REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 13 (2024) • e72932 • DOI 10.5354/0719-2584.2024.72932
RECIBIDO: 30/11/2023 • APROBADO: 7/6/2024 • PUBLICADO: 30/10/2024

DOCTRINA

# La facilitación de medios al interior de la empresa para la comisión de un fraude informático: Problemas dogmáticos y relativos al *compliance*

*The provision of means within the company for the commission of computer fraud: Dogmatic and compliance related problems*

**Laura Mayer Lux y Angela Toso Milos**
*Pontificia Universidad Católica de Valparaíso, Chile*

**RESUMEN** Analizamos uno de los delitos más novedosos de Ley 21.459, a saber, la «facilitación de medios» para la comisión de un fraude informático, específicamente cuando se verifica al interior de una empresa, cuyo giro se relaciona con las transferencias electrónicas. El texto se centra en diferenciar entre la comisión de dicho delito y otros supuestos, como la falta de un modelo (adecuado y efectivo) de *compliance*. El artículo defiende una interpretación restrictiva del tipo de facilitación de medios, basada en el sentido de dicha expresión y en la diversa naturaleza jurídica que cabe atribuir a la comisión de un delito, por un lado, y a la ausencia de un modelo de *compliance*, por otro.

**PALABRAS CLAVE** Delitos informáticos, riesgos empresariales, prevención de delitos, ley de delitos económicos, ciberseguridad.

**ABSTRACT** The paper analyzes one of the most innovative crimes of Law 21,459, namely, the «facilitation of means» for the commission of computer fraud, specifically when it is verified within a company, whose business is related to electronic transfers. The text focuses on differentiating between the commission of said crime and other cases, such as the lack of an (adequate and effective) compliance model. The article defends a restrictive interpretation of the crime of facilitation of means, based on the significance of said expression and on the diverse legal nature that can be attributed to the commission of a crime, on the one hand, and the absence of a compliance model, on the other.

**KEYWORDS** Cybercrimes, business risks, crime prevention, white-collar-crime law, cybersecurity.

## Introducción y planteamiento del problema

La Ley 21.459, de Delitos Informáticos, del 20 de junio de 2022, regula dos supuestos de fraude informático: uno relacionado con la manipulación de datos, que provoca un perjuicio patrimonial y es realizada con ánimo de lucro (artículo séptimo inciso primero); y otro que se vincula con la facilitación de medios para la comisión de un fraude informático en los términos señalados (artículo séptimo inciso final), que en lo sucesivo también denominaremos simplemente como delito de «facilitación de medios», o bien mediante alguna expresión análoga.

Esta segunda figura delictiva, que constituye una de las novedades introducidas por la ley de delitos informáticos, plantea varias problemáticas en caso de que la facilitación de medios referida tenga lugar al interior de una empresa, cuyo giro se relaciona con las transferencias electrónicas u otras actividades similares, paradigmáticamente bancos e instituciones financieras. Entre ellas se encuentra el asunto consistente en delimitar la comisión del tipo penal de facilitación de medios de otros casos que podrían confundirse con el mismo, como podría ser la falta de un modelo adecuado y efectivo de *compliance* penal o la omisión de medidas de ciberseguridad al interior de la persona jurídica. Para examinar dicho asunto, el texto partirá de la base de que el tipo penal de facilitación de medios no ha sido derogado en virtud de las modificaciones introducidas en materia de estafa y de fraude informático al artículo 468 del Código Penal, a través de la Ley 21.595, de Delitos Económicos, del 17 de agosto de 2023.[1]

Como cuestión previa, surge la duda relativa a qué podemos entender por facilitación de medios para la comisión de un fraude informático. En ese sentido, pese a que en la historia de la ley de delitos informáticos y a nivel doctrinal se postula un nexo directo entre dicho caso y el de los denominados «cibermuleros» (Miró Llinares, 2013; Riquert, 2017), «intermediarios electrónicos» (Bascur y Peña, 2022: 25) o *bankdrops* (Kochheim, 2015: 379),[2] el texto del artículo séptimo inciso final de la Ley 21.459 no se limita expresamente a ese supuesto. Ello lleva a preguntarnos si caben otros casos de facilitación de medios, distintos del de los cibermuleros, que pudieran castigarse de acuerdo con el artículo referido.

En esta materia es posible plantear, básicamente, dos interpretaciones de la conducta: una restrictiva, de acuerdo con la cual la facilitación de medios para la comisión de un fraude informático se identifica, fundamentalmente, con casos de complicidad *(lato*

1. No existe una derogación expresa ni una derogación tácita fundada, por ejemplo, en la incompatibilidad del supuesto de fraude informático establecido en el artículo 468 inciso segundo del Código Penal, con el tipo de facilitación de medios del artículo séptimo inciso final de la Ley 21.459.

2. Aclaramos que es ese el caso de facilitación de medios que examinaremos y no otras hipótesis que también podrían relacionarse con el fenómeno de los cibermuleros, como es el supuesto del lavado de activos asociado al fenómeno referido, donde también se utiliza el concepto de *money mules*. Véase, por ejemplo, a Arevalo (2015) y Pickles (2021).

*sensu)* relacionados con dicho delito. Adicionalmente, puede plantearse una interpretación amplia, donde la idea de facilitación de medios podría comprender cualquier comportamiento que, directa o indirectamente, implique favorecer la comisión de un fraude informático.

Concretamente, la cuestión principal que debe dilucidarse es si la falta de un modelo adecuado y efectivo de *compliance* penal puede ser valorada, en determinados supuestos, como un caso de facilitación de medios para la comisión de un fraude informático, lo que torna indispensable examinar qué función dogmática desempeña el *compliance* respecto de la responsabilidad penal de una persona jurídica. Junto con ello, se vuelve necesario analizar si la falta de adopción de medidas de ciberseguridad al interior de la empresa puede valorarse como un caso de *non-compliance* y, consiguientemente, de facilitación de medios para la comisión de un fraude informático, especialmente cuando el giro de la empresa supone el empleo de sistemas informáticos que han de operar dentro de márgenes tolerables de riesgo, por ejemplo, para realizar transacciones electrónicas u otras operaciones análogas.

Paralelamente, una cuestión que también debe resolverse es si cabe sancionar el *non-compliance* como un caso de omisión de acciones debidas, específicamente, como una hipótesis de participación punible omisiva o como un supuesto de omisión impropia (particularmente respecto de un fraude informático). Como veremos, dicha posibilidad resulta problemática en el contexto chileno, donde no es clara la punibilidad de casos de participación omisiva, en tanto no existe una norma legal habilitante (equivalente al artículo 11 del Código Penal español o al § 13 del Código Penal alemán), que permita sancionar supuestos de omisión impropia.

El presente trabajo defenderá una interpretación restrictiva del delito de facilitación de medios, basada en el sentido de dicha expresión y en la diversa naturaleza jurídica que cabe atribuir a la comisión de ese delito, en comparación a la ausencia de un modelo de *compliance* u otras hipótesis análogas. Secundariamente, el texto cuestionará la punibilidad de casos de participación omisiva y descartará derechamente la aplicación de la omisión impropia por razones de legalidad.

## Regulación del fraude informático y de la facilitación de medios para su comisión

El fraude informático se encuentra tipificado en la ley de delitos informáticos a partir de dos figuras delictivas que pueden diferenciarse nítidamente. La primera de ellas tiene como antecedente directo el artículo octavo del Convenio de Ciberdelincuencia[3]

3. El artículo octavo, respecto del fraude informático, detalla: «Las partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de

y corresponde a la manera en que tradicionalmente se ha regulado el fraude informático (por ejemplo, en Alemania y España),[4] esto es, como un caso de producción de un perjuicio patrimonial ajeno, llevada a cabo con ánimo de lucro, mediante una alteración o manipulación de datos o programas de sistemas informáticos (Mayer y Oliver, 2020; y similar, en Vinelli, 2021). Tal supuesto puede ser denominado «fraude informático propiamente tal» (Bascur y Peña, 2022: 18), a fin de enfatizar que esa es la hipótesis que paradigmáticamente corresponde a dicha clase de delito informático.

El segundo de los casos de fraude informático que establece la Ley 21.459 dispone lo siguiente: «Para los efectos de este artículo [que regula el fraude informático] se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito». Dicha figura delictiva no surge de la regulación establecida en el Convenio de Ciberdelincuencia, lo que permite sostener que se trata de un supuesto tipificado a partir del debate legislativo a que dio lugar la ley de delitos informáticos (Mayer y Vera, 2024). En ese sentido, si se revisa la historia de la ley, se advertirá que hubo principalmente dos instituciones que destacaron la necesidad de regular una hipótesis de facilitación de medios para la comisión de un fraude informático.

Por un lado, la Asociación de Bancos planteó la conveniencia de castigar penalmente a quienes reciben en sus cuentas corrientes bancarias fondos provenientes de la perpetración de fraudes informáticos,[5] individuos que pueden incluirse bajo la idea de «cibermulero», de «intermediario electrónico» o de *bankdrop*, a la que hicimos referencia anteriormente.

Por otro lado, el Ministerio Público relevó las dificultades probatorias que suponía la comisión de supuestos como el que hoy se sanciona a título de facilitación de medios

---

un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona».

4. Para el caso español, véase el artículo 249 1. a) del Código Penal español, de acuerdo con el cual «también se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años: a) los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro». A propósito de dicho delito, incluidas sus recientes reformas, consultar a Bustos Rubio (2023). Igualmente, a Mata y Martín (2007). Y en el caso alemán, véase el § 263a del Código Penal alemán, que regula la denominada «estafa informática», y castiga «al que, con el propósito de obtener para sí o para un tercero un beneficio patrimonial ilícito, perjudica el patrimonio de otro influyendo en el resultado de un proceso de tratamiento de datos mediante la incorrecta configuración del programa, mediante la utilización de datos incorrectos o incompletos, mediante el uso no autorizado de datos o de cualquier otra intervención indebida en el proceso», con pena privativa de libertad de hasta cinco años o con multa. En relación con dicho supuesto, véase a Kindhäuser (2017).

5. Historia de la Ley 21.459, 20 de junio de 2022, disponible en https://tipg.link/PlsP.

para la perpetración de un fraude informático. Entre ellas, dicho organismo planteó lo complejo que resultaba demostrar la existencia de un concierto previo entre quien lleva a cabo el fraude y quien facilita su comisión, razón que hacía difícil sancionar al cibermulero como autor, de acuerdo con el artículo 15 número 3, primera parte, del Código Penal (Historia de la Ley 21.459: 120; Bascur y Peña, 2022; Hernández Basualto, 2024).

## La facilitación de medios más allá de la actuación de los cibermuleros

Pese a que la hipótesis de facilitación de medios del artículo séptimo inciso final de la Ley 21.459 tiene una vinculación muy estrecha con el caso de los «muleros» de un fraude informático, la amplitud con la que ella se encuentra regulada permite abarcar otra clase de supuestos, distintos de aquel.

En ese orden de ideas, la manera en la que está tipificado dicho ilícito evoca directamente la hipótesis regulada en el artículo 15 número 3 y se vincula, asimismo, con la hipótesis establecida en el artículo 16 del Código Penal. La primera de ellas refiere a casos que se consideran como autoría, en que los intervinientes «concertados para su ejecución, facilitan los medios con que se lleva a efecto el hecho», mientras que la segunda, que sanciona a los cómplices, se extiende a casos no comprendidos en el artículo 15, de modo que en él pueden subsumirse hipótesis de facilitación de medios que no cumplan con todos los requisitos que establece el artículo 15 número 3 del Código Penal (Mayer y Vera, 2024). Lo interesante de estas relaciones entre el tipo penal de facilitación de medios y los casos de intervención delictiva referidos es que permiten aplicar al delito que ahora nos ocupa varias de las consideraciones que la doctrina ha efectuado a propósito de dichos casos.

Antes de examinar brevemente tales planteamientos, conviene consignar qué significa «facilitar» y cómo debe interpretarse la expresión «medio». De acuerdo con el Diccionario de la Real Academia Española, «facilitar» implica hacer fácil o posible la ejecución de algo,[6] en este supuesto, de un fraude informático, o bien, proporcionar o entregar, en este caso, los medios para llevarlo a cabo. Los nexos que cabe identificar entre el tipo de facilitación de medios para la comisión de un fraude informático e hipótesis de intervención delictiva, como las que son propias de la complicidad (artículo 16) o de situaciones análogas (artículo 15 número 3), permiten postular un vínculo muy estrecho entre la conducta consistente en «facilitar» y aquellas que implican «cooperar», «ayudar» o «auxiliar» en la realización,[7] en lo que aquí interesa, de un fraude informático (Mayer y Vera, 2024: 287).

6. Real Academia Española, «Facilitar», disponible en https://tipg.link/PlqW.

7. En esa misma línea, respecto del delito de auxilio al suicidio, consultar a Politoff y otros (2011). Véase también, desde un punto de vista más general, Novoa Monreal (2019).

A su vez, «medio», según el diccionario citado, es una cosa que puede servir para un determinado fin, en este supuesto, la realización de un fraude informático. Por consiguiente, se incluyen en dicha cláusula todos aquellos mecanismos que resulten idóneos para su ejecución. La doctrina, a propósito de las formas de intervención delictiva que se relacionan con la complicidad (o con la idea de facilitación) plantea que aquella puede abarcar medios materiales,[8] pero también intelectuales,[9] con los cuales se comete el delito (Hernández Basualto, 2011; Vargas Pinto, 2013). Si llevamos dichas consideraciones al asunto que nos ocupa, es posible sostener que la facilitación de medios para la comisión de un fraude informático puede abarcar ejemplos como poner a disposición de un tercero un *malware* o información relevante para perpetrar un fraude informático;[10] proporcionar una cuenta bancaria a la que se transfieran los fondos provenientes de un fraude informático (caso que correspondería al de los cibermuleros), etcétera (Cabrera Guirao y Contreras Chaimovich, 2024).

Una cuestión que resulta mucho más discutida es la de si cabe una intervención delictiva, como la que implica una facilitación de medios, a través de una omisión. La pregunta resulta pertinente en relación con el problema que aquí se analiza, en el contexto de un sistema de responsabilidad penal derivada como el que se establece en la Ley 20.393. En efecto, podría entenderse que el *non-compliance* corresponde, justamente, a un caso de omisión (penalmente relevante) y, en ese sentido, a un eventual supuesto de facilitación de medios para la ejecución de un fraude, por omisión de la existencia de un programa adecuado y efectivo de *compliance*.[11] En lo que respecta a la intervención delictiva por omisión, la doctrina acepta la posibilidad de una complicidad por omisión, en la medida en que quien omite sea garante (Gómez Martín, 2020; Haas, 2011; Mir Puig, 2016; Bustos Cárdenas, 2022), aunque reconoce que se trata de una materia polémica y en la que falta desarrollo dogmático, al menos en el contexto chileno (Hernández Basualto, 2011).

Supuesto que se admita la complicidad (o facilitación de medios) por omisión o, más ampliamente, la intervención delictiva por omisión, cabría preguntarse si ese caso abarca hipótesis de *non-compliance*. Esta última cuestión, a su turno, obligaría a resolver

8. Cuyo caso paradigmático es la entrega de un arma para cometer el delito.

9. Por ejemplo, dar consejos o asistencia para perpetrar el hecho. Al respecto, véase a Van Weezel (2023).

10. Por ejemplo, nombre de usuario, contraseña, claves que genera un dispositivo de seguridad o que se requieren para llevar a cabo transferencias electrónicas, etcétera.

11. En esta materia, es posible distinguir al menos tres supuestos: i) la ausencia (absoluta) de un programa de *compliance*; ii) la existencia de un programa inadecuado de *compliance* (que básicamente no contempla todos los elementos indicados en el artículo cuarto de la Ley 20.393), y iii) la existencia de un programa adecuado de *compliance*, pero que no está efectivamente implementado (también conocido como *paper compliance).* Respecto de este último supuesto, véase González Uriel (2022). Por otra parte, para valorar si un modelo de *compliance* es o no adecuado han de tenerse en cuenta los criterios del nuevo artículo cuarto de la Ley 20.393, a saber, objeto, tamaño, complejidad, recursos y actividades de la persona jurídica.

un asunto previo, a saber, la existencia de un garante en relación, específicamente, con la perpetración del delito de fraude informático, cuestión que resulta muy difícil de sostener sobre la base de la legislación chilena. Efectivamente, en términos generales, el desarrollo de la teoría de las fuentes de la posición de garante carece de una base positiva sólida en el Código Penal (Mayer, 2014), cuerpo legal que no cuenta con una disposición análoga, por ejemplo, al artículo 11 del Código Penal español o al § 13 del Código Penal alemán, que son los preceptos que posibilitan su construcción, en el contexto de la omisión impropia,[12] en la doctrina española y alemana, respectivamente. En ese sentido, si bien son imaginables diversos supuestos teóricos de intervención delictiva omisiva (Mañalich, 2014), incluso en materia de fraude informático,[13] su castigo penal a la luz de la normativa chilena puede implicar una vulneración del principio de legalidad.

Además, a efectos de determinar la responsabilidad penal de un banco o una institución financiera, cabría preguntarse cuál sería la fuente concreta en virtud de la cual aquel podría llegar a ser garante del patrimonio de sus clientes, en el sentido de que tendría el deber de adoptar medidas de salvataje orientadas a evitar daños patrimoniales provenientes de la comisión de fraudes informáticos.[14] Ello, sin perjuicio de la responsabilidad administrativa o civil que pudiera corresponder a la entidad de crédito frente a la infracción de las normas formuladas por el legislador y el regulador en este ámbito[15] o de las obligaciones contempladas al respecto en los contratos suscritos con sus clientes. En esa línea, no resulta sencillo identificar, desde el punto de vista penal, deberes de garante como el referido a partir de la normativa que rige a los bancos o instituciones financieras, conclusión que también puede plantearse si se revisan los términos de los contratos de cuenta corriente de uso común en el medio nacional. Si ello es efectivo, cabría descartar una facilitación de medios omisiva por parte de entidades tales como las aludidas, posibilidad sobre la que volveremos al examinar la función dogmática del *non-compliance* en el sistema jurídico chileno.

12. En ese sentido, la doctrina chilena plantea que «la complicidad omisiva se encuentra inmersa en lo que se denomina delitos de omisión impropia» (Bustos Cárdenas, 2022: 3), planteamiento que puede resultar necesario si se parte de la base de que las diversas hipótesis del artículo 15 y del artículo 16 del Código Penal implican la realización de actos ejecutivos de autoría o de complicidad.

13. Como cuando el garante, debiendo haber realizado acciones tendientes a evitar la existencia de una brecha de seguridad al interior del sistema informático, omite ejecutarlas.

14. Tales deberes serían mucho más intensos que aquellos que pueden predicarse respecto de la persona jurídica, pues se entiende que los deberes de dirección y vigilancia no suponen «deberes positivos de "evitación" absoluta de los delitos que puedan ser desarrollados por sus empleados y directivos» (García Palominos, 2020: 830).

15. Como es el caso de lo dispuesto en el «Capítulo 20-10 de la Recopilación Actualizada de Normas para Bancos», de la Comisión para el Mercado Financiero.

## Presupuestos de imputación de responsabilidad penal de una persona jurídica

La Ley 20.393, de Responsabilidad Penal de las Personas Jurídicas, del 2 de diciembre de 2009, establece diversos presupuestos de imputación que han sido recientemente modificados por la Ley 21.595, de Delitos Económicos. Como se adelantó, el modelo seguido por el legislador chileno es de «responsabilidad derivada», lo que implica que «se hace recaer sobre la persona jurídica la responsabilidad penal de una persona natural en virtud de algún criterio de conexión entre una y otra, generalmente la circunstancia de ser la persona natural órgano o al menos subordinado del ente moral» (Hernández Basualto, 2010: 216). También se sabe que, adicionalmente, la ley de responsabilidad penal de las personas jurídicas fundamenta esa clase de responsabilidad en el denominado «defecto de organización» (Bedecarratz, 2020; García Cavero, 2012; Valenzano y Serra Cruz, 2021), a la vez que permite que una persona jurídica, que crea e implementa efectivamente un modelo de compliance adecuado (Boehler y Montiel, 2021) pueda verse exenta de responsabilidad penal (Mayer y Vera, 2020).

Los presupuestos de imputación de responsabilidad penal de una persona jurídica pueden desprenderse, fundamentalmente, del artículo tercero de la Ley 20.393, incluida su reciente reforma a través de la ley de delitos económicos. De acuerdo con la disposición referida, resulta necesario que alguno de los delitos que pueden acarrear esa clase de responsabilidad (indicados en el artículo primero) sea perpetrado:

1. En el marco de la actividad de la persona jurídica.
2. Por o con la intervención de alguna persona natural que ocupe un cargo, función o posición en ella, o le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación; o bien, por o con la intervención de alguna persona natural relacionada en los términos indicados con una persona jurídica distinta, en la medida en que esta le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, o carezca de autonomía operativa a su respecto, cuando entre ellas existan relaciones de propiedad o participación.[16]
3. Siempre que la comisión del hecho se vea favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de prevención de tales delitos, por parte de la persona jurídica.

El análisis dogmático de cada una de esas exigencias desbordaría las finalidades del presente trabajo, en especial si se compara la legislación previa a la Ley 21.595 con la que fue introducida por este último cuerpo legal. Por lo mismo, nos centraremos en aquellos aspectos que más directamente se relacionan con el problema de la facilitación

16. Este último supuesto podría darse, por ejemplo, respecto de la filial de un banco que ha sido creada con el único objeto de prestar servicios informáticos de soporte en línea para los clientes de dicha entidad de crédito matriz.

de medios para la comisión de un fraude informático como caso que podría acarrear responsabilidad penal para una persona jurídica.

Una primera cuestión que resulta destacable es la referencia a la comisión del delito de que se trate en el marco de la actividad de la persona jurídica, exigencia que puede entenderse en el sentido de que el delito debe perpetrarse en relación con el giro de dicha entidad. Esta delimitación del requisito aludido resulta relevante teniendo en cuenta que la Ley 21.595 establece expresamente que las personas jurídicas pueden incurrir en responsabilidad penal por alguno de los delitos a que se refieren los artículos 1, 2, 3 y 4 de la ley de delitos económicos, sean o no considerados como delitos económicos por esa ley. En ese sentido, una persona jurídica podría incurrir en responsabilidad penal, aunque un fraude informático no sea considerado como delito económico de acuerdo con la Ley 21.595. Recordemos que, en virtud del artículo segundo número veinte de esta última ley, los delitos informáticos corresponden a la denominada «segunda categoría» de delitos económicos, que considera como tales, entre otros, a los delitos informáticos que fueren perpetrados «en ejercicio de un cargo, función o posición en una empresa, o cuando lo fuere en beneficio económico o de otra naturaleza para una empresa». Tal precepto debe ser complementado con lo que establece el artículo tercero inciso final de la Ley 20.393, de acuerdo con el cual, no surgirá responsabilidad penal para la persona jurídica cuando el hecho punible se perpetre exclusivamente en su contra.

Pues bien, la exigencia en orden a que el delito respectivo debe ser perpetrado en el marco de la actividad de la persona jurídica neutraliza en parte la excesiva amplitud que podría subyacer a una imputación por delitos con independencia de su carácter económico. En esa línea, si bien no se descarta la imputación de un fraude informático que no sea delito económico según el artículo segundo de la Ley 21.595, por expresa disposición del artículo primero número uno de la Ley 20.393, ello no obsta a su consideración como delito económico *(lato sensu)* en virtud de otras consideraciones, por ejemplo, la circunstancia de que el ilícito sea cometido en relación con el giro de una empresa (paradigmáticamente un banco).

Por otra parte, pese a que la ley de delitos económicos amplió de forma relevante el elenco de personas jurídicas que pueden incurrir en responsabilidad penal, que en caso alguno se circunscribe exclusivamente a empresas o sociedades, sigue teniendo vigencia la idea de que la Ley 20.393 constituye un modelo de atribución de responsabilidad penal referido «esencialmente a "delitos corporativos" generados durante la operación del negocio» (García Palominos, 2020: 830).

Más conflictiva, en cambio, es la exigencia en orden a que la imputación penal a la persona jurídica solo se descartará si el hecho es perpetrado exclusivamente en su contra, idea que podría interpretarse en el sentido de que el delito en cuestión se limitó a generarle perjuicios o, desde otro punto de vista, no envolvió beneficios (ya sea directa o indirectamente) para la persona jurídica. Podría plantearse entonces que, por ejemplo, la falta de adopción de medidas adecuadas para evitar la comisión de fraudes

informáticos (sea en la forma de un sistema de *compliance*, de mecanismos de ciberseguridad, etcétera) implicó un ahorro de costos económicos para la persona jurídica, lo que impediría sostener que el hecho se cometió «exclusivamente» en contra de ella.

Una segunda cuestión que resulta destacable es la exigencia relativa a facilitar (o favorecer) la comisión del hecho respectivo, por la falta de implementación efectiva de un modelo adecuado de prevención de tales delitos, por parte de la persona jurídica. A la inversa que el primer requisito indicado en el artículo tercero de la Ley 20.393, este implica una reducción de las probabilidades de imputación de la persona jurídica, pues se ha pasado de un sistema en que, al menos según la literalidad de la ley de responsabilidad penal de las personas jurídicas,[17] basta con que la comisión del delito «fuere consecuencia del incumplimiento […] de los deberes de dirección y supervisión» (texto previo a la Ley 21.595) a un sistema en que dicho incumplimiento debe facilitar (o favorecer) la perpetración del hecho (requisito modificado por la Ley 21.595). Si pensamos en la comisión de un fraude a través de la página web de un banco, la antigua normativa parecía contentarse con la exigencia de una relación causal entre la inexistencia (o falta de implementación) de un sistema adecuado de *compliance* (o el incumplimiento de los deberes de dirección y supervisión) y la perpetración del fraude informático de que se trate.

Hoy, en cambio, el incumplimiento de los deberes de dirección y supervisión, de acuerdo con la nomenclatura previa a la Ley 21.595, que subyace a la falta de un modelo de *compliance* (Artaza Varela, 2013; Navas y Jaar, 2018) y configura el defecto de organización, ha de haber hecho posible la ejecución de aquel delito, en el sentido de proporcionar de alguna manera los medios necesarios para llevarlo a cabo. En este contexto, cobra especial fuerza el planteamiento de Salvo Ilabel, a juicio de quien, en el ámbito de la responsabilidad penal de la persona jurídica, la empresa se erige como «escenario» pero también como «motor» de la perpetración de delitos (Salvo Ilabel, 2015: 10).

## Función dogmática del *non-compliance*

En la doctrina especializada se ha ido asentando la idea de que la naturaleza jurídica del compliance en materia penal corresponde a la de una eximente de responsabilidad penal[18] (Blanco Cordero, 2023; Morón Vera, 2021; Gutiérrez Pérez, 2015; Riquert, 2020; Turienzo Fernández, 2022; Valenzano y Serra Cruz, 2021), que puede ser invocada a favor de la persona jurídica de que se trate (Bacigalupo, 2021). Eso significa que el delito

17. Hacemos esta aclaración, pues con anterioridad a la ley de delitos económicos ya existían autores que planteaban un incumplimiento de los deberes de dirección y supervisión que facilita la comisión del delito que hace surgir la responsabilidad penal de la persona jurídica. Al respecto, véase a Navas y Jaar (2018).

18. En términos más procesales, la existencia de un modelo adecuado de *compliance* puede ser invocada como una defensa en el proceso penal que se siga en contra de la persona jurídica. Véase, en esa línea, Mayer y Vera (2020); con énfasis en el derecho administrativo sancionador, Hernández Basualto (2018).

imputable a la persona jurídica en realidad no se ha configurado, pues falta alguno de sus elementos: conducta, tipicidad, antijuridicidad o culpabilidad. Igualmente, existe consenso en orden a que el programa de compliance penal debe cumplir ciertos requisitos para que pueda eximir de responsabilidad penal a la persona jurídica. En concreto, ha de tratarse de un sistema adecuado (Gutiérrez Pérez, 2015; Mayer y Vera, 2020) en atención al giro de la persona jurídica, que opere efectivamente en la práctica (Blanco Cordero, 2023; Morón Vera, 2021), no bastando la existencia de un modelo genérico y meramente formal de cumplimiento en materia penal.

El hecho de que un programa de *compliance* constituya una eximente de responsabilidad penal de la persona jurídica plantea la necesidad de comparar la forma en que opera dicha eximente y otras eximentes, por así decirlo, tradicionales. Si examinamos las circunstancias que se regulan en la legislación chilena y que tradicionalmente se han considerado como tales (por ejemplo, legítima defensa, estado de necesidad o miedo insuperable), advertiremos que todas ellas suponen la ausencia de un elemento del delito (Novoa Monreal, 2015), lo que genera una falta de verificación del delito respectivo y, con ello, la no concurrencia de un requisito esencial para que surja responsabilidad penal. Tratándose de la eximente de *compliance* ocurre lo mismo, en el sentido de que la existencia e implementación efectiva de un modelo de *compliance* adecuado elimina un elemento del delito imputable a la persona jurídica, el que, de acuerdo con un sector de la doctrina, correspondería a la tipicidad (Mayer y Vera, 2020; Ontiveros Alonso, 2017).

Si se parte de esa base, puede sostenerse que la configuración de la eximente de que se trate provoca la no configuración del delito respectivo, planteándose entonces qué ocurre si la eximente en cuestión no se verifica. Desde ya debe tenerse en cuenta que la no verificación de una eximente es una cuestión que puede admitir grados (Náquira Bazán, 2020), en el sentido de que es posible que se presenten supuestos en los que concurran ciertos requisitos de la eximente (faltando uno o más para que ella tenga lugar), o bien, en los que falten cada uno de sus presupuestos.

En la primera hipótesis podríamos encontrarnos ante un caso de la llamada eximente incompleta, situación que en realidad corresponde a una atenuante de responsabilidad penal de efectos penológicos particularmente intensos (Mir Puig, 2016; Navarro Dolmestch, 2022). El supuesto regulado en la Ley 20.393, que más se asemeja a dicha hipótesis, es el de la circunstancia atenuante del artículo sexto número tres.[19] No obstante, si se parte de la base de que esa disposición no establece un caso específico de eximente incompleta, habría que recurrir al precepto relativo a la eximente

19. Según el cual, constituirá una circunstancia atenuante: «La adopción por parte de la persona jurídica, antes de la formalización de la investigación, de medidas eficaces para prevenir la reiteración de la misma clase de delitos objeto de la investigación. Se entenderá por medidas eficaces la autonomía debidamente acreditada del encargado de prevención de delitos, así como también las medidas de prevención y supervisión implementadas que sean idóneas en relación con la situación, tamaño, giro, nivel de ingresos y complejidad de la estructura organizacional de la persona jurídica».

incompleta en el Código Penal (artículo 11 número 1), debiendo además resolverse qué «elementos mínimos» del sistema de prevención han de concurrir (Valenzano y Serra Cruz, 2019: 56) para hacer aplicable el supuesto descrito en el referido cuerpo legal.

En la segunda hipótesis, en cambio, atendido a que faltan todos los requisitos de la eximente de que se trate, no habría duda de que el elemento del delito con el cual aquella se vincula sí se verificaría. Sin perjuicio de la posibilidad de discutir la eventual configuración de una eximente incompleta en materia de responsabilidad penal de las personas jurídicas, por ahora nos detendremos en el segundo caso referido, esto es, aquel en el que falta el sistema de *compliance* penal en los términos de la Ley 20.393.

## ¿Puede considerarse el non-compliance como un caso de facilitación de medios para la comisión de un fraude informático?

Esta pregunta puede ser respondida en términos particulares, esto es, i) considerando la regulación del artículo séptimo inciso final de la nueva ley de delitos informáticos; y, también puede ser respondida en términos generales, o sea, teniendo en cuenta ii) los presupuestos de imputación de responsabilidad penal a la persona jurídica previstos en el artículo tercero de la Ley 20.393, o bien, iii) la regulación que, en materia de autoría y participación delictivas, se relaciona con casos de facilitación de medios, es decir, los artículos 15 número 3 y 16 del Código Penal.

Desde un punto de vista particular, la falta (dolosa) de un sistema adecuado de *compliance* penal puede ser valorada como un comportamiento que facilita (o favorece) la comisión de delitos al interior de la persona jurídica, no siendo sin embargo claro si ello puede contar, específicamente, como una facilitación de medios para la comisión de un fraude informático. Esto es relevante, pues de lo que se trata, al menos en este nivel, es de determinar si la conducta del agente ha resultado funcional a la comisión de un delito en concreto (fraude informático) y no de cualquier delito imaginable, que pudiera acarrear responsabilidad penal para la persona jurídica.

Si se parte de esa base, cabría discutir la relevancia penal de la omisión de ese agente, consistente en no contar con un programa efectivo y adecuado de *compliance* en atención a los riesgos particulares que afectan a la persona jurídica de que se trate. No obstante, en este contexto se plantea el problema de la falta de un fundamento legal en la normativa chilena sobre el cual pueda sustentarse el castigo por la omisión (impropia) subyacente a dicha hipótesis. En nuestra opinión, tal problema no se resuelve simplemente a través de la interpretación del derecho vigente, como ha intentado un sector de la doctrina (Izquierdo Sánchez, 2016), sino que requiere de texto expreso, por razones de legalidad (Mayer, 2014).

Desde una perspectiva general, la falta de un sistema adecuado de *compliance* penal puede ser considerada como un caso subsumible en uno de los presupuestos de imputación de responsabilidad penal previstos en el artículo tercero de la Ley 20.393,

de acuerdo con las reformas introducidas en esta materia por la Ley 21.595 sobre delitos económicos. Recordemos que, según la nueva configuración del precepto aludido, para que una persona jurídica pueda ser responsabilizada penalmente es necesario que concurran, copulativamente, los siguientes presupuestos.

Primero, se requiere que se haya cometido uno de los delitos que indica el artículo primero de la Ley 20.393 sobre responsabilidad penal de las personas jurídicas que, tras las modificaciones efectuadas por la ley de delitos económicos, se han ampliado considerablemente en términos cuantitativos. En efecto, junto con los delitos que ya establecía el artículo primero con anterioridad a la publicación de la Ley 21.595 que, como sabemos, se habían ido incrementando paulatinamente con varias de las últimas reformas introducidas a la legislación penal, hoy se agregan todos los delitos señalados en la ley de delitos económicos. Gracias a ello, si bien el catálogo de delitos sigue siendo de *numerus clausus,* él abarca una gran cantidad de figuras delictivas, las que además se extienden a comportamientos de muy variada naturaleza. Dicho presupuesto se cumple perfectamente en el caso de la facilitación de medios para la comisión de un fraude informático, atendido a que la Ley 20.393 se remite expresamente a todos los delitos informáticos, regulados en la Ley 21.459.

Segundo, el delito en cuestión debe ser perpetrado en el marco de la actividad de la persona jurídica. En primera instancia, es posible plantear que el ilícito penal debe tener alguna clase de vínculo con el giro de la persona jurídica, exigencia que, no obstante, puede generar discusiones en cuanto a su aplicación práctica. Así, por ejemplo, podría debatirse si lo que interesa es la actividad que formalmente haya declarado la persona jurídica, o bien, aquella que, materialmente, es decir, en los hechos es efectivamente realizada por dicha entidad y, por tanto, razonablemente le puede ser atribuida.

Esta última interpretación tiene la ventaja de evitar posibles fraudes a la ley, en el sentido de que se cometan delitos fuera del marco de la actividad declarada, justamente, para eludir la imputación penal. Sin embargo, se trata de una interpretación que puede provocar importantes niveles de incerteza y extensiones injustificadas del ejercicio del *ius puniendi* estatal. Como sea, en el caso que analizamos, en que se comete un fraude informático a través del sistema informático de un banco o de una institución financiera, es evidente que se está perpetrando un delito que tiene directa relación con la actividad o con el giro de la persona jurídica, de suerte que en él, sin duda, también se cumpliría el segundo presupuesto de imputación que examinamos.

Tercero, el delito debe ser cometido por o con intervención de una persona natural que ocupe un cargo, una función o posición, o que preste servicios gestionando asuntos suyos ante terceros, con o sin su representación; o bien, el delito ha de ser perpetrado por o con intervención de una persona natural relacionada con una persona jurídica distinta, siempre que ella preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, o carezca de autonomía operativa a su respecto, cuando entre ellas existan relaciones de propiedad o participación.

La doctrina ya ha destacado la enorme cantidad de hipótesis que podrían verse abarcadas por la nueva redacción del presupuesto en comento (Balmaceda y otros, 2023), que dan cuenta de las pretensiones fuertemente expansivas de la reforma legal.[20] En todo caso, en lo que aquí interesa, podría quedar comprendido el trabajador de la empresa que, por ejemplo, se concierta con un tercero para utilizar el sistema informático del banco como vehículo para perpetrar un fraude informático; pero, también podrían quedar abarcados supuestos como el de un sujeto que, por ejemplo, presta servicios en una persona jurídica a la que el banco o la institución financiera ha externalizado el manejo de sus plataformas informáticas para efectuar transacciones o pagos, y se concierta con ese mismo tercero, facilitando los medios para la perpetración del fraude en cuestión. Por cierto, también es posible incluir el caso en que el sujeto indicado pertenece a una persona jurídica que integra el mismo grupo empresarial de aquella, cuyos sistemas informáticos son utilizados para la ejecución de un fraude informático, y que opera facilitando los medios para su comisión.

Cuarto, la perpetración del hecho debe haberse visto favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de *compliance* en materia penal, presupuesto que expresa lo que doctrinalmente se entiende como defecto de organización. Igualmente, este presupuesto es el que más directamente se vincula con el tenor literal del delito de facilitación de medios para la comisión de un fraude informático, toda vez que tanto el presupuesto como el delito giran en torno a la noción de «facilitar» (o «favorecer») la comisión de un comportamiento delictivo. Esta última cuestión refuerza la idea de que la infracción de los deberes relacionados con la prevención de delitos que tiene la persona jurídica no puede valorarse tanto como hipótesis de *non-compliance*, que impide enervar la imputación penal de la persona jurídica y, al mismo tiempo, como perpetración de un delito autónomo de facilitación de medios para la comisión de un fraude informático. Hay, en esta posibilidad, una doble valoración del mismo elemento normativo, en términos perjudiciales para el acusado,[21] posibilidad que constituye una infracción al principio *non bis in idem*.[22]

Igualmente, como plantea Bacigalupo, «el Código Penal no impone a las empresas una obligación legal de implementar un modelo de prevención de delitos. Solo establece las condiciones bajo las cuales, llegado el caso, las personas jurídicas podrían

20. Pretensiones que también han sido planteadas a propósito de la legislación española. Al respecto, postulando criterios que apuntan a una interpretación restrictiva de dicha normativa, véase a Fernández Teruelo (2011).

21. Entendemos que sería en términos perjudiciales, pues una institución que está pensada para eximir de responsabilidad penal a la persona jurídica y, en ese sentido, para operar como mecanismo de defensa de dicha entidad, estaría siendo considerada, en caso de no concurrir o de concurrir defectuosamente, también como la comisión de un delito en cuanto tal. Dicha posibilidad debe ser diferenciada del hecho de que la ausencia de un sistema (adecuado y efectivo) de *compliance* pueda operar —junto con otros— como criterio de imputación, en los términos de la Ley 20.393.

22. A propósito de la conceptualización de dicho principio, véase a Ossandón Widow (2018).

quedar exentas de responsabilidad penal» (Bacigalupo, 2021: 267). En ese sentido, la Ley 20.393 no parece contener reglas que permitan equiparar la mera falta de un sistema (adecuado y efectivo) de *compliance* en materia penal con la facilitación de medios para la perpetración de un delito, en este caso, de un fraude informático. Ello es así, pues la ley referida más bien apunta a establecer si y en qué medida una persona jurídica puede invocar la existencia de un sistema (adecuado y efectivo) de *compliance* como defensa frente a una posible imputación de responsabilidad penal (Mayer y Vera, 2024).

Asimismo, desde un punto de vista general, la falta de un sistema adecuado y efectivo de *compliance* penal puede ser valorada como un comportamiento que facilita (o favorece) la comisión de delitos al interior de la persona jurídica, en cuyo caso cabría examinar la posibilidad de sancionar al sujeto responsable de esa omisión. En principio, su castigo implicaría vincular las disposiciones que reglan el delito de que se trate con lo que establece el artículo 15 número 3 o el artículo 16 del Código Penal, que son los preceptos que inequívocamente abarcan supuestos de facilitación de medios (para la comisión de un delito).

En todo caso, pese a que a nivel doctrinal se ha planteado que la regulación de un sistema de responsabilidad penal de la persona jurídica, basado en la existencia de deberes de dirección y supervisión, «erige formalmente a la persona jurídica en *garante de vigilancia* respecto de su personal y connota que [esos] deberes […] incluyen la prevención de delitos» (Hernández Basualto, 2010: 225, cursivas en el original),[23] volvemos a topar con el problema del fundamento legal de la omisión impropia en la normativa penal chilena.

Luego, cabría precisar qué implica exactamente que la persona jurídica sea garante de vigilancia, materia en la que se requiere el desarrollo de criterios que apunten a delimitar ese supuesto, especialmente si se considera que existe acuerdo en orden a que los deberes de controlar los riesgos de comisión de delito al interior de la persona jurídica nunca son absolutos (Artaza Varela, 2013; García Palominos, 2020).

Por de pronto, a ella solo pueden imputársele delitos que «haya podido razonablemente evitar en caso de haber aplicado los mecanismos de vigilancia y control apropiados para aquello» (Baldomino Díaz, 2022: 69), lo cual implicará adoptar precauciones idóneas y necesarias (Bock, 2013), así como materiales y personales (Robles Planas, 2006) para alcanzar dicha finalidad. Adicionalmente, puede discutirse si la omisión en la que incurre el garante de vigilancia permite afirmar una hipótesis de autoría —como se sostiene respecto del garante de protección— o si, en cambio, solo faculta a sostener un supuesto de participación delictiva (Hilgendorf y Valerius, 2012).

Este estado de cosas, sin embargo, podría cambiar en el futuro. En efecto, en los últimos años se han desarrollado diversas propuestas destinadas a regular la omisión impropia en la legislación chilena. Entre ellas destaca el último proyecto de Código

23. Un planteamiento análogo efectúan autores como Bedecarratz (2020), Robles Planas (2006) y Valenzano y Serra Cruz (2019).

Penal, correspondiente al Boletín 14.795-07, de acuerdo con el cual, el delito puede estar constituido por una acción o por una omisión ilícita y culpable, implicando esta última el hecho de:

> Evitar un resultado siempre que quien omite se encuentre especialmente obligado a ello en razón de la protección debida a una o más personas o de su deber de controlar una situación peligrosa, que la producción de tal resultado se encuentre prevista por la ley bajo señalamiento de pena y que la omisión de evitar el resultado sea equiparable a producirlo.

El precepto propuesto sería perfectamente aplicable a los fraudes informáticos, pues alude expresamente a la producción de resultados, que en este caso se identificarían con el perjuicio patrimonial ajeno. Además, entraría en especial consideración, en materia de responsabilidad penal de las personas jurídicas, la referencia al control (Riquert, 2020) de una situación peligrosa (Balmaceda y otros, 2023; con énfasis en los riesgos para personas externas a la persona jurídica, Silva Sánchez, 2014), que es precisamente el supuesto que corresponde a los llamados garantes de vigilancia, en oposición a los garantes de protección, a los que también apunta la disposición citada.

Por otra parte, la posibilidad de que se regule expresamente la omisión impropia en Chile y se confirme a nivel positivo la posición de garante de la persona jurídica respecto de la prevención de delitos, refuerza la importancia práctica que puede tener la existencia de un sistema adecuado y efectivo de *compliance* a la hora de enervar la responsabilidad penal de aquella entidad. La comisión de delitos al interior de la empresa, no obstante la posición de garante de la persona jurídica, podría resultar neutralizada por la adopción e implementación de un modelo de prevención de delitos que dé cuenta, según la nomenclatura previa a la Ley 21.595, de un cumplimiento de sus deberes de dirección y supervisión (Valenzano y Serra Cruz, 2019).

## ¿Puede considerarse la falta de adopción de medidas de ciberseguridad como un caso de facilitación de medios para la comisión de un fraude informático?

El análisis realizado debe, a nuestro juicio, ser complementado con el examen de un asunto que puede vincularse con la facilitación de medios al interior de la empresa para la comisión de un fraude informático: a saber, la falta de adopción de medidas de ciberseguridad tendientes a evitar la perpetración de esa clase de delito. Si bien dicho supuesto puede ser analizado como una hipótesis independiente, también es posible valorarlo como un caso de ausencia de un modelo adecuado y efectivo de compliance o —vinculado con ello— como un supuesto de omisión impropia.

Desde un punto de vista general, es común que se sostenga que la persona jurídica, en tanto foco de eventuales comportamientos delictivos, tiene deberes particulares

orientados a neutralizar conductas ilícitas (también de carácter penal) (Hernández Basualto, 2010). Analizado desde otra perspectiva, se afirma que la creación de una persona jurídica no debe poner en riesgo la vigencia del orden legal (Bock, 2013) y que, si ello acontece, surge a su respecto el deber de llevar a cabo medidas tendientes a eliminar o al menos disminuir, en la mayor medida posible, los riesgos generados en virtud de su existencia e interacción al interior del tráfico jurídico. Tales ideas, que pueden compartirse, resultan problemáticas si se las interpreta, derechamente, como base para el castigo de hipótesis de omisión impropia a la luz del ordenamiento jurídico chileno, cuestión sobre la que volveremos en seguida.

Como sea, las medidas de control de los propios riesgos, que subyacen a los sistemas de autorregulación (forzada) (Artaza Varela, 2013; García Palominos, 2020), como el que caracteriza a la responsabilidad penal de las personas jurídicas (Marcazzolo, 2023), pueden abarcar diversos ámbitos, entre los que ciertamente es posible referir aquellos que se vinculan con los mecanismos de ciberseguridad. Con dicha expresión se alude a la organización e implementación de recursos, procesos e infraestructuras orientados a proteger al ciberespacio y a los sistemas vinculados con él (Craigen y otros, 2014) ante la verificación de eventos que afectan bienes jurídicos de titularidad individual o colectiva.

En ese orden de ideas, dicha protección puede proyectarse tanto para enfrentar las vulnerabilidades o fallos informáticos que pueda experimentar un sistema de tratamiento automatizado de la información como para hacer frente a las amenazas de diversa naturaleza que aprovechan tales vulnerabilidades (Ballester García, 2019). En consecuencia, la ciberseguridad comprende todas aquellas acciones orientadas a proteger la información presente en el ciberespacio, así como la infraestructura que la soporta, y tiene por objeto evitar o mitigar las consecuencias adversas derivadas de sus riesgos y amenazas inherentes, que puedan afectar la seguridad de la información y la continuidad del negocio.[24]

De otro lado, el control al que se alude puede operar en términos eminentemente preventivos, pero también como reacción frente a peligros que se han concretado y que han implicado afectaciones de bienes jurídicos, eventualmente constitutivas de responsabilidad penal. De cierta forma, ambas alternativas están recogidas en la Ley 20.393, sea a través de la implementación efectiva de sistemas adecuados de *compliance* para la evitación de delitos (artículo cuarto), sea a través de la adopción tardía, antes de la formalización de la investigación, de un sistema de esa índole, destinado a evitar la reiteración de delitos, como los que se investigan (artículo sexto) (Mayer y Vera, 2020).

Tratándose de personas jurídicas, mediante las cuales se realizan transacciones o transferencias electrónicas, las medidas de ciberseguridad deben apuntar a mantener tales operaciones dentro de un margen tolerable de riesgo, margen que a su vez permite

24. Comisión para el Mercado Financiero, «Capítulo 20-10 Gestión de seguridad de la información y ciberseguridad», disponible en https://tipg.link/PlxJ.

sostener que el sistema de que se trate es funcional, en el sentido de que opera en la práctica y es razonablemente seguro.[25] Para lograr dicho objetivo, en relación con el supuesto específico que analizamos, cabe tener en cuenta las siguientes variables.

En primer lugar, desde el punto de vista del deber de diligencia (Toso Milos, 2021) que pesa sobre los administradores societarios, y que comprende «la obligación de vigilancia, a partir de la supervisión y el control de la gestión de la sociedad» (Vásquez Palma, 2021: 189-190), es necesario que estos adopten e implementen medidas tendientes a evitar la concreción de riesgos tanto para la persona jurídica misma como para terceros. Ello implica mantener un sistema de gestión de la ciberseguridad, basado en una estructura organizacional y políticas definidas, concordantes con el volumen y complejidad de las operaciones desarrolladas por la entidad. También se debería contemplar una función o posición encargada de la identificación, seguimiento, mitigación y control de los riesgos de ciberseguridad,[26] así como protocolos o planes diseñados para responder oportunamente y recuperarse tras los incidentes o crisis que puedan presentarse en este ámbito.[27]

En este contexto, resulta relevante que la persona jurídica identifique y proteja aquellos activos de ciberseguridad considerados críticos para el funcionamiento del negocio. En relación con esto último, la entidad debería disponer, por ejemplo, de programas antivirus y cortafuegos, así como de mecanismos para la actualización de *softwares* idóneos para minimizar lo más posible las amenazas de ataques informáticos que pudieran derivar en casos de fraude. Igualmente, ella debe contar con sistemas de almacenamiento seguro de datos en servidores o en la nube (Montero Ulate y otros, 2020),[28] particularmente en lo que respecta a los datos personales de los clientes y a la información necesaria para efectuar transacciones y transferencias electrónicas.

En términos más específicos, la persona jurídica ha de prever mecanismos de reacción destinados a hacer frente a la comisión de fraudes informáticos, pero también de ilícitos conectados con ellos, como el acceso ilícito o el abuso de los dispositivos (artículos segundo y octavo de la Ley 21.459, respectivamente). En dicho contexto, el directorio ha de aprobar políticas y normas de conducta dirigidas a los trabajadores de la entidad y a las personas externas que le prestan servicios, orientadas a la utilización responsable de las tecnologías de la información y la comunicación puestas a su disposición.[29]

25. En esa línea, véase a Mayer (2017).

26. Este aspecto es abordado con detalle en la página cuatro del ya citado «Capítulo 20-10 Gestión de seguridad de la información y ciberseguridad».

27. Respecto de los bancos, consultar páginas uno, dos y siete del «Capítulo 20-10 Gestión de seguridad de la información y ciberseguridad».

28. Otras medidas de protección pueden encontrarse en la página cuatro del «Capítulo 20-10 Gestión de seguridad de la información y ciberseguridad».

29. Respecto a los bancos, ver página dos de «Capítulo 20-10 Gestión de seguridad de la información y ciberseguridad».

Además, el uso de dispositivos y equipos personales de los trabajadores de la persona jurídica en principio debería descartarse, salvo casos de fuerza mayor que así lo ameriten, y siempre durante periodos acotados.[30] En esa línea, la existencia de sistemas de teletrabajo[31] no obsta al cumplimiento de los deberes del empleador, en orden a proporcionar equipos, herramientas y materiales, tanto seguros como actualizados, que puedan ser utilizados por los trabajadores para desempeñar sus labores de forma remota; así como soporte y asistencia técnica en caso de ser necesario (Lizama Portal y Lizama Castro, 2021).

Luego, la persona jurídica debe contar con protocolos claros referentes al uso de sus sistemas informáticos y de sus casillas de correo electrónico,[32] que sean conocidos y aplicados por los trabajadores, a fin de que, por ejemplo, no se visiten páginas riesgosas o se descarguen archivos que pudieran dañar tales sistemas. Pero, junto con ello, la persona jurídica ha de adoptar medidas de supervigilancia en esta materia específica,[33] de modo que la evitación de riesgos cibernéticos no dependa exclusivamente de lo que haga (o deje de hacer) un trabajador o un grupo de trabajadores. Con todo, tales medidas de supervigilancia deben tener en cuenta la dignidad y los derechos fundamentales del trabajador (en especial, su intimidad, su vida privada y su honra), así como aplicarse de acuerdo con criterios de necesidad y proporcionalidad (Guidi, 2023).

Si bien la adopción e implementación de medidas como las indicadas puede suponer costos de diversa índole para la persona jurídica (por ejemplo, inversión en *softwares* adecuados o en personal experto en ciberseguridad), el tamaño y la complejidad de los bancos y de las instituciones financieras provoca que tales costos sean parte de las necesidades básicas de operatividad de la persona jurídica y que, por tanto, correspondan —al igual como ocurre con compañías de envergadura análoga— a parte importante de su presupuesto en tecnologías de la información y la comunicación (Kemp, 2023).

En ese sentido, la discusión relativa a si el cumplimiento de medidas de ciberseguridad puede resultar demasiado complejo, sobre todo por los desembolsos económicos

30. Siendo un ejemplo paradigmático de ello la pandemia por Covid-19. Respecto de los problemas que ha implicado en ese contexto el uso de equipos de propiedad del trabajador, véase a Giniger (2020).

31. Cuyo fundamento normativo se encuentra en el artículo 152 quáter L del Código del Trabajo. A partir de esta norma, la Dirección del Trabajo ha interpretado que la obligación del empleador de proporcionar equipos y herramientas no impide que las partes acuerden que el trabajador pueda utilizar elementos de su propiedad y que el empleador pueda pagar una asignación por su uso para efectos laborales (dictamen 258/03, de 22 de enero de 2022).

32. Por ejemplo, planteando que tales casillas tendrán un uso exclusivamente laboral (Vargas y Agustina, 2021), o que solo será posible visitar determinadas páginas web, descartando otras. En todo caso, cabe considerar que en materia laboral las cuestiones relativas al uso de dispositivos tecnológicos deben estar establecidas en el reglamento interno de orden, higiene y seguridad, de modo que las directrices señaladas han de valorarse como reglas adicionales a las contenidas en el referido reglamento.

33. Que también deben estar en el reglamento interno referido anteriormente.

que ello implicaría, tiene una importancia marginal en el contexto que analizamos. Por lo mismo, desde el punto de vista de la imputación penal, la eventual defensa de la persona jurídica no debería radicar en un cumplimiento de medidas de imposible o muy difícil consecución —como sí podrían plantear entidades de pequeño y mediano tamaño (Mayer, 2018)—; antes bien, las posibles alegaciones en esta materia deberían basarse en consideraciones vinculadas con el propio sistema jurídico penal y, entre ellas, con las atingentes a la función dogmática del *non-compliance* y, en el caso específico de la normativa chilena, con las relativas al fundamento legal del castigo aplicable a la omisión impropia.

En esa línea, pese a que la persona jurídica tiene deberes de control de determinados riesgos que se generan producto o en el contexto de su propia actividad, esos deberes no pueden traducirse en una atribución de responsabilidad penal por la mera omisión de medidas de ciberseguridad. Pero, incluso si en el futuro se consagrara un fundamento legal para el castigo de la omisión impropia, los deberes que pudieran surgir de la posición de garante tendrían que ser específicos y, por ende, traducirse en la adopción de medidas concretas.

Consiguientemente, tratándose de bancos e instituciones financieras, así como de la realización de transacciones y transferencias electrónicas, las medidas en cuestión tendrían que vincularse, particularmente, con la evitación de fraudes informáticos (u otros delitos informáticos que estén relacionados con el desarrollo de su giro). La responsabilidad de la persona jurídica surge siempre a propósito de ciertos delitos, así como en el marco de su actividad, y no respecto de cualquier comportamiento delictivo imaginable que pueda perpetrarse a través de ella o gracias a ella.

Adicionalmente, no debe perderse de vista que muchas personas jurídicas, en especial de gran tamaño, externalizan los servicios relacionados con las tecnologías de la información y la comunicación, situación que provoca que exista un intermediario entre el banco y el cliente respectivo (Zunzunegui Pastor, 2019). Dicha circunstancia puede generar dudas en torno a si y hasta qué punto puede imputársele responsabilidad penal al banco o a la institución financiera por la omisión de medidas de ciberseguridad (o por la existencia de casos de facilitación de medios) que pudieran culminar en la perpetración de un fraude informático, pero en las que ha incurrido un tercero comercialmente vinculado con ella.

En dicho ámbito, parece razonable aplicar los planteamientos, según los cuales, en materia de *outsourcing* o, en general, de la realización de negocios por cuenta de quien los contrata (actualmente expresamente previstos en el artículo tercero de la Ley 20.393), regiría un sistema mixto: «De entrada existe un deber de selección correcta (adecuación *ex ante* para realizar la tarea que se subcontrata) y, a partir de ahí, operatividad del principio de confianza (lo que significa: no operatividad del principio de desconfianza/no vigilancia)» (Silva, 2014: 190). Ese «deber de selección», en el supuesto que analizamos, debería llevar a exigir que los terceros en cuestión cuenten, a su vez,

con modelos tanto adecuados como efectivos de *compliance* penal, posibilidad que ha de ir unida a una verificación periódica de la implementación práctica de tales modelos.

## Conclusiones

Gracias a una interpretación restrictiva del tipo penal de facilitación de medios para la comisión de un fraude informático (artículo séptimo inciso final de la Ley 21.459) es posible diferenciar de forma certera entre la perpetración de dicho delito y otros supuestos que podrían confundirse con aquel. En particular, un entendimiento de dicha figura delictiva que se centre en la idea de realizar conductas activas orientadas específicamente a favorecer la perpetración de un fraude informático permite distinguir la perpetración de ese delito de la falta de un modelo adecuado y efectivo de compliance penal.

Para ello resulta decisivo esclarecer la naturaleza jurídica de este último instituto que, como es sabido, puede ser invocado como una eximente de responsabilidad en un juicio penal seguido en contra de una persona jurídica. De lo señalado se sigue que la falta de un modelo de *compliance* en los términos de la Ley 20.393 se circunscribe a la imposibilidad de alegar la referida eximente como defensa respecto de la imputación efectuada en contra de la persona jurídica. Dicho en otras palabras, la inexistencia de un modelo adecuado y efectivo de *compliance* penal no implica realizar el tipo penal de facilitación de medios para la comisión de un fraude informático, conclusión que en caso alguno supone restar importancia a la elaboración de un programa adecuado y efectivo de *compliance* al interior de la persona jurídica.

Junto con ello, en este contexto adquiere relevancia la punibilidad (o no) de hipótesis de omisión de acciones debidas, como podría ser el hecho de no contar con un modelo adecuado y efectivo de *compliance* penal o, vinculado con ese caso, de no contar con medidas de ciberseguridad orientadas a impedir la comisión de fraudes informáticos a través de o gracias a una determinada persona jurídica (paradigmáticamente un banco o una institución financiera). En relación con este asunto resulta cuestionable la punibilidad de casos de participación omisiva respecto de un fraude informático, mientras que la posibilidad de recurrir a la omisión impropia ha de ser descartada, al menos por ahora, fundamentalmente en atención a la inexistencia de normas legales habilitantes para esos efectos en el ordenamiento penal chileno.

## Referencias

Arevalo, Brenda (2015). *Money Mules: Facilitators of Financial Crime. An Explorative Research on Money Mules*. Tesis de maestría. Utrech: Universidad de Utrech.

Artaza Varela, Osvaldo (2013). «Sistemas de prevención de delitos o programas de cumplimiento. Breve descripción de las reglas técnicas de gestión del riesgo

empresarial y su utilidad en sede jurídico penal». *Política Criminal*, 8 (16): 544-573. DOI: 10.4067/S0718-33992013000200006.

Bacigalupo, Silvina (2021). «Compliance». *Eunomía Revista en Cultura de la Legalidad*, 21: 260-276. DOI: 10.20318/eunomia.2021.6348.

Baldomino Díaz, Raúl (2022). *Bases de la responsabilidad penal de las personas jurídicas*. Valencia: Tirant lo Blanch.

Ballester García, Javier (2019). «Capítulo 24. *Compliance* y las nuevas tecnologías. Ciberseguridad». En José Miguel Alcolea y Juana María Pardo (coordinadores), *Defensa corporativa y compliance* (pp. 589-606). Navarra: Thomson Reuters Aranzadi.

Balmaceda, Matías, Francisco Cox y Juan Ignacio Piña (2023). *Nuevo estatuto de los delitos económicos en Chile*. Santiago: BCP.

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

Bedecarratz, Francisco (2020). «Defecto de organización y reglas de comportamiento en la imputación de las personas jurídicas». *Política Criminal*, 15 (30): 694-728. DOI: 10.4067/S0718-33992020000200694.

Blanco Cordero, Isidoro (2023). «Responsabilidad penal de la persona jurídica extranjera por delitos cometidos en España». *Revista Electrónica de Ciencia Penal y Criminología*, 25-04: 1-32.

Bock, Dennis (2013). «*Compliance* und Aufsichtspflichten im Unternehmen». En Lothar Kuhlen y Hans Kudlich (editores), *Compliance und Strafrecht* (pp. 57-70). Heidelberg: C.F. Müller.

Boehler, Carolina y Juan Pablo Montiel (2021). «¿Cómo testear la adecuación de un programa de *compliance*? Introducción al "modelo de los tres filtros"». *Política Criminal*, 16 (31): 197-219. DOI: 10.4067/S0718-33992021000100197.

Bustos Cárdenas, Alejandra (2022). «Complicidad por omisión: Análisis doctrinal y propuesta». *Revista Chilena de Derecho y Ciencia Política*, 14 (1): 1-31. DOI: 10.7770/rchdcp-V14N1-art311.

Bustos Rubio, Miguel (2023). «La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal». *Revista de Internet, Derecho y Política*, 38: 1-11. DOI: 10.7238/idp.voi38.413222.

Cabrera Guirao, Jorge y Lautaro Contreras Chaimovich (2024). «Capítulo VII: El delito de fraude informático». En Samuel Malamud y Guillermo Chahuán (coordinadores), *Delitos informáticos. Análisis dogmático y comentarios a la Ley número 21.459* (pp. 205-231). Valencia: Tirant lo Blanch.

Fernández Teruelo, Javier (2011). *Derecho penal e internet*. Valladolid: Lex Nova.

García Cavero, Percy (2012). «Esbozo de un modelo de atribución de responsabilidad penal de las personas jurídicas». *Revista de Estudios de la Justicia*, 16: 55-74. DOI: 10.5354/rej.voi16.29493.

García Palominos, Gonzalo (2020). «Relevancia del elemento "interés o provecho" en la responsabilidad penal de las personas jurídicas en Chile». *Revista Chilena de Derecho*, 47 (3): 821-848. DOI: 10.7764/R.473.10.

Giniger, Nuria (2020). «Teletrabajo. Modalidad de trabajo en pandemia». *Revista Observatorio Latinoamericano y Caribeño*, 4 (1): 23-39.

Gómez Martín, Víctor (2020). «Delegación de competencias y *compliance* penal: Un estudio sobre la transferencia y transformación de los deberes (de vigilancia) en el derecho penal económico». *Derecho PUCP Revista de la Facultad de Derecho*, 85: 115-138. DOI: 10.18800/derechopucp.202001.004.

González Uriel, Daniel (2022). «La responsabilidad penal de las personas jurídicas y el delito de blanqueo de dinero en España». En Fiscalía General del Estado, *Responsabilidad penal de personas jurídicas: Una visión crítica en torno a sus fundamentos dogmáticos y praxis* (pp. 65-82). Quito: Fiscalía General del Estado.

Guidi, Caterina (2023). *Teletrabajo, trabajo a distancia y nuevas formas de organización. Actualizado con la Ley número 21.561*. Santiago: Der.

Gutiérrez Pérez, Elena (2015). «Los *compliance programs* como eximente o atenuante de la responsabilidad penal de las personas jurídicas. La "eficacia e idoneidad" como principios rectores tras la reforma de 2015». *Revista General de Derecho Penal*, 24: 1-24.

Haas, Volker (2011). «Die Beihilfe durch Unterlassen». *ZIS*, 5: 392-397.

Hernández Basualto, Héctor (2010). «La introducción de la responsabilidad penal de las personas jurídicas en Chile». *Política Criminal*, 5 (9): 207-236. DOI: 10.4067/S0718-33992010000100005.

—. (2011). «Artículo 16». En Jaime Couso y Héctor Hernández (directores), *Código Penal comentado. Parte general, doctrina y jurisprudencia* (pp. 413-415). Santiago: Abeledo Perrot.

—. (2018). «Procedencia de una "eximente o defensa de cumplimiento" de las personas jurídicas en el derecho administrativo sancionador chileno». *Revista Chilena de Derecho*, 45 (2): 427-451. DOI: 10.4067/S0718-34372018000200427.

—. (2024). «La esperada consagración de un genuino delito de fraude informático en el derecho penal chileno». En Christian Scheechler (editor), *Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley número 21.459* (pp. 207-237). Santiago: Der.

Hilgendorf, Eric y Brian Valerius (2012). *Computer und Internetstrafrecht*. 2.ª ed. Heidelberg: Springer.

Izquierdo Sánchez, Cristóbal (2016). *«Engaño» y silencio. Bases para un tratamiento unitario de la comisión activa y omisiva del delito de estafa*. Tesis doctoral. Barcelona: Universidad Pompeu Fabra.

Kemp, Steven (2023). «Exploring Public Cybercrime Prevention Campaigns and Victimization of Businesses: A Bayesian Model Averaging Approach». *Computer & Security*, 127: 1-14. DOI: 10.1016/j.cose.2022.103089.

Kindhäuser, Urs (2017). *Strafgesetzbuch. Lehr- und Praxiskommentar*. Baden-Baden: Nomos.

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

Lizama Portal, Luis y Diego Lizama Castro (2021). *El derecho del trabajo en las nuevas tecnologías*. Santiago: DER.

Mañalich, Juan Pablo (2014). «Omisión del garante e intervención delictiva. Una reconstrucción desde la teoría de las normas». *Revista de Derecho Universidad Católica del Norte*, 21 (2): 225-276. DOI: 10.4067/S0718-97532014000200007.

Marcazzolo, Ximena (2023). «Análisis del catálogo de sanciones contempladas en la Ley número 20.393 desde la autorregulación». En Raúl Carnevali (director), *Libro Homenaje al profesor Carlos Künsemüller Loebenfelder. Hacia un Derecho penal liberal* (pp. 383-402). Valencia: Tirant Lo Blanch.

Mata y Martín, Ricardo (2007). *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*. Cizur Menor: Thomson Reuters Aranzadi.

Mayer, Laura (2014). «El engaño concluyente en el delito de estafa». *Revista Chilena de Derecho*, 41 (3): 1017-1048. DOI: 10.4067/S0718-34372014000300010.

—. (2017). «El bien jurídico protegido en los delitos informáticos». *Revista Chilena de Derecho*, 44 (1): 235-260. DOI: 10.4067/S0718-34372017000100011.

—. (2018). «Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos». *Ius et Praxis*, 24 (1): 159-206. DOI: 10.4067/S0718-00122018000100159.

Mayer, Laura y Guillermo Oliver (2020). «El delito de fraude informático: Concepto y delimitación». *Revista Chilena de Derecho y Tecnología*, 9 (1): 151-184. DOI: 10.5354/0719-2584.2020.57149.

Mayer, Laura y Jaime Vera (2020). «*Criminal compliance* y defensa en el proceso penal: Una aproximación a la luz de la Ley número 20.393». En Ángela Toso Milos, Laura Mayer Lux y Eduardo Cordero (coordinadores), *Cumplimiento normativo y gestión de riesgos legales en la empresa* (pp. 129-162). Valencia: Tirant Lo Blanch.

—. (2024). *Delitos informáticos y cibercriminalidad: Aspectos sustantivos y procesales*. Montevideo y Buenos Aires: B de F.

Mayer, Laura y Jaime Vera (2024). «La facilitación de medios para la comisión de un fraude informático: ¿Un delito necesario?». En Javier Contesse S. y Guillermo Silva O. (coordinadores), *Racionalidad y escepticismo en el Derecho penal. Estudios en memoria de Miguel Soto Piñeiro* (pp. 775-796). Santiago: Thomson Reuters.

Mir Puig, Santiago (2016). *Derecho Penal. Parte General.* 10.ª ed. Barcelona: Reppertor.

Miró Llinares, Fernando (2013). «La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del *phishing*». *Revista Electrónica de Ciencia Penal y Criminología*, 15-12: 1-56. Disponible en: http://criminet.ugr.es/recpc/15/recpc15-12.pdf.

Montero Ulate, Betzaida, Kattia Lizzett Vasconcelos Vásquez y Gustavo Arias Murillo (2020). «Teletrabajo: Fortaleciendo el trabajo en tiempos de pandemia por Covid-19». *Revista de Comunicación y Salud*, 10 (2): 109-125. DOI: 10.35669/rcys.2020.10(2).109-125.

Morón Vera, Valeria (2021). *Las circunstancias modificativas de la responsabilidad penal de la persona jurídica ¿Puede la implementación de un modelo de prevención de delitos defectuoso aplicarse como una eximente incompleta de la responsabilidad penal de la persona jurídica?* Tesis de magíster. Lima: Pontifica Universidad Católica del Perú.

Náquira Bazán, Roberto (2020). «Artículo 11 número 1 del Código Penal: "Eximentes incompletas"». En Manuel Ángel González Jara (coordinador), *Circunstancias atenuantes y agravantes en el Código Penal chileno* (pp. 41-60). Santiago: Jurídicas de Santiago.

Navarro Dolmestch, Roberto (2022). «Configuración y apreciación de los requisitos de la legítima defensa». *Revista de Ciencias Penales*, XLVIII (2): 81-92.

Navas, Iván y Antonia Jaar (2018). «La responsabilidad penal de las personas jurídicas en la jurisprudencia chilena». *Política Criminal*, 13 (26): 1027-1054. DOI: 10.4067/S0718-33992018000201027.

Novoa Monreal, Eduardo (2015). *Curso de derecho penal chileno. Parte general. Tomo I*. 3.ª ed. Santiago: Jurídica de Chile.

—. (2019). *Curso de derecho penal chileno. Parte general. Tomo II*. Santiago: Jurídica de Chile.

Ontiveros Alonso, Miguel (2017). «*Compliance*, empresa y sistema penal (comentarios a las sentencias del Tribunal Supremo Español)». *Revista Eletrônica de Direito Penal e Política Criminal*, 5 (2): 30-39. DOI: 10.57042/rmcp.v1i1.5.

Ossandón Widow, María Magdalena (2018). «El legislador y el *principio ne bis in idem*». *Política Criminal*, 13 (26): 952-1002. DOI: 10.4067/S0718-33992018000200952.

Pickles, Rob (2021). «"Money Mules": Exploited Victims or Collaborators in Organised Crime?». *Irish Probation Journal*, 18: 231-243.

Politoff, Sergio, Jean Pierre Matus y María Cecilia Ramírez (2011). *Lecciones de derecho penal chileno. Parte especial*. Santiago: Jurídica de Chile.

Riquert, Marcelo (2017). «Las defraudaciones informáticas y los cibermuleros: entre la *willfulblindness*, el dolo eventual y la imprudencia». *Revista de Derecho Penal*, 25: 129-152.

—. (2020). «La responsabilidad penal de las personas jurídicas en Argentina y el "ciberconvenio" de Budapest». En Mariana Kieffer (coordinadora), *Cibercrimen II* (pp. 443-482). Montevideo y Buenos Aires: B de F.

Robles Planas, Ricardo (2006). «¿Delitos de personas jurídicas? A propósito de la ley austríaca de responsabilidad de las agrupaciones por hechos delictivos». *InDret*, 2: 1-25.

Salvo Ilabel, Nelly (2015). *Modelos de imputación penal a personas jurídicas: Estudio comparado de los sistemas español y chileno*. Tesis doctoral. Barcelona: Universidad Autónoma de Barcelona.

Silva Sánchez, Jesús María (2014). *Fundamentos del derecho penal de la empresa*. Montevideo y Buenos Aires: B de F.

Toso Milos, Ángela (2021). «El oficial de cumplimiento en el marco de un modelo integrado de *compliance* en las sociedades anónimas». *Revista de Derecho (Coquimbo)*, 28: 1-43. DOI: 10.22199/issn.0718-9753-2021-0007.

Turienzo Fernández, Alejandro (2022). «Consideraciones acerca de la responsabilidad penal por omisión de los socios en relación con la criminalidad corporativa». *Estudios Penales y Criminológicos*, 42: 1-44.

Valenzano, Anna y Diva Serra Cruz (2019). «El "defecto de organización" en la estructura de imputación de responsabilidad a la persona jurídica por la comisión de delito. Especial referencia a los sistemas chileno, peruano y argentino». *Revista de Derecho Penal y Criminología*, IX (6): 28-62.

—. (2021). «El control de las reglas de prevención de delitos en los sistemas chileno, peruano y argentino ¿en la órbita del *compliance officer* estadounidense o del organismo *di vigilanza* italiano?». *La Ley: Compliance Penal*, 4: 1-58.

Van Weezel, Alex (2023). *Curso de derecho penal. Parte General*. Santiago: Pontificia Universidad Católica de Chile.

Vargas Pinto, Tatiana (2013). *Manual de Derecho Penal Práctico*. 3.ª ed. Santiago: Thomson Reuters.

Vargas, María Alejandra y José Agustina (2021). «Capítulo III: Obtención de evidencias digitales y privacidad en el correo electrónico en el marco de investigaciones internas». En Miquel Fortuny (director), *Las investigaciones internas en compliance penal. Factores clave para su eficacia* (pp. 95-137). Cizur Menor: Thomson Reuters Aranzadi.

Vásquez Palma, María Fernanda (2012). «Gobiernos corporativos y deberes de los administradores de las sociedades anónimas: Cuestiones actuales (desde la Ley 20.382) y reformas pendientes». *Cuadernos de Extensión Jurídica* (Universidad de Los Andes), 22: 173-205.

Vinelli, Renzo (2021). «Los delitos informáticos y su relación con la criminalidad económica». *Ius et Praxis Revista de la Facultad de Derecho*, 53: 95-110. DOI: 10.26439/iusetpraxis2021.n053.4995.

Zunzunegui Pastor, Fernando (2019). «Capítulo 3: Open Banking». En Fernando Zunzunegui (director), *Regulación financiera y fintech* (pp. 59-90). Cizur Menor: Thomson Reuters Aranzadi.

## Financiamiento

Este trabajo ha sido redactado en el marco del Proyecto Fondecyt Regular 1230509.

## Sobre las autoras

Laura Mayer Lux es abogada. Es licenciada en ciencias jurídicas por la Pontificia Universidad Católica de Valparaíso, Chile, y doctora en derecho por la Universidad de Bonn, Alemania. Es profesora de derecho penal en la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es laura.mayer@pucv.cl. https://orcid.org/0009-0008-0136-5294.

Angela Toso Milos es abogada. Es licenciada en ciencias jurídicas y sociales por la Universidad Diego Portales, Chile, y doctora en derecho por la Universidad de Salamanca, España. Es profesora de derecho comercial en la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es angela.toso@pucv.cl. https://orcid.org/0000-0001-5271-3158.