REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 12 (2023) • e67546 • DOI 10.5354/0719-2584.2023.67546
RECIBIDO: 20/6/2022 • APROBADO: 17/4/2023 • PUBLICADO: 28/8/2023

DOCTRINA

La autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos

Authorized access to a computer system as an exclusion clause from the definition of the criminal offense of illegal access in the Chilean legislation on cybercrime

Roberto Navarro-Dolmestch
Universidad Católica del Maule, Chile

RESUMEN Este artículo examina el ámbito y aplicación de la cláusula de exclusión de pena regulada en el artículo 16 de la Ley 21.459, sobre delitos informáticos —prevista para el acceso autorizado a un sistema informático en el marco de investigaciones de seguridad— para concluir que ella no es necesaria a la luz de la descripción que la ley chilena hace del delito de acceso ilícito. En tal sentido se sostiene que el artículo 16 tiene, en realidad, un efecto expresivo-integrador sobre la importancia de las investigaciones de seguridad de sistemas informáticos.

PALABRAS CLAVE Acceso ilícito, ciberdelito, acceso autorizado, investigación de seguridad.

ABSTRACT This paper examines the scope and application of the clause of exclusion of penalty passed in article 16 of Act number 21.459 on cybercrime, which regulates authorized access to a computer system in the framework of security research, concluding that it is unnecessary in light of the definition of the criminal offense of illegal access in the Chilean legislation. In that sense, it is concluded that article 16 has, in fact, an expressive-integrating effect on the importance of computer system security research.

KEYWORDS Illegal access, cybercrime, authorized access, security research.

Introducción

El artículo 2 de la Ley 21.459, que «establece normas sobre delitos informáticos, deroga la Ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest» (*Diario Oficial*, 20 de junio de 2022), describe el delito de acceso ilícito, prohibiendo penalmente la entrada a un sistema informático sin autorización o excediendo la que se había concedido al sujeto que ingresa. Paralelamente, el artículo 16 de la Ley sobre delitos informáticos prevé la no punibilidad del acceso a un sistema informático cuando el sujeto activo cuente con la autorización expresa de su titular «en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática». Ambas disposiciones de la nueva ley operan en el ámbito de las exploraciones de la seguridad de tales sistemas. Estos necesitan ser sometidos a pruebas para el descubrimiento de vulnerabilidades de sus mecanismos y, con ello, diseñar remedios para tales fallas *(bugs)*.

Los sistemas informáticos adolecen inevitablemente de vulnerabilidades en su seguridad y muchas de ellas derivan de *bugs* en sus códigos de programación (Bambauer y Day, 2011: 1060). Los riesgos en esta materia que representa, por ejemplo, el crecimiento exponencial de los dispositivos conectados a la red y que conforman la Internet de las Cosas, sugieren que los esfuerzos en investigación requieren ser redoblados; sobre todo si se tienen en cuenta los déficits con los que ha operado la industria en este ámbito (Kilovaty, 2019). Por ello, las leyes que restringen en exceso el estudio de vulnerabilidades de software y hardware son contrarias a la necesidad de aumentar los niveles de seguridad. Una férrea protección de los sistemas informáticos, del software y aun del hardware, puede terminar generando un escenario ideal para un mundo cada vez más inseguro. Sostienen Álvarez-Valenzuela y Hevia Angulo (2020: 2) que: «Las leyes de acceso ilícito sin salvaguardias legales para la investigación y la búsqueda de vulnerabilidades han sido usadas para intentar silenciar la investigación en ciberseguridad»

La explotación de una vulnerabilidad puede conducir a que un software funcione de una forma diferente a la prevista en su diseño original u obtener un acceso no autorizado a un sistema informático.

La hipótesis de este artículo consiste en que la disposición contenida en el artículo 16 de la Ley 21.459 no es necesaria —a la luz del tipo penal de acceso ilícito— para excluir de pena las actividades de búsqueda de vulnerabilidades de seguridad en sistemas informáticos que se hagan con autorización del titular. Porque, en consecuencia, ella solo cumple una función expresivo-integradora respecto de los procedimientos de búsqueda de vulnerabilidades («pruebas de penetración» o simples escaneos). Asimismo, se sostiene que el legislador desperdició una buena oportunidad para prever normas conducentes avanzar en seguridad informática.

Este artículo describe el contexto en el que el artículo 16 está llamado a desenvolverse; analiza los elementos centrales sobre los que se construye la prohibición penal de acceso ilícito y determina su naturaleza como una causal de atipicidad. Desde la premisa que dicho artículo es una causal de atipicidad, se describirá, en primer lugar, su naturaleza; luego, su función expresivo-integradora y las posibilidades perdidas por la adopción del texto en vigor. El artículo finaliza con un apartado de conclusiones.

El contexto: vulnerabilidades y hackers

Los sistemas informáticos, dispositivos personales y objetos de la Internet de las Cosas adolecen de vulnerabilidades de seguridad que son imposibles de evitar, en la medida que sistemas completamente seguros aún no han podido ser diseñados y producidos (Álvarez-Valenzuela y Hevia Angulo, 2020: 1 y 2; Viega, 2009: 139 y ss.; Beale y Berris, 2017: 167 y ss.; 2018: 26 y ss.). A las vulnerabilidades conocidas o previsibles deben agregarse las emergentes y, por tanto, desconocidas e imprevisibles que surgen de los avances tecnológicos y «fruto de la convergencia tecnológica vigente» (Cano, 2021b: 83). En un sistema informático, su vulnerabilidad es «un conjunto de condiciones o conductas que permiten la violación de una política de seguridad explícita o implícita» (Householder y otros, 2017: 2) o «una falla o debilidad en el diseño, implementación u operación y administración de un sistema que podría explotarse para violar la política de seguridad del sistema» (*Internet Security Glossary*, RFC 4949).

Por otro lado, hay personas que con distintas motivaciones y fines, están dispuestas a hacer actividades de explotación de esas vulnerabilidades que caen dentro del concepto genérico de *hacking*. La conjunción entre vulnerabilidad y su explotación configura peligros inminentes para un conjunto extenso de bienes jurídicamente protegidos. Cuando este binomio vulnerabilidad-explotación se concreta en determinadas acciones origina un ciberataque y es muy probable que dé origen a un daño a bienes protegidos. Esto puede significar afectaciones a la vida e integridad física de personas que ocupan servicios o dispositivos[1] controlados u operados por esos sistemas informáticos (Kjaerland, 2006: 523), a la intimidad de quienes tienen registrados sus datos en los sistemas intervenidos (Cunningham, 2012), al patrimonio de los titulares o responsables de dichos sistemas o de sus usuarios o clientes, a la correcta provisión de servicios públicos, a la seguridad nacional (Sabillon, Cavaller y Cano, 2016), etcétera.

1. Solo basta pensar en los dispositivos médicos inalámbricos como implantes cardíacos, bombas de insulina o generadores de pulso neurológicos implantables en el cuerpo del paciente. En el caso de estos, «la comunicación entre el dispositivo y una estación-base o un dispositivo de programación puede interceptarse y, si las señales no están protegidas por protocolos de encriptación o autentificación, un atacante puede recolectar o alterar la información» (Pycroft y Aziz, 2018: 403).

Según Donaldson y otros (2015: 7 y ss.) y Willems (2019: 47 y ss.), los ciberataques pueden dirigirse a una de las funciones que materializan los sistemas informáticos, en la medida que ellos pueden presentarse como afectaciones a la *confidencialidad* (sustracción de información), a la *integridad* (modificación de información almacenada) o a la *disponibilidad* (denegación de servicios), que son los principios básicos de un sistema informático en materia de seguridad (Krutz y Vines, 2007: 3; Sarwar, 2021: 6; Anchugam, 2021: 118; Donaldson y otros, 2015: 10 y 33). Los ciberatacantes, por su parte, pueden actuar por medio de amenazas a los activos (*random malware*, virus, troyanos, gusanos, *botnets*, *ransomware*, etcétera); ser calificados como *hacktivistas* —usan el *hacking* como forma de expresión política o reivindicatoria—(Romagna, 2020); actuar dentro del esquema del crimen organizado; tener finalidades de espionaje o actuar en contextos de ciberguerra.

Sin embargo, dicha conjunción entre vulnerabilidad y explotación no necesariamente debe conducir a la concreción del peligro, esto es, a la producción de un daño. En otras palabras: una intrusión de seguridad[2] no es, siempre y necesariamente, dañina. De hecho, bajo ciertas circunstancias controladas, la explotación de una vulnerabilidad forma parte de los procedimientos necesarios para el aseguramiento de los sistemas informáticos. En términos de prevención de riesgos y del incremento de los estándares de seguridad, los informáticos y las informáticas han desarrollado métodos que operan en dos planos. Uno previo, de evaluación de una vulnerabilidad, que es el proceso de revisión de servicios y sistemas en la búsqueda de potenciales problemas o debilidades. Y un proceso posterior que involucra pruebas de penetración y ataques de conceptos que consisten en la explotación de una vulnerabilidad para comprobar que ella existe (Engebretson, 2013: 2), cuantificar su peligro potencial e identificar las acciones posibles para su corrección.[3] La prueba de penetración *(penetration testing)* es más que un simple escaneo de una vulnerabilidad en el que «se usa un producto automatizado de búsqueda para probar los puertos y servicios en un rango de direcciones IP» (Harper y otros, 2018: 5). Una prueba de penetración es el «intento autorizado de localizar y explotar con éxito los sistemas informáticos» (Engebretson, 2013: 1) y comprende «un conjunto de métodos y procedimientos que tienen como objetivo probar-proteger la seguridad de una organización [y] resultan útiles para encontrar vulnerabilidades en una organización y verificar si un atacante

2. Una intrusión de seguridad se define como «un evento de seguridad, o una combinación de múltiples eventos de seguridad, que constituye un incidente de seguridad en el que un intruso obtiene, o intenta obtener, acceso a un sistema o a un recurso de sistema sin tener autorización para hacerlo» (*Internet Security Glossary*, RFC 4949).

3. Existen disponibles varios modelos de procedimientos de mejoramiento de la seguridad informática. A modo de ejemplo, el Framework for Improving Critical Infrastructure Cybersecurity desarrollado por el National Institute of Standards and Technology (2018); el CyberSecurity Audit Model (CSAM) (Sabillon y otros, 2018); o el propuesto por Donaldson y otros (2015).

podrá explotarlas para obtener acceso no autorizado a un activo» (Baloch, 2015: 3). En una prueba de penetración se obtiene «acceso lógico a datos confidenciales eludiendo las protecciones de un sistema» (*Internet Security Glossary,* RFC 4949) y en ella «se llevan a cabo emulaciones de ataques… [en la que quienes la realizan] usan la perspectiva de un atacante malicioso para ejecutar ataques controlados» (Harper y otros, 2018: 5).

Hay modelos y pautas disponibles, a modo de códigos éticos, para guiar el *hackeo* en el descubrimiento y corrección de vulnerabilidades.[4] También se publican manuales y textos especializados en la materia (Conteh y otros, 2021; Engebretson, 2013; Krutz y Vines, 2007; Wilhelm, 2010; Baloch, 2015; Harper y otros, 2018; Maurushat, 2019; Cano, 2021c); se ofrecen certificaciones para ser un *hacker* ético;[5] y, en Estados Unidos, ser *hacker* se ofrece como una carrera (Wilhelm, 2010: 43 y ss.). En Chile, el Gobierno incentiva el reporte de vulnerabilidades que sean descubiertas en los sistemas y redes que opera la administración del Estado. En la página web del Equipo de Respuesta ante Incidentes de Seguridad Informática, dependiente del Ministerio del Interior y Seguridad Pública, hay dispuesto un formulario electrónico para reportar incidentes;[6] y este mismo organismo informa semanalmente los reportes de vulnerabilidades en sus Boletines de Seguridad Cibernética.[7] Lo mismo hacen empresas que ofrecen recompensas por el descubrimiento y reporte de *bugs* de seguridad en sus sistemas y aplicaciones.[8]

Pruebas de penetración y otras técnicas similares son conductas bien valoradas, en la medida que: a) se desarrollen con fines de exploración y mejoramiento de las condiciones de seguridad de los sistemas informáticos; b) cuenten con el consentimiento del titular del sistema; c) se aplique un procedimiento técnicamente hábil y previamente acordado y d) los resultados de la prueba sean manejados en la forma que se concertó con el titular del sistema evaluado. Dentro de estos límites, tal actividad de *hackeo* de un sistema informático es parte de lo que se denomina *hacking ético* (*ethical hacking*) (Maurushat, 2013: 9). Esta conducta forma parte de los dispositivos y mecanismos que existen para el mejoramiento de la seguridad de los sistemas infor-

4. A modo de ejemplo: Information Systems Security Association (ISSA), Code of ethics. Disponible en https://bit.ly/3Kvssqz. También, International Information Systems Security Certification Consortium (ICS)² Code of ethics. Disponible en https://bit.ly/442DGKN.

5. Por ejemplo, los programas que ofrece International Council of E-Commerce Consultants (EC-Council Group), una empresa certificadora que opera a nivel mundial.

6. Véase https://bit.ly/3P7UA61.

7. Los Boletines están disponibles en https://bit.ly/3QObYoW.

8. Como es el caso de: Google (*Bug Hunters:* https://bit.ly/3YM3ysU), Microsoft (*Microsoft Bug Bounty Program*: https://bit.ly/3XAaicK), Sony (*Playstation Bug Bounty Program*: https://bit.ly/3JBLPOi), el Deutsche Bank (*Responsible Disclosure Process*: https://bit.ly/46FmTzs) o el Banco de Inglaterra (*Vulnerability disclosure policy*: https://bit.ly/3NT7QL7) por nombrar algunas empresas.

máticos (Álvarez-Valenzuela y Hevia Angulo, 2020: 2). Esto es, de la ciberseguridad entendida como «la organización y el conjunto de recursos, procesos y estructuras utilizados para proteger el ciberespacio y los sistemas habilitados en él, de sucesos que desalinean tanto de *jure* como de *facto* los derechos de propiedad» (Craigen, Diakun-Thibault y Purse, 2014: 17). El *hacking* ético puede agregar valor a la función de seguridad y correcto funcionamiento de los sistemas informáticos.

Tales estrategias de descubrimiento, evaluación y corrección de vulnerabilidades implican atacar o acceder a redes y sistemas informáticos; y las herramientas que se utilizan para efectuar estos procedimientos pueden ser las mismas que se usan en ataques maliciosos. De hecho, «cuanto más se acerque la prueba de penetración a un ataque del mundo real, más valor proporcionará al cliente que paga por la prueba de penetración» (Engebretson, 2013: 2 y 3). Una prueba de penetración puede incluir acciones como: los ataques de denegación de servicio (*Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks*); la alteración o destrucción de información; bucear en la basura (*dumpster diving*), esto es, la búsqueda en la información eliminada; la falsificación de direcciones IP (*spoofing of IP addresses*) o la introducción de código malicioso, entre otras acciones. En este sentido, el testeo de los sistemas informáticos es funcionalmente equivalente a las pruebas de choques a que son sometidos los automóviles (Jamil y Ali Khan, 2011: 3758), aunque estos se desarrollan antes de su salida al mercado.

En su inicio, al concepto de *hacker* se le asignó una connotación positiva, como la persona enfocada en desarrollar y mejorar el software para incrementar el desempeño de sistemas de computación. Por simple desconocimiento o estimulado por intereses económicos —con los medios de comunicación y el cine actuando como amplificadores— la actividad de *hacking* se confundió con la del *cracker*, esto es, él o la que usa sus habilidades con propósitos dañinos en contra de sistemas informáticos (Krutz y Vines, 2007: 5).[9] Así, el concepto de *hacking* llegó a estar en el imaginario colectivo asociado a ilicitud y a ser vinculado a conductas que causan daños. Ataques de denegación de servicio, usurpaciones de identidad, *malware*, virus informáticos

9. En el mismo sentido, *cracker*, según Internet Users' Glossary, RFC (1983) es: «un individuo que intenta acceder a los sistemas informáticos sin autorización [y que] a menudo son maliciosos, a diferencia de los *hackers*» (Disponible en https://bit.ly/3QN8RGc). El catálogo, en todo caso, no se agota en los *hackers* y *crackers*. De acuerdo con Krutz y Vines (2007: 5), junto con ellos, se identifican: el *phreaker* —*hacker* que se enfoca en sistemas de comunicación para sustraer números de tarjetas de prepago y hacer llamadas telefónicas sin pagar por ellas—(Alcobero, 2012: 65; Steinmetz, Goe, y Pimentel, 2020: 175; Coleman, 2012: 101); el *whacker* —*hacker* novato que ataca Redes de Área Amplia— (*Wide Area Networks*, WAN) y redes inalámbricas; el *script kiddie* o *skid* —generalmente una persona muy joven que, careciendo de habilidades de programación, usa software de ataque de libre disposición en Internet o conseguido a través de otras fuentes— (Baloch, 2015: 2; Kremling y Parker, 2018: 305; Alexandrou, 2022: 232).

y *phishing*, entre otras, se consideran conductas propias de los *hackers*. Pero, el concepto común de la actividad de *hacking* y la imagen prototípica de un *hacker* han experimentado una nueva evolución (Baloch, 2015: 1; Black, 1993). Fue Steven Levy en 1984 quien asoció la noción de eticidad a la actividad de los *hackers* (Coleman, 2012: 99), rompiendo así la imagen negativa que habían llegado a adquirir, cuando los describió afirmando que:

> Los *hackers* creen que se pueden aprender lecciones esenciales sobre los sistemas —y sobre el mundo— desarmando cosas, viendo cómo ellas funcionan y usando el conocimiento para crear cosas nuevas y aún más interesantes. Les molesta cualquier persona, barrera física o ley que intente evitar que lo hagan (Levy, 2010: 28).[10]

No todos los *hackers* desarrollan actividades para aumentar los niveles de seguridad o la calidad de los sistemas y productos informáticos. De hecho, se distingue entre *black* y *white hackers* (Wilhelm, 2010: 15 y ss.; Kremling y Parker, 2018: 195 y ss.). Los primeros desarrollan ataques no autorizados de acceso a sistemas informáticos, mientras que el *white hacking* consiste en el acceso autorizado previamente por el titular del sistema.

En este punto estimo necesario hacer un inciso sobre el concepto de *hacker* ético. Existen al menos dos concepciones de *ethical hacking*. La primera, de carácter restrictivo, es generalmente empleada en el ámbito comercial de la ciberseguridad. De acuerdo con esta, el *hacking* ético es la actividad de descubrimiento de vulnerabilidades de seguridad de redes y sistemas informáticos que se admite siempre que quien lo desarrolle cuente con el consentimiento previo y expreso del titular de la red o sistema. En este sentido, el *hacker* ético es definido, por ejemplo, como la persona que es «contratada y autorizada por una organización para atacar sus sistemas con el fin de identificar vulnerabilidades, que un atacante podría aprovechar» (Baloch, 2015: 2). De esta forma es la autorización previa del titular o su consentimiento lo que, en esta concepción débil, marca la diferencia entre una actividad de *hacking* permitida de una ilícita (Wilhelm, 2010: 17). En esta primera concepción, el término queda reducido, en realidad, a un prestador de servicios, a un *commodity* (Cano, 2021a) que, previo acuerdo o contrato con el titular de un sistema informático o de una red, realiza la evaluación de su seguridad. Los aspectos «éticos» del *hacking* quedan, en este primer sentido, confinados al cumplimiento de buena fe del contrato y de la sujeción del *hacker* a la *lex artis* informática en la prestación de sus servicios.

Existe una segunda concepción, de mayor amplitud que la primera, que es más afín con la carga axiológica que evoca la referencia a la eticidad en el *hacking* ético.

10. En sentido similar, Internet Users' Glossary, RFC 1983: «Una persona que se deleita con tener una comprensión íntima del funcionamiento interno de un sistema, computadoras y redes informáticas en particular» (Disponible en https://bit.ly/3QN8RGc).

Maurushat adhiere a esta segunda concepción, en la que el *hacking* ético se define no por el acuerdo previo con el titular de un sistema o red, sino por la finalidad o motivación de la persona, grupo u organización que realiza la actividad de *hackeo*. Ella define al *hacking* ético como el «uso no violento de una tecnología en beneficio de una causa, una política o de otro tipo, que a menudo es jurídica y moralmente ambigua» (Maurushat, 2019: 7) e incluye dentro del concepto acciones de desobediencia civil en línea, *hacktivismo*, pruebas de penetración-intrusión y descubrimiento de vulnerabilidades, contraataque-*hackback* y activismo de seguridad. Como puede apreciarse, este concepto amplio de *hacking* ético ofrece interesantes perspectivas de análisis para el derecho penal. Aunque no es posible abordar en detalle el tema en este lugar, creo que, al adoptarse esta concepción amplia surgen varios escenarios en los que la motivación del *hacking* puede hacer operar causas de justificación o de exculpación. Por ejemplo, un ataque a un sistema informático que se haga en la lógica de una participación política no violenta puede ser una conducta que llegue a estar justificada por el ejercicio legítimo de un derecho (libertad de expresión u otros), como quienes interrumpen el tránsito por una calle están amparados por el derecho de reunión. En ambos casos, claro, si nos tomamos en serio el contenido de los derechos fundamentales. También, el sujeto que realiza un acceso no autorizado a un sistema informático, ejecutado con el fin de detectar vulnerabilidades de seguridad y evitar daños futuros, puede alegar como defensa el estado de necesidad. Sin embargo, adoptar este concepto amplio de *hacking* ético tiene un inconveniente: ubica a la actividad de *hacking* ético muy próxima a un estado de cibervigilantismo que puede ser incompatible con el sistema democrático, como la propia autora lo reconoce (Maurushat, 2019: 8). Sobre el concepto y su relación con las tecnologías de la información, véase Galleguillos (2021) y Kosseff (2016).

La autorización y la violación como elementos estructurantes

El objeto de este artículo aconseja, como paso previo, fijar algunas consideraciones en torno al delito de acceso ilícito previsto en el artículo 2 de la nueva ley. Esta cuestión se abordará desde una teorización normológica.

La señalada disposición legal describe la conducta típica de acceso ilícito como la que ejecuta: «El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático». La comprensión del ámbito de esta descripción típica pasa por identificar la prohibición penal que emana de este tipo, esto es, la norma primaria de conducta o norma prohibitiva. Según el tenor literal de la disposición, los contornos que marcan la extensión de la prohibición de acceso son la ausencia de una autorización para ello, el exceso en la utilización de una autorización conferida o quebrantar o sobrepasar las barreras técnicas o medidas tecnológicas de seguridad dispuestas para regular el

ingreso. En consecuencia, la prohibición penal de acceder a un sistema informático prevista en la Ley 21.459 puede reconstruirse interpretativamente sobre la base de dos supuestos normativamente relevantes:

- el déficit de autorización (que cubre los supuestos de ausencia de autorización y exceso de una autorización previamente concedida) y
- la violación de las barreras técnicas.

La definición que ha hecho el legislador es compatible con la existencia de distintos tipos de sistemas informáticos. Por una parte, los sistemas abiertos, aquellos que carecen de barreras técnicas o medidas tecnológicas de seguridad para controlar el ingreso y respecto de los que nunca podría configurarse una conducta típica de acceso ilícito por inexistencia de objeto. En estos debe considerarse la existencia de una autorización general e indeterminada para acceder al sistema informático. Y, por otra parte, los sistemas cerrados, que cuentan con barreras técnicas o medidas tecnológicas de seguridad para discriminar el ingreso.

En síntesis, está prohibido acceder a un sistema informático:

- con un déficit de autorización para ello (careciendo de ella o excediendo una concedida); o
- violando medidas de seguridad dispuestas para regular y discriminar el acceso a él.

Una primera derivación que puede obtenerse de la reconstrucción expuesta es que el déficit de autorización tiene un sentido objetivo. Esto significa que cualquier acceso que se haga sin contar con ella verifica la prohibición. En consecuencia, vale como autorización cualquier expresión de la que ella pueda razonablemente derivarse, no requiriéndose un acto expreso y formal de entrega de una autorización. Por eso quedan fuera de los límites de la prohibición penal, en términos de su ilicitud, los accesos que se hagan con una autorización expresa, perfectamente delimitada y formalmente comunicada, que sería la prototípica. Pero también son lícitos, por quedar fuera de la prohibición, los accesos que se hagan con permisos que muestren niveles inferiores de perfección, siempre que de dichos actos pueda derivarse una autorización, como la entrega de las claves de acceso o de información técnica acerca de puertas de entrada al sistema. El acceso que se haga excediendo la autorización con que efectivamente se contaba es, objetivamente, un caso de ausencia de autorización, una hipótesis que ha sido calificada como «superflua» (Mayer Lux y Vera Vega, 2022: 280).

Una segunda derivación es que: un déficit en la autorización se configura, *a contrario sensu*, ante la ausencia de una expresión que pueda indicar dicha autorización. En consecuencia, el caso en que el sujeto activo accede a un sistema informático creyendo tener una autorización, pero sin contar con ella, verifica objetivamente la prohibición penal de acceder a un sistema informático cerrado; pero tal sujeto activo

actúa adoleciendo de un error de tipo, lo que impide la configuración de su faz subjetiva y, en consecuencia, tampoco verifica la prohibición penal.

Aunque el déficit de autorización y la violación de barreras técnicas como configuradores de la prohibición penal están unidos por la conjunción copulativa «y» en el texto de la ley, la relación entre ellos no es simplemente aditiva. Por el contrario, entre ellos existe una relación de implicación. Esto se demuestra porque, en principio, un acceso autorizado hará innecesaria la violación de los dispositivos de seguridad, como cuando el permiso signifique proporcionar al usuario las herramientas para superar esas barreras técnicas (entrega de claves u otras formas de autentificación). Pero el acceso sin métodos de autentificación proporcionados por el titular no significa, necesariamente, la configuración de una conducta típica, porque puede haber, de todos modos, autorización para el acceso.

De esta forma, cuando el cliente de un banco —usando sus dispositivos de autentificación— accede a información de su cuenta corriente a través de la página web de la institución bancaria está efectuando un acceso lícito. O un usuario de un servicio de correo electrónico que ingresa a él con su clave personal. O un estudiante que ingresa a una plataforma de *e-learning*. En todos estos casos, la conducta queda completamente fuera de los márgenes descritos por el legislador: todos los ejemplos de acceso son conductas atípicas porque no se ha verificado alguno de los dos elementos que requiere el tipo penal. Sin embargo, y en atención a que ambos elementos son copulativos (la ley los une con la conjunción «y»), también es atípico el ingreso a un sistema informático que se haya efectuado superando las barreras técnicas o medidas tecnológicas de seguridad dispuestas por el titular, siempre que el que ingresa lo haga con autorización de este último. Si el titular de un sistema informático olvida o pierde la clave de acceso y contrata a un *hacker* para que ingrese y recupere su acceso al sistema, la conducta del *hacker* es atípica. La razón: aunque el ingreso quebrantó barreras técnicas o medidas tecnológicas de seguridad, el usuario contaba, de todos modos, con autorización del titular para ingresar al sistema informático.

Finalmente, también debe concluirse que el que accede a un sistema informático, pero sin violar medidas de protección, configura una conducta atípica. Lo que podría ocurrir, por ejemplo, cuando las medidas de protección han sido deshabilitadas temporalmente, ya sea por un proceso de mantenimiento del sistema o por una falla que hizo que las barreras dejaran de funcionar adecuadamente.

La evaluación de seguridad en el artículo 16 de la Ley 21.459

Este artículo dispone:

> Para efectos de lo previsto en el artículo 2 se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones

de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.

La conexión lógica y sistemática de esta disposición con la del tipo penal de acceso ilícito del inciso primero del artículo 2 de la misma ley salta a la vista por la remisión de la primera a la segunda: «Para efectos de lo previsto en el artículo 2»; y entonces los ámbitos regulativos de ambas deberían intersecarse. En consecuencia, estimo que es necesario analizar qué tipo de relación puede establecerse entre ambas. En ese sentido, y desde la perspectiva normológica adoptada, la pregunta relevante es si, de alguna manera, la disposición del artículo 16 modifica los contornos de la prohibición que emana del tipo penal de acceso ilícito.

Una primera lectura del artículo 16 indica que esa disposición vendría a constreñir los contornos de la prohibición penal de acceso ilícito, estableciendo supuestos distintos de los contenidos en el artículo 2 que harían que otros casos quedaran fuera del ámbito de la prohibición penal. Esto es, que el artículo 16 agregaría nuevos supuestos de atipicidad para el acceso a un sistema informático, adicionales a los ya previstos en el propio tipo penal. Esos nuevos supuestos serían, *prima facie*: a) que la actuación del que accede se verifique en el «marco de investigaciones de vulnerabilidad» o b) con el objeto de «mejorar la seguridad informática». Con lo dicho —y siempre términos provisionales— el acceso a un sistema informático no verificaría la prohibición del artículo 2 en la medida que se efectuara en uno de los dos casos recién indicados.

Sin embargo, la misma ley prescribe que los supuestos de investigaciones de vulnerabilidad y de mejoramiento de la seguridad informática están sujetos a una condición cuyo cumplimiento determina su operatividad: la autorización expresa del titular del sistema.

Desde una perspectiva formal, la disposición del artículo 16 adolece de un evidente sentido tautológico porque prescribe que debe entenderse que cuenta con autorización. Para los efectos del artículo 2 de la Ley 21.459, el que accede a un sistema informático «mediando la autorización expresa del titular del mismo».

Aunque tanto el tipo penal del artículo 2 como el del artículo 16 se refieren a la autorización del titular para el acceso al sistema informático, es necesario notar, en todo caso, que este último introduce una modificación: en el artículo 16 la autorización debe ser «expresa», exigencia que el legislador no incluye en el tipo penal.

Naturaleza del artículo 16 de la Ley 21.459

El delito de acceso ilícito del artículo 2 tiene similitudes importantes con el delito de violación de morada del artículo 144 del Código Penal chileno. Y es así por dos razones. La primera, porque en ambos delitos la conducta típica está definida como un ingreso: a una morada ajena, en el caso del delito de violación de morada; y a un sis-

tema informático, en el de la Ley 21.459. La segunda, porque en ambos tipos penales la autorización del titular de la morada y del sistema informático, respectivamente, es relevante porque ella ha sido incluida por el legislador en los tipos penales.

Parte de la doctrina más consultada en el ámbito académico y forense chileno no está conteste en el rol que desempeña la autorización del titular de la morada en el delito del artículo 144 del Código Penal. En efecto, Etcheberry Orthusteguy (1999: 257) estima que tal consentimiento configura una causal de justificación que «puede eliminar la antijuridicidad [y] llama la atención del intérprete acerca del hecho de que ordinariamente la entrada en morada ajena no es antijurídica, pues se verifica con la aquiescencia del morador». Por su parte, Garrido Montt (2010: 427) estima que el consentimiento en tal delito actúa como causal de atipicidad, de modo que «si la entrada [en morada ajena] tiene lugar con su consentimiento el hecho carece de tipicidad». Ninguno de los dos autores entrega argumentos para sostener una y otra de las calificaciones que efectúan sobre la naturaleza del consentimiento en el tipo penal en cuestión. Esta ausencia no me parece particularmente relevante, así como tampoco la discrepancia misma. Desde una perspectiva de la aplicación forense del tipo penal y de sus resultados en una sentencia condenatoria, la determinación de la naturaleza debería ser considerada como un problema con poca trascendencia, sobre todo si dicha diferencia tampoco impacta en los efectos sobre la responsabilidad civil que podrían derivarse de un acto que, sin ser penalmente relevante (por ser atípico o por estar justificado), pueda ser considerado un delito o cuasidelito civil que haga surgir responsabilidad civil extracontractual. La cuestión sobre la naturaleza sí tiene importancia desde la perspectiva de comprender sistemáticamente las normas contenidas en la ley de delitos informáticos, razón por la que un esfuerzo al respecto aparece como justificado.

La decisión del legislador de delimitar la prohibición penal con arreglo a la autorización en el acceso por parte del titular del sistema informático significa que el consentimiento juega en ella un rol trascendente. El consentimiento, que es expresión de la autorización, es interno a la prohibición penal misma, es decir, que está incardinado en la definición de los límites de la prohibición penal. Así como en los delitos sexuales el consentimiento de la persona que es accedida carnalmente no constituye una «condición de cancelación de la validez situacional de la norma respectiva» (Mañalich Raffo, 2014: 55), sino que tal acceso consentido «no satisface la descripción que pudiera convertirla en prohibida *sub specie* violación» (Mañalich Raffo, 2014: 56), en el delito de acceso ilícito ocurre lo mismo con el ingreso consentido al sistema informático. En consecuencia, estimo que el consentimiento del titular de un sistema informático para el acceso a él cumple una función de atipicidad en el delito de acceso ilícito.

Sin embargo, de acuerdo con lo expuesto más abajo en el esquema, en el ámbito de las investigaciones de vulnerabilidad y en el de las mejoras de seguridad, regulado en

el artículo 16, el consentimiento tendría un rango de menor aplicación. Quiero decir que, en ese punto, puede sostenerse una interpretación que contradice el esquema, en función de argumentos relacionados con el bien jurídico y con elementos sistemáticos.

Con relación al bien jurídico protegido, este desempeña un papel no solo en la antijuricidad material, sino también —y muy importantemente— en la definición de los contornos de la prohibición penal.[11] La comprensión del bien jurídico estriba en su consideración «designativa de alguna *propiedad* que, en cuanto exhibida por una persona, una cosa, una institución o en general un objeto (*lato sensu*) cualquiera, es valorada positivamente»(Mañalich Raffo, 2021: 136) y cuya finalidad es que «sea evitada la realización de una determinada forma de comportamiento que habría de traer aparejada una merma del valor del respectivo bien jurídico, desde el punto de vista de su titular o de sus beneficiarios» (Mañalich Raffo, 2021: 151). Luego, debe constatarse que los sistemas informáticos están presentes en la vida cotidiana de miles de millones de personas, y a través de ellos se ejecutan interacciones de datos digitales que sirven a innumerables fines (sociales, económicos, gubernamentales, de entretenimiento, etcétera). Sobre la base de esas premisas, estimo adecuada la propuesta de Mayer Lux en orden a que lo protegido por los delitos informáticos[12] es la «funcionalidad informática» (2017: 248-255) que se expresa en tres variables: confidencialidad, integridad y disponibilidad[13] (Mayer Lux, 2017: 251) de los datos que se almacenan,

11. Sobre la base del contenido del bien jurídico puede decidirse sobre la tipicidad o atipicidad de casos, según si ellos infringen o no la prohibición penal, ya que tal contenido concurre, junto con otros elementos, a delimitar la prohibición. En el ámbito de la antijuricidad, en cambio, el bien jurídico ayuda a determinar si una conducta previamente calificada como típica (esto es, que ha verificado la prohibición penal) justifica o no la aplicación a ese caso de la norma de sanción prevista para la infracción de la norma prohibitiva.

12. La identificación del bien jurídico en los delitos informáticos no se ha caracterizado por el consenso. Al respecto, Mayer Lux (2017: 239-248) ha efectuado una muy ilustrativa síntesis de las discusiones que se han suscitado en la dogmática sobre él o los bienes jurídicos protegidos.

13. Un sistema informático puede estar diseñado para la completa confidencialidad de los datos que forman parte de él o, al contrario, puede estar estructurado para que todos sus datos sean accesibles y públicos. La integridad se refiere a si el sistema permite que los datos sean modificados, borrados o sustituidos por sus usuarios o si está hecho para procurar la indemnidad completa de ellos, es decir, su inalterabilidad.La idoneidad se refiere a las posibilidades de acceder a los datos de un sistema informático en niveles que van desde la disponibilidad completa, media, limitada hasta la ausencia de disponibilidad, ya sea en cuanto a los datos mismos o en una dimensión temporal (siempre, algunos días, algunas horas, etcétera). Así, los servicios web de un banco son típicamente de alto nivel de confidencialidad (solo el titular de la cuenta bancaria puede conocer sus datos), de alto nivel de integridad (los registros se refieren a haberes o deberes que el cliente registra en sus productos bancarios) y de completa disponibilidad (los servicios de *web-banking* u *on-line banking*, que pretenden sustituir los modos tradicionales de atención, solo serán atractivos para los clientes en la medida que estén siempre disponibles, todos los días del año y a toda hora). Una red social, en cambio, tiene un espectro más reducido en lo que se refiere a confidencialidad porque los datos del titular de la cuenta son, por regla general, públicos (o, al

procesan, consultan e interactúan en un sistema informático y se transmiten cuando ellos trabajan interconectadamente a través de internet o de otras redes de datos. El concreto rendimiento de tales aspectos puede ser medido según tres baremos: efectividad, eficiencia e idoneidad (o eficacia).[14] Luego, el desempeño de un sistema informático puede ser más o menos efectivo, eficiente e idóneo en verificar la confidencialidad, la integridad y la disponibilidad definidas para un sistema en concreto.

Cada sistema informático ha sido diseñado con una determinada configuración de confidencialidad, integridad y disponibilidad y con determinados niveles de efectividad, eficiencia e idoneidad. La ciberseguridad pretende que esas configuraciones permanezcan inalteradas, esto es, pretende la indemnidad del sistema informático. La configuración determinada de este se define con relación a la naturaleza de los servicios que vaya a prestar, el tipo de datos que va a procesar, las condiciones de mercado y los costes involucrados. Tal configuración, globalmente comprendida, es la funcionalidad informática y lo que protege el derecho penal es su indemnidad, que opera como un presupuesto para que el sistema desarrolle sus actividades (Mayer Lux, 2017: 250 y 251).[15]

---

menos, los que el titular decida hacer públicos). Tales datos siempre pueden ser cambiados por el titular, por lo que la integridad no se presenta en niveles elevados; y, al igual que en los servicios web del banco, las redes sociales operan con la lógica de una disponibilidad permanente.

14. La propuesta de Mayer Lux se refiere solo a dos parámetros: eficiencia y eficacia (2017: 251). Por otra parte, la efectividad se refiere a la capacidad neta del sistema informático de ejecutar los niveles de confidencialidad, integridad y disponibilidad definidos para él. La eficiencia, se refiere a la cantidad de recursos necesarios para desarrollar los niveles definidos de los tres aspectos fundamentales, donde menos recursos es mayor eficiencia. Y la idoneidad, a la aptitud de cada unidad de recurso aplicada para conseguir los niveles definidos en esos tres aspectos básicos.

15. A juicio de Mayer Lux «todas las actividades que se desarrollan a través de la informática requieren que los sistemas informáticos operen de manera correcta» (2017: 250). No estoy de acuerdo con esta posición porque considero que exigir que los sistemas informáticos funcionen de manera correcta es un extremo que no condice con la realidad. En primer lugar, porque no existen sistemas informáticos libres de errores que hacen que no funcionen de manera correcta. Los sistemas informáticos se componen de millones de líneas de códigos escritas por seres humanos, de modo que un error siempre es esperable. Por el contrario, creo que es preferible operar con la idea de que el sistema informático opere en la forma en la que fue diseñado, con sus aciertos y errores; y que el derecho penal lo que hace es proteger esa forma específica, con tales errores y aciertos. Podría sostenerse que, con esta visión, llegaríamos al extremo de sostener que se protege penalmente incluso un sistema informático tan erróneamente diseñado u operado que hasta una persona sin conocimientos especiales pueda acceder a él. La adopción del criterio de la indemnidad no permite llegar hasta tan lejos. Los sistemas completamente deficientes no necesariamente están protegidos en atención a la propia estructura del tipo penal: si a un sistema puede accederse escribiendo una clave cualquiera porque, en realidad, carece de sistemas de autentificación idóneos, quien ingresa de esa forma puede alegar como defensa que su acceso no ha superado barreras técnicas o medidas tecnológicas de seguridad porque ellas eran inexistentes.

Mayer Lux (2017: 253) también destaca el carácter instrumental de la funcionalidad informática como bien jurídico, en la medida que su protección se justifica pues mediante ella se busca disminuir el riesgo para la afectación de otros bienes jurídicos tales como: la vida o la integridad física de usuarios de aparatos médicos conectados a un sistema informático, la intimidad de los titulares de los datos almacenados o la propiedad de quienes realizan transacciones financieras en uno de ellos. Atendido este carácter instrumental, si el ataque a la funcionalidad informática de un sistema produce, adicionalmente, puesta en peligro o lesión de otros bienes jurídicos; la conducta será, a la vez, típica del delito de acceso ilícito y de las otras figuras concurrentes en régimen de concurso real, sin que sea posible apreciar un concurso aparente.

La propia naturaleza de la funcionalidad informática hace que a su ejercicio como bien jurídico pueda asignársele un carácter disponible.[16] Esto justifica, nuevamente, la consideración de la autorización del titular para el acceso a un sistema informático como un límite interno de la prohibición penal de acceso ilícito. Pero, a su vez, plantea un problema: ¿cómo conciliar el carácter interno que el consentimiento tiene en la prohibición, con la reducción que parece contener el artículo 16 a solo el consentimiento expreso? El problema adquiere especial connotación a la luz del bien jurídico: las acciones de investigación de vulnerabilidad y de mejoramiento de la seguridad informática a que se refiere la citada disposición son completamente simétricos con la funcionalidad informática.

Como ilustrativamente afirmó Daniel Álvarez en la discusión parlamentaria:

> Muchas de las acciones que realiza un investigador de seguridad cumplen con los requisitos del tipo, al intentar descubrir la brecha o vulnerabilidad de la red e identificar al responsable. Por lo mismo, cabría incluir una causal de exención de responsabilidad penal para quien, en el ejercicio de una labor investigativa privada, descubre una vulnerabilidad y la reporta inmediatamente al responsable del sistema para adoptar las medidas técnicas de resguardo de la información comprometida, con arreglo a cierto estándar (Senado de Chile, 2019: 25).

La realidad muestra que no solo los expertos contratados para hallar vulnerabilidades pueden encontrarlas. Supuesto un nivel avanzado de conocimiento y habilidades informáticas, o incluso, niveles iniciales (como el caso de los *script kiddies* o *skids)*,[17] el

16. Se trata de la disponibilidad de las condiciones materiales que emanan del bien jurídico protegido y no del bien mismo. Si un banco decide rebajar el presupuesto en ciberseguridad, lo que está haciendo es renunciando a parte de la protección que dicha inversión le otorgaría. En la práctica, el sistema informático de ese banco va a tener inferiores niveles de ciberseguridad que antes del recorte presupuestario, lo que puede generar reclamos de sus clientes; pero tales reclamaciones configuran un conflicto jurídico diferente. El banco no ha renunciado a la jurídicamente protegida funcionalidad informática como bien jurídico, sino a su ejercicio concreto. La distinción en Ackermann Hormazábal y Ovalle Donoso (2018: 55).

17. Véase nota al pie número 9.

hallazgo de una vulnerabilidad y su explotación pueden efectuarse en muchos otros escenarios distintos de la investigación. Estos pueden ser, a modo ejemplar, desde hallazgos casuales, los efectuados en actividades de *hacktivismo,*[18] hasta los realizados en operaciones con una intencionalidad maliciosa.[19] También el de un investigador contratado expresamente, pero que descubre fallas de seguridad en otra parte del sistema informático diferente de aquel para el que se requirieron sus servicios.

La compatibilidad de la investigación de vulnerabilidad y el mejoramiento de la seguridad con la preservación del bien jurídico es evidente, y podría sostenerse que ellas son conductas que deberían quedar fuera del ámbito de la prohibición penal (atípicas), requiriéndose a su respecto solamente autorización, y no autorización expresa. Sin embargo, esta interpretación choca con el tenor literal de la disposición del artículo 16 de la Ley 21.459, cuya configuración requiere la señalada autorización expresa.

La reconstrucción de la prohibición penal propuesta debería ser complementada con el material normativo aportado por el artículo 16, bajo la premisa de la exigencia de la autorización expresa, como vemos en el siguiente esquema de reformulación de la prohibición penal de acceso a un sistema informático.

Está prohibido acceder a un sistema informático:

- con un déficit de autorización, que puede ser

  i) expresa, si el acceso es en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, o

  ii) aun implícita (careciendo de ella o excediendo una concedida), en los demás casos; o violando medidas de seguridad dispuestas para regular y discriminar el acceso a él.

Aplicado este esquema a casos de prueba, debería concluirse: a) que verifica la prohibición penal, afirmándose la tipicidad de la conducta, quien ejecuta un test de penetración para detectar fallas de seguridad, pero que lo hace careciendo de una autorización *expresa* para ello de parte de titular del sistema informático, aun cuando se comporte de acuerdo con la *lex artis* del *hacking* y demuestre un fuerte compromiso

18. Como el caso supuesto de un grupo que aboga por el mejoramiento de la sanidad pública y, en ese contexto, ejecuta una actividad de *graffiti* en la página web del servicio de salud. Pero en esa labor, descubre una puerta informática para acceder a la base de datos de los usuarios del sistema que contiene información sobre la salud de esas personas, es decir, datos sensibles protegidos por el derecho a la intimidad. El *graffiti* es un ataque común de organizaciones con motivaciones políticas y ciberactivistas, e implica desfigurar las páginas web de las víctimas para hacer declaraciones políticas o ideológicas (Donaldson y otros, 2015: 294).

19. Como el de un *cracker* que, para obtener el listado de correos electrónicos de los ejecutivos de una empresa, accede a uno de sus sistemas informáticos, pero descubre vulnerabilidades en otros que comprometen derechos de terceros o aspectos patrimoniales de la misma empresa, razón por la que decide abstenerse de seguir hurgando y notifica la vulnerabilidad al titular.

con estándares éticos (por ejemplo, avisa reservadamente de la falla al titular del sistema informático, no condiciona el descubrimiento del hallazgo a una recompensa, etcétera); b) que, en cambio, no incurre en la prohibición el que descubre fallas en virtud de autorizaciones otorgadas por el titular de un sistema informático en forma general e indeterminada, pero expresa, en el contexto de programas definidos por el titular, recompensados o no, de detección de vulnerabilidades[20] ; o c) el que habiendo olvidado las claves de acceso a un sistema, recurre a un *hacker* para la reposición de sus credenciales de acceso.

La diferencia entre los dos primeros casos radica en que en a), por la labor de investigación que desarrolla, la ley le exige contar con una autorización expresa con la que sí cuenta b); mientras que en c), por no estar desarrollando dicha función, sino solo recuperando un acceso perdido, dicha exigencia no le es aplicable y para él vale la autorización original conferida cuando se le entregaron las claves extraviadas. Planteado así, la disposición del artículo 16 de estaría lejos de constreñir la prohibición penal; en cambio, estaría ampliándola.

En síntesis, el acceso a un sistema informático es atípico si se cuenta con autorización para el ingreso a él, aun en formas imperfectas o implícitas; salvo en el caso de las acciones de investigación de vulnerabilidad o de mejoramiento de la seguridad informática. En estas, la conducta es atípica solo si el sujeto activo del ingreso cuenta con una autorización expresa del titular del sistema informático. La definición por el legislador de los límites de la prohibición penal muestra que tales casos se encuentran fuera de ella, en la zona de conductas penalmente lícitas.

Sin embargo, el acceso para investigación de vulnerabilidad o de mejoramiento de la seguridad informática sigue siendo una conducta que no necesariamente justificaría la aplicación de la norma de sanción; como en los casos en los que la conducta de quien detecta una vulnerabilidad y la explota, pero se abstiene de cualquier conducta maliciosa adicional y notifica su descubrimiento al titular; o si el hallazgo notificado al titular evitó daños futuros, como si la vulnerabilidad hubiera llegado a ser explotada por un *cracker*. La respuesta para este tipo de casos está en la no activación de la norma de sanción, y su fundamento está a mi juicio en el ámbito de la antijuricidad, ya sea porque se excluye la antijuricidad material o se configura una causa de justificación como el estado de necesidad o el ejercicio legítimo de una profesión u oficio.

Función del artículo 16 de la Ley 21.459

Como se ha sostenido, la autorización del titular de un sistema informático en tanto causa de atipicidad presenta una doble regulación (en el artículo 2 y en el artículo 16). En otras palabras, ambas disposiciones se intersecan parcialmente; y, de hecho, la disposición del artículo 16 amplía los márgenes de la prohibición penal.

20. Véase nota al pie número 8.

Sin perjuicio de los problemas que plantea el artículo 16, estimo que esta disposición presta una utilidad: cumple una función expresivo-integradora, extendiendo a esta materia la conceptualización propuesta por Díez Ripollés (2003: 151).[21] En este enfoque, la finalidad del artículo 16 es motivar en los destinatarios de la prohibición de acceso a un sistema informático una actitud positiva frente a los test de penetración —en tanto actividades de investigación sobre la seguridad de los sistemas informáticos— y, a la vez, generar en ellos una valoración positiva, en el sentido de licitud, de estas estrategias y técnicas para el incremento de los estándares de seguridad.

En otras palabras, que junto con el reconocimiento de la ley de que no existen sistemas informáticos completamente seguros (de ahí el sentido de prohibir penalmente su acceso no autorizado), el legislador también reconoce la importancia de los testeos de seguridad, como una estrategia de mejoramiento de tal seguridad. El testeo de la idoneidad de las barreras técnicas y de las medidas de seguridad es una labor del todo compatible con el bien jurídico protegido por los delitos previstos en la Ley de delitos informáticos, esto es, de la funcionalidad informática, como lo ha propuesto Mayer Lux, entre otros. En este caso, la protección de la funcionalidad informática de los sistemas se hace no a través de la prohibición penal de conductas que la afectan, sino de conductas que contribuyen a robustecerlo. Asimismo, esta norma busca instalar la ciberseguridad como un tema permanente en la cultura organizacional de empresas y organismos titulares de sistemas informáticos; también quiere contribuir a generar un estado de «resiliencia digital» que tienda a la anticipación de disrupciones, resistencia de interrupciones, recuperación posterior a un ataque, aprendizaje de los riesgos y por último, a la adaptación y modificación de las capacidades vigentes (Cano, 2021d: 5).

21. El concepto de función expresivo-integradora es desarrollado por su autor con relación a los efectos y función que se espera cumpla la pena estatal. Sin embargo, desde una perspectiva normológica, como a la que aquí se adhiere, nada obsta a extender dicho concepto a la prohibición penal. Los criterios de justificación de la potestad punitiva se han construido, principalmente, enfocados en la legitimación de la pena; pero ese esquema ha obviado la pregunta por la justificación de la prohibición penal. Si del tipo penal emanan dos normas (la primaria de conducta, con un carácter prohibitivo; y la secundaria, de sanción para aquellos que verifiquen la primera), debe reconocerse que entre ellas existe una relación íntima que justifica aplicarle a la primera el aparado justificador de la segunda. La relevancia de la vida no solo se logra mostrar a la sociedad a través de la pena con la que se amenaza matar a otra persona; ese cometido también se logra indicando el valor que se le asigna a la vida por medio de la prohibición de matar a otro. Al respecto, véase Navarro-Dolmestch (2022: 171). Asimismo, tampoco puede establecerse una separación radical que impida extender la conceptualización de Díez Ripollés a la prohibición penal porque, como el propio autor lo plantea, ella es una forma alternativa de comprender el fenómeno de la utilización simbólica del Derecho. Esta última no solo se relaciona con la pena, sino con todas las decisiones de política criminal. Al respecto, véase, por ejemplo, Díaz Pita y Faraldo-Cabana (2002).

La oportunidad perdida

En el mensaje con el que se inició la discusión de la actual Ley 21.459 (Boletín 12192-25) no se preveía disposición alguna sobre la permisión de actividades de investigación de seguridad de los sistemas informáticos. El artículo 16 de este cuerpo legal adquirió su forma, con la que finalmente fue aprobado y entró en vigor, en el primer trámite constitucional ante el Senado.

En segundo trámite constitucional, la Cámara de Diputados y Diputadas aprobó el siguiente artículo 16:

> Artículo 16. Investigación Académica. En el caso del delito previsto en el inciso primero del artículo 2, y sin que haya mediado actuación policial, judicial o del Ministerio Público de ninguna especie, constituirá eximente de responsabilidad penal el hecho que el partícipe, en el contexto de una investigación académica de seguridad informática previamente registrada, reporte el acceso y la vulnerabilidad informática detectada al responsable del sistema informático y, en todo caso, a la autoridad competente, de manera inmediata. Lo anterior se entenderá sin perjuicio de la responsabilidad civil o administrativa que corresponda por la conducta descrita.
>
> Un reglamento dictado por el Ministerio del Interior y Seguridad Pública determinará los requisitos para acceder al registro a que hace referencia el inciso anterior y la forma en que se deberá realizar el reporte respectivo.

Sin embargo, en tercer trámite constitucional esta propuesta se rechazó. Finalmente, en comisión mixta, se optó por mantener la propuesta original del Senado y el artículo 16 adquirió su actual fisonomía como texto legal en vigor.

El análisis de la historia de la Ley sobre delitos informáticos permite, al menos, dos reflexiones interesantes.

La primera, que fue el aporte de expertos en el área informática el que permitió que la ley comprendiera una norma como su actual artículo 16. La inquietud por incluir una regulación como esta no surgió ni de los parlamentarios ni del Gobierno, sino de expertos, tal como puede leerse en las actas de las discusiones parlamentarias. Y, aunque debe reconocerse que su importancia fue comprendida por los legisladores, ella no estuvo exenta de reticencias.

La segunda reflexión es que el legislador perdió una buena oportunidad para incorporar una regulación administrativa que podría sentar bases para el desarrollo de un mercado de aseguramiento informático, con controles como un registro público de prestadores y estándares de *due diligence* en la realización de estas funciones como: plazos para notificar al titular de una vulnerabilidad descubierta o el nivel de reserva exigible a quien efectuara el hallazgo. De hecho, en la tramitación parlamentaria, expertos defendieron la propuesta de contenido del artículo 16 —que se formuló en segundo trámite constitucional ante la Cámara de Diputados y Diputadas— cuando se afirmó que:

> La enmienda efectuada por la Cámara de Diputados, captura bastante bien la necesidad de permitir el desarrollo de la seguridad informática como se ha hecho hasta ahora en Chile y en todas partes del mundo, en tanto involucra a investigadores de la academia como profesionales y empresas privadas, por lo que hizo hincapié en que no sea coartado por una legislación demasiado agresiva (Alejandro Hevia, en Senado de Chile 2021: 20).

Conclusiones

En atención a la imposibilidad de diseñar y operar sistemas informáticos completamente seguros, el legislador ha previsto una prohibición penal de acceder a tales sistemas sin autorización de su titular. En consecuencia, la autorización del titular de un sistema informático actúa, en la Ley 21.459, como una causal de atipicidad.

Asimismo, consciente de la necesidad del mejoramiento continuo en materia de seguridad informática, la ley ha previsto la exclusión de pena, a título de atipicidad, para quienes efectúen hallazgos de vulnerabilidades y los exploten. La atipicidad, en este caso, queda subordinada a la autorización expresa del titular del sistema informático. Por lo tanto, los accesos no permitidos expresamente, pero efectuados para producir un mejoramiento del estándar de seguridad de un sistema informático podrían quedar comprendidos dentro del ámbito de causales de justificación generales, como el estado de necesidad o el ejercicio legítimo de una profesión u oficio.

El legislador ha pretendido ubicar esa regulación en una disposición especial de la Ley sobre delitos informáticos: su artículo 16. Sin embargo, dicha regulación no es, en estricto rigor, necesaria para concluir en la atipicidad de la conducta de investigación de *bugs* de seguridad. Para tal efecto, basta con el propio tipo penal del artículo 2, que contiene el requisito de la autorización previa. En virtud de esta disposición, cualquier acceso autorizado no es típico del delito de acceso ilícito, ya sea que él se produzca en el marco de una investigación de seguridad, en un proceso de mejoramiento de esta, por motivos causales o, incluso, con una motivación maliciosa.

Aunque existe una evidente superposición parcial de la autorización como elemento negativo del tipo penal de acceso ilícito y como supuesto de hecho de la causal de atipicidad en el artículo 16, esta última no es, por ello, prescindible. Esta disposición puede llegar a cumplir una importante función expresivo-integradora sobre la trascendencia de la seguridad de los sistemas informáticos e, incluso, como fuente de un deber general de solidaridad con el bien jurídico protegido por los delitos previstos en la Ley 21.459.

Referencias

Ackerman Hormazábal, Ignacio y María Fernanda Ovalle Donoso (2018). «La disponibilidad en los bienes jurídicos». *Revista de Ciencias Sociales* (Universidad de Valparaíso), 72: 39-61.

Alcobero, Ramón (2012). «Estudio de la ética hacker. Ética aplicada en Internet». *Comunicación*, 159-160: 61-67.

Alexandrou, Alex (2022). *Cybercrime and information technology. Theory and practice: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices*. Boca Raton: CRC Press.

Álvarez-Valenzuela, Daniel y Alejandro Hevia Angulo (2020). «Protección legal para la búsqueda y la notificación de vulnerabilidades de ciberseguridad en Chile». *Revista Chilena de Derecho y Tecnología,* 9 (2): 1-4.

Anchugam, C. V. (2021). «Essential security elements and phases of hacking attacks». En Nabie Y. Conteh (editor), *Ethical hacking techniques and countermeasures for cybercrime prevention*, (pp. 114-143). Hershey: IGI Global.

Baloch, Rafay (2015). *Ethical hacking and penetration test guide*. Boca Raton: CRC Press.

Bambauer, Derek y Oliver Day (2011). «The hacker's aegis». *Emory Law Journal*, 60 (5): 1051-1108.

Beale, Sara Sun y Peter Berris (2017). «Hacking the Internet of Things: Vulnerabilities, dangers, and legal responses». *Duke Law & Technology Review*, 16 (1): 21-40.

—. (2018). «Hacking the Internet of Things: Vulnerabilities, dangers, and legal responses». En Eric Hilgendorf y Jochen Feldle (editores), *Digitization and the Law* (pp. 21-40). Baden-Baden: Nomos.

Black, Deirdre (1993). «The Computer Hacker: Electronic Vandal or Scout of the Networks?». *Journal of Law, Information and Science*, 1: 65-79.

Cano, Jeimy (2021a). «Desinstalando los fundamentos del "hacking ético". De los "equipos tigre" al flujo de permisos y los espacios de conversación no técnicos». *Global Strategy Report*, 11.

—. (2021b). «La "falsa sensación de seguridad"». *Sistemas*, 159: 82-95.

—. (2021c). «Modelos formales de seguridad y control. Una reflexión no convencional de estrategias y prácticas probadas para un contexto digital». *Global Strategy Report*, 19.

—. (2021d). «Resiliencia digital: más allá de la continuidad del negocio». *Sistemas*, 159: 4-7.

Coleman, E. Gabriella (2012). «Phreaks, Hackers, and Trolls. The politics of transgression and spectacle». En Michael Mandiberg (editor), *The social media reader*, (pp. 99-119). Nueva York: New York University Press.

Conteh, Nabie Y., Paul J. Schmick, Malcolm D. Royer, Anjelica B. Jackson, Sara A. Syed, Alicia Leslie-Jones, Alusine Jalloh, Sahar A. El-Rahman, Quinnesha N. Staton y DeAngela "Dee" Sword (2021). *Ethical hacking. Techniques and countermeasures for cybercrime prevention*. Hershey: IGI Global.

Craigen, Dan, Nadia Diakun-Thibault y Randy Purse (2014). «Defining cybersecurity». *Technology Innovation Management Review*, 4 (10): 13-21.

Cunningham, McKay (2012). «Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law». *George Washington International Law Review*, 44 (4): 643-696.

Díaz Pita, María del Mar y Patricia Faraldo-Cabana (2002). «La utilización simbólica del derecho penal en las reformas del código penal de 1995». *Revista de Derecho y Proceso Penal*, 7: 119-152.

Díez Ripollés, José Luis (2003). «El Derecho penal simbólico y los efectos de la pena». En Luis Arroyo Zapatero, Ulfrid Neumann y Adán Nieto Marín (editores), *Crítica y justificación del Derecho penal en el cambio de siglo* (pp. 147-172). Cuenca: Ediciones de la Universidad de Castilla-La Mancha.

Donaldson, Scott E., Stanley G. Siegel, Chris K. Williams y Abdul Aslam (2015). *Enterprise cybersecurity. How to build a successfull cyberdefense program against advanced threats*. Nueva York: Apress.

Engebretson, Patrick (2013). *The basics of hacking and penetration testing. Ethical hacking and penetration testing made easy*. 2.ª ed. Waltham: Syngress.

Etcheberry Orthusteguy, Alfredo (1999). *Derecho Penal. Parte especial. Tomo 3*. 3.ª ed. Santiago: Jurídica de Chile.

Galleguillos, Sebastián (2021). «Digilantism, discrimination, and punitive attitudes: A digital vigilantism model». *Crime, Media, Culture: An international journal,* 18 (3). DOI: 10.1177/17416590211017937.

Garrido Montt, Mario (2010). *Derecho Penal. Parte especial. Tomo 3*. 4.ª ed. Santiago: Jurídica de Chile.

Harper, Allan, Daniel Ragalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martínez, Michael Baucom, Chris Eagle y Shon Harris (2018). *Gray hat hacking. The ethical hacker's handbook*. 5.ª ed. Nueva York: McGraw-Hill Education.

Householder, Allen C., Garret Wassermann, Art Manion y Chris King (2017). «The CERT Guide to Coordinated Vulnerability Disclosure». *Software Engineering Institute* (Carnegie Mellon University). Disponible en https://bit.ly/3CSCaz5.

Jamil, Danish y Muhammad Numan Ali Khan (2011). «Is ethical hacking ethical?» *International Journal of Engineering Science and Technology*, 3 (5): 3758-3763.

Kilovaty, Ido (2019). «Freedom to hack». *Ohio State Law Journal*, 80 (3): 455-520.

Kjaerland, Maria (2006). «A taxonomy and comparison of computer security incidents from the commercial and government sectors». *Computers and Security*, 25 (7): 522-538.

Kosseff, Jeff (2016). «The hazards of cyber-vigilantism». *Computer Law & Security Review*, 32 (4): 642-649.

Kremling, Janine y Amanda M. Sharp Parker (2018). *Cyberspace, cybersecurity, and cybercrime*. Thousand Oaks: Sage.

Krutz, Ronald L. y Russell Dean Vines (2007). *The CEH prep guide. The comprehensive guide to certified ethical hacking*. Indianapolis: Wiley Publishing.

Levy, Steven (2010). *Hackers. Heroes of the computer revolution*. Sebastopol, CA: O'Reilly.

Mañalich Raffo, Juan (2014). «La violación como delito contra la indemnidad sexual bajo el derecho penal chileno. Una reconstrucción desde la teoría de las normas». *Ius et Praxis*, 20 (2): 21-70.

—. (2021). «Los delitos contra la salud pública en situación de pandemia como delitos de peligro abstracto contra la salud individual. Una propuesta de interpretación de los artículos 318, 318 bis y 318 ter del Código Penal». En Fernando Londoño Martínez, Francisco Maldonado Fuentes y Juan Mañalich Raffo (editores), *Los delitos contra la salud pública durante la pandemia* (pp. 128-237). Santiago: Thomson Reuters.

Maurushat, Alana (2013). *Disclosure of security vulnerabilities. Legal and ethical issues*. London: Springer.

—. (2019). *Ethical hacking*. Ottawa: University of Ottawa Press.

Mayer Lux, Laura (2017). «El bien jurídico protegido en los delitos informáticos». *Revista Chilena de Derecho*, 44 (1): 235-260.

Mayer Lux, Laura y Jaime Vera Vega (2022). «La nueva ley de delitos informáticos». *Revista de Ciencias Penales*, 48 (3): 267-336.

National Institute of Standards and Technology, USA (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. (Versión 1.1). Disponible en https://bit.ly/43beYXn.

Navarro-Dolmestch, Roberto (2022). *Legalidad penal como limitación al poder punitivo*. Madrid: Reus.

Pycroft, Laurie y Tipu Z Aziz (2018). «Security of implantable medical devices with wireless connections: The dangers of cyber-attacks». *Expert Review of Medical Devices*, 15 (6): 403-406.

Romagna, Marco (2020). «Hacktivism: Conceptualization, techniques, and historical view». En Thomas J. Holt y Adam M. Bossler (editores), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 743-769). Cham: Palgrave Macmillan.

Sabillon, Regner, Victor Cavaller y Jeimy Cano (2016). «National Cyber Security Strategies: Global Trends in Cyberspace». *International Journal of Computer Science and Software Engineering*, 5 (5): 67-81.

Sabillon, Regner, Jordi Serra-Ruiz, Victor Cavaller y Jeimy Cano (2018). «A comprehensive cybersecurity audit model to improve cybersecurity assurance: The Cybersecurity Audit Model» (CSAM). *Proceedings 2017 International Conference on Information Systems and Computer Science*, INCISCOS. DOI: 10.1109/INCISCOS.2017.20.

Sarwar, Fahad Ali (2021). *Python ethical hacking from scratch*. Birmingham: Packt Publishing.

Senado de Chile (2019). «Primer Informe de la Comisión de Seguridad Pública, Primer trámite constitucional» (Senado). Mensaje Boletín número 12.192-25. Disponible en https://bit.ly/45ahbUz.

—. (2021). «Primer informe de la Comisión de Seguridad Pública, Tercer trámite constitucional» (Senado). Mensaje Boletín número 12.192-25. Disponible en https://bit.ly/3OiddCx.

Steinmetz, Kevin, Richard Goe y Alexandra Pimentel (2020). «On social engineering». En Rutger Leukfeldt y Thomas J. Holt (editores), *The human factor of cybercrime* (pp. 173-193). Oxon: Routledge.

Viega, John (2009). *The myths of security. What the computer security industry doesn't want you to know.* Sebastopol CA: O'Reilly.

Wilhelm, Thomas (2010). *Professional penetration testing. Creating and operating a formal hacking lab*. Oxford: Syngress.

Willems, Eddy (2019). *Cyberdanger. Understanding and guarding against cybercrime*. Cham: Springer.

Agradecimientos

Este artículo se elaboró en el marco del Proyecto de investigación «La responsabilidad de la inteligencia artificial: Un desafío para las ciencias penales» (PID2020-112637RB-I00), financiado por el Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia, Subprograma Estatal de Generación de Conocimiento, del Ministerio de Economía y Competitividad, España.

Sobre el autor

Roberto Navarro es abogado, profesor adjunto de Derecho Penal en la Universidad Católica del Maule. Su correo electrónico es: ronavarro@ucm.cl. https://orcid.org/0000-0003-0907-5714.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático 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).