REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 14 (2025) • e74317 • DOI 10.5354/0719-2584.2025.74317
RECIBIDO: 6/4/2024 • APROBADO: 27/10/2025 • PUBLICADO: 31/12/2025

DOCTRINA

La responsabilidad penal de las personas jurídicas por los delitos informáticos

Criminal liability of legal entities for cybercrime

Francisco Javier Bedecarratz Scholz
Universidad Autónoma de Chile

RESUMEN Este artículo analiza la responsabilidad penal de las personas jurídicas en Chile respecto a los delitos informáticos y sus implicancias, considerando el cambio de paradigma introducido por reformas recientes: las entidades ya no se conciben solo como víctimas, sino también como potenciales responsables. Se examinan los desafíos del sistema de imputación penal previsto en la Ley 20393 y la necesidad de un modelo de prevención efectivo, que contemple la identificación de riesgos, medidas preventivas y una cultura organizacional ética. Además, se enfatiza la necesidad de adaptar los modelos de prevención a las dinámicas contemporáneas de la ciberdelincuencia, poniendo el foco en la importancia de una evaluación continua y de actualizaciones periódicas como condición para una gobernanza eficaz del riesgo cibernético.

PALABRAS CLAVE Cumplimiento normativo, ciberseguridad, delitos informáticos, cibercrimen, incumbencia.

ABSTRACT This article analyzes the criminal liability of legal persons in Chile for cybercrimes and its implications, particularly in light of the paradigm shift brought about by recent legal reforms: legal persons are no longer regarded solely as victims, but also as potentially responsible for cybercrime offences. In this context, the article examines the challenges faced by the imputation framework established under Chile's Law No. 20393 and the need for an effective crime prevention and compliance programme that includes risk identification, preventive measures, and an ethical organizational culture. Furthermore, it emphasizes the need to adapt prevention models to the contemporary dynamics of cybercrime, focusing on the importance of ongoing assessment and regular updates as a condition for effective cyber-risk governance.

KEYWORDS Compliance, cybersecurity, computer crimes, cybercrime, incumbency.

Introducción

La Ley 21459, publicada el 20 de junio de 2022, constituye el principal cuerpo normativo en Chile consagrado a la tipificación y sanción de los delitos informáticos. Junto con introducir ocho nuevas figuras delictivas, concebidas en conformidad con el modelo dispuesto por el Convenio sobre la Ciberdelincuencia de 2001 —también denominado Convenio de Budapest—, la ley establece en su artículo 21 un importante cambio respecto de los posibles sujetos activos. Además de las personas naturales, también las jurídicas pueden ser penalmente responsables por la comisión de alguno de estos hechos punibles. Esta modificación cambia diametralmente la situación procesal de sociedades, fundaciones, corporaciones y demás entidades: han pasado de ser consideradas —tradicionalmente, al menos— víctimas de accesos ilícitos, fraudes informáticos o ataques a la integridad de sistemas, a ser sus potenciales responsables. Dicho cambio generó, a lo menos, dos fenómenos relevantes desde una perspectiva normativa y criminológica. En primer lugar, la atribución de responsabilidad penal a una persona jurídica por la comisión de un delito informático al interior de sus estructuras repercute en un conjunto de problemas respecto de los requisitos del modelo de imputación. Tales han experimentado una evolución a partir de la dictación de la Ley 21595 de Delitos Económicos, que reformó el corazón del artículo 3 de la Ley 20393 sobre responsabilidad penal de las personas jurídicas. En segundo lugar, no existe claridad respecto de los riesgos jurídico-penales en materia de criminalidad informática que emanan de organizaciones, ni de las medidas preventivas respectivas. Hasta ahora, el enfoque estaba puesto en que la entidad no fuera víctima de un delito informático, mas no que al interior de esta también pudieran cometerse dichos ilícitos. Considerando lo anterior, es indispensable identificar los riesgos más relevantes de delitos informáticos que le incumben a las personas jurídicas, con el fin de que estas puedan diseñar modelos internos de organización adecuados para prevenirlos.

Este trabajo aborda los dos problemas antes mencionados, con el fin de facilitar la aplicación de la Ley 21459 en la imputación de delitos informáticos a personas jurídicas. Para ello se describe, en primer lugar, el contexto y los antecedentes de la introducción de la responsabilidad penal organizacional en el derecho penal chileno. Acto seguido se revisan los principales perfiles de ciberdelincuentes y su incidencia en el contexto organizacional. A partir de lo anterior, se identifican y analizan los problemas que enfrenta el modelo de responsabilidad penal previsto en el artículo 3 de la Ley 20393 en la imputación de delitos informáticos, lo cual se analiza desde la perspectiva de sus requisitos de imputación. El análisis finaliza con algunas consideraciones para tener en cuenta al momento de determinar las medidas preventivas idóneas a ser implementadas mediante el modelo de prevención de delitos consagrado en el artículo 4 de la Ley 20393.

Antecedentes normativos y político-criminales

La incorporación de las personas jurídicas como posibles sujetos activos de un delito informático en el ordenamiento jurídico chileno tiene su fuente en el texto del Convenio sobre la Ciberdelincuencia del Consejo de Europa. En su artículo 12 se establece que los Estados signatarios deberán adoptar las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos allí descritos.[1] Esta última norma es fruto de la tradición jurídica de la Unión Europea, que ha propendido a la introducción de la responsabilidad penal de las personas jurídicas en distintas áreas. Es frecuente encontrar su símil en otros tratados multilaterales de la época como, por ejemplo, el artículo 14 del «*Corpus iuris* para la protección penal de los intereses financieros de la Unión Europea» (1997) (Silva Sánchez, 2002: 116-117).[2]

Los fundamentos para la implementación de un régimen de responsabilidad penal de las personas jurídicas en el ámbito de los delitos informáticos estriban en la necesidad de enfrentar los desafíos que presenta esta clase de criminalidad, emanada desde —o facilitada por— estructuras corporativas. Tradicionalmente se ha argumentado que el derecho penal individual sería, por sí solo, insuficiente para sancionar formas complejas de criminalidad emanadas desde corporaciones, motivo por el cual debe ser complementado mediante un sistema de responsabilidad organizacional capaz de sancionar el injusto generado en dicho entorno (Fisse y Braithwaite, 1993: 2 y ss.; Nieto Martín, 2008a: 48 y ss.; Artaza Varela, 2013a: 45 y ss.; De la Cuesta Arzamendi y Pérez Machío, 2013: 53; Heine, 1995: 53 y ss.). Luego, la naturaleza, complejidad y el alcance de los delitos informáticos, caracterizados por su capacidad de ser cometidos a gran escala y más allá de fronteras nacionales (Mayer Lux, 2018: 165), hace necesaria la adopción de un sistema de responsabilidad organizacional capaz de hacer frente a este tipo de criminalidad.

Por otra parte, la estructura interna de una persona jurídica puede jugar un rol fundamental en la facilitación de estos delitos. Una persona jurídica representa una concentración de individuos, medios e infraestructuras que pueden ser aprovechadas

1. El Convenio sobre la Ciberdelincuencia no exige una responsabilidad estrictamente penal, pues dicha obligación puede satisfacerse también por una vía civil o una administrativa. Destacan este aspecto Riveros Saavedra (2023: 318); Mayer Lux y Vera Vega (2023: 148-149); y Silva Sánchez (2002: 122); entre otros. Pese a lo anterior, el legislador chileno optó por exigir una de naturaleza criminal, integrando tales delitos al catálogo de la Ley 20393.

2. Respecto del combate contra el cohecho y el lavado de activos vinculados a la protección de los intereses financieros de las Comunidades Europeas, el instrumento que ha tenido mayor alcance es el Segundo Protocolo al «Convenio relativo a la protección de los intereses financieros de las Comunidades Europeas», establecido sobre la base del artículo K.3 del Tratado de la Unión Europea o Tratado de Maastricht, del 19 de junio de 1997 (Bedecarratz Scholz, 2016: 184-191).

para realizar delitos informáticos con mayor eficacia en contra de personas y organizaciones. Lo anterior se enlaza con el hecho de que las estructuras corporativas pueden ser utilizadas no solo para la facilitación de delitos informáticos, sino también para ocultar la identidad de los verdaderos autores, diluyendo la responsabilidad individual dentro de la organización. Tal es el fenómeno de la «irresponsabilidad organizada» (Schünemann, 1979: 34), traducida en la segmentación de responsabilidades y descentralización de toma de decisiones, lo que dificulta la atribución de culpabilidad a individuos específicos.[3]

En respuesta a lo anterior, la amenaza de sanción penal en contra de las personas jurídicas no solo genera un efecto disuasivo o de *deterrence* (Fisse, 1978: 370; Artaza Varela, 2013a: 52 y ss.), sino que también busca incentivar a las empresas a autorregularse, promoviendo la creación y mantenimiento de una cultura organizacional que limite la comisión de conductas delictivas en su seno (Nieto Martín, 2008a: 81 y ss.; Feijoo Sánchez, 2016: 20 y ss.; Engelhart, 2012: 83; Artaza Varela, 2013a: 55 y ss.), priorice el cumplimiento con el derecho (Gómez-Jara Díez, 2005: 272)[4] y, en este contexto delictivo, fomente el respeto por los derechos de los usuarios en el entorno digital. En este sentido, las conductas constitutivas de delitos informáticos incumben a las personas jurídicas en tanto corresponden a una especial fuente de riesgo delictivo organizacional, lo cual se encuentra influenciado por el fenómeno de digitalización general de la gestión empresarial, así como por las características particulares de la persona jurídica respectiva, cuestiones que darán origen a perfiles de riesgo específicos según el caso (Mayer Lux y Vera Vega, 2023: 151 y ss.).

En este contexto, la amenaza de sanción tiene por objeto fomentar la denominada «autorregulación regulada» (Fisse y Braithwaite, 1993: 2 y ss.; Nieto Martín, 2008a: 48), la que se traduce en la implementación de medidas preventivas dentro de la organización que, a su vez, generan las condiciones para descubrir a delincuentes individuales de manera más eficiente y esclarecer los hechos con mayor rapidez. Así, se busca incentivar a la entidad para que diseñe e implemente sistemas de control y medidas preventivas que puedan prevenir delitos de manera anticipada, o simplificar el trabajo de los órganos estatales en la investigación de delitos de manera posterior (Nieto Martín, 2008a: 49-50). En este contexto, las empresas intentan establecer una mejor política corporativa mediante la implementación de sistemas de prevención,

3. La controversia sobre la división del trabajo al interior de una empresa y sus efectos a nivel de imputación penal se tematiza en Heine (1995: 34 y ss.). Sobre el fenómeno de la dilución de responsabilidades, véase Nieto Martín (2008a: 39).

4. Para más información respecto a los fundamentos de la estrategia, véase Bedecarratz Scholz (2020: 696 y ss.). Para el trasfondo político-jurídico de la misma, véase Silva Sánchez (2016: 677 y ss.) y Gómez-Jara Díez (2016: 95), entre otros.

con la esperanza de beneficiarse de una reducción de la pena o incluso de una exención total en el marco de un posible proceso penal.

Concordantemente, la implementación de la responsabilidad penal para personas jurídicas en el contexto de los delitos informáticos refleja un enfoque ajustado a la era digital, donde la capacidad de las entidades corporativas para influir en el ciberespacio, tanto positiva como negativamente, tiene su correlato en la imposición de obligaciones legales específicas destinadas a asegurar un entorno digital seguro para todos los usuarios.[5] Sin embargo, el logro de estos propósitos político-criminales, relativos a sancionar la criminalidad organizacional e impulsar modelos internos de organización y gestión que limiten su surgimiento, están condicionados por los aspectos fenomenológicos relativos a los perfiles de la cibercriminalidad expuestos a continuación.

Perfiles de ciberdelincuentes y personas jurídicas

La incidencia práctica de la responsabilidad penal de las personas jurídicas por delitos informáticos depende directamente del hecho relativo a si esta clase de conductas pueden ser cometidas por o a través de asociaciones de personas. Por lo mismo, es pertinente esclarecer si los perfiles de autor vigentes en el presente contexto engloban de forma significativa a este tipo de entidades.

La evolución tecnológica de las últimas décadas ha repercutido en una diversificación no solo de las tipologías de los delitos informáticos previstos en la ley, sino que también del perfil de los sujetos que pueden llevarlos a cabo. La doctrina concuerda en que no existe un perfil único o estático de ciberdelincuente, sino que existen múltiples (Mayer Lux y Vera Vega, 2023: 47; Miró Llinares, 2012: 229), los cuales pueden ser diferenciados en atención a distintos criterios. En este sentido, aún se reconoce la existencia de una categoría genérica que incluye a individuos con conocimientos informáticos avanzados que realizan conductas ilícitas en el ciberespacio. Sin perjuicio de lo anterior, también existen ciertas especialidades a partir de la modalidad del delito, particularmente cuando se persiguen fines políticos o se actúa motivado por el lucro (Miró Llinares, 2012: 232 y ss.).[6]

5. El sinalagma libertad-responsabilidad al cual están sujetas las empresas constituye uno de los fundamentos más extendidos para la introducción de la responsabilidad penal organizacional (Hernández Basualto, 2010: 219; Artaza Varela, 2013b: 547; Nieto Martín, 2008a: 51; 2008b: 14; Dopico Gómez-Aller, 2014: 341; Gómez-Jara Díez, 2005: 278 y ss.).

6. Los subgrupos de hackers citados a continuación provienen de las taxonomías sistematizadas por McQuade (2006), así como por Sabillon y otros (2016).

Cibercriminalidad tradicional

Históricamente, el perfil tradicional del ciberdelincuente se ha identificado con el del hacker popularizado en la literatura e industria cinematográfica: sujetos jóvenes, socialmente aislados, altamente competentes en tecnologías de la información y comunicación y que buscan superar barreras o desafíos por el mero hecho de su existencia.[7] Las motivaciones de estas personas para realizar las conductas típicas pueden radicar en fines reputacionales, altruistas o bien consistir en la búsqueda de beneficio económico individual. La atribución de un carácter ilícito al hackeo ha sido disputada desde antiguo por sus adeptos y ha motivado una distinción conceptual originada en los años setenta: por una parte, están los hackers propiamente tales, esto es, expertos informáticos con capacidad de explorar los límites de sistemas informáticos para ampliar sus capacidades;[8] y por otra están los *crackers*, es decir, aquellos que usan sus habilidades informáticas para fines maliciosos.

Según estos parámetros, es perfectamente posible que el perfil de autor descrito opere bajo el alero de una persona jurídica. Sin embargo, ello constituiría una circunstancia accidental, pues no existe obstáculo para que este tipo de criminal informático ejecute las conductas típicas en solitario. No resulta imprescindible que los delitos informáticos sean llevados a cabo por sujetos activos con grandes medios económicos a su disposición (Mayer Lux y Vera Vega, 2023: 56). Por ejemplo, la ejecución de grandes ciberataques puede ser precedida de la creación de *botnets*, esto es, la unión de numerosos sistemas informáticos, generalmente a través de una infección deliberada con programas maliciosos o *malware*, con el objetivo de usar posteriormente esa capacidad de procesamiento multiplicada para realizar ataques coordinados, como una denegación de servicio distribuido (Haase, 2015: 149; Van der Wagen y Pieters, 2015: 580 y ss.). Para ejecutar dicha acción no son imprescindibles recursos económicos extraordinarios, sino que solo un computador con conexión a internet, el conocimiento del *modus operandi* del ataque y de las vulnerabilidades pertinentes a explotar. En este contexto, el avance tecnológico actual (Navarro Dolmestch, 2023: 666-667) ha puesto medios a disposición de la delincuencia informática, que en la vasta mayoría de los casos hacen innecesario contar con recursos empresariales para su ejecución.

Sin perjuicio de lo anterior, la delincuencia informática común o individual ha experimentado en los últimos años un fenómeno de estructuración a partir del cual

7. Según Cámara Arroyo (2020: 484), se trataría de una criminalidad joven, masculina y con cierto grado de conocimientos o educación. Estudios realizados durante el imperio de la antigua Ley 19223 confirmarían el perfil de una delincuencia joven y altamente digitalizada (López Medel, 2002: 408).

8. La obra clásica de Levy (1984) es expresión de esta perspectiva cuasirromántica de hackeo. Para el concepto de *hacking* ético y su diferenciación respecto de otras subespecies puede consultarse Bedecarratz Scholz (2023: 115 y ss.).

se han conformado grupos delictivos que operan coordinadamente para cometer delitos informáticos de modo sistemático.[9] Esta ha evolucionado a formas más complejas según el modelo del «crimen como servicio» —*crime as a service*—, que facilita el comercio ilícito y la entrega de herramientas maliciosas o bien explota la automatización y los *botnets* para ataques a gran escala. La estructura de estas redes criminales no se ajusta a los modelos tradicionales jerárquicos de criminalidad organizada, pues ponen un énfasis en redes flexibles de personas con habilidades complementarias que operan en el ciberespacio a partir de distintos lugares geográficos (Tropina, 2012: 158 y ss.; Miró Llinares, 2012: 236).[10]

Dicho esto, las características inherentes de la criminalidad informática general exhiben rasgos que no se adecúan al contexto empresarial. Como se ha descrito, esta suele ser ejecutada por individuos que actúan de manera independiente o en redes flexibles, explotando las oportunidades que brinda el ciberespacio sin necesidad de recursos significativos. En contraste, la criminalidad corporativa se manifiesta en conductas cometidas en nombre o a beneficio de una persona jurídica, lo que implica una estructura organizacional y recursos económicos más robustos. Siguiendo la teoría de los «sistemas de injusto constituido» (Lampe, 1994: 695; Mañalich Raffo, 2011: 283 y ss.; Bedecarratz Scholz, 2022: 247 y ss.), que sugiere que los tipos de injusto deben analizarse en función de los sistemas dentro de los cuales estos surgen, la criminalidad informática general se vincula a un sistema diferente a la criminalidad empresarial: mientras que la primera emerge de un sistema más difuso y descentralizado, la segunda se desenvuelve dentro de un sistema organizacional económico, con actividades y objetivos corporativos estables. En este sentido, este tipo de organizaciones materializan un injusto sistémico propio, equivalente a sistemas orientados criminalmente, mas no a sistemas propensos criminalmente, los cuales son el verdadero objeto de la Ley 20393. Consecuentemente, esta forma de agrupación de personas es por esencia ilegítima y sancionada a través de los delitos de asociación delictiva o criminal, según sea el caso, quedando fuera del campo de aplicación de dicha ley.

Cibercriminalidad económica

A partir de la categoría general comúnmente asociada a la cibercriminalidad es posible observar una especialización relevante desde una perspectiva económica. Este perfil abarca a personas que realizan ataques con ánimo de obtener una ganancia pa-

9. Ello puede evidenciarse, por ejemplo, a través de las bandas organizadas que recolectan credenciales de acceso a través de campañas de *phishing* o *pharming*, como se detalla en Oxman Vilches (2013: 243).

10. Para más información al respecto, véase Timothy Quintero, «Mercados negros conectados: Cómo la web oscura ha potenciado el crimen organizado en Latinoamérica», *InSight Crime*, 12 de septiembre de 2017, disponible en https://tipg.link/m8Vi.

trimonial directa o indirecta a partir del hecho. La doctrina ha considerado que este constituye el grupo más relevante en la práctica, manifestándose en la mayoría de los crímenes en el ciberespacio una preeminencia del móvil de lucro por sobre otras motivaciones (Mayer Lux y Vera Vega, 2023: 48; Miró Llinares, 2012: 237).

Esta clase de cibercriminalidad puede englobar una amplia gama de actividades y fenómenos ilícitos. Tales pueden incluir, entre otros, a fraudes informáticos,[11] compromisos de correos electrónicos empresariales,[12] establecimiento de mercados en línea ilegales,[13] el «hurto o robo» de identidad digital,[14] o bien la «ciberextorsión», es decir, la práctica de exigir pagos a las víctimas bajo la amenaza de infligir daños en sus datos y sistemas computacionales. Entre estos últimos destacan los ataques del tipo *ransomware*, esto es, la infección del sistema objetivo a través de un software malicioso que lo secuestra y encripta los datos contenidos en este (Sabillon y otros, 2016: 6) con el fin de exigir un rescate, normalmente en Bitcoin u otra moneda virtual, bajo amenaza de eliminarlos definitivamente si no es pagado. Como ya se indicó, este tipo de actividades tienen por objeto adquirir de manera ilegítima dinero, recursos o información financiera sensible de individuos, organizaciones o incluso instituciones públicas.

Como se puede observar, este perfil abarca un rango de acciones que van desde el fraude individual a la cibercriminalidad organizada. Si bien la cibercriminalidad económica está tradicionalmente asociada a individuos y organizaciones delictivas de pequeño tamaño, es posible observar una creciente preocupación acerca del involucramiento de personas jurídicas en la comisión de —o contribución a— este tipo de actividades, también de forma indirecta a causa de controles internos inadecua-

11. Entiéndase por tal la «producción de un perjuicio patrimonial ajeno mediante una alteración o manipulación de datos o programas de sistemas informáticos» (Mayer Lux y Vera Vega, 2023: 268).

12. El compromiso del correo electrónico empresarial es un tipo sofisticado de estafa, que apunta a las empresas que realizan transferencias bancarias a sus proveedores. Este fraude implica que los ciberdelincuentes comprometen cuentas legítimas de correo electrónico empresarial mediante técnicas de ingeniería social o intrusiones informáticas, para llevar a cabo transferencias de fondos no autorizadas a cuentas distintas de su verdadero destinatario. Para una descripción del *modus operandi* y sus variantes, véase Cross y Gillett (2020: 871 y ss.).

13. Tales se entienden como una infraestructura sociomaterial ubicada en el ciberespacio que hace posible las transacciones ilícitas de mercado, como la compraventa de software malicioso, claves y credenciales de acceso de terceros, datos bancarios y de tarjetas de crédito, documentos oficiales reservados, entre otras. Para más información respecto a una propuesta de tipología, véase Wehinger (2011: 209 y ss.). Ejemplo paradigmático de un *marketplace* ilegal en el ciberespacio es la extinta SilkRoad (Werbach, 2018: 493 y ss.).

14. Ello implica la obtención fraudulenta de datos personales e identificadores en línea de usuarios, con el fin de sustituirlos ante instituciones comúnmente bancarias, lo cual se encuentra estrechamente vinculado al concepto de *phishing* u obtención de datos personales. Sobre el nexo entre fraude informático, *phishing* y hurto de identidad, véase Mayer Lux y Oliver Calderón (2020: 157).

dos. Como han identificado Mayer Lux y Toso Milos, las personas jurídicas pueden facilitar los medios para cometer actividades delictivas en el ciberespacio al omitir la implementación de medidas mínimas de ciberseguridad (2024: 5 y ss.). Ello puede convertirlas en plataformas para la ejecución de ataques a terceros por parte de actores maliciosos y trabajadores descontentos o en búsqueda de represalias.

Una clase de conductas delictivas relevantes cometidas por personas jurídicas en el ciberespacio está constituida por el espionaje informático, así como por los delitos contra la propiedad intelectual. El espionaje informático no posee un concepto unívoco, dado que se vincula con distintos comportamientos y figuras punibles en el ordenamiento jurídico chileno (Mayer Lux y Vera Vega, 2020: 224 y ss.). En el contexto empresarial, sin embargo, dice relación con conductas que impliquen acceder a informaciones secretas de un competidor por medios ilícitos, normalmente con el fin de adquirir ventajas competitivas, obtener una ganancia patrimonial o evitar una pérdida. Las modalidades comisivas pueden ser diversas y traducirse, por ejemplo, en un acceso ilícito a sistemas informáticos para apoderarse, usar o conocer información (artículo 2 inciso segundo de la Ley 21459); la interceptación ilícita de transmisiones secretas (artículo 3 de la Ley 21459); o bien la instalación de un software malicioso (por ejemplo, troyanos) para recopilar datos de la víctima (Fernández Díaz, 2018: 28 y ss.). Esta clase de conductas puede ser un antecedente útil o necesario para la realización de otros delitos contra la propiedad intelectual, como los previstos en el artículo 79 letras a) y b) de la Ley 17336,[15] o en el artículo 52 de la Ley 19039,[16] presentándose una situación de concurso medial entre el delito informático con respecto al ilícito contra la propiedad intelectual e industrial (Mayer Lux y Vera Vega, 2020: 237-238).

Aunque no toda «información» se encuentra protegida automáticamente por los derechos de autor o de patente, la información estratégica para las operaciones comerciales de las empresas —como las listas de clientes, modelos de financiación, estudios de mercado o datos contables— constituye un activo especialmente sensible. La concentración de estos contenidos en servidores corporativos incrementa su

15. Estas figuras sancionan el uso de obras ajenas en los siguientes términos: «a) El que, sin estar expresamente facultado para ello, utilice obras de dominio ajeno protegidas por esta ley, inéditas o publicadas, en cualquiera de las formas o por cualquiera de los medios establecidos en el artículo 18.

b) El que, sin estar expresamente facultado para ello, utilice las interpretaciones, producciones y emisiones protegidas de los titulares de los derechos conexos, con cualquiera de los fines o por cualquiera de los medios establecidos en el Título II».

16. El artículo 52 de la Ley 19039 establece la imposición de multas de entre veinticinco y mil unidades tributarias mensuales a quienes incurran en violaciones de derechos de propiedad industrial relacionadas con patentes. Esto incluye la fabricación, uso, oferta, comercio, importación o posesión maliciosa de un invento patentado con fines comerciales, así como el uso comercial de un objeto no patentado o cuya patente haya expirado o sido anulada, pretendiendo que está patentado. También sanciona el uso comercial malicioso de un procedimiento patentado y la imitación o uso de un invento con patente en trámite.

atractivo para quienes buscan obtener ventajas competitivas mediante el espionaje informático, ya sea a través de accesos ilícitos, interceptaciones o diversas modalidades de intrusión digital.

No es posible estimar con precisión la incidencia real del espionaje informático en contexto organizacional. Ello se debe, en parte, al carácter insidioso de este tipo de operaciones, que repercute en una «cifra negra» insospechada, y también a que muchos de estos casos se resuelven mediante transacciones extrajudiciales que los sustraen del escrutinio público. Sin embargo, en el contexto nacional y comparado han existido diversos casos de espionaje corporativo que evidencian su creciente prevalencia en contextos organizacionales y empresariales.[17]

Otro caso relevante en este contexto está constituido por el delito de receptación de datos del artículo 6 de la Ley 21459, figura concebida con el objeto de penalizar la posesión o tráfico de bases de datos obtenidas ilícitamente mediante accesos (artículo 2) o interceptaciones ilícitas (artículo 3), así como generada a través de falsificaciones informáticas (artículo 5) (Bascur Retamal y Peña Sepúlveda, 2022: 27; Gutiérrez Peña, 2023: 198). En este sentido, el almacenamiento de datos informáticos con origen incierto puede constituir una importante fuente de riesgos para las empresas (Mayer Lux y Vera Vega, 2023: 153), sobre todo cuando el uso de estos no tenga un objeto totalmente lícito y pueda generar beneficios económicos significativos para la entidad. En específico, aquellos sectores económicos basados en el uso y almacenamiento intensivo de datos, como los servicios financieros, la atención sanitaria, la tecnología y el comercio electrónico, están particularmente expuestos y corren el mayor riesgo de incurrir en un tratamiento de bases de datos provenientes de fuentes ilícitas.[18]

Por otra parte, esta figura punible también presenta un riesgo para la actividad periodística desarrollada por agencias de prensa, en la que se recurre como fuente a bases de datos que, al mismo tiempo, pueden haber tenido su origen en accesos no

17. Por ejemplo, la intercepción de transmisiones satelitales de la empresa alemana Siemens por una empresa francesa, respecto de un contrato relacionado a un tren de alta velocidad en Corea del Sur, intercepción que permitió a la empresa atacante conocer los precios de oferta y proponer uno más bajo (Oxman Vilches, 2013: 233). En el ámbito nacional, se han registrado varios casos de espionaje informático corporativo que, a la fecha de publicación de este trabajo, no han culminado en sentencias en el marco de la Ley 20393. Para más información al respecto, véase Ulrich Sieber (1998), «Legal aspects of computer-related crime in the information society – COMCRIME Study», *European Commission*, disponible en https://tipg.link/m8Wo.

18. Cabe tener presente que el artículo 6 de la Ley 21459 exige un elemento subjetivo especial, consistente en la intención de usar los datos para cualquier «fin ilícito». Esto se refiere a todo acto futuro contrario a derecho, que involucre la gestión de los datos, incluyendo a objetivos no exclusivamente constitutivos de una infracción penal, sino portadores de ilicitud bajo otros sectores del ordenamiento jurídico (Bascur Retamal y Peña Sepúlveda, 2022: 28).

autorizados o interceptaciones.[19] En los hechos, organizaciones enfocadas en el periodismo investigativo trabajan frecuentemente con filtraciones o *leaks*, es decir, con material obtenido al margen de la ley por informantes o *whistleblowers*, que luego es utilizado para exponer problemas sociales o políticos sensibles. En tanto dicho material provenga de accesos o interceptaciones ilícitas, la persona jurídica respectiva se expone a verse envuelta en querellas fundamentadas en el tipo penal de la receptación informática.[20]

Ahora bien, la probabilidad efectiva de que una empresa caiga en esta clase de conductas depende en gran medida de los estándares de gobierno corporativo que imperen en su seno, así como de los lineamientos éticos y las prácticas de manejo del riesgo implementadas. Si bien es cierto que la abrumadora mayoría de las personas jurídicas buscan operar legal y éticamente en el ámbito de sus actividades negociales, las presiones competitivas, la necesidad de mantenerse a flote frente a una estructura de costos en constante aumento y, en algunos casos, la falta de supervisión y control interno, pueden tener como resultado acciones constitutivas de delito por parte de sus directivos o trabajadores.

Sin perjuicio de lo anterior, cabe tener presente que una gran parte de los delitos informáticos cometidos al interior de una empresa tienen como protagonistas a los denominados *insiders*: sujetos ligados a una empresa y que por distintas razones son autores o partícipes de un delito informático cometido en contra de la misma institución a la cual pertenecen o con la que se encuentran vinculados contractualmente (Mayer Lux, 2018: 187; Miró Llinares, 2012: 238). La incidencia de esta modalidad de conducta tiene su origen en las relaciones de confianza entre el hechor y la organización, relaciones que dan origen a una serie de accesos y privilegios de usuario que son aprovechados para cometer las conductas típicas como, por ejemplo, accesos ilícitos o delitos contra la propiedad intelectual. Sin embargo, esta clase de criminalidad queda completamente fuera del campo de acción de la responsabilidad penal de la persona jurídica, pues el *insider* realiza hechos en contra de los intereses de la

19. La materia fue intensamente discutida en Alemania con la introducción del tipo penal de *Datenehlerei* —o receptación de datos— en el § 202d inciso primero del Código Penal alemán, en donde se criticaron no solo los errores de técnica legislativa, sino también el considerable riesgo que el delito representa para las libertades de prensa e información (Singelnstein, 2016: 432 y ss.; Tassi, 2017: 745 y ss.).

20. La problemática incluso fue objeto de una sentencia del Tribunal Constitucional Federal alemán, en la que se dejó exento del tipo penal al periodismo investigativo (al respecto, véase el auto del Tribunal Constitucional Federal alemán, dictado el 30 de marzo de 2022 por la Segunda Sala del Primer Senado, en el recurso constitucional número 1 BvR 2821/16, específicamente los párrafos 1 a 29). Si bien en Chile el elemento subjetivo especial del tipo presenta un resguardo frente a querellas infundadas y, en último término, podría ser aplicable la eximente del artículo 10 número 10 del Código Penal relativa al ejercicio legítimo del oficio (periodístico), el análisis de esta problemática, aunque interesante, escapa al objeto de estas líneas.

organización a la cual pertenece o perteneció, lo cual verifica el criterio de exclusión previsto en el artículo 3 inciso final de la Ley 20393.

Cibercriminalidad política

La categoría de cibercriminalidad política engloba la comisión de delitos informáticos realizados con el fin de lograr objetivos políticos, influenciar la opinión pública, perturbar procesos electorales o adquirir acceso a información pública reservada o secreta. A diferencia de las demás clasificaciones, que normalmente se encuentran motivadas por un ánimo de lucro o reputacional, la cibercriminalidad política está impulsada por fines ideológicos u orientados a acrecentar el poder o desestabilizar instituciones públicas. Esta puede ser caracterizada según el destinatario de las conductas y el objetivo ulterior perseguido a través de ellas. Así, las principales víctimas son instituciones gubernamentales, figuras políticas e infraestructura crítica para la seguridad nacional. Además, este tipo de conductas buscan influenciar decisiones políticas, minar la confianza de la ciudadanía —o de una parte de ella— en instituciones gubernamentales, o bien adquirir ventajas estratégicas o geopolíticas. Esta clase de delitos involucran a menudo tácticas sofisticadas, como campañas de desinformación y la explotación de redes sociales, pero se traduce principalmente en conductas como el «hacktivismo», el discurso de odio en internet, la ciberguerra o el ciberterrorismo (Miró Llinares, 2012: 250).

A partir de lo anterior, las características particulares de este tipo de cibercriminalidad varían de acuerdo con la zona geográfica en la que esta se desarrolla. Por ejemplo, en Europa han surgido preocupaciones en torno a ciberataques en contra de redes gubernamentales, infraestructura crítica y la manipulación de la opinión pública, especialmente durante épocas electorales o en el contexto de conflictos armados internacionales, como el de Ucrania a partir de 2014 (Baezner, 2018: 10 y ss.). En Estados Unidos se manifiestan constantemente altos niveles de cibercriminalidad política, con entidades extranjeras acusadas de interferencia electoral,[21] así como de ciberespionaje en contra de objetivos geopolíticos o militares. Por su parte, en América Latina una fracción significativa de la cibercriminalidad evidencia motivaciones político-activistas, como muestran casos regionales recientes.[22] Este tipo de inciden-

21. En las elecciones presidenciales de Estados Unidos de 2016 se registró un incremento significativo de la cibercriminalidad política. Este fenómeno se manifestó en la manipulación de las redes sociales y la usurpación de identidades de usuario, acciones orientadas a influir en el electorado según criterios como la orientación política, el nivel educativo, las opiniones y otros factores que incrementaban su susceptibilidad (Alexandrou, 2022: 68 y ss.).

22. Véase Luis Alberto Andres, Hualong Diao, Stephane Straub y Estefanía Belén Vergara Cobos, «Cybersecurity in Latin America and the Caribbean», *Grupo Banco Mundial*, 2 de mayo de 2024, disponible en https://tipg.link/l__d.

tes se caracterizan por una amplia gama de actividades como, por ejemplo, ataques a sitios gubernamentales y filtraciones de información reservada, con el fin de poner en jaque o desestabilizar estructuras políticas dominantes.

En este contexto, el hacktivismo ha adquirido una posición preeminente entre los grupos de cibercriminalidad. El nombre de esta categoría proviene de la contracción de las palabras en inglés *hacking* y activismo (Sabillon y otros, 2016: 3), y dice relación con conductas como el acceso ilícito a sistemas informáticos de terceros para conocer o divulgar información reservada, la vandalización de sitios web (denominado en inglés *defacement*) o bien el lanzamiento de ataques de denegación de servicio distribuido, conductas que pueden ser subsumidas en el delito de ataque contra la integridad de un sistema informático (artículo 1 de la Ley 21459) o de ataque contra la integridad específicamente de datos informáticos (artículo 4 de la Ley 21459), según sea el caso.[23] Tales acciones tienen como denominador común la persecución de una agenda política, religiosa o social. Este fenómeno delictivo se ha expandido por diferentes países, como Brasil, Chile, Colombia, Ecuador, Perú y Venezuela, afectando a diferentes sectores, como el de la minería, el petróleo y el gas. La evidencia comparada indica, además, que la administración pública es uno de los principales sectores atacados y que la motivación política explica una proporción relevante de incidentes.[24]

La diversidad de finalidades políticas, económicas o sociales que pueden perseguirse en el ciberespacio repercute en un amplio abanico de posibles perpetradores de cibercriminalidad política. Los actores estatales, como los Gobiernos centrales o grupos patrocinados estatalmente, están normalmente implicados en los casos más sofisticados y con mayor trascendencia de cibercriminalidad política, consistentes en actividades diseñadas para influenciar políticas públicas o desestabilizar Estados rivales. Entidades no estatales, como organizaciones no gubernamentales, grupos terroristas y facciones políticas extremistas, aprovechan la naturaleza descentralizada, anónima y transnacional del ciberespacio[25] para propugnar su agenda, realizar propaganda y coordinar acciones activistas individuales. Por su parte, los hacktivistas individuales se encuentran motivados por convicciones particulares o afiliaciones a movimientos más amplios, y conducen operaciones para exponer causas célebres, realizar protestas de políticas públicas o impulsar un cambio social. Sin embargo,

23. En relación con el sabotaje informático en general, véase Bascur Retamal y Peña Sepúlveda (2023: 6 y ss.).

24. Un ejemplo relevante es el hackeo del Estado Mayor Conjunto de la Defensa de Chile, adjudicado por un grupo hacktivista, que implicó la difusión de cuatrocientos mil correos electrónicos reservados. Para más información al respecto, véase Nicolás Sepúlveda, «Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa», *Ciper Chile*, 22 de septiembre de 2009, disponible en https://tipg.link/mBS6.

25. Respecto de la naturaleza y características del ciberespacio, véase Barrio Andrés (2018: 25).

quedan fuera del anterior grupo la mayor parte de las personas jurídicas de derecho privado objeto de la Ley 20393, esto es, las personas jurídicas con fines de lucro o sociedades, debido a que las actividades políticas no forman parte de sus objetivos y actividades normales.

En contraste con las empresas, las personas jurídicas sin fines de lucro, en tanto constituyen instrumentos fundamentales para la articulación de ideales sociales y políticos, junto con la movilización de decisiones públicas, exhiben un perfil de riesgo singular en el contexto de la cibercriminalidad política. La naturaleza de este tipo de entidades, intermediarias entre la sociedad organizada y el Estado (Simsa, 2013: 128; Habermas, 1992: 443 y ss.), las sitúa en la intersección entre el discurso y la acción política. Esta función dual incrementa su potencial para erigirse, al mismo tiempo, en instrumentos de cambio social positivo y vehículos para la cibercriminalidad política. La evolución de los movimientos sociales, particularmente en la era digital, subraya esta dicotomía: si bien históricamente el discurso político y social se desarrollaba en espacios físicos, en el siglo XXI este ha migrado al ámbito digital (Anheier, 2013: 77 y ss.), donde las personas jurídicas sin fines de lucro continúan jugando un rol significativo en la formación de la opinión pública y las políticas estatales. Sin embargo, la digitalización también las expone al riesgo de ser capturadas o utilizadas como plataformas para actividades lesivas con motivaciones políticas en el ciberespacio, incluyendo el espionaje, la manipulación de datos o sabotajes informáticos de adversarios ideológicos, entre otras.

El riesgo de involucramiento de personas jurídicas sin fines de lucro en la cibercriminalidad política se ve aumentado por sus características operativas. Estas poseen frecuentemente huellas digitales sustanciales[26] y manejan datos sensibles de afiliados y *stakeholders*, lo cual las convierte en medios atractivos para sujetos que buscan influenciar de forma ilegítima en procesos políticos. Adicionalmente, la naturaleza de estas entidades, que frecuentemente realizan campañas en materias altamente contenciosas o en conflictos polarizados, puede borrar las líneas entre la persecución legítima de ideales y acciones constitutivas de expresiones delictivas.

En este contexto, resulta fundamental diferenciar entre personas jurídicas sin fines de lucro que se involucran inadvertidamente en cibercriminalidad política, y aquellas dedicadas a esta clase de delitos de forma dolosa y con plena conciencia de la ilicitud. Las primeras pueden ser víctimas de ciberataques que explotan sus estructuras para conseguir réditos políticos, mientras que las segundas incluyen a entida-

26. Ello se traduce en una activa presencia en línea a través de sitios web y redes sociales, la gestión de grandes volúmenes de datos de donantes, beneficiarios y operaciones, y sus frecuentes interacciones digitales. Además, campañas de concienciación y movilización en línea, junto con la colaboración a través de plataformas digitales, amplían esta huella digital al generar y almacenar una cantidad significativa de datos y al estar altamente interconectadas en el ciberespacio.

des que perpetran directamente delitos informáticos o son cómplices de este tipo de iniciativas. La inclusión de los delitos informáticos en el catálogo del artículo 1 de la Ley 20393 permite discernir estas particularidades, individualizar las responsabilidades y atribuir sanciones a organizaciones que cruzan la línea desde la lucha política pacífica a actividades ilegales en el ciberespacio.[27] Ello es esencial para mantener la integridad de la sociedad civil, así como del sistema político más amplio en el cual esta se desenvuelve.

Valoración

El impacto de la evolución tecnológica en la tipología de los delitos informáticos repercute en un amplio espectro de perpetradores, que van desde individuos aislados hasta entidades organizadas y el Estado. La intersección descrita entre la criminalidad informática y las personas jurídicas permite concluir provisionalmente que la diversidad y complejidad de los perfiles involucrados en estos actos delictivos individuales tiene repercusiones importantes cuando se insertan en un contexto organizacional.

En el ámbito de la criminalidad económica, la búsqueda de beneficio constituye un motor significativo de la cibercriminalidad, lo cual extiende su relevancia más allá de los actores individuales y hacia las estructuras empresariales. De este modo, es plausible argumentar que una entidad puede verse implicada en la perpetración de delitos informáticos en el desarrollo de su giro, con la finalidad de incrementar sus beneficios o conseguir ventajas competitivas en el mercado. Esta propensión está intrínsecamente ligada a la eficacia de los sistemas de prevención de delitos que dicha entidad tenga implementados, así como a la cultura organizacional imperante en sus estructuras. Así, una cultura empresarial sólida y éticamente orientada, combinada con un modelo de prevención efectivo, puede guiar a la entidad hacia un comportamiento conforme a la ley, mientras que la ausencia de estos puede predisponerla a transgresiones legales. Por tanto, el riesgo de que una empresa se vea envuelta en actividades cibercriminales económicas no solo se deriva del mapa de riesgos relacionados a su objeto, sino que también depende de su compromiso y capacidad para fomentar un entorno corporativo que priorice el cumplimiento legal y la integridad.

En el contexto de las personas jurídicas sin fines de lucro, es posible observar un debate relevante sobre el papel que estas organizaciones desempeñan hoy en la sociedad. La articulación de ideales políticos y sociales puede convertirse bajo ciertas circunstancias en canales para actividades cibercriminales con motivaciones políticas. Esta dualidad de funciones, como agentes de cambio social y simultáneamente como potenciales plataformas para la cibercriminalidad, constituye un desafío normativo y

27. Acerca de la radicalización de las personas jurídicas sin fines de lucro como fundamento político-criminal para la atribución de pena, véase Bedecarratz Scholz (2022: 60 y ss.).

de política pública. En este contexto, la labor de los tribunales de justicia, relativa a la atribución de la responsabilidad penal a aquellas que transgreden las reglas básicas, resulta indispensable para preservar la integridad de estas entidades y del sistema político en su conjunto, así como para mitigar el riesgo de su explotación para fines ilícitos.

Sin embargo, la consecución de estos objetivos depende directamente de la idoneidad de la Ley 20393 que establece la responsabilidad penal de las personas jurídicas para perseguir esta clase de criminalidad. Tal como a continuación se expone, esta aptitud se encuentra condicionada por la resolución de distintos problemas de naturaleza dogmática que traban el proceso de imputación.

Desafíos para la responsabilidad penal de las personas jurídicas

Una desarmonía fundamental

La responsabilidad penal de las personas jurídicas en el contexto de los delitos informáticos exhibe importantes desafíos. Estos tienen su origen en la disonancia entre la conceptualización criminológica de dichos delitos y el modelo de imputación aplicable a estas entidades. La naturaleza de la cibercriminalidad radica en su ejecución predominante por individuos aislados o grupos criminales. Ello contrasta con la percepción de las personas jurídicas, que a menudo son víctimas y no perpetradoras de este tipo de actos. Esta discordancia radica en la dificultad de establecer un vínculo claro y directo entre los actos delictivos cometidos en este contexto y la estructura o funcionamiento interno de la entidad, lo cual constituye un requisito que subyace al sistema de imputación penal previsto en el artículo 3 inciso primero de la Ley 20393. Lo anterior complejiza una atribución de responsabilidad, debido a que esta clase de conductas suelen ser perpetradas para beneficiar a individuos o entidades externas, mas no a la organización.

Desde una perspectiva general, los modelos de responsabilidad penal de las personas jurídicas se basan en la existencia de una conexión entre el acto delictivo y la entidad, sea a través de la relación orgánica del individuo que ejecuta materialmente el delito (modelos de heterorresponsabilidad),[28] por fallas internas que permiten o favorecen ese mismo hecho (modelos de autorresponsabilidad)[29] o mediante una

28. Los modelos de heterorresponsabilidad, también llamados «vicariales», se basan en la comisión de un delito individual, denominado «hecho de conexión», por parte de un agente de la organización. Tal hecho punible se imputa a la persona jurídica, sobre la base de ciertas características que muestren un efecto comunicativo entre el acto del individuo y la persona jurídica, como por ejemplo el carácter de directivo o superior del hechor en el organigrama de la entidad. Para más explicaciones al respecto, véase Bedecarratz Scholz (2022: 78). Para una crítica de estos modelos, véase Gracia Martín (2016: 20-21).

29. Los modelos de autorresponsabilidad se basan en que la persona jurídica genera su propia respon-

combinación de ambos criterios (modelos mixtos). Sin embargo, en el ámbito de la criminalidad informática, dichas conexiones son a menudo tenues o indirectas, puesto que los delitos pueden ser cometidos sin un beneficio claro o directo para la entidad, o incluso en su perjuicio. Esto plantea un problema para el modelo de atribución contenido en la Ley 20393. La distinción criminológica entre autor y víctima del delito se vuelve en este contexto borrosa, especialmente cuando las acciones delictivas se realizan desde dentro de la entidad sin su conocimiento o consentimiento.

La desarmonía fundamental expuesta repercute en dificultades para la evaluación de los requisitos de imputación previstos en la ley en un caso concreto. En las siguientes líneas se realiza una revisión de dichos criterios de atribución, en consideración a las complejidades de la cibercriminalidad y su impacto en las estructuras corporativas, con el fin de lograr una interpretación que concilie efectivamente las dinámicas del fenómeno delictivo con los principios de la Ley 20393.

Del «interés o provecho» al «en el marco de su actividad»

Como se ha venido anunciando, las reglas contempladas en el artículo 3 inciso primero de la Ley 20393 puntualizan la medida de vinculación necesaria para que el comportamiento de la persona natural pueda ser considerado como parte de los procesos dirigidos o controlados por la persona jurídica (García Palominos, 2020: 830) y, de tal forma, serle imputado. En cuanto al primero de estos requisitos, la norma ha experimentado una evolución desde un enfoque restrictivo hacia uno más amplio, proceso que ha ejercido un efecto directo en la imputación de los delitos informáticos a personas jurídicas.

En el texto original de la Ley 20393, el artículo 3 inciso primero establecía como requisito de imputación que el delito debe cometerse «en interés o provecho» de la persona jurídica. Si bien han existido diversas interpretaciones respecto del verdadero sentido y alcance de este presupuesto (Bedecarratz Scholz, 2022: 120 y ss.), la posición mayoritaria de la antigua doctrina y la jurisprudencia sostenía que el hecho debía haber sido cometido objetivamente en beneficio de la persona jurídica, independiente de las intenciones del autor al momento de ejecutarlo.[30] Esto es, que la conducta delictiva individual debía acarrear una ventaja de cualquier índole para la entidad, lo cual debía verificarse, por añadidura, de manera directa e inmediata.

---

sabilidad, sobre la base de un comportamiento propio de la organización ocurrido antes o después de la comisión del delito (Nieto Martín, 2008a: 127). Para una crítica al respecto, véase Van Weezel (2010: 122).

30. La postura más razonable y acorde con los fines del modelo de responsabilidad precisa es que el hecho debe haber tenido objetivamente la aptitud de haber sido cometido en interés o generar un provecho para la persona jurídica, independiente de si este se generó en los hechos o no, lo cual debe ser apreciado *ex ante*. Al respecto, véase García Palominos (2020: 834).

Este requisito presentaba complejidades significativas para la atribución de responsabilidad penal a una persona jurídica, particularmente en el contexto de los delitos informáticos. Desde una perspectiva criminológica, y como se planteó en el capítulo anterior, la mayoría de estas conductas delictivas son cometidas por individuos que actúan en contra de los intereses de las personas jurídicas o en donde los resultados del comportamiento son en todo sentido indiferentes a la entidad. En dichos casos, la naturaleza de esta clase de ilícitos colisionaba con el requisito en estudio, que en la práctica podía operar como un criterio de exclusión de punibilidad excesivamente riguroso.

En contraposición a este escenario, la dictación de la Ley 21595 modificó sustancialmente la redacción del artículo 3 de la Ley 20393, reestructurando el modelo de imputación. A través de ella, se eliminó el requisito de «interés o provecho», estableciendo en su lugar un nuevo presupuesto: el delito individual debe haber sido cometido por o con la intervención de alguno de los sujetos que consagra la norma, «en el marco de la actividad» de la persona jurídica. Con ello se impuso como exigencia que el acto delictivo debe haber sido realizado dentro del marco de las operaciones de la entidad y exhibir una conexión con su actividad organizacional concreta para que el hecho le sea imputable.[31] No se trata solo de actividades formalmente declaradas por la persona jurídica, sino de cualquier acción que se realice en el curso normal de sus operaciones y que esté alineada con sus objetivos y prácticas.

Es importante destacar que la modificación del requisito admite que conductas devenidas en exclusivo interés de la persona natural también puedan irrogar la responsabilidad penal de la persona jurídica, aun cuando sean totalmente indiferentes o neutrales con respecto a los intereses corporativos. Solamente se excluyen hechos perpetrados en exclusivo perjuicio de la persona jurídica, conforme al artículo 3 inciso final de la Ley 20393. Como correctamente indica Artaza Varela (2024: 287), la persona jurídica está obligada a gestionar riesgos asociados a que sus integrantes cometan delitos en su propio interés en todos aquellos casos en que resulte previsible que un individuo se aproveche del desarrollo de una actividad empresarial.

La modificación de este criterio obedece a razones preventivas especiales, pues se enlaza con el riesgo generado por las actividades organizacionales para atribuir la sanción. De tal modo, la modificación profundiza el «modelo de incumbencia»

31. Desde una perspectiva comparada, pese a que el artículo 31 bis del Código Penal español posee un requisito similar que exige la comisión del delito «en el ejercicio de actividades sociales», su sentido es distinto que en el derecho chileno. Para la doctrina española, la expresión se orienta más bien a que el delito debe haberse originado en el marco de las competencias que el trabajador detenta. De tal modo, sería equivalente a la exigencia de que el sujeto actúe en nombre de la persona jurídica (Fernández Teruelo, 2019: 3; Nieto Martín, 2008a: 99-100). En el caso de la norma chilena, en cambio, el pronombre «su» alude a la persona jurídica mencionada al inicio de la disposición.

(García Palominos, 2020: 830) implementado en la Ley 20393,[32] que fundamenta la atribución de responsabilidad en una vulneración de deberes de autorregulación, consistentes en un control defectuoso de los riesgos originados por las actividades u operaciones desarrolladas por la entidad.[33] Sin embargo, este modelo de incumbencia desempeña también una importante función de exclusión: solo es responsable la persona jurídica cuando el delito individual se ejecute en el marco de las actividades de la entidad, es decir, en el contexto del desarrollo de sus operaciones normales. En caso contrario, no es posible aseverar que el delito individual sea producto del riesgo delictivo generado por las operaciones de la entidad y, en consecuencia, que esta última sea causante del mismo.

La repercusión de este requisito para la imputación de delitos informáticos a las personas jurídicas puede ser ilustrada de la siguiente forma. Por ejemplo, en el caso de una empresa dedicada al desarrollo de software, si durante el proceso de creación los empleados acceden sin autorización a datos confidenciales de un cliente, los modifican o destruyen, o causan daños al sistema informático objetivo, entonces puede darse por sentada una conexión con las operaciones empresariales. Esto se debe a que los actos se ejecutan en el entorno y durante las actividades de la empresa. En contraste, si un empleado de una oficina de arquitectura, responsable solo del manejo de tecnologías de información internas, comete un delito informático que afecta los datos de una persona privada y este acto no está relacionado con las actividades empresariales de la oficina, entonces no es posible dar por establecida esta conexión entre el delito y la actividad empresarial. En este último escenario, el acto delictivo se considera ajeno a las responsabilidades corporativas y, por ende, no implicaría directamente la responsabilidad penal de la persona jurídica.[34]

32. La Ley 20393 establece, como fundamento de la iniciativa, el servir «como un verdadero aliciente para que [las personas jurídicas] adopten medidas de autorregulación».

33. Idea matriz que fue mantenida durante la tramitación de su reforma por la Ley 21595. Al respecto, el profesor Héctor Hernández, durante la tramitación de la ley, dijo lo siguiente: «La concepción o fundamento de la responsabilidad penal de las personas jurídicas […] se ha conformado en torno a la idea de que se trata de una responsabilidad configurada por una fuente de peligro, cuando por su complejidad, acciones, medios a su cargo, la empresa se transforma en una fuente potencial de delitos de diferente tipo como corrupción, contaminación o fraude, entre otros. Así, se impone responsabilidad como contrapartida del riesgo que la actividad empresarial implica, o como contrapartida del ejercicio de la libertad empresarial, por lo que existe un deber de velar porque el ejercicio de tal libertad no afecte bienes jurídicos y no dé lugar a delitos» («Historia de la Ley 21595», *Biblioteca del Congreso Nacional de Chile*, 17 de agosto de 2023, p. 130, disponible en https://tipg.link/mEaS).

34. Ejemplos provenientes de la fundamentación del proyecto de ley de reforma del derecho penal alemán para el combate de la criminalidad computacional. Para más información al respecto, véase Gobierno Federal de Alemania, «Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität», 30 de noviembre de 2006, disponible en https://tipg.link/m8VW.

Como puede observarse, la sustitución del criterio de «interés o provecho» por el de «actuar en el marco de su actividad» mitigó la discordancia entre el contexto de comisión de los delitos informáticos, frecuentemente situado al margen de los intereses de la entidad más que en su beneficio, y la finalidad del modelo de imputación previsto en la Ley 20393. La nueva redacción del artículo 3 inciso primero se orienta hacia una conexión entre la conducta delictiva y el ámbito operativo de la entidad. Ello facilita la atribución de responsabilidad, al centrarse en la relación entre el delito cometido y la actividad de la organización, más que en el beneficio obtenido. Sin embargo, dicho cambio, aunque amplía el espectro de imputación, no resuelve completamente el dilema descrito, ya que las conductas constitutivas de delitos informáticos no necesariamente son cometidas en el contexto de actividades regulares de la entidad. Lo anterior evidencia una tensión persistente entre la estructura legal y la dinámica real de la cibercriminalidad y, con ello, un desafío para la aplicación efectiva de la ley.

Modelos efectivos de prevención de delitos informáticos

El elemento fundamental del modelo de responsabilidad radica en que el delito individual debe vincularse a un fallo estructural de la persona jurídica, consistente en una organización interna defectuosa. Para la concepción original de la teoría de la «culpabilidad por defecto organizacional» (Tiedemann, 1988: 1172), esta se traduce en la ausencia de implementación de medidas preventivas en la persona jurídica, tendentes a disminuir el riesgo de comisión de delitos.

Dicho requisito se encuentra concretizado en el artículo 3 inciso primero de la Ley 20393, disposición que ha experimentado una evolución a partir de la dictación de la Ley 21595 sobre Delitos Económicos. En su nueva redacción, esta exige que la comisión del delito individual debe haberse visto «favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de prevención de tales delitos, por parte de la persona jurídica». A través de esta norma, la ley impone sobre la entidad una obligación, consistente en velar por que sus actividades no generen un mayor riesgo de comisión de delitos por parte de sus miembros.[35]

El cumplimiento de la obligación antes referida se logra mediante la implementación de un modelo de prevención de delitos, también denominado modelo de *compliance*.[36] Dicha ley prevé, en su artículo 4, los aspectos mínimos a considerar en su

35. Sobre los riesgos delictivos estructurales que emanan de la empresa, véase Nieto Martín (2008a: 38-39). En relación con el nexo entre el fallo organizativo y el reproche social, véase Artaza Varela (2013b: 547).

36. Según Neira Pena (2016: 469), los programas de *compliance* son «sistemas organizativos que incluyen principios, reglas, procedimientos e instrumentos orientados a asegurar el cumplimiento de la legalidad en el desarrollo de las actividades de una organización». Según Rotsch (2013: 494), las funciones

implementación, los cuales son fundamentales para acceder a la exención de responsabilidad penal. Tales pueden ser resumidos en la identificación de actividades o procesos generadores de riesgo penal; el establecimiento de protocolos y procedimientos para prevenir y detectar conductas delictivas en el marco de las actividades organizacionales; la asignación de uno o más sujetos responsables, con debida independencia, autonomía, así como provisto de medios y facultades suficientes para desempeñar las obligaciones propias de su cargo; y la previsión de evaluaciones regulares por terceros independientes, junto a mecanismos para una mejora y actualización a partir de ellas.

La implementación de esta clase de modelos en el contexto de la prevención de delitos informáticos presenta desafíos singulares. Como se reseñó, estos deben identificar las actividades generadoras de riesgo penal y establecer protocolos para mitigarlos. Sin embargo, las peculiaridades de la cibercriminalidad, concretamente su dinamismo y carácter transfronterizo, requiere que los modelos sean flexibles, que estén constantemente actualizados y que sean capaces de adaptarse a los cambios en los *modus operandi* delictivos. Concordantemente, los sistemas de prevención deben ser especialmente dinámicos y experimentar una actualización constante, cada vez que en la empresa se produzcan cambios organizativos, estructurales o se emprendan nuevas operaciones o actividades, para así identificar las nuevas vulnerabilidades y amenazas informáticas a los cuales se está expuesto. Ello implica no solo la implementación de medidas técnicas como sistemas de seguridad informática avanzados y procedimientos de auditoría digital, sino también la capacitación continua de empleados en prácticas de ciberseguridad y la creación de una cultura organizacional respetuosa de la protección de datos personales y la seguridad informática.

Por otro lado, la efectividad de los modelos de prevención de delitos informáticos en pequeñas y medianas empresas está condicionada por la limitación de recursos y una menor conciencia del riesgo delictivo en este contexto. Ello, pese a que las probabilidades de comisión de un delito informático en su interior no son bajas (Mayer Lux y Vera Vega, 2023: 151-152). Lo anterior tiene su origen en que las grandes empresas han constituido desde antiguo objetivos comparativamente más atractivos para la comisión de delitos informáticos, lo cual las ha obligado a implementar mecanismos más refinados de protección y a desarrollar una cultura de ciberseguridad. En contraste, las pequeñas y medianas empresas enfrentan obstáculos financieros y de conocimientos para la adopción de medidas preventivas adecuadas (Mayer Lux, 2018: 195). Esta problemática las expone no solo a ser víctimas, sino que también a incurrir en este tipo de conductas a causa de la inconsciencia del riesgo delictivo.

---

del *compliance* se traducen en: i) disminuir el riesgo de que la organización o sus miembros perpetren un delito y ii) mejorar las posibilidades de una exención penal en el marco de un proceso seguido en contra de la persona jurídica.

Si bien el artículo 4 inciso primero de la Ley 20393 contempla una regla de razonabilidad que reconoce estas dificultades y permite escalar la implementación de los modelos de prevención según las capacidades económicas y el tamaño de pequeñas y medianas empresas, una reducción en densidad de las medidas institucionales, organizativas y técnicas de *compliance*[37] puede repercutir en la efectividad preventiva del modelo y, en consecuencia, incidir en un incremento del riesgo de ser fuente de delitos informáticos.

Prevención de la cibercriminalidad organizacional

El cambio de paradigma experimentado por las personas jurídicas a raíz de la Ley 21459, que las desplazó desde su lugar tradicional de víctimas de delitos informáticos hacia una posición en que también pueden ser consideradas eventuales responsables, hace necesario profundizar en la prevención de la cibercriminalidad organizacional. Ello es pertinente desde la perspectiva del modelo de imputación previsto en el artículo 3 inciso primero de la Ley 20393, que establece la ausencia de implementación efectiva de un modelo adecuado de prevención de delitos como un requisito de imputación. A través de la citada disposición, la ley impone una obligación a la persona jurídica, consistente en instaurar un modelo de organización y gestión idóneo para mitigar el riesgo de conductas criminalmente desviadas en su interior.

Los elementos del modelo se orientan según lo previsto en el artículo 4 de la Ley 20393, que define los lineamientos básicos para su implementación. Aunque la estructura general de un modelo de cumplimiento se ha aclarado tras casi quince años de aplicación de la ley, todavía persiste una falta de certeza respecto de las medidas concretas requeridas para prevenir un delito informático. La reciente inclusión de estos delitos en el catálogo del artículo 1 y la ausencia de un consenso doctrinal sobre los componentes que deben integrar un modelo efectivo en este contexto se confabulan para complicar su concreción práctica (Riveros Saavedra, 2023: 322).

Para resolver esta problemática es necesario tener presente que la implementación de un modelo de prevención conforme a la Ley 20393 constituye un proceso sistemático y complejo compuesto de distintos pasos orientados según un enfoque basado en el riesgo (Piña Rochefort, 2012: 15 y ss.; Bedecarratz Scholz, 2022: 184 y ss.). En este contexto, dicho proceso debe comenzar con la identificación de las actividades o procesos internos que presentan un riesgo elevado de ser utilizados para cometer delitos informáticos (artículo 4 número 1), lo cual implica realizar un estudio criminológi-

37. Una medida normativa consistiría, por ejemplo, en la formulación de directrices internas de la empresa; una medida institucional sería la creación del cargo de oficial de cumplimiento (*compliance officer*); y una medida técnica podría ser el establecimiento de un canal automatizado de comunicaciones para denunciantes internos (*whistleblower*) (Rotsch, 2013: 484).

co de la entidad a partir de sus características particulares que generan una mayor exposición a ciertas conductas delictivas. Ello debe incluir un análisis detallado de la estructura organizacional, los procedimientos operativos, los sistemas y redes informáticas utilizadas, las relaciones con clientes y proveedores, así como todos los aspectos de la operación de la entidad que puedan ser fuente de riesgos delictivos.

En este sentido, no se trata de identificar el riesgo de que un dependiente de la persona jurídica se transforme en hacker individual y realice actos por cuenta propia, sino más bien de que este sujeto cometa ilícitos informáticos en el marco de las actividades sociales. Como se indicó anteriormente, los crímenes deben exhibir una conexión directa o indirecta con el desarrollo de las operaciones asociativas. Por ejemplo, una agencia de prensa no necesariamente está expuesta al mismo riesgo delictivo que una empresa de marketing, pues en el primer caso puede existir un riesgo mayor de acceso ilícito, mientras que en la segunda uno de receptación de datos.

Posteriormente, hay que clasificar y evaluar el riesgo identificado en base a una metodología transparente y sistemática, que permita determinar su magnitud conforme a la probabilidad de ocurrencia y el impacto potencial. En esta cuantificación inciden factores que incluyen el carácter lucrativo o no lucrativo de la entidad; las operaciones que realiza, lo que determina el nivel de exposición a riesgos informáticos; el grado de autonomía y discrecionalidad que los trabajadores y dependientes tienen en sus funciones, ya que mayores niveles pueden facilitar la comisión de actos delictivos; las políticas internas de control y supervisión, las que deben ser suficientemente robustas para prevenir y detectar conductas indebidas; la capacitación y sensibilización en materia de ciberseguridad; entre otros. Este análisis se condensa en una escala ordinal para cada riesgo identificado, de alto a bajo, que es fundamental para los pasos subsecuentes.

Una vez identificadas las actividades o procesos que representan un riesgo relevante de comisión de delitos informáticos en el marco de las operaciones de la persona jurídica, se debe establecer un sistema de prevención que desarrolle protocolos, reglas y procedimientos específicos para mitigar dichos riesgos (artículo 4 número 2). El diseño de dichas medidas debe ser cuidadoso y ajustado al riesgo identificado, con un enfoque prioritario en las áreas donde la incidencia de delitos informáticos sea, estimativamente, alta. Lo anterior puede incluir, por ejemplo, la implementación de protocolos de acceso y autentificación o bien la formación de empleados en seguridad y conciencia sobre los riesgos. Por otro lado, en cuanto a riesgos no asociados a una actividad o proceso específico sino más bien inherente a las operaciones de la entidad, es necesario establecer políticas y normas de aplicación general para toda la organización. Ello implica el desarrollo de un marco de gobernanza interno que integre la ciberseguridad como un elemento de gestión de riesgos continuo (Harich, 2021: 71 y ss.).

Cabe destacar que los avances en el marco jurídico regulatorio de la ciberseguridad a nivel nacional permiten identificar una serie de normas extrapenales que cristalizan medidas de protección de organizaciones respecto de ataques. La Ley 21663 o Ley Marco de Ciberseguridad (26 de marzo de 2024) establece estándares generales de ciberseguridad que los sujetos obligados[38] deben adoptar para asegurar sus sistemas. Otro tanto ocurre con la normativa sectorial en la materia. Por ejemplo, los bancos e instituciones financieras pueden recurrir a los estándares y medidas dispuestos en la Recopilación Actualizada de Normas de la Comisión para el Mercado Financiero, que en su capítulo 1-13 regula la administración del riesgo operacional en dichas instituciones y en el 20-10 prevé reglas para gestionar el riesgo de seguridad de la información y ciberseguridad. También puede citarse como una fuente de orientación los estándares extrajurídicos y las reglas técnicas de gestión de esta clase de riesgos, como los pertenecientes a la serie ISO 27.00X sobre sistemas de gestión de seguridad de la información y ciberseguridad.

Sin embargo, cabe tener presente que esta normativa se enfoca en prevenir el riesgo de delitos informáticos cometidos por terceros en contra de la persona jurídica, es decir, en la protección de los sistemas informáticos internos frente a amenazas comúnmente externas. Por lo tanto, no tienen por objeto aquellas amenazas que puedan originarse desde la propia organización como agente criminógeno. En otras palabras, los estándares o regulaciones mencionados apuntan a una fuente de riesgo diametralmente opuesta a aquella que las personas jurídicas deben atender bajo la Ley 20393, una que comúnmente queda excluida del ámbito de dicha ley en virtud del artículo 3 inciso final.

Luego, toda medida prevista en este corpus extrapenal debe pasar por un filtro de idoneidad, relativo a si es igualmente capaz de reducir el riesgo interno de comisión de delitos, previo a ser implementada. Por ejemplo, un sistema de detección de intrusiones permite monitorear el tráfico de la red en busca de actividades sospechosas y emitir alertas automáticas cuando se detecta tal actividad, lo cual puede ser constitutivo de una tentativa de acceso ilícito. Ello puede ser idóneo para prevenir ataques informáticos externos hacia la organización, pero no necesariamente para detectar aquellos originados internamente hacia terceros.

Como corolario, es posible afirmar que la prevención de la cibercriminalidad organizacional en las personas jurídicas, particularmente en el marco de los delitos informáticos, exige una aproximación que abarque desde el análisis criminológico y la implementación de medidas preventivas específicas, hasta la previsión de evaluaciones periódicas por terceros independientes y mecanismos de perfeccionamiento o actualización a partir de tales evaluaciones (artículo 4 inciso cuarto). En este contex-

38. Tales son servicios esenciales (artículo 4 inciso segundo de la Ley 21663) y operadores de importancia vital (artículo 5 de la Ley 21663).

to, la responsabilidad que asume la entidad no es (solo) de protegerse contra amenazas externas —como ha sido en el pasado—, sino que de mitigar el riesgo de que sus dependientes cometan delitos informáticos. Esto implica la adopción de un modelo de prevención que sea dinámico, capaz de evolucionar a la par del cambiante panorama de la ciberdelincuencia y que esté alineado con los estándares de ciberseguridad vigentes en el ámbito extrapenal.

Conclusiones

A partir del estudio realizado sobre la responsabilidad penal de las personas jurídicas en el ámbito de los delitos informáticos en Chile es posible arribar a las siguientes conclusiones: primero, la Ley 21459 ha generado un profundo cambio respecto de la esfera de las conductas prohibidas en materia informática para las personas jurídicas, las que deben reorientar sus tareas preventivas para enfrentar no solo amenazas externas que buscan explotar vulnerabilidades con el fin de acceder ilícitamente, defraudar o sabotear sus sistemas informáticos, sino que también a delitos informáticos que pueden originarse al interior de sus propias estructuras. Concordantemente, las personas jurídicas se han transformado en incumbentes respecto del riesgo de ciberdelitos cometidos en el marco de sus actividades asociativas, debiendo implementar medidas normativas, institucionales y técnicas idóneas para disminuir el riesgo de que la organización o sus miembros perpetren un delito informático, así como para mejorar las posibilidades de influenciar positivamente un proceso sancionatorio dirigido en su contra, en conformidad con lo dispuesto en la Ley 20393.

En segundo lugar, el análisis criminológico realizado refleja la complejidad de la atribución de responsabilidad penal de las personas jurídicas por esta clase de ilícitos. Se evidencia la necesidad de distinguir claramente entre los actos que se desarrollan en el marco de las actividades de la entidad y aquellos que se perpetran fuera de este. Ello plantea desafíos para la aplicación efectiva del modelo de responsabilidad penal en la era posterior a la Ley 21595, pues se requiere no solo una conexión clara entre la conducta delictiva y la actividad organizacional, sino también sistemas de prevención eficaces e implementados correctamente.

Vinculado a lo anterior, es indispensable establecer modelos de prevención robustos, conforme a la ley, pero también dinámicos y adaptables frente al constante cambio que experimenta la delincuencia informática. Ello debe integrar medidas enfocadas a la prevención de riesgos emanados de la propia persona jurídica, así como protocolos de actuación generales y la promoción de una cultura de respeto y buena fe en el ciberespacio. En este cometido, la persona jurídica debe diseñar medidas idóneas según su potencial criminógeno y el análisis de riesgos efectuado a fin de que se establezca una política de gestión de riesgos sólida y bien definida, que incluya la identificación, evaluación y tratamiento de los riesgos relacionados con la ciberse-

guridad. En este proceso incide una larga lista de factores y criterios que deben ser considerados cuidadosamente para cumplir con el mandato de «efectividad» previsto en el artículo 3 inciso primero de la Ley 20393.

Finalmente, el respeto a la Ley 21459 y la efectiva implementación de modelos de prevención de delitos informáticos constituyen desafíos significativos para las personas jurídicas en Chile. Con todo, también ofrecen una oportunidad para fortalecer las prácticas de gobernanza corporativa y establecer un entorno digital más seguro para las personas, para otras entidades y, en definitiva, para la sociedad en su conjunto. Los riesgos asociados con la delincuencia informática, cada vez más prominentes en el panorama actual, hacen evidente la necesidad de abordar estos desafíos de manera proactiva, efectiva y urgente.

Reconocimientos

Este trabajo ha sido elaborado en el marco del proyecto DIUA 258-2023 de la Vicerrectoría de Investigación y Doctorados de la Universidad Autónoma de Chile.

Referencias

Alexandrou, Alex (2022). *Cybercrime and information technology*. Boca Ratón: CRC Press.

Anheier, Helmut (2013). «Entwicklungen der internationalen Zivilgesellschaft». En Ruth Simsa, Michael Meyer y Christoph Badelt (editores), *Handbuch der Nonprofit-Organisation. Strukturen und Management* (pp. 77-88). 5.ª ed. Stuttgart: Schäffer-Poeschel.

Artaza Varela, Osvaldo (2013a). *La empresa como sujeto de imputación de responsabilidad penal: Fundamentos y límites*. Madrid: Marcial Pons.

—. (2013b). «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.

—. (2024). «Responsabilidad penal de las personas jurídicas». En Iván Navas Mondaca (director), *Derecho penal económico. Parte general* (pp. 279-302). Valencia: Tirant Lo Blanch.

Baezner, Marie (2018). «Cyber and information warfare in the Ukrainian conflict». *CSS Cyberdefense Hotspot Analyses*, 1: 1-56. DOI: 10.3929/ethz-b-000321570.

Barrio Andrés, Moisés (2018). *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*. Valencia: Tirant Lo Blanch.

Bascur Retamal, Gonzalo y Rodrigo Peña Sepúlveda (2022). «Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la

Ley 21459. Primera parte». *Revista de Estudios de la Justicia*, 37: 1-38. DOI: 10.5354/0718-4735.2022.67885.

—. (2023). «Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21459. Segunda parte». *Revista de Estudios de la Justicia*, 38: 1-27. Disponible en https://tipg.link/mo1W.

Bedecarratz Scholz, Francisco Javier (2016). *Rechtsvergleichende Studien zur Strafbarkeit juristischer Personen. Eine Untersuchung ihrer Strafzurechnungsmerkmale in den Rechtsordnungen von Chile, Deutschland, England, Frankreich, Spanien und den Vereinigten Staaten*. Baden-Baden: Nomos.

—. (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.

—. (2022). *La responsabilidad penal de las personas jurídicas sin fines de lucro*. Valencia: Tirant Lo Blanch.

—. (2023). «El delito de acceso ilícito en el derecho penal chileno». En Christian Scheechler Corona (editor) y Rocío Riveros Saavedra (coordinadora), *Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley 21459* (pp. 101-123). Santiago: Der.

Cámara Arroyo, Sergio (2020). «Estudios criminológicos contemporáneos (IX): La cibercriminología y el perfil del ciberdelincuente». *Revista Derecho y Cambio Social*, 60: 470-512. Disponible en https://tipg.link/mo2e.

Cross, Cassandra y Rosalie Gillett (2020). «Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud». *Journal of Financial Crime*, 27 (3): 871-884. DOI: 10.1108/JFC-02-2020-0026.

De la Cuesta Arzamendi, José Luis y Ana Isabel Pérez Machío (2013). «La responsabilidad penal de las personas jurídicas en el marco europeo: Las directrices comunitarias y su implementación por los Estados». En José Luis de la Cuesta Arzamendi (director) y Norberto J. de la Mata Barranco (coordinador), *Responsabilidad penal de las personas jurídicas* (pp. 129-159). Navarra: Thomson Reuters.

Dopico Gómez-Aller, Jacobo (2014). «Posición de garante del *compliance officer* por infracción del "deber de control": Una aproximación tópica». En Santiago Mir Puig, Mirentxu Corcoy Bidasolo y Víctor Gómez Martín (directores), *Responsabilidad de la empresa y compliance* (pp. 337-363). Buenos Aires: Edisofer.

Engelhart, Marc (2012). *Sanktionierung von Unternehmen und Compliance*. 2.ª ed. Berlín: Duncker & Humblot.

Feijoo Sánchez, Bernardo (2016). *El delito corporativo en el Código Penal español*. 2.ª ed. Pamplona: Civitas.

Fernández Díaz, Carmen (2018). «La amenaza de las nuevas tecnologías en los negocios: El ciberespionaje empresarial». *Revista de Derecho UNED*, 23: 17-57. DOI: 10.5944/rduned.23.2018.24001.

Fernández Teruelo, Javier (2019). «Responsabilidad penal de las personas jurídicas: El contenido de las obligaciones de supervisión, organización, vigilancia y control referidas en el artículo 31 bis 1 b) del Código Penal español». *Revista Electrónica de Ciencia Penal y Criminología*, 21: 1-25. Disponible en https://tipg.link/m056.

Fisse, Brent (1978). «The social policy of corporate criminal responsibility». *Adelaide Law Review*, 6 (3): 361-412. Disponible en https://tipg.link/m05Q.

Fisse, Brent y John Braithwaite (1993). *Corporations, crime and accountability*. Cambridge: Cambridge University Press.

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.

Gómez-Jara Díez, Carlos (2005). *La culpabilidad penal de la empresa*. Madrid: Marcial Pons.

—. (2016). «Fundamentos de la responsabilidad penal de las personas jurídicas». En Miguel Bajo Fernández, Bernardo Feijoo Sánchez y Carlos Gómez-Jara Díez, *Tratado de la responsabilidad penal de las personas jurídicas* (pp. 89-119). 2.ª ed. Pamplona: Civitas.

Gracia Martín, Luis (2016). «Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica». *Revista Electrónica de Ciencia Penal y Criminología*, 18: 1-95. Disponible en https://tipg.link/m05x.

Gutiérrez Peña, Paulina (2023). «La receptación de datos informáticos (artículo 6 de la Ley 21459)». En Christian Scheechler Corona (editor) y Rocío Riveros Saavedra (coordinadora), *Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley 21459* (pp. 195-206). Santiago: Der.

Haase, Adrian (2015). *Computerkriminalität im Europäischen Strafrecht*. Tubinga: Mohr-Siebeck.

Habermas, Jürgen (1992). *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*. Fráncfort: Suhrkamp Verlag.

Harich, Thomas (2021). *IT-Sicherheitsmanagement*. 3.ª ed. Frechen: Mitp.

Heine, Günter (1995). *Die strafrechtliche Verantwortlichkeit von Unternehmen*. Baden-Baden: Nomos.

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.

Lampe, Ernst-Joachim (1994). «Systemunrecht und Unrechtssysteme». *Zeitschrift für die gesamte Strafrechtswissenschaft*, 106: 683-745. DOI: 10.1515/zstw.1994.106.4.683.

Levy, Steven (1984). *Hackers. Heroes of the computer revolution*. Nueva York: Delta.

López Medel, Macarena (2002). «Ley 19233 y su aplicación en los tribunales». En Iñigo De la Maza (coordinador), *Derecho y tecnologías de la información* (pp. 397-

414). Santiago: Fundación Fernando Fueyo Laneri y Escuela de Derecho Universidad Diego Portales.

Mañalich Raffo, Juan Pablo (2011). «Organización delictiva. Bases para su elaboración dogmática en el derecho penal chileno». *Revista Chilena de Derecho*, 38 (2): 279-310. Disponible en https://tipg.link/m07T.

Mayer Lux, Laura (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 Lux, Laura y Ángela Toso Milos (2024). «La facilitación de medios al interior de la empresa para la comisión de un fraude informático: Problemas dogmáticos y relativos al *compliance*». *Revista Chilena de Derecho y Tecnología*, 13: 1-27. DOI: 10.5354/0719-2584.2024.72932.

Mayer Lux, Laura y Guillermo Oliver Calderón (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 Lux, Laura y Jaime Vera Vega (2020). «El delito de espionaje informático: Concepto y delimitación». *Revista Chilena de Derecho y Tecnología*, 9 (2): 221-256. DOI: 10.5354/0719-2584.2020.59236.

—. (2023). *Delitos informáticos y cibercriminalidad. Aspectos sustantivos y procesales*. Buenos Aires: BdeF.

McQuade, Samuel C. (2006). *Understanding and managing cybercrime*. Boston: Pearson.

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

Navarro Dolmestch, Roberto (2023). «El concepto de delito informático según la nueva legislación chilena (Ley 21459)». *Política Criminal*, 18 (36): 666-689. Disponible en https://tipg.link/moEg.

Neira Pena, Ana María (2016). «La efectividad de los *criminal compliance programs* como objeto de prueba en el proceso penal». *Política Criminal*, 11 (22): 467-520. DOI: 10.4067/S0718-33992016000200005.

Nieto Martín, Adán (2008a). *La responsabilidad penal de las personas jurídicas: Un modelo legislativo*. Madrid: Iustel.

—. (2008b). «Responsabilidad social, gobierno corporativo y autorregulación: Sus influencias en el derecho penal de la empresa». *Política Criminal*, 5: 1-18. Disponible en https://tipg.link/moF1.

Oxman Vilches, 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://tipg.link/moG6.

Piña Rochefort, Juan Ignacio (2012). *Modelos de prevención de delitos en la empresa*. Santiago: Legal Publishing.

Riveros Saavedra, Rocío (2023). «Responsabilidad de las personas jurídicas en la nueva Ley 21459 sobre delitos informáticos». En Christian Scheechler Corona (editor) y Rocío Riveros Saavedra (coordinadora), *Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley 21459* (pp. 309-325). Santiago: Der.

Rotsch, Thomas (2013). «Compliance und Strafrecht — Fragen, Bedeutung, Perspektiven. Vorbemerkungen zu einer Theorie der sog. "Criminal Compliance"». *Zeitschrift für die gesamte Strafrechtswissenschaft*, 125: 481-498. DOI: 10.1515/zstw-2013-0024.

Sabillon, Regner, Víctor Cavaller, Jeimy Cano y Jordi Serra-Ruiz (2016). «Cybercriminals, cyberattacks and cybercrime». *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*: 1-9. DOI: 10.1109/ICCCF.2016.7740434.

Schünemann, Bernd (1979). *Unternehmenskriminalität und Strafrecht: eine Untersuchung der Verantwortlichkeit der Unternehmen und ihrer Führungskräfte nach geltendem und geplantem Straf- und Ordnungswidrigkeitenrecht*. Colonia: Carl Heymanns.

Silva Sánchez, Jesús-María (2002). «La responsabilidad penal de las personas jurídicas en el convenio del consejo de Europa sobre cibercriminalidad». *Cuadernos de Derecho Judicial*, 9: 113-142.

—. (2016). «La eximente de "modelos de prevención de delitos". Fundamento y bases para una dogmática». En Silvina Bacigalupo Saggese, Bernardo José Feijoo Sánchez y Juan Ignacio Echano Basaldua (coordinadores), *Estudios de derecho penal* (pp. 669-692). Madrid: Editorial Universitaria Ramón Areces.

Simsa, Ruth (2013). «Gesellschaftliche Restgröße oder treibende Kraft? Soziologische Perspektiven auf NPOs». En Ruth Simsa, Michael Meyer y Christoph Badelt (editores), *Handbuch der nonprofit-organisation. Strukturen und management* (pp. 125-142). 5.ª ed. Stuttgart: Schäffer-Poeschel.

Singelnstein, Tobias (2016). «Ausufernd und fehlplatziert: Der Tatbestand der Datenhehlerei (§ 202d StGB) im System des strafrechtlichen Daten- und Informationsschutzes». *Zeitschrift für Internationale Strafrechtsdogmatik*, 7: 432-439. Disponible en https://tipg.link/m8Lc.

Tassi, Smaro (2017). «Die Einführung der Datenhehlerei. Der gesetzgeberische Akt und seine Peripetie: § 202d StGB». *Datenschutz und Datensicherheit*, 41: 745-749. DOI: 10.1007/s11623-017-0871-3.

Tiedemann, Klaus (1988). «Die Bebußung von Unternehmen nach dem 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität». *Neue Juristische Wochenschrift*, 19: 1169-1174.

Tropina, Tatiana (2012). «The evolving structure of online criminality». *Eucrim*, 4: 158-165. Disponible en https://tipg.link/m8ME.

Van der Wagen, Wytske y Wolter Pieters (2015). «From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks». *The British Journal of Criminology*, 55 (3): 578-595. DOI: 10.1093/bjc/azv009.

Van Weezel, Alex (2010). «Contra la responsabilidad penal de las personas jurídicas». *Política Criminal*, 5 (9): 114-142. DOI: 10.4067/S0718-33992010000100003.

Wehinger, Frank (2011). «The dark net: Self-regulation dynamics of illegal online markets for identities and related services». *European Intelligence and Security Informatics Conference*: 209-213. DOI: 10.1109/EISIC.2011.54.

Werbach, Kevin (2018). «Trust, but verify: Why the blockchain needs the law». *Berkeley Technology Law Journal*, 33: 489-552. DOI: 10.2139/ssrn.2844409.

Sobre el autor

Francisco Javier Bedecarratz Scholz es abogado. Licenciado en Ciencias Jurídicas y Sociales por la Universidad Autónoma de Chile (2009). Magíster (2011) y doctor (2015) en Derecho por la Universidad de Marburgo, Alemania. Profesor asociado de la Facultad de Derecho de la Universidad Autónoma de Chile. Su correo electrónico es francisco.bedecarratz@uautonoma.cl. 0000-0002-0108-7422.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho, Tecnología y Sociedad de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

DIRECTOR
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@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).