acceso no autorizado a un sistema informático,[98] sin que aspectos relacionados a la entidad *cuantitativa* o *cualitativa* de los datos almacenados en este,[99] y representativos de la posible afectación de otros bienes jurídicos —por ejemplo, intimidad, honor, patrimonio o seguridad nacional—, juegue papel alguno en la apreciación de la *tipicidad* de la conducta,[100] aunque sí podría tenerlo con relación a la circunstancia agravante prevista en el artículo 10 inciso segundo.

En torno a la faz subjetiva se castiga exclusivamente el hecho perpetrado a título de dolo en toda su amplitud (dolo eventual), siendo relevante la advertencia o representación de encontrarse ingresando de forma indebida (no autorizada) y contra mecanismos de seguridad a un sistema ajeno,[101] con total independencia de la motivación específica del acto de intrusismo.[102]

Finalmente, el hecho se castiga a título de *simple delito* con pena alternativa de multa de 11 a 20 unidades tributarias mensuales (UTM) o bien 61 a 540 días de privación de libertad. Como se aprecia, se trata de un hecho de bajo disvalor comparativo a otros delitos de la Ley 21.459.[103]

Respecto a los concursos, esta conducta es referida como el paso previo (o de entrada) para la eventual ejecución de otros ilícitos,[104] sean delitos cibernéticos en sentido estricto o bien simples delitos computacionales. Respecto a los primeros, deberá apreciarse un concurso *aparente* teniendo en cuenta el parentesco de injusto,[105]

95. Mayer y Vera (2020: 244, número 46). En contra, Becker y Viollier (2020: 90).

96. Similar, Moscoso (2004: 33-34). En contra, aludiendo a las referencias subjetivas de la regulación previa, Donoso y Reusser (2021: 119-120).

97. A favor de este rango de cobertura típica, Rueda (2020: 210).

98. Críticos, Becker y Viollier (2020: 80).

99. En contra, de *lex ferenda*, Jijena (2008: 151-152), quien estima que solo debiesen tutelarse aquellos datos informáticos de especial naturaleza, tales como los íntimos, financieros y estratégicos (156-159).

100. Similar, respecto a la normativa previa, Lara y otros (2014: 111). Una propuesta de *lex ferenda* en sentido restrictivo, bajo la denominada teoría de la imputación objetiva, en Mayer y Vera (2020: 242-243, 245-246).

101. Becker y Viollier (2020: 92) cuestionan la eliminación de la exigencia de acceso «deliberado» prevista en el Convenio de Budapest, pues ello implicaría castigar potencialmente el acceso por error o bajo la falsa representación de actuar con autorización. Esto no se comparte, básicamente por el contenido del dolo.

102. Mayer y Oliver (2020: 177).

103. Mayer y Vera (2020: 247).

104. Destacado por Aboso (2017: 355), Castillo (2017: 41), González (2013: 1089), Mayer y Vera (2022: 279) y Moscoso (2014: 29-31).

105. Véase sección 1.2. Similar, Mayer y Vera (2020: 229-230).

mientras que, respecto de los segundos, aplicación de las reglas generales sobre concurso efectivo (concurso real, medial o ideal).[106]

2.2 Espionaje informático y divulgación ilegal (artículo 2 inciso segundo e inciso tercero)

En doctrina, el injusto de *espionaje informático* propiamente tal se configura por acceder y conocer los datos contenidos en un sistema,[107] vale decir, por la adquisición ilegal de su conocimiento.[108] En la Ley de Delitos Informáticos esta conducta ha sido tipificada bajo una particular configuración en la primera oración del inciso segundo del artículo 2.[109] Complementariamente, bajo la segunda oración y en el inciso tercero se castigan los actos de difusión de los datos obtenidos antijurídicamente.

Con relación a la acción prevista en la primera oración del inciso segundo, y que denominaremos tipo de espionaje informático, se trata de la misma conducta tipificada en el inciso primero, pero complementada por dos elementos subjetivos y alternativos del tipo, los cuales adicionan al contenido de ilicitud del acceso, el sentido de injusto que resulta propio del espionaje informático,[110] circunstancia que explica su carácter de subtipo agravado respecto del primero y que torna a la figura como un delito de intención en su variante de tipo mutilado en dos actos.[111]

En específico, se exige que la conducta sea ejecutada con el i) «ánimo de apoderarse» de los datos, en el sentido de ejercer *custodia* o *tenencia* sobre estos,[112] por ejemplo, extrayéndolos o realizando copia de aquellos, cualquiera sea el objetivo posterior de tal conducta (almacenarlos, transferirlos, etcétera), sea o no que estos se hayan conocido,[113] o bien, para ii) «usar la información contenida» en el sistema informático,[114] lo cual dice relación con la utilización de los datos con cualquier objetivo o en cualquier otro tipo de acción, por ejemplo, con una finalidad económica (coacción), periodística (ulterior revelación) o simplemente personal (venganza).[115] Si bien dichas acciones (apoderamiento y uso) son recortadas del tipo objetivo y no

106. Respecto a la regulación previa Moscoso (2014: 49-53).
107. Así lo conceptualizan Mayer y Vera (2020: 226-227).
108. Lo destaca como núcleo de la conducta, Tiedemann (2010: 448).
109. Resaltan la especial fórmula legislativa, Mayer y Vera (2020: 247).
110. Mayer y Vera (2020: 247).
111. Similar, Mayer y Vera (2020: 248). Sobre la regulación previa, Moscoso (2014: 43-44).
112. Con relación a la normativa derogada, Alvarado (2022: 529) y Magliona y López (1999: 158).
113. Alvarado (2022: 529). Una opinión divergente en Mayer y Vera (2020: 227).
114. Críticos, al no incorporar expresamente el conocimiento de los datos, Mayer y Vera (2020: 247).
115. Magliona y López (2014: 159). Como se aprecia, a diferencia del artículo 2 de la LTDI, no se contempla el ánimo de simplemente conocer los datos informáticos, sin perjuicio de comprenderse abarcado por los móviles i) y ii), como apuntan Mayer y Vera (2020: 247).

exigidas para apreciar la consumación, es probable que dichos móviles se den por acreditados en la práctica a través de su efectiva materialización,[116] por ejemplo, con la instalación de software malicioso o manipulaciones informáticas destinadas a obtener los datos necesarios para suplantar la identidad del titular del sistema, incluyendo actos de *phishing* o *pharming*.

El objeto de referencia de los elementos subjetivos son datos constitutivos de «información», esto es, datos según la definición del artículo 15 literal b), representativos de contenido escrito, imágenes, videos, mensajes de audio y cualquier otra expresión informática de conceptos.[117] Ello es relevante por cuanto refleja que se protege la expectativa de *indiscreción* sobre cualquier dato ajeno, excediendo la sola dimensión de intimidad de una persona natural,[118] limitando así, a nuestro juicio, la posibilidad de una interpretación teleológica-restrictiva del alcance de la norma en dicho sentido (vale decir, basada en la clase de dato objeto de la acción).[119]

Por lo anterior, sirven como referencia de este tipo delictivo, datos representativos de información corporativo-industrial, relativos a ciertas actividades estatales, tales como defensa, inteligencia, justicia, policía y registro civil, sin que las implicancias de su obtención ilegal (por ejemplo, seguridad exterior, estabilidad política, confidencialidad de los registros judiciales y policiales), incidan en la gravedad del hecho (en la sanción).[120]

También se tipifica la «divulgación» de los datos informáticos provenientes de un acceso ilícito,[121] esto es, su revelación o propagación hacia potenciales terceros,[122] mediante cualquier forma o método.[123] Para efectos de la pena aplicable, se distingue según el autor de la revelación. El inciso segundo, segunda oración del artículo 2 castiga a cualquier sujeto distinto del autor de la obtención de los datos. El objeto de la conducta es «la información a la cual se accedió de manera ilícita», de modo que el autor debe conocer (dolo) que proviene de un acceso ilícito. El inciso tercero del artículo 2 exaspera la sanción del autor del acto de espionaje por constituir (la divulgación)

116. Consideran a esta técnica un obstáculo operativo del tipo penal, Mayer y Vera (2020: 247-248).

117. Aboso (2017: 159-160).

118. En el contexto español, De la Mata y Bariñas (2014: 77-78).

119. En contra, Magliona y López (1999: 170).

120. Afirma Alvarado (2022: 526), que su tutela se explicaría solo por estar contenidos en un sistema informático.

121. Una reconstrucción de la regulación previa sobre los delitos contra la intimidad se encuentra en Contreras (2020: 216-222).

122. Similar, Oxman (2013: 223).

123. Alvarado (2022: 497), respecto del artículo 146 del Código Penal, señala que consiste en enterar a lo menos a una persona de la información, incluso exigiéndole reserva, planteando la duda respecto del artículo 161-A inciso segundo (2022: 514-515).

una intensificación del contenido ofensivo del acto,[124] en la medida que descarta un concurso aparente de delitos (consunción) entre la de conducta los incisos primero y segundo,[125] en tanto posibles actos anteriores copenados.[126] Como se adelantó, tampoco se contemplan propiedades típicas acerca de la clase de información divulgada,[127] abarcando datos de cualquier naturaleza.

En torno a la faz subjetiva de la conducta de espionaje, en la medida que los elementos del tipo se encuentran referidos específicamente a los datos informáticos, el conocimiento de estos por parte de quien accede al nivel de dolo eventual no es punible bajo esta figura,[128] lo cual no obsta a que el hecho basal (el acceso ilícito) resulte sancionable a través del subtipo base del inciso primero.[129] Y debido a las dificultades probatorias que exhiben dichos elementos subjetivos,[130] es probable que esta última figura sea el tipo aplicable por defecto sobre esta clase de investigaciones.[131] Por el contrario, los tipos de *divulgación* de la información admiten dolo directo y dolo eventual, descartándose la imprudencia.

El espionaje informático (artículo 2 inciso segundo, primera oración) constituye simple delito castigado con pena privativa de libertad con marco penal integrado por dos grados, consistentes en 61 días a 3 años de privación de libertad.

Si quien revela la información es alguien que no ha obtenido por sí mismo previamente los datos (artículo 2 inciso segundo, segunda oración), la pena es idéntica a lo referido previamente. A la inversa, tratándose del mismo autor del acceso ilícito, se exaspera la sanción en un grado generando un marco compuesto por dos grados que van de 541 días a 5 años de privación de libertad.

124. Con matices, Oxman (2013: 225-227).

125. Otra opinión, respecto del artículo 161-A inciso tercero del Código Penal, en Alvarado (2022: 515), así como también respecto de esta situación en la LTIF (2022: 530-531).

126. Mayer y Vera (2020: 247) consideran esta acción como parte de la fase de agotamiento del espionaje informático. Similar, Oxman (2013: 224).

127. Mayer y Vera (2020: 248) son críticos de que no se diferencie la penalidad según la clase de información que resulta divulgada.

128. Respecto a la figura ya derogada, Alvarado (2022: 530). Acerca del nivel de conocimiento exigido por los elementos subjetivos del tipo, véase Hernández (2011: 89). Favorables a castigar de *lex ferenda* el dolo eventual, Mayer y Vera (2020: 243-244). Por otra parte, Moscoso (2014: 20) entiende que tales elementos equivaldrían a dicha clase de dolo.

129. Pues al constituir una derivación típica de una estructura nuclear, satisface sus circunstancias de hecho.

130. Becker y Viollier (2020: 89-90).

131. Coincidentes, Mayer y Vera (2020: 248).

En caso de que el autor sea responsable en la gestión o custodia del sistema o de los datos albergados, se aplica la circunstancia agravante del artículo 10 número 1, en términos similares al previo delito del artículo 4, segunda oración de la LTFI.[132]

Con relación a los concursos, y tomando en cuenta los supuestos más relevantes de la praxis, se puede generar una realización conjunta de espionaje informático y atentado contra la intimidad (artículo 161-A inciso primero del Código Penal), si los datos objeto de espionaje representan conversaciones o comunicaciones, documentos o instrumentos, o bien hechos de carácter privado,[133] el cual nos parece constituye un concurso ideal (artículo 75 del Código Penal), básicamente por comprometer injustos diversos (confidencialidad informática e intimidad, respectivamente).[134] Con relación al acceso sobre correos electrónicos, se descarta la realización de los artículos 146 inciso primero y 156, ambos del Código Penal por cuanto el objeto de la acción de estos últimos consistiría exclusivamente en correspondencia *epistolar* y no electrónica.[135]

Dado que, al igual que el acceso ilícito, el espionaje informático constituye un acto necesario para la ejecución de otros delitos informáticos en sentido estricto, las posibles relaciones concursales deben ser evaluadas con arreglo a la teoría del concurso aparente de delitos.

3. Fraude informático (artículo 7)

El artículo 7 constituye la manifestación más reciente del esfuerzo legislativo por castigar los atentados patrimoniales ejecutados en el contexto de la expansión del comercio electrónico.[136] El primero consistió en la publicación de la Ley 20.009,[137] LTP, recientemente modificada por la Ley 21.234 (publicada en el *Diario Oficial* el 20 de mayo de 2020),[138] la cual en su artículo 7 tipifica diversas acciones que involucran

132. Alvarado (2022: 530).

133. Cumpliéndose las particulares exigencias de lugar de existencia del objeto de la acción y de ejecución de la conducta, como sugieren Mayer y Vera (2020: 230-231). En contra, debido a la naturaleza virtual del entorno, Couso (2018: 40-41).

134. Con matices, Mayer y Vera (2020: 229-231).

135. Alvarado (2022: 487-488, 522), Couso (2018: 42-53, 72-74) y Matus y Ramírez (2021: 413), como también Mayer y Vera (2020: 231), con desarrollo de ulteriores relaciones concursales (232-238).

136. Aboso (2017: 302-303) y Choclán (2002: 250-251) indican que tales casos consisten en: i) fraudes mediante manipulación informática; ii) obtención fraudulenta de servicios o mercancías de un aparato electrónico, y; iii) conductas ilícitas o abusivas por empleo de tarjetas magnéticas en cajeros automáticos, panorama semejante a lo expuesto por Magliona y López (1999: 181-205).

137. Ley 20.009, publicada en el *Diario Oficial* el 1 de abril de 2005: «limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas», y actualmente «establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude».

138. Mayer y Vera (2021: 519 y ss.).

la utilización ilegal de «tarjetas de pago» y de los «datos» necesarios para realizar transacciones electrónicas.[139] Por ello, la publicación de la Ley de Delitos Informáticos y la tipificación del artículo 7 representa una herramienta complementaria en este contexto,[140] al castigar la alteración y manipulación no consentida de datos para la transferencia electrónica de fondos (ánimo de lucro), subsanando los problemas interpretativos que exhibían los delitos contra el patrimonio tradicionales para captar esta clase de hechos.[141]

3.1 Fraude informático propiamente tal (artículo 7 inciso primero)

La disposición tipifica la producción de un perjuicio patrimonial mediante conductas asimilables, en su mayoría, a supuestos de acceso ilícito (artículo 2) y de sabotaje informático sobre datos o sistemas informáticos (artículos 1 y 4),[142] hecho que estadísticamente exhibe mayor relevancia práctica en este contexto.[143]

La figura ha sido designada «fraude informático» y no «estafa informática», descartándose por la doctrina como una variante específica de este último delito,[144] básicamente porque el método ejecutivo no consiste en engañar a otro (mediante inducción) para que disponga (por error) de su patrimonio, sino más bien en ejecutar una transfe-

139. Según el artículo 1, inciso primero, primera oración de la Ley 20.009, constituyen tarjetas de pago las «tarjetas de crédito, tarjetas de débito, tarjetas de pago con provisión de fondos, o cualquier otro sistema similar», recogiendo así las críticas efectuadas en su momento por Hernández (2008: 31). Por su parte, Matus y Ramírez (2021: 287) aluden a instrumentos electrónicos de pago y crédito. Mayer y Oliver (2020: 168) caracterizan a la regulación por la necesidad de una interacción comunicativa entre personas (en gran parte de los casos).

140. Como apunta Hernández (2008: 32), no siempre la información de una tarjeta de pago corresponde estrictamente a la de una cuenta bancaria.

141. Becker y Viollier (2020: 84). También, aludiendo a regulación de la Ley 20.009, Matus y Ramírez, (2021: 633). Respecto a las posibilidades de subsunción previas a esta regulación, Magliona y López (1999: 207-238), Oxman (2013: 219-257). Asimismo, Rosenblut (2008: 256 y ss.).

142. Balmaceda (2009: 94-95), Mayer y Vera (2020: 229), Mayer y Oliver (2020: 153) y, con matices, Donoso y Reusser (2021: 103-105). Lo reconoce como una posición de la doctrina nacional, en el caso de la regulación previa, Rosenblut (2008: 259-260). Por su parte, Oxman (2013: 213) califica el hecho como atentado contra la integridad y confidencialidad, además del patrimonio de la entidad bancaria y a la confianza depositada por el titular de la cuenta.

143. Recalcado por Mayer y Oliver (2020: 152-153, 174) y también por Miró (2013: 7-17).

144. Véase, Donoso y Reusser (2021: 134-135), Mayer y Oliver (2020: 162-164), Oxman (2013: 251-257), Pastor (2020: 270-271) y Tiedemann (2010: 442). En contra, previamente a la publicación de la Ley 21.234, Balmaceda (2009: 362-369), sin perjuicio de constituir opinión minoritaria en nuestro medio, como indica Mayer (2018b: 67-68). Críticos respecto de esta última tesis, Matus y Ramírez (2021: 641). En la actualidad, Balmaceda (2021: 612-617) reconoce tipificada la denominada estafa informática en el artículo 7 inciso segundo de la LTP. Similar, Matus y Ramírez (2021: 642-643).

rencia patrimonial no consentida alterando y manipulando datos.[145] Tampoco se admite su calificación como hurto,[146] puesto que no se trata del enriquecimiento ilícito vía aprehensión física (ruptura de custodia) de una cosa corporal ajena,[147] ni el menoscabo de la propiedad *stricto sensu* como bien jurídico.[148] El aspecto medular de su fisionomía típica como defraudación radica entonces en el medio empleado para menoscabar el patrimonio ajeno, esto es, la manipulación y alteración indebida de datos y sistemas,[149] característica que lo erige como un tipo delictivo de ofensividad mixta.[150]

La figura constituye un tipo de resultado con método comisivo especificado,[151] vale decir, cuya estructura requiere la i) producción de un perjuicio patrimonial (resultado típico) mediante la ejecución de alguna de las ii) conductas taxativamente determinadas por el legislador. El comportamiento es designado como «manipulación» de un sistema informático y detallado alternativamente como la ejecución de las acciones de a) «introducir» datos, b) «alterarlos», c) «dañarlos», d) «suprimirlos» mediante la ejecución de una acción *genérica* descrita en la parte final del inciso primero como e) «interferir» de cualquier forma sobre un sistema,[152] acto que representaría el contenido basal de todos los actos de manipulación fraudulenta, esto es, la *distorsión* de la configuración del sistema informático objeto de incidencia.[153]

Se exige, como elemento subjetivo del tipo, que las referidas acciones sean ejecutadas con «la finalidad de obtener un beneficio económico para sí o para un tercero», circunstancia (subjetiva) que diferencia los actos de manipulación o perturbación de los tipos de espionaje (artículo 2) o sabotaje informático (artículos 1 y 4),[154] en la medida que otorga al hecho el sentido de la motivación de obtener un futuro *enriquecimiento* propio o ajeno, y no el simple objeto de dañar los intereses de la víctima,[155] constituyendo así, en nuestra opinión, un equivalente funcional al ánimo de lucro requerido en las figuras tradicionales.

145. Aboso (2017: 318) y Jijena (2008: 149, 154). Lo cual constituye una hipótesis diferente a una genuina estafa perpetrada a través de la interacción con la víctima mediante dispositivos telemáticos, como apuntan Mayer (2018b: 67) y Miró (2013: 6-7, 11-12).

146. Véase Mayer y Oliver (2020: 165-167), sin dar mayor importancia a la naturaleza corporal del objeto de la acción. Asimismo, Oxman (2013: 240-241).

147. Miró (2013: 11) y Jijena (2008: 149, 154).

148. Mayer y Oliver (2020: 170).

149. Véase Mayer y Oliver (2020: 172, 176-177,179), como también la propuesta de regulación planteada por Magliona y López (1999: 257-261).

150. Véase apartado 1.3.

151. Respecto a lo previsto en el Convenio de Budapest, Mayer y Oliver (2020: 170-171).

152. Mayer y Oliver (2020: 177-178).

153. Idea planteada por Mayer y Oliver (2020: 172-173), con crítica a la actual tipificación (178).

154. Mayer y Oliver (2020: 176), como asimismo Galán (2005: 727, número 1217).

155. Para Mayer y Oliver (2020: 178) esta circunstancia representa el injusto patrimonial, además de propiamente informático de la figura.

En el derecho comparado, se han clasificado las modalidades de ejecución de fraude informático conforme al momento en que el autor incide sobre el proceso ejecutado por el respectivo sistema:[156] durante el i) ingreso de los datos (*input*), tal como incorporar movimientos falsos, eliminar la entrada de operaciones reales o incorporar acreedores; actos perpetrados durante ii) el tratamiento o procesamiento de los datos ya ingresados, como la desfiguración (redondear sumas de dinero), efectuar asignaciones irregulares de dinero o eliminación de saldos negativos; y, finalmente, injerencias durante el iii) momento de emisión de los resultados exteriores del proceso (*output*).

Un caso debatido de *input* es aquel donde el autor utiliza datos reales para conseguir una transferencia electrónica no consentida por el titular,[157] vale decir, casos de utilización abusiva, incorrecta o indebida de datos informáticos ajenos,[158] generalmente ilícitamente obtenidos, pero sin ocasionar un funcionamiento incorrecto del sistema.[159] En el derecho español, el debate está centrado en si la acción típica debe *interferir* en sentido estricto sobre el sistema, vale decir, representar actos de intrusismo y sabotaje,[160] o bien bastaría el simple uso indebido de datos (claves personales reales) para rellenar la tipicidad, esto es, la mera suplantación de identidad digital para efectuar una transferencia.[161] A nuestro juicio, esta última postura se desprende de la sola redacción del artículo 7 inciso primero, al establecer como acción típica el simple acto de «introducir» datos,[162] y de la posibilidad de realizar los tipos de acceso ilícito o espionaje informático por dicha conducta.

El perjuicio patrimonial constituye el resultado típico y puede ser comprendido bajo la teoría dominante en nuestro medio, esto es, la concepción jurídico-económi-

156. Entre otros: Aboso (2017: 324-325), Balmaceda (2009: 109, 111-114), Choclán (2002: 252-253), Galán, (2005: 39), Magliona y López (1999: 191-195), Mata (2003: 63), Miró (2013: 14) y Rovira (2002: 121). Por su parte, Galán (2005: 571-572) añade momentos previos al inicio del procesamiento, y la fase iv) de retroalimentación, tratándose de sistemas informáticos interconectados (575-576). En nuestro medio, Balmaceda (2021: 613).

157. Dopico (2018: 230). En el contexto de la regulación alemana, Galán (2005: 128-152). Lo ponen de relieve en nuestro medio, Moscoso (2014: 25) y Oxman (2013: 238).

158. Aboso (2017: 348-349).

159. Entre otros, Choclán (2002: 253-255), Balmaceda (2009: 281-284), Fernández (2007: 236-242) y Pastor (2020: 271-272).

160. De esta opinión, Aboso (2017: 318-319), Choclán (2002: 266-267), Dopico (2018: 230-231) y Fernández (2007: 48-49). En nuestro medio, Rosenblut (2008: 256-257) con relación a la normativa previa, y bajo el panorama actual, al menos de forma implícita, Mayer y Oliver (2020: 158, 171, 173, 176-177) al reconocer similitud en la estructura del tipo con actos de sabotaje.

161. Lo consideran un acto de manipulación informática punible, Faraldo (2007: 41-43), Fernández (2022: 1145-1146), Galán (2005: 585) y Miró (2013: 16, 29 y 43).

162. Respecto del artículo 8 del Convenio de Budapest, Rovira (2003: 127-129).

ca del patrimonio,[163] de forma que el resultado se identifica con la producción de una disminución del valor monetario del mismo, en este caso, representado por cualquier operación electrónica vinculada con el ánimo de lucro exigido por el tipo, tal como una transferencia de fondos, de una deuda, la cancelación de aquella o el reconocimiento de un crédito,[164] etcétera.

Como tipo de resultado, se exige que el perjuicio patrimonial sea producido mediante la acción de manipulación informática.[165] Esta exigencia relacional, nos parece, impide subsumir directamente bajo esta figura a todo el conjunto de acciones ejecutadas previamente para la obtención no consentida de la información del titular y necesaria para ejecutar las operaciones electrónicas defraudatorias,[166] vale decir, de aquellas conductas informáticas que constituyen mecanismos anteriores o preparatorios de la acción típica.

En este sentido, tales actos han sido categorizados bajo dos grupos de casos:[167] aquellas conductas denominadas i) *phishing* o *pesca de claves*,[168] consistentes en la obtención de la información del perjudicado mediante a) engaño, persuasión o amenaza sobre este (correos electrónicos, SMS, mensajes de aplicaciones, etcétera) como también por b) la instalación subrepticia de un software malicioso en el sistema que la almacena; y los denominados actos de ii) *pharming*, esto es, la implantación de accesos y sitios web falsificados que permiten engañar al usuario para que ingrese por error sus datos reales y así estos puedan ser conocidos y registrados indebidamente por el autor. Sin perjuicio de lo anterior, la atipicidad del *phishing* o del *pharming* como fraude informático del artículo 7 inciso primero no implica la impunidad de tales hechos, dado que igualmente pueden realizar el tipo del artículo 7 inciso segundo de la LTP o inclusive otras figuras de la Ley de Delitos Informáticos, tales como acceso ilícito (artículo 2, inciso primero, primera oración), espionaje (artículo 2, inciso primero, segunda oración) o falsificación informática (artículo 5).[169]

El tipo es doloso y al exigir un elemento subjetivo, dado por el ánimo de lucro,

163. Mayer y Oliver (2020: 174).

164. Balmaceda (2009: 305-307) y Choclán (2002: 251, 255-256).

165. Aboso (2017: 317, 324-325). Críticos respecto a la redacción, por aludir a la ejecución durante la producción del resultado, Mayer y Oliver (2020: 178).

166. Mayer (2018a: 173-174), Mayer y Oliver (2020: 152-153, 156), Rosenblut (2008: 258). Similar, Aboso (2017: 325-332). Constatan la dificultad, Becker y Viollier (2020: 86-87). En contra, admitiendo su tipicidad a este título, Miró (2013: 28-31).

167. Véase, Aboso (2017: 326-332, 335-336), Matus y Ramírez (2021: 640-641), Mayer (2018b: 173-176), Mayer y Oliver (2020: 156-160), Miró (2013: 7-11), Oxman (2013: 215-218), y Rosenblut (2008: 254-255).

168. Así, Hernández (2008: 2, número 1). Por su parte Jijena (2008: 155) lo estima una clase de fraude tradicional.

169. Una actualizada revisión sobre la evolución y estado actual de los mecanismos de extracción de información puede verse en Fernández (2022: 1135 y ss.).

se configura como tipo de tendencia interna trascendente bajo la modalidad de un delito de resultado cortado.[170]

Se trata de un simple delito, castigado con similar pena de aquella establecida para las figuras tradicionales de defraudaciones (artículo 467 del Código Penal),[171] según lo dispuesto en el artículo 7: i) cuantía mayor a 400 UTM (inciso segundo), 3 años y un día a 5 años de presidio, y multa de 21 a 30 UTM; ii) inferior a la previa y superior a 40 UTM (número 3), 541 días a 5 años de presidio, y multa de 11 a 15 UTM; iii) cuantía inferior a la previa y superior a 4 UTM (número 2), 541 días a 3 años, y multa de 6 a 10 UTM, y finalmente, iv) de hasta 4 UTM, 61 a 540 días, y multa de 1 a 10 UTM.

Desde la perspectiva concursal, es necesario distinguir la clase de delitos conjuntamente realizados. En primer lugar, con relación a los delitos establecidos en la Ley de Delitos Informáticos, los actos de acceso ilícito (artículo 2 inciso primero, primera oración) o espionaje (artículo 2 inciso primero, segunda oración) pueden verificarse como actos *previos* al fraude informático,[172] mientras que los de sabotaje (artículos 2 y 4) que coincidan con la descripción, actos *coetáneos* a su ejecución.[173] En ambos casos, atendido el contenido de injusto de las realizaciones involucradas, se debe considerar un concurso *aparente* de delitos.[174]

Respecto a otras realizaciones concurrentes y en el contexto de las operaciones patrimoniales electrónicas no consentidas es posible identificar claramente dos fases de desarrollo:[175] una etapa de i) obtención y almacenamiento de los datos necesarios para realizarlas, también denominada como robo de identidad digital,[176] y; ii) la ejecución de la operación patrimonial electrónica propiamente tal, fase que involucra, en la mayoría de los casos, tanto el uso de los datos ilícitamente obtenidos como también la suplantación de identidad del usuario. Teniendo en cuenta lo anterior, el artículo 7 inciso segundo de la LTP castiga el siguiente hecho:[177]

> El que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

170. Así lo conceptualiza Galán (2005: 755-756) y con menor detalle, Mayer y Oliver (2020: 172).

171. Salvo en la hipótesis menos grave. Críticamente, Mayer y Oliver (2020: 178-179).

172. En el contexto español, Miró (2013: 21).

173. Destacan estas relaciones concursales, Mayer y Oliver (2020: 153, 173).

174. Están de acuerdo Mayer y Oliver (2020: 161-162, 173).

175. Fernández (2007: 240-242). Respecto al *phishing,* Castillo (2017: 44-45) y Hernández (2008: 2).

176. Se trata de identificadores digitales que pueden ser atribuidos a una persona, véase Aboso (2017: 303).

177. Este delito fue recientemente incorporado por la Ley 21.234 publicada en el *Diario Oficial* el 29 de mayo de 2020. Al respecto, Mayer y Vera (2021: 542-544, 548-549).

Como se aprecia, este último tipo delictivo abarca la gran mayoría de los hechos constitutivos de *phishing* y de *pharming*,[178] acciones que podrían constituir actos preparatorios de la conducta de manipulación informática, y atípicos según lo dicho como tentativa del artículo 7 inciso primero de la Ley de Delitos Informáticos.[179] En cuanto a su estructura, se trata de un tipo mutilado en dos actos,[180] que anticipa la ejecución de las acciones de i) suplantación del titular y de ii) ejecución de las transacciones electrónicas no consentidas, perfeccionándose con la sola obtención de la información financiera o la vulneración de medidas de seguridad de una cuenta bancaria o similar.[181]

Es importante destacar que el artículo 9 de la LTP estableció de manera explícita una regla concursal para los casos de realización múltiple de (alguno de los) tipos del artículo 7 y aquellos previstos (o a ser establecidos) en la Ley de Delitos Informáticos. Esta regla cumple una función de *clarificación* o *esclarecimiento*,[182] indica al juzgador que los delitos realizados representan contenidos de injusto diversos,[183] y por ello, generan un concurso *efectivo* y no *aparente* de delitos.[184] Si bien el específico contenido de antijuridicidad de una y otra clase de tipos es un asunto todavía abierto al debate, especialmente si se comprende que el fraude informático lesiona el patrimonio individual del titular y la integridad informática,[185] restando elaborar un sentido ofensivo específico para los tipos previstos en la LTP;[186] en definitiva, esta norma concursal

178. A favor de su tipicidad bajo esta figura, Matus y Ramírez (2021: 642-643).

179. Mayer y Oliver (2020: 167-168) y Miró (2013: 17-18).

180. Mayer y Oliver (2020: 168).

181. Otra opinión, Mayer y Vera (2021: 543) para quienes el tipo exigiría de forma copulativa tanto la afectación de medidas de seguridad como de la información. En nuestra opinión, la figura tipifica con variantes de ejecución alternativas: vulnerar medidas de seguridad y obtener información.

182. Para el concepto, véase Escuchuri (2004: 199-200). En esta línea, Matus y Ramírez (2021: 643-644).

183. En esta línea, Mayer y Vera (2021: 527, 552-553). Sin embargo, Mayer y Oliver (2020: 178-179) critican la regulación del fraude informático por tener asignada idéntica pena que la estafa, sugiriendo una mayor sanción tomando en cuenta la pluriofensividad del hecho.

184. Regla que, a nuestro juicio, impide la configuración de una infracción al principio *ne bis in idem* de aplicarse ambas sanciones, en la medida que el propio legislador ha expresado su decisión de castigar uno y otro hecho. En este sentido, Maldonado (2020: 505-506) y Mañalich (2018: 71-72).

185. Plantean, de *lex ferenda*, tipificar este hecho tomando en cuenta ambas clases de disvalor Mayer y Oliver (2020: 175). Es interesante la consideración de Jijena (2008: 153) quien indica como afectado al sistema bancario de procesamiento de datos patrimoniales.

186. Hernández (2008: 32), además del patrimonio (36-37) señala al tráfico comercial o, inclusive, desliza la fe pública (36, nota número 97). En este último sentido, Mayer y Oliver (2020: 168-169) aludiendo a la funcionalidad documental, mientras que, respecto al fraude informático, al patrimonio y la funcionalidad informática (174-175). Matus y Ramírez (2021: 643) señalan como uno de los intereses protegidos, la seguridad de los medios de pago. Por su parte, Rojas (2017: 384-385) identifica la función que cumplen dichos instrumentos en el tráfico económico (equivalentes funcionales del dinero). Mayer y Vera (2021: 528-531, 532, 547, 554) postulan como bien jurídico (colectivo) de base en estas infracciones, el

dispone la aplicación de las reglas generales en la materia, vale decir, estimar la configuración de un concurso ideal, medial o real, dependiendo del caso específico que se trate.[187]

Con detalle, respecto a la fase previa a la manipulación informática, la ejecución de las conductas tipificadas por el artículo 7 inciso segundo de la LTP,[188] esto es, la obtención de la información financiera por engaño o simulación configura un supuesto de concurso efectivo en pluralidad de hecho (concurso real o medial) con los delitos de la Ley de Delitos Informáticos. Así, la obtención asociada al *phishing* puede resultar constitutiva de acceso ilícito o espionaje contra datos o sistemas informáticos (artículo 2), mientras que aquella vinculada al *pharming*, sabotaje de un sistema (artículo 1) y falsificación informática (artículo 5).[189] En todos los casos, según el artículo 9 LTP, se debe castigar por el tipo del artículo 7 inciso segundo de la misma en concurso con el respectivo delito de la Ley de Delitos Informáticos.[190]

Con relación a la fase de incidencia sobre el procesamiento de la transacción electrónica, el concurso se genera en unidad de hecho (concurso ideal) por la realización de la acción de vulnerar medidas de seguridad de una cuenta financiera a través de simulación (artículo 7 inciso segundo de la LTP),[191] por una parte, y la producción de un perjuicio patrimonial mediante la introducción indebida de datos (artículo 7 inciso primero), por otra.[192] En estos casos, el tipo de usurpación de nombre (artículo 214 del Código Penal) no se configuraría, pues la identidad digital no es equivalente al nombre real de una persona.[193]

---

orden público económico en sentido estricto, en su dimensión de incidencia sobre el sistema de medios de pago (en conjunto a otros bienes, dependiendo de la específica modalidad de conducta que se trate).

187. En contra, Matus y Ramírez (2021: 643-644) quienes la interpretan como directriz para aplicar la regla del artículo 74 del Código Penal. Como resulta natural, la posibilidad de configurar un concurso en todos los casos previamente señalados se encuentra supeditada a la acreditación en el proceso de las respectivas conductas (circunstancia particularmente difícil respecto del artículo 7 inciso segundo de la LTP), de modo que, si tan solo se prueba una de aquellas, constituirá la única sanción aplicable.

188. Destacan las diferencias entre ambos tipos delictivos, Mayer y Oliver (2020: 167-168).

189. Mayer y Oliver (2020: 153, 158, 160).

190. Y si se configura un concurso aparente entre los tipos de la Ley de Delitos Informáticos, con el tipo preferente que corresponda.

191. Respecto al uso indebido de tarjetas de pago, si involucran la utilización de sistemas informáticos al efectuarse su reconocimiento, puede comprenderse como un supuesto de concurso entre los literales b), d), f) o g) del artículo 7 de la LTP, y el respectivo tipo de fraude informático. Destaca esta circunstancia, Hernández (2008: 34-35).

192. Esto en caso de que se estime como típica la conducta de abuso de datos informáticos como forma de manipulación constitutiva de fraude, como aquí se sostiene.

193. Véase Oxman (2013: 236-237).

3.2 Facilitación de medios para la comisión de fraude informático (artículo 7 inciso segundo)

La disposición tipifica actos de colaboración con la manipulación informática del inciso primero y fue incorporada a instancia del Ministerio Público para zanjar la dificultad procesal de acreditar supuestos de coautoría concertada (artículo 15, número 1 o 3 del Código Penal) entre el colaborador y el autor del fraude. Específicamente, se buscó castigar a los denominados *muleros o intermediarios electrónicos*,[194] vale decir, casos de facilitación de cuentas bancarias para la recepción de los fondos ilícitamente obtenidos, de forma que el legislador recogió dicho supuesto de intervención delictiva como una figura completamente autónoma,[195] por lo que su tipicidad no involucra probar la convergencia subjetiva entre los involucrados en la operación de fraude.

Sin perjuicio de lo anterior, con su introducción se buscó generar un incentivo de colaboración para el descubrimiento del hecho principal (fraude) a través de la posibilidad de reconocer al imputado la circunstancia atenuante de efecto extraordinario de cooperación eficaz del artículo 9,[196] toda vez que la regla general en esta clase de investigaciones es que el único detenido sea el *mulero electrónico*.[197]

La acción típica consiste en «facilitar los medios» con los que se «comete» el delito previsto en el inciso primero. Esto quiere decir que, como presupuesto de la conducta, debe existir la posibilidad de *contribuir* a su comisión, vale decir, el comportamiento debe ejecutarse hasta antes que se halle definitivamente perpetrado el fraude informático, en este caso, hasta el instante en que se produce el perjuicio patrimonial.[198]

Esta descripción comprende un rango de actos más extenso que el originalmente pensado, por ejemplo, el suministro de los dispositivos físicos para ejecutar la manipulación (el hardware), de la información necesaria (datos de identificación, contraseñas, códigos de seguridad, etcétera), y programas informáticos (malware), entre otros, lo cual genera relaciones concursales con los artículos 6 y 8.

El caso de colaboración típica más desarrollado en la praxis es el denominado *mulero electrónico*, vale decir, quien interviene aportando una cuenta bancaria propia para transferir el dinero obtenido por el fraude, permitiendo la desviación de los fondos electrónicos, generalmente sin conocer al autor originario y con ánimo de lucro

194. Por todos, véase Fernández (2022: 1146 y ss.).

195. Respecto a las diversas formas de intervención delictiva reconocibles en el supuesto, de no existir esta figura especial, véase, por todos, Flores (2013: 163 y ss.) y Miró (2013: 31-41).

196. Véase Biblioteca del Congreso Nacional (2022: 121-122). Lo reconoce como posible caso de intervención a título del artículo 15, número 3 del Código Penal en un fraude patrimonial, Rosenblut (2008: 258).

197. En el contexto español, Miró (2013: 31-32).

198. Con relación al encubrimiento como forma de participación posejecutiva, Mañalich (2020a: 200).

(obtención de una comisión).[199] La preexistencia de una cuenta bancaria *receptora* constituye un eslabón necesario para la producción del perjuicio patrimonial,[200] y en tal sentido, *simultáneo* a la verificación del resultado típico,[201] en la medida que la propia disminución del saldo se ocasiona mediante la dependencia lógico-digital entre el sistema emisor y el receptor,[202] de forma que dicho medio —la puesta a disposición de la cuenta— no puede estimarse como un evento posterior a la perpetración del ilícito principal.[203] De lo contrario, si la cuenta es aportada para una ulterior transferencia (segunda o más), cabe más bien estimar un acto de encubrimiento de fraude informático.[204]

El punto decisivo para el castigo de los actos de colaboración en fraudes informáticos, esto es, de los *muleros electrónicos*, radica en la imputación subjetiva.[205] Por ello no es extraño que el artículo 2 inciso segundo subjetivamente exija la i) representación («conociendo») o ii) la posible advertencia («no pudiendo menos que conocer») de la ilicitud de la conducta descrita en el inciso primero, vale decir, el conocimiento de la ejecución de la acción de manipulación informática. Ahora bien, esta última expresión, empleada originalmente en el diseño del tipo de receptación (artículo 456 bis inciso primero del Código Penal), ha sido objeto de diversas interpretaciones,[206] sin perjuicio de que, según los antecedentes de producción del texto legal, aludiría comportamientos dolosos en todo su espectro,[207] básicamente, quien facilita una cuenta bancaria para la perpetración del fraude,[208] limitando la aplicación de la figura sobre personas instrumentalizadas (engañadas) o que derechamente desconocerían

199. Aboso (2017: 332-335, 343-344). Lo destacan como acto vinculado al fraude, Mayer y Oliver (2020: 158).

200. Aquí se descarta la recepción de dinero ajeno en cuenta corriente propia como hecho constitutivo del tipo del artículo 448 inciso primero del Código Penal (hurto de hallazgo), en la medida que se estima que dicha figura exhibe una conexión de accesoriedad con la normativa de la ocupación como modo de adquirir el dominio, especialmente, tratarse de una cosa corporal (no así el dinero giral) y cosas al parecer perdidas (artículos 606 y 629 del Código Civil).

201. Miró (2013: 33, número 75, 43). Crítico al respecto, Oxman (2013: 220-222, número 25, 45 y 230).

202. Matus y Ramírez (2021: 64) apuntan que se trata de transferencias entre anotaciones contables automatizadas. Similar, Jijena (2008: 153) quien refiere asientos contables magnéticos. Sobre la consideración del entorno virtual para el análisis de la causalidad, Posada (2017: 98-100).

203. Al respecto, Fernández (2022: 1147), y asumiendo una opinión similar, Miró (2013: 35-36).

204. Sostenido por Aboso (2017: 333-335).

205. Fernández (2022: 1147-1149), Flores (2013: 167-174) y Miró (2013: 41-53).

206. Por todos, véase Ossandón (2008: 57-63).

207. Podría considerarse dicha expresión como un indicador de dolo, tal como lo expone Mañalich (2020b: 31-38), esto es, un señalamiento al tribunal de tomar en consideración circunstancias objetivas que representen por sí mismas (indicativas), el nivel de representación mínimo para atribuir dolo (eventual).

208. Véase Biblioteca del Congreso Nacional (2022: 116).

el origen ilícito de los fondos.[209] Esta conducta se castiga con idénticas penas a las previstas en el inciso primero.

Respecto a los concursos, se puede destacar el supuesto en que los medios aportados por el autor consisten en información digital necesaria para ingresar a un sistema o a una plataforma informática. En este caso, se podría realizar simultáneamente el tipo de receptación de datos en su variante de transferencia de estos (artículo 6) o con el tipo de abuso de los dispositivos (artículo 8) por la acción de entrega de datos, concurrencia que debe ser zanjada como un concurso aparente de delitos según las reglas generales (por ejemplo, subsidiariedad o consunción).[210]

4. Receptación de datos informáticos (artículo 6)

El artículo 6 fue incorporado por iniciativa del Ministerio Público y pensado inicialmente para castigar dos grupos de casos:[211] el i) empleo y circulación indebida de datos obtenidos en forma ilícita, esto es, provenientes de actos de intrusismo (artículo 2) o de interceptación informática (artículo 3); y el ii) uso de datos falsificados, especialmente considerando que bajo el artículo 5 (falsificación) no se encuentra tipificada la utilización de tales datos (también denominado *uso malicioso* de instrumento), desempeñando así una función análoga a la reconocible en los artículos 196 y 198 con relación a los artículos 193, 194 y 197 del Código Penal, respectivamente.

Esta figura no responde al contenido de la receptación en sentido estricto,[212] sino que se orienta, en primer lugar, a la evitación de la circulación indebida de información,[213] intensificando así la afectación de la *confidencialidad* de los datos que fueron objeto de un delito informático antecedente; y, en segundo lugar, a impedir su empleo como *instrumento* para ulteriores comportamientos ilícitos.

En este sentido, el tipo castiga dos grupos de acciones claramente diferenciadas: i) la tenencia digital, denominada «almacenamiento», ejecutada sobre a) cualquier clase de dato obtenido por actos de intromisión ilícita (acceso ilícito, espionaje o interceptación) o b) provenientes de un acto de falsificación informática y; determinadas ii) conductas de intermediación o tráfico ilegal de datos informáticos ilícitamente obtenidos o falsificados. En ambos casos, el objeto de la acción corresponde a datos

209. Véase Biblioteca del Congreso Nacional (2022: 120-121).

210. La detentación previa de la información, cumpliéndose las exigencias subjetivas del artículo 7 inciso segundo de la LTP, podría ser castigada por dicha figura también, según dispone el artículo 9 o inclusive, con el tipo delictivo del artículo 7 literal e). Sobre esta última figura, véase Mayer y Vera (2021: 539-540).

211. Véase Biblioteca del Congreso Nacional (2022: 113, 116-118).

212. A nuestro juicio, no todas las variantes constituyen actos de favorecimiento real o aprovechamiento de los efectos de un delito previo.

213. Véase Biblioteca del Congreso Nacional (2022: 262-263).

que *provengan* de la ejecución de los tipos de acceso ilícito (artículo 2), interceptación (artículo 3) o falsificación informática (artículo 5), y por lo mismo, constituye una circunstancia objeto del dolo. En la medida que la propia receptación informática no es prevista como antecedente del objeto de la conducta, la denominada receptación *sustitutiva* no es punible, sin perjuicio de la posesión de los datos que provengan de este ilícito cumpla las exigencias del tipo de abuso de los dispositivos (artículo 8).

Respecto a la simple detentación sobre datos, la conducta de almacenamiento exige la concurrencia de un elemento subjetivo como la intención de utilizarlos para cualquier «fin ilícito». Esta variante representa, además del injusto de aprovechamiento o favorecimiento, un acto de preparación. Si bien en principio la atención de la doctrina bajo la normativa previa estuvo centrada en la posesión y uso de datos relativos a una cuenta bancaria o de tarjetas de pago con fines de fraude patrimonial,[214] la redacción actual permite castigar prácticamente toda posesión ilegal incluyendo la de documentos o datos informáticos falsificados en el contexto de su utilización.[215] La referida *ilicitud* de la finalidad, y que justifica el castigo de la posesión, se refiere a todo acto futuro contrario a derecho que involucre la gestión de los datos, como pueden ser: el uso de un documento informático falsificado,[216] la perpetración de ulteriores delitos informáticos como la divulgación ilegal de datos (artículo 2 inciso segundo, segunda oración) o bien del tipo previsto en el artículo 7, inciso segundo de la LTP. Incluso, objetivos no exclusivamente constitutivos de una infracción penal, sino que portadores de ilicitud bajo otros sectores del ordenamiento (por ejemplo, difusión de contenido íntimo, conversaciones privadas, etcétera).

Este comportamiento es importante en la medida que sirve como tipo de recogida para castigar supuestos de extracción de datos sin poder comprobar el acto de obtención,[217] como lo son el *phishing* o *pharming* en sentido amplio, cuando el móvil del autor no se refiere a la posterior realización de una operación patrimonial, como exige el artículo 7 inciso segundo de la LTP, y no se cuente con evidencia para acreditar los tipos de acceso ilícito o espionaje informático (artículo 2), o alteración sobre datos informáticos (artículo 4). Pero también la figura capta la posesión de software potencialmente utilizable,[218] especialmente si no se considera la acción de obtención del artículo 8 como una conducta posesoria.

214. Por todos, véase Oxman (2013: 237-238).

215. Véase la segunda parte de este trabajo, respecto al tipo de falsificación informática (artículo 5).

216. Biblioteca del Congreso Nacional (2022: 113, 115-116).

217. En esta línea, Biblioteca del Congreso Nacional (2022: 265).

218. Entendiendo por programa un conjunto codificado de datos informáticos bajo la forma de una aplicación.

Con relación a las conductas de intermediación ilegal, se castigan directamente las acciones de «comercialización» y «transferencia» de datos obtenidos ilícitamente (por ejemplo, la venta o intercambio de bases de datos, bancos de claves, etcétera), pero también la mera tenencia de estos en la medida que se vea acompañada de los elementos subjetivos alternativos de posterior i) comercialización y/o ii) transferencia de datos, variante que constituye una anticipación de la sanción de los actos de intermediación propiamente tales mediante el castigo de su almacenamiento previo. Como se aprecia, esta hipótesis refleja las circunstancias propias de actos de aprovechamiento o favorecimiento.

El dolo, además de la advertencia de ejecutar la acción típica, abarca el origen de los datos informáticos, esto es, su derivación de la perpetración de las acciones de acceso ilícito, interceptación y falsificación. Tal como se dijo a propósito del artículo 7, inciso segundo, en nuestra opinión la expresión «no pudiendo menos que conocerlo» representa un llamado de atención al juzgador sobre el parámetro de atribución del dolo.

El marco penal abstracto se establece conforme al delito-base del cual provienen, rebajado en un grado, a saber: i) acceso ilícito: a) 61 días (artículo 2, inciso primero, hipótesis constitutiva de falta), b) 541 días a 5 años de privación de libertad (artículo 2, inciso segundo); ii) interceptación ilícita: a) 61 a 540 días (artículo 3, inciso primero), b) 41 a 540 días (artículo 3, inciso segundo) y; iii) falsificación informática: a) 61 días a 3 años (artículo 5, inciso primero) o b) 541 días a 5 años (artículo 5, inciso segundo).

El autor de los delitos base no puede ser castigado por la ejecución de receptación informática, en la medida que, sobre la base del mismo contenido de injusto, esta última constituye un acto posterior copenado o bien un caso de subsidiariedad tácita (concurso aparente de delitos).[219]

Como supuestos concursales, el almacenamiento de datos para ejecutar una manipulación electrónica puede concurrir con la obtención de lo necesario para el ingreso a una cuenta bancaria o similar (artículo 7, inciso segundo de LTP), caso en el cual debe aplicarse la regla concursal del artículo 9, que dará forma, por regla general, a concurso en unidad de hecho (artículo 75 del CP). Por otra parte, dicho almacenamiento puede significar también realización del tipo de abuso de dispositivos por obtención de datos para la ejecución de otros delitos (artículo 8), caso en el cual deberá aplicarse la norma preferente según los principios del concurso aparente.

219. Véase De la Mata (2018: 736).

5. Abuso de los dispositivos (artículo 8)

El artículo 8 tipifica actos generalmente integrantes de la *fase preparatoria* de los delitos informáticos,[220] específicamente, conductas de intermediación y posesión de dispositivos, software o datos que resultan *instrumentales* para su perpetración,[221] de manera similar al tipo previsto en el artículo 445 del Código Penal[222] Se trata de una fórmula prevista en el artículo 6 del Convenio de Budapest y con positiva acogida por los Estados signatarios,[223] pero no así por la doctrina, al identificar en su tipificación un adelantamiento de la protección penal sobre los bienes tutelados por los delitos-fines,[224] circunstancia puesta de relieve durante su tramitación y zanjada mediante la redacción final del articulado.[225]

Como supuesto prototípico de este hecho se ejemplifica la tenencia de ciertos datos personales (cuentas bancarias, números de tarjetas de crédito, sus respectivas contraseñas, etcétera), dispositivos y/o softwares destinados a la penetración de sistemas o la captación de comunicaciones realizadas mediante aquellos.[226]

El artículo 8 sanciona dos grupos de conductas que presentan elementos típicos comunes para su configuración, a saber: la concurrencia de i) un preciso elemento subjetivo del tipo y ii) el respectivo objeto de la acción.

El primero, y que define a la figura como un delito mutilado en dos actos, reside en un elemento subjetivo especial consistente en la ejecución de la acción típica con la finalidad («para la perpetración») de alguno de los siguientes delitos:[227] i) atentados contra la integridad informática (artículos 1 y 4), ii) conductas de acceso ilícito (artículo 2), iii) interceptación ilícita (artículo 3) y iv) de aquellas tipificadas en el artículo 7 de la LTP, esto es, aquellas relacionadas con tarjetas de pago (literales a hasta h) del inciso primero) o bien sobre cuentas bancarias u otras similares (inciso segundo).

220. Véase Cruz (2020: 78 y ss.).

221. En el derecho español, estos actos se recogen en el artículo 197 ter (intimidad informática), 248.2 b) (estafa informática), 264 ter (daños informáticos), 270.6 (propiedad intelectual) y 400 (falsedades documentales) del Código Penal, tal como indican Castiñeira y Estrada (2021: 171-172), Cruz (2022: 8 y ss.), De la Mata (2018: 736) y Pastor (2020: 273-274).

222. Véase la analogía a una ganzúa electrónica en Biblioteca del Congreso Nacional (2022: 209).

223. Weigend (2013: 87-88) destaca la falta de oposición de los Estados a su tipificación. Críticos al respecto, Aboso (2017: 363-367), Balmaceda (2021: 334-335), Mayer y Vera (2019: 446-447).

224. Véase, por todos, Cruz (2020: 78 y ss.). Refieren una posible tensión con derechos fundamentales por la tipificación de esta figura, Lara y otros (2014: 120). En defensa de esta clase de figuras, Gómez (2002: 16-28).

225. Según consta en Biblioteca del Congreso Nacional (2022: 122-123), mediante la i) exigencia subjetiva y aquella ii) objetiva con relación a los programas informáticos.

226. Véase, Weigend (2013: 87-88). Con relación al injusto, reconocen intereses colectivos como protegidos por esta clase de actos, Galán (2004: 4-5) y Muñoz (2015: 348-349).

227. Como destacan Castiñeira y Estrada (2021: 171) puede resultar problemática la determinación del grado de concreción del plan delictivo (autor, objeto, víctima, etcétera).

Es llamativo que, a diferencia del derecho español, no se ha previsto el fraude informático tipificado en el artículo 7 inciso primero, ni a su variante de colaboración del inciso segundo, como delito-referencia de este elemento subjetivo, sin perjuicio de que, a nuestro juicio, los actos que constituyen una operación de manipulación informática defraudatoria igualmente resulten objeto de esta remisión como actos ejecutivos de los tipos de atentado contra la integridad de sistemas o datos informáticos (artículos 1 y 4), acceso ilícito (artículo 2) y del tipo previsto en el artículo 7 inciso segundo de la LTP.

Este elemento subjetivo desempeña la función de excluir de la tipicidad determinadas acciones habituales que son ejecutadas con hardware o software en el contexto empresarial y comercial, por ejemplo, con fines de investigación, ciberseguridad y entrenamiento, académico e inclusive, policial.[228] Asimismo, esta exigencia identifica a la conducta con tipo de preparación o emprendimiento, exigiendo el conocimiento de que la conducta se encuentra dirigida a contribuir a la ejecución de un delito propio o ajeno.[229]

La segunda circunstancia típica común consiste en la previsión de tres posibles objetos de la conducta (dispositivos, programas computaciones e información), respecto de los cuales se exige haber sido «creados» o «adaptados» de forma primordial («principalmente») para la ejecución de los delitos referidos por el elemento subjetivo, esto es, encontrarse diseñados de forma originaria para ello, como paradigmáticamente sucede con el *software malicioso*, o bien, acondicionados o ajustados para este fin, vale decir, en el caso de programas de uso neutral pero con posibilidad de ser empleados delictivamente. En uno u otro caso, los elementos han de incidir externa o internamente sobre el funcionamiento de un sistema informático (o también sobre tarjetas de pago), aunque, como se desprende de la redacción, dicha propiedad solo resulta exigible de los dispositivos y programas, pero no así de la información.[230]

Por i) «dispositivos» se comprenden aparatos o hardware destinados para ejecutar el respectivo delito-fin. Se abarca con ello, por ejemplo, a los elementos utilizados

228. Biblioteca del Congreso Nacional (2022: 122-123), y, en el derecho español, Dopico (2018: 232). Lo destaca como un aspecto problemático en el contexto alemán, Tiedemann (2010: 441).

229. Exigencia subjetiva que permite matizar las duras críticas realizadas sobre esta clase de conductas, como explica Galán (2004: 2-3).

230. En el debate comparado se plantea la necesidad de constatar una especial aptitud de los dos primeros elementos para neutralizar los protocolos de seguridad del sistema informático objeto de la acción como una especie de exigencia o cláusula de lesividad u ofensividad. Véase, Aboso (2017: 364-365), Cruz (2020: 84-87), Galán (2004: 5) y Gómez (2002: 29-43). Esto, para así compensar interpretativamente la tipificación de un hecho criticado por constituir un extremo adelantamiento de la punibilidad de los respectivos delitos-fines. Sin embargo, consideramos que dicho elemento típico implícito no integra el injusto de esta figura, en la medida que dicha exigencia no parece extensible a todas las hipótesis de conducta que prevé el artículo 8 (por ejemplo, con relación a los atentados contra la integridad de datos o sistemas).

para la obtención de los datos de tarjetas de pago,[231] o aquellos dispuestos para la vigilancia electrónica no consentida. Los ii) «programas computacionales» consisten en un específico conjunto de instrucciones o comandos destinados a cumplir una determinada función en un sistema,[232] abarcando, en general, aunque no exclusivamente, al denominado *malware* o *software malicioso*,[233] entre otros. Finalmente, por iii) «contraseñas», «códigos de seguridad», «códigos de acceso» u «otros datos similares» se comprende la información necesaria para acceder o manipular datos o servicios informáticos, incluyendo aquellos para suplantar la identidad digital de una persona.

Ahora bien, el primer grupo de comportamientos típicos consiste en actos de intermediación y/o facilitación de los objetos a terceros bajo las fórmulas de «entregar», «importar», «difundir» o genéricamente, «realizar formas de puesta a disposición». Se trata de la inserción en el tráfico bajo cualquier título jurídico-patrimonial de los referidos objetos, con la finalidad de ejecutar los delitos comprendidos por el elemento subjetivo (por ejemplo, la venta de claves o *malware*).

El segundo grupo de conductas consiste en la acción de «obtener» alguno de los objetos para su posterior «utilización» en la perpetración de alguno de los delitos-fines.[234] A nuestro juicio, se trataría de una variante de *tenencia* o *posesión*,[235] configurada por la mantención o almacenamiento de los objetos por el autor,[236] y que seguramente ocupará un lugar privilegiado en la aplicación práctica de la norma. Esta conducta posesoria puede superponerse con la receptación por almacenamiento con un fin ilícito (artículo 8), cuando el objeto de la conducta esté dado por información para el acceso informático a un sistema o una determinada plataforma, supuesto que debe ser evaluado bajo los parámetros del concurso aparente de delitos (subsidiariedad o consunción), aspecto especialmente relevante en los casos de *phishing* o *pharming*.[237] Finalmente, la simple detentación de datos ajenos sin la concurrencia de los elementos subjetivos requeridos por la receptación (artículo 6) o esta figura (artículo 8) constituye un hecho atípico.

El dolo requiere advertencia de la acción y de las propiedades del respectivo objeto, complementado por el elemento subjetivo de tendencia ya desarrollado.

Se trata de un simple delito castigado con pena privativa de libertad de 61 a 540 días y multa de 5 a 10 UTM.

---

231. Biblioteca del Congreso Nacional (2022: 123).

232. Arocena (2012: 981), Balmaceda (2009: 110-111) y Dopico (2018: 231).

233. Sobre estos conceptos, Mayer (2018a: 168-171).

234. Galán (2004: 6) reconoce en dicha exigencia subjetiva un criterio de legitimación de la conducta.

235. Así también se desprende del debate a que dio lugar esta regla, Biblioteca del Congreso Nacional (2022: 122-123).

236. Críticos, Balmaceda (2009: 336-337) y Cruz (2020: 85-86).

237. En contra de su tipicidad bajo el derecho español, Castiñeira y Estrada (2021: 171-172).

Desde la perspectiva concursal, si quien detenta el objeto lesivo también ejecuta los delitos informáticos previstos en alguno de los móviles, debe apreciarse un concurso aparente,[238] salvo en el caso del artículo 7 inciso segundo de la LTP en razón de la existencia de la regla concursal especial del artículo 9 de la misma. Por otra parte, la entrega de datos representativos de información para el acceso a cuentas bancarias o similares puede realizar el acto de colaboración en un fraude informático (artículo 7 inciso segundo) o la transferencia de datos con fin ilícito (artículo 6), configurando un concurso aparente a ser solucionado según las reglas generales.

Referencias

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

Alvarado, Agustina (2022). «Capítulo V. Delitos contra la intimidad». En Luis Rodríguez (director), *Derecho Penal. Parte Especial* (pp. 461-546). Volumen I. Valencia: Tirant lo Blanch.

Arocena, Gustavo (2012). «La regulación de los delitos informáticos en el Código Penal argentino: Introducción a la Ley Nacional 26.388». *Boletín Mexicano de Derecho Comparado*, 135: 945-988. DOI: 10.22201/iij.24484873e.2012.135.4776.

Balmaceda, Gustavo (2009). *El delito de estafa informática*. Santiago: Ediciones Jurídicas de Santiago.

—. (2021). *Manual de Derecho Penal. Parte especial*. 4.ª ed. Tomo II. Santiago: Librotecnia.

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.

Castiñeira, María Teresa y Albert Estrada (2021). «Tema 7. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio». En Jesús-María Silva (director), *Lecciones de Derecho Penal. Parte Especial* (pp. 157-182). 7.ª ed. Barcelona: Atelier.

238. De la Mata (2018: 736), Dopico (2018: 231) y, con matices, Gómez (2002: 18-20).

Choclán, José Antonio (2002). «Infracciones patrimoniales en los procesos de transferencia de datos». En Oscar Morales (director), *Delincuencia informática. Problemas de responsabilidad* (pp. 243-280). Madrid: Consejo General del Poder Judicial.

Contreras, Marcos (2020). «El objeto material del delito del artículo 4 de la Ley 19.223: Información no accesible normativamente por terceros». *Revista de Ciencias Penales*, 1: 214-222. Disponible en https://bit.ly/3h23CD4.

Cortés, José Luis (2017). «Sobre la distinción de aspectos criminológicos y dogmáticos en el ámbito de la criminalidad informática». *Revista Jurídica del Ministerio Público*, 69: 175-190. Disponible en https://bit.ly/3VL25A5.

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.

Cruz, Roberto (2020). «La penalidad del delito de programa de ordenador fraudulento en el Código Penal español. Régimen vigente y posibilidades de reforma». *Estudios de Deusto*, 2: 75-95. DOI: 10.18543/ed-68(2)-2020pp75-95.

—. (2022). «La estructura de las normas en los delitos de preparación. Un estudio a propósito de la legitimidad de la intervención en materia de preparación delictiva». *Revista Electrónica de Ciencia Penal y* Criminología, 24: 1-37. Disponible en http://criminet.ugr.es/recpc/24/recpc24-11.pdf.

De la Fuente, Felipe (2016). *El error sobre los elementos típicos de antinormatividad. Tesis doctoral*. Valencia: Universitat Pompeu Fabra.

De la Mata, Norberto (2016). «Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (artículo 197 bis CP). El concepto de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación». *Cuadernos de Política Criminal*, 118: 43-86.

—. (2018). «Tema 18. Delitos contra los sistemas de información». En Norberto de la Mata, Jacobo Dopico, Juan Antonio Lascuraín y Adán Nieto (autores), *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.

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

Dopico, Jacobo (2018). «Estafas y otros fraudes en el ámbito empresarial». En Norberto de la Mata, Jacobo Dopico, Juan Antonio Lascuraín y Adán Nieto (autores), *Derecho Penal Económico y de la Empresa* (pp. 169-235). Madrid: Dykinson.

Escalona, Eduardo (2004). «El hacking no es (ni puede ser) delito». *Revista Chilena de Derecho Informático*, 4: 149-167. Disponible en https://bit.ly/3FoDReo.

Escuchuri, Estrella (2004). *Teoría del concurso de leyes y de delitos. Bases para una revisión crítica*. Granada: Comares.

Faraldo, Patricia (2007). «Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática». *Eguzkilore*, 21: 33-57. Disponible en https://bit.ly/3ukbbbr.

Fernández, Javier (2007). «Respuesta penal frente a fraudes cometidos en internet: Estafa, estafa informática y los nudos de la red». *Revista de Derecho Penal y Criminología*, 19: 217-243. Disponible en https://bit.ly/3H5AIg1.

—. (2022). «Clásicas y nuevas conductas fraudulentas ejecutadas en la red y su subsunción en los tipos de estafa y estafa informática contenidos en el Código Penal». En Carolina Bolea, José-Ignacio Gallego, Víctor Gómez, Juan Carlos Hortal y Ujala Joshi (directores), *Un modelo integral de derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo* (pp. 1135-1149). Madrid: Agencia Estatal Boletín Oficial del Estado. Disponible en https://bit.ly/3Vu8obx.

Flores, Fátima (2013). «La responsabilidad penal del denominado mulero o "phisher-mule" en los fraudes de banca electrónica». *Cuadernos de Política Criminal*, 110: 155-188.

Galán, Alfonso (2004). «El nuevo delito del artículo 248.3 CP: ¿un adelantamiento desmedido de las barreras de protección penal del patrimonio?». *La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía*, 6037: 1-7.

—. (2005). *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 C.P.* Valencia: Tirant lo Blanch.

Gómez, Víctor (2002). «El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (artículo 270, párrafo tercero, CP). A la vez, un estudio sobre los delitos de emprendimiento o preparación en el CP de 1995». *Revista Electrónica de Ciencia Penal y Criminología*, 4: 1-46. Disponible en https://bit.ly/3Utouhx.

González, Jorge (2016). «La seguridad en los sistemas de información como un bien jurídico de carácter autónomo. Perspectiva europea y española». *Revista Penal México*, 9: 59-76. Disponible en https://bit.ly/3B4tt4f.

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 Chile.

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.

Hernández, Héctor (2008). «Uso indebido de tarjetas falsificadas o sustraídas y de sus claves». *Política Criminal*, 5: 1-38. Disponible en https://bit.ly/3EUhpUp.

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

Londoño, Fernando (2004). «Los delitos informáticos en el proyecto de reforma en actual trámite parlamentario». *Revista Chilena de Derecho Informático*, 4: 171-190. Disponible en https://bit.ly/3WEyiJI.

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.

Maldonado, Francisco (2020). «Sobre la naturaleza del concurso aparente de leyes penales». *Política Criminal*, 30: 493-525. Disponible en https://bit.ly/3VNvius.

Mañalich, Juan Pablo (2018). *Estudios sobre la fundamentación y determinación de la pena*. Santiago: Legal Publishing.

—. (2020a). «El favorecimiento personal habitual como forma de encubrimiento punible». *Revista de Derecho* (Universidad de Concepción), 247: 195-220. DOI: 10.29393/RD247-6JMFP10006.

—. (2020b). «El dolo como creencia predictiva». *Revista de Ciencias Penales*, 1: 13-42. Disponible en https://bit.ly/3Fmkz4z.

Mata, Ricardo (2003). *Delincuencia informática y Derecho Penal.* Managua: Hispamer.

Matus, Jean Pierre y María Cecilia Ramírez (2021). *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*, 1: 235-260. DOI: 10.4067/S0718-34372017000100011.

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

—. (2018b). *Delitos económicos de estafa y otras defraudaciones*. Santiago: DER.

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.

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

Medina, Gonzalo (2014). «Estructura típica del delito de intromisión informática». *Revista Chilena de Derecho y Tecnología*, 1: 79-99. DOI: 10.5354/0719-2584.2014.32221.

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

—. (2013). «La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing». *Revista Electrónica de Ciencia Penal y Criminología*, 15: 1-56. Disponible en https://bit.ly/3B2ZTMk.

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.

Muñoz, Francisco (2015). *Derecho Penal. Parte Especial*. 20.ª ed. Valencia: Tirant lo Blanch.

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.

Ossandón, Magdalena (2008). «El delito de receptación aduanera y la normativización del dolo». *Ius et Praxis*, 1: 49-85. Disponible en https://bit.ly/3iqRkVb.

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.

Pastor, Nuria (2020). «Tema 9. El delito de estafa». En Jesús-María Silva (director), *Lecciones de Derecho Penal Económico y de la Empresa. Parte General y Especial* (pp. 247-282). Barcelona: Atelier.

Posada, Ricardo (2017). «El cibercrimen y sus efectos en la teoría de la tipicidad: De una realidad física a una realidad virtual». *Revista Nuevo Foro Penal*, 88: 72-112. Disponible en https://bit.ly/3EYYAPH.

Rodríguez, Carmen (2003). «Criminalidad y sistemas informáticos». En María Rosario Diego Díaz-Santos y Eduardo Fabián (coordinadores), *El sistema penal frente a los retos de la nueva sociedad* (pp. 139-162). Madrid: Colex.

Rojas, Luis Emilio (2017). «Modelos de regulación de los delitos de falsedad y de los delitos patrimoniales». *Política Criminal*, 23: 380-408. DOI: 10.4067/S0718-33992017000100010.

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.

Rovira, Enrique (2002). *Delincuencia informática y fraudes informáticos*. Granada: Comares.

—. (2003). «Hacia una expansión doctrinal y fáctica del fraude informático». *Revista de Derecho y Nuevas Tecnologías*, 3: 109-143.

Rueda, María Ángeles (2020). «La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español». *Diritto Penale Contemporaneo*, 3: 199-216. Disponible en https://bit.ly/3VN9wXz.

Solari, Mariana (2022). «Suplantación de identidad digital: ¿Necesidad de criminalización?». *Cuadernos de Política Criminal*, 136: 125-164.

Suazo, Carolina (2013). «Protección penal de información íntima almacenada en computadores y dispositivos portátiles». *Revista Chilena de Derecho y Ciencias Penales*, 2: 149-152.

Tiedemann, Klaus (2010). *Manual de Derecho Penal Económico. Parte general y especial*. Traducción por Alfonso Galán Muñoz (pp. 439-450). Valencia: Tirant lo Blanch.

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.

Winter, Jaime (2013). «Elementos típicos del artículo segundo de la Ley 19.223: Comentario a la SCS de 03/07/2013 Rol número 9238-12». *Revista Chilena de Derecho y Ciencias Penales*, 4: 277-282. Disponible en https://bit.ly/3FjxKmX.

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, 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)