UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO COMERCIAL

HACKING ÉTICO: ANÁLISIS DE LA DISCUSIÓN EN TORNO A LA AUTORIZACIÓN EXPRESA COMO REQUISITO QUE PERMITE SU DESARROLLO SIN CONSIDERARLO COMO UNA CONDUCTA ANTIJURÍDICA

Memoria para optar al grado de Licenciados en Ciencias Jurídicas y Sociales

FERNANDA CAMILA JIMÉNEZ FERNÁNDEZ
ISIDORA ANDREA IZQUIERDO LOYOLA

Profesor guía:
CLAUDIO MAGLIONA MARKOVICTH

Santiago de Chile
2023

Tabla de contenido

RESUMEN

El presente trabajo tiene como objetivo analizar el hacking ético, una herramienta utilizada en todo el mundo para detectar los errores y eventuales vulnerabilidades en los sistemas de información y por consiguiente, para prevenirlos y para minimizar sus efectos en caso de ocurrir algún ataque cibernético. Lo anterior en el contexto actual de la tecnología en que un mayor desarrollo de la misma lleva consigo mayores riesgos que son propios de los sistemas de información.

Nuestro país no está exento de estos riesgos y por esta razón es que se ha desarrollado una Política Nacional de Ciberseguridad, con el objetivo de no solo proteger los sistemas, sino también los distintos bienes jurídicos que pueden vulnerarse mediante el uso fraudulento del internet.

Para dicho análisis, un objetivo específico será abordar la discusión en torno a la exigibilidad de la autorización expresa para la licitud del hacking ético a la luz de la legislación actual de delitos informáticos en nuestro país. Así, se analizará las posturas existentes, por un lado la que considera este requisito como una limitación al desarrollo del hacking ético y por consiguiente de sus beneficios, en contraposición de la segunda postura que establece como necesaria esa limitación para evitar la comisión de otros delitos informáticos y poner en riesgo la información propiamente tal y los bienes jurídicos asociados a ello.

Además, se analizará la forma en cómo se ha regulado la figura del hacking ético en nuestro país y en el plano internacional, mediante el examen de las disposiciones legales de nuestro país y su evolución, e instrumentos internacionales que sientan directrices con respecto a su regulación.

Palabras claves: Hacking ético, Consentimiento; Autorización expresa, Sistemas informáticos; Ciberseguridad.

ABSTRACT

We know that greater technological development brings with it greater risks for information systems. Our country is no exception to this, and for this reason a National Cybersecurity Policy has been developed with the aim of not only protecting the systems, but also the rights of individuals that can be violated through fraudulent use of the Internet.

This research aims to examine a tool used worldwide to prevent errors in information systems and to minimize their effects in the event of a cyber attack, we are talking about ethical hacking.

Chapter I will consist of analyzing ethical hacking from its concept, and how Chilean law has regulated its application, making for this a timeline of the laws that have developed cybersecurity in the country.

Subsequently, chapter II will address the dichotomy of consent, a discussion in which we will seek to understand whether the enforceability of express consent limits the development of ethical hacking, or whether it is essential to avoid violating the control that the owner has over the information system and that is affected if it is carried out without consent.

Keywords: ethical hacking, consent, computer systems, cybersecurity.

INTRODUCCIÓN

La rápida y constante evolución de la tecnología de la que estamos siendo testigos trae consigo innumerables beneficios, como por ejemplo, el desarrollo de nuevas actividades, la mejoría en las formas de comunicación y el acceso a la información, por nombrar solo algunos. Pero tal situación no es la panacea, dado que la informática, entendida como la ciencia que desarrolla el procesamiento de información de forma automatizada[1], ha implicado el surgimiento de nuevos riesgos y ataques contra bienes jurídicos social y penalmente relevantes, algunos de los cuales no se encuentran protegidos desde la óptica penal[2].

Los sistemas informáticos pueden ser definidos como, ya sea, un dispositivo aislado o un conjunto de ellos que tienen como función el tratamiento automatizado de datos en la ejecución de un programa[3]. Se entiende entonces, que lo componen tanto su soporte lógico como el dispositivo propiamente tal (*software* y *hardware*). En la misma línea, en el artículo 15 letra b) de la ley N° 21.459, en adelante "Ley sobre Delitos Informáticos", se definen los sistemas informáticos[4].

Por estos riesgos mencionados es que se ha vuelto necesario regular esta arista con el fin de proteger los sistemas en sí y la información que almacenan y procesan; los datos informáticos, que entenderemos como toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función[5].

Estos riesgos y ataques informáticos hacen que estos datos sean vulnerables y debido a las consecuencias que todo lo anterior conlleva, es que la regulación y el mantener de

---

[1] Jijena Leiva, R. J. (2010). Debate parlamentario en el ámbito del derecho informático. Análisis de la ley n° 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información. Revista De Derecho - Pontificia Universidad Católica De Valparaíso, (15).

[2] CHILE. Proyecto de Ley iniciado en mensaje de S. E. el Presidente de la República, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. Boletín N° 12.192-25, 25 de octubre de 2018. Disponible en: https://www.diarioconstitucional.cl/wp-content/uploads/2022/03/Boletin-12192-25-ciberseguridad.pdf

[3] CHILE. Proyecto de ley, iniciado en Mensaje del ex Presidente de la República, señor Sebastián Piñera Echeñique, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14.847-06, 2 de marzo de 2022. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06

[4] CHILE. Ley N° 21.459 que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Diario Oficial de la República de Chile, Junio del 2022. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1177743

[5] Artículo 1 del Convenio de Budapest.

constante actualización la materia se vuelve necesario para proteger a los usuarios y prevenir la comisión de delitos.

Además, hay que considerar que estas situaciones e interacciones entre personas, naturales o jurídicas y el internet no existían antes, por lo que se trata de un fenómeno relativamente reciente si se compara con el derecho penal, lo que lleva a una multiplicación de casos y a la necesidad de utilizar diversas normas para garantizar la protección de numerosos bienes y derechos que pueden verse vulnerados mediante el uso de las nuevas tecnologías[6].

Un claro ejemplo de las inseguridades de los sistemas es el ciberataque al Banco Estado que provocó la paralización de diversas sucursales de dicha institución financiera en 2020[7], o el caso más reciente del virus que afectó al Poder Judicial el año pasado[8]. Otro suceso recordado es el ataque cibernético que sufrió en el año 2020 la División de Desarrollo Digital de la Presidencia de la República en que se vulneró la seguridad al obtener información de la Clave Única, información personal de los ciudadanos que permite realizar trámites en línea[9].

La evolución del cibercrimen conlleva una evolución en sus protagonistas esenciales, los criminales y las víctimas, estas últimas pueden ser tanto personas naturales que por el hecho de tener acceso y hacen uso del internet se exponen a la posibilidad de sufrir algún delito de este tipo, tanto como personas jurídicas, empresas que son víctimas debido al uso generalizado de las Tecnologías de la Información y Comunicación (TIC) o por índole económica[10].

---

[6] Cadoppi, Canestrari, Manna, Papa. Cibercrime. UTET. https://iris.univr.it/retrieve/26cf3a84-9eca-408e-b8f7-f925fa099353/Diritto%20penale%2c%20tecnologie%20informamtiche%20ed%20intelligenza%20artificiale%20LP.pdf

[7] Banco Estado en 2020 fue víctima de sabotaje informático mediante un virus que encripta información, que a pesar de no haberse reportado ningún robo de dinero ni de información, debieron activar el protocolo y la Comisión para el Mercado Financiero (CMF) fue informada del ataque informático entre otras instituciones. El incidente afectó computadores de distintas sucursales a lo largo del país, por lo que debieron cerrar sus puertas, además de paralizar plataformas digitales como la página web y el sistema de transferencias. Disponible en: https://www.senado.cl/noticias/ciberseguridad/comision-de-economia-conocio-detalles-del-ciberataque-del-banco estado>

[8] En septiembre de 2022 se detectó un malware en equipos del Poder Judicial, que si bien afectó a un número menor de computadores, estos debieron ser dejados fuera de funcionamiento y reemplazados, entorpeciendo algunas audiencias y la revisión de causas producto del ataque.

[9] La Clave Única es una identidad virtual que permite realizar trámites y acceder a distintos servicios como por ejemplo obtener distintos certificados, y en 2020 la División de Gobierno Digital de la Presidencia de la República fue víctima de un ataque cibernético en que se robó información sobre las claves únicas e identificación biométrica. Disponible en: https://www.senado.cl/noticias/ciberseguridad/hackeo-a-clave-unica-demandan-esclarecimiento-de-las-circunstancias-del.

[10] Miró, Fernando. El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. 2012, p.27.

Estos ataques configuran una clase de delitos que se denomina delitos informáticos, definidos en el Mensaje N° 13-348 del 2002 como cualquier acto que atente contra bienes jurídicos relevantes que impliquen el uso de medios informáticos[11], en definitiva, una nueva realidad.

Ahora bien, el concepto de delitos informáticos puede ser entendido en un sentido amplio y en uno estricto, siendo el primero delitos tradicionales que se cometen a través o mediante sistemas informáticos, y en sentido estricto sería el delito cometido contra un sistema, delitos nuevos producto de los avances tecnológicos[12].

Si nos centramos en la definición en sentido amplio, podemos dilucidar que esta clase de delitos poseen notorias diferencias con el resto de los clásicos tipificados en el Código Penal o en algunas leyes especiales, por ejemplo, en la forma de comisión, dado que deben ser realizados mediante el uso de un sistema informático y de las formas tradicionales.

Otra diferencia es el bien jurídico que se busca proteger con la tipificación de las conductas que atentan contra sistemas de información y la ciberseguridad, en contraposición a los delitos que, por el contrario, protegen bienes jurídicos clásicos como la vida o la integridad física, cuestión que será parte del análisis[13].

Según el Comisario Danic Maldonado, de la Brigada Investigadora del Cibercrimen Metropolitana de la PDI, durante el programa Información y Tecnología, de la Vicerrectoría de Tecnologías de la Información de la Universidad de Chile, los ciberataques según la cantidad de denuncias recibidas en la PDI han aumentado cerca de un 29% en comparación del 2019 con el 2020, y un 89% si se consideran los cinco primeros meses de 2021 con igual período del año anterior[14].

---

[11] Mensaje N° 13-348 de S.E. El presidente de la República con el que inicia un proyecto de ley que modifica el Código Penal, con el objeto de recepcionar, en los tipos penales tradicionales, nuevas formas delictivas surgidas a partir de la informática. Septiembre de 2002. Disponible en: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=3083-07

[12] Seminario virtual: La regulación chilena de los delitos informáticos. 8 de mayo de 2020. [Archivo de video] https://www.youtube.com/watch?v=AKN6s8tJI-g&t=2992s

[13] Véase el Capítulo II en lo referido al bien jurídico protegido.

[14] Sesión Nº 16 del programa Información y Tecnología, de la Vicerrectoría de Tecnologías de la Información de la Universidad de Chile, <https://vti.uchile.cl/durante-la-pandemia-aumentaron-los-ciberataques/>

Tal como nos demuestran las cifras y las situaciones antes mencionadas, existe una imperiosa necesidad de regular respecto a los ciberataques, así como el interés por encontrar nuevas formas de resguardo.

La adopción de medidas por brechas de seguridad y su notificación a los organismos pertinentes, son de importancia mundial en la actualidad, siendo la ciberdelincuencia e inseguridad cibernética uno de los principales riesgos de gravedad e impacto mundial a largo y corto plazo, según lo declara el Reporte de Riesgos Globales 2023 del Foro Económico Mundial (WEF, por sus siglas en inglés)[15].

Para que un sistema de información sea seguro debe contar con cinco elementos. El primero es la integridad, referido a que la información se modifique sin previa autorización; en segundo lugar, la confidencialidad de los datos que contiene el sistema, además del control de acceso al mismo. El cuarto elemento corresponde a la autenticidad, como la capacidad de comprobar que la persona que accede al sistema corresponde efectivamente a ella, y por último la disponibilidad del sistema para los usuarios en cualquier momento para satisfacer sus requerimientos[16].

Chile es uno de los países de Latinoamérica que más avance ha realizado en el tema en cuanto a la legislación de los delitos informáticos, destacando en la promulgación de leyes como la ley N° 21.459 que establece una serie de esta clase de delitos y sus respectivas sanciones.

Es en dicha ley que se regula el hacking ético, figura central de este trabajo, que consiste en la detección de vulnerabilidades y defectos de los sistemas de información mediante el acceso a los mismos.

Los errores, también denominados *bugs*, en los sistemas informáticos pueden generar dos situaciones. La primera es simplemente hacer fallar el sistema, lo que se conoce coloquialmente como una “caída del sistema” y la segunda es que provoque una vulnerabilidad, la que se entiende como un error que puede ser manipulado por un agente malicioso de tal forma que afecte la ciberseguridad[17].

---

[15] WORLD ECONOMIC FORUM (WEF). *The Global Risks Report 2020.* Suiza, Enero de 2023, p.29, 45 y 70. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[16] Vallejo, M. R. L. (2017). Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. *Revista Publicando*, *4*(10 (1)), 31-51.

[17] Canal Uchilederecho. Ciclo de charlas sobre derecho informático [archivo de video], minuto 10:40. https://www.youtube.com/watch?v=Y-TV3oRY82U

El experto que detecte lo anterior debe alertar a las autoridades competentes de administrar dicho sistema del hallazgo, esto con el fin de corregir las fallas velando por su correcto funcionamiento, permitiendo frenar a tiempo las consecuencias de esos fallos, a la vez que genera la posibilidad de prevenir situaciones similares a futuro reforzando las medidas de seguridad. Ahora bien, los incentivos para realizar este informe dependen de la forma en que esté regulado en la ley.

Para lo anterior, existe el llamado Proceso Coordinado de Divulgación de Vulnerabilidades (*Coordinated Vulnerability Disclosure Process*) como un estándar en la realización de la alerta de la vulnerabilidad al dueño del sistema y posterior divulgación. Este contempla diversas etapas, siendo la primera la recopilación de información y evaluación inicial; luego se procede al análisis de las vulnerabilidades encontradas; la tercera etapa es coordinar la mitigación para su posterior aplicación; y por último la etapa de la divulgación al público de las vulnerabilidades[18].

Ahora bien, la preocupación de nuestro país respecto a la regulación de los delitos informáticos se remonta a 1991, año en que se presentó el Proyecto de Ley sobre Delitos Informáticos (Boletín N° 412-07)[19] que finalmente fue promulgada en 1993, convirtiéndose en la Ley N° 19.223[20].

Este documento definió a la tecnología, en su primera moción parlamentaria, como uno de los recursos más preciados que en la actualidad tenemos, dado que no existe organización social alguna que prescinda de la utilización de sistemas automatizados de tratamiento de la información[21].

Luego, en el año 2017 Chile se adhirió a la normativa internacional sobre dicha materia, mediante el Decreto 83 del Ministerio de Relaciones Exteriores[22]. Con lo cual en 2022, dimos paso a regular la ciberseguridad de forma más sólida al promulgar la ley N° 21.459

---

[18]Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/coordinated-vulnerability-disclosure-process

[19] CHILE. Proyecto de Ley sobre Delito Informático. Boletín Nº 412-07, Agosto de 1992. Disponible en https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=2167&prmBOLETIN=412-07

[20] CHILE. Ley N° 19.223 que tipifica figuras penales relativas a la informática. Diario Oficial de la República de Chile, Junio de 1993. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=30590&buscar=ley%2B19223

[21] Historia de la Ley N° 19.223. Primer Trámite Constitucional: Cámara de Diputados, https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/7025/ , [Consultado: 23/07/2023].

[22] CHILE. Decreto 83 del Ministerio de Relaciones Exteriores que promulga el Convenio sobre la Ciberdelincuencia. 27 de abril de 2017. Disponible en: https://bcn.cl/2yv71

que modifica diferentes cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

En la actualidad se encuentra en tramitación en su segundo trámite constitucional, un Proyecto de Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información (Boletín 14.847-06)[23] que no deja de lado la regulación del hacking ético.

La ley N° 21.459 antes mencionada, establece en el artículo 16 que se permite el acceso a un sistema de información con el objeto de investigar la vulnerabilidad del mismo para así poder mejorar su seguridad, siempre que se tenga la autorización expresa del titular de dicho sistema[24]. Esto es, se habla de hacking ético con el requisito esencial del consentimiento, la autorización que permite que se trate de un servicio seguro y legal.

Lo anterior genera discusión, dado que por un lado puede sostenerse que al establecer como requisito la autorización expresa se está limitando el desarrollo del hacking ético. Figura, que dentro de sus objetivos y principios no está la comisión de un delito, por ejemplo, respecto de la información de los servidores que se pueda obtener al acceder. Esta postura lleva a sostener que no puede considerarse como riesgoso para un sistema informático el permitir o proteger el hacking ético, teniendo en consideración su contribución a la ciberseguridad.

Alejandro Hevia es adepto a esta postura y sostiene que la criminalización de la búsqueda y notificación de vulnerabilidades constituye, más que un beneficio para los sistemas, los vuelve más inseguros[25].

Ahora bien, una postura contraria a la anterior es la que sostiene que al no contar con dicha autorización, los también llamados *white hackers*[26] vulneran el control que tiene el

---

[23] CHILE. Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14847-06. 15 de marzo de 2022. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06

[24] Artículo 16.- Autorización e Investigación Académica. 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.

[25] Informe de la Comisión de Seguridad Ciudadana recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14.847-06 (S). 27 noviembre de 2023. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/informes.aspx?prmID=15344&prmBOLETIN=14847-06

[26] SANDRA MILENA CASTRO CUBILLOS, White hat: Hacking étic, <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2679/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y> [Consulatdo: 23/07/2023]

encargado o dueño del sistema sobre el mismo, situación que puede convertirse en el medio de comisión de otros delitos.

Es por esto que se analizarán, en primer lugar, las leyes nacionales sobre la materia, haciendo un barrido por su evolución y analizando cómo estas han regulado la figura del hacking ético. Mencionando además el Convenio de Budapest, instrumento intencional elaborado con objeto de sentar bases que permitan la persecución de los delitos informáticos en el mundo. Posteriormente nos adentraremos en la discusión en torno a la exigibilidad de la autorización expresa antes mencionada, volviendo constantemente a las leyes sobre las que se tratará en el capítulo 1, dado que desarrollaremos el requisito de la autorización expresa para la realización del hacking ético en base a las leyes que se mencionaron anteriormente.

En base a la forma de desarrollar la investigación es que el objetivo específico de la misma es abordar el hacking ético como herramienta de la informática y desarrollar la cuestión relativa a la autorización exigida para su realización conforme a la ley.

CAPÍTULO I. SOBRE EL HACKING ÉTICO

Debido a la era digital en la que estamos viviendo y a los riesgos que esto conlleva, tanto para los sistemas como para los datos en ellos contenidos, es que se necesita protegerlos contra los ataques cibernéticos. Una forma de hacerlo es justamente a través del hacking ético, un proceso sistemático que tiene por objeto la elaboración de estrategias defensivas para fortalecer las políticas de ciberseguridad de una empresa o institución[27].

La forma de realización del hacking ético consta de varios pasos. En primer lugar encontramos el alcance de la prueba que comienza con conseguir el permiso del cliente y determinar qué es lo que se va a evaluar. Luego viene el descubrimiento y la enumeración, etapa en que se busca recolectar información que servirá para elaborar el plan, ya sea mediante reconocimiento pasivo, en que se recolecta la información de forma discreta, o por reconocimiento activo, que a diferencia del anterior, hay interacción del hacker con el objetivo. En tercer lugar, está el mapeo de las vulnerabilidades, que es básicamente buscarlas. Luego, en la etapa de explotación es que se realiza el acceso al sistema, para

[27] Muñoz Villanueva, A. A., & Sánchez Méndez, J. D. (2015). Modelo referencial de aprendizaje para la implementación de Hacking ético. https://repository.unilibre.edu.co/handle/10901/10909

luego pasar a la documentación y los reportes en que se recopila la información obtenida para ser presentada al administrador del sistema[28].

Es relevante tener en cuenta, que su importancia de estudio y legislación, deberá entenderse bajo un contexto en que la tecnología actual de diseño y creación de sistemas informáticos no ha logrado producir sistemas seguros desde su origen[29]. Sin existir un sistema informático completamente seguro, por lo que "todo se puede hackear"[30]. En relación a que su creador, el ser humano, nunca será perfecto y cometerá errores.

Con ello, debemos entender que ningún sistema es perfecto, por lo cual siempre existirán fallas. Tal como lo menciona el profesor Alejandro Hevia, existen dos tipos de sistemas informáticos (software): Aquellos en que se han descubierto fallas y aquellos que donde todavía aún no se han descubierto las fallas[31].

Dichas fallas podrán derivar en errores en el funcionamiento del sistema y/o vulnerabilidades en la seguridad de ella. Pero al ser "propias" son mucho más difíciles de reconocer por el mismo titular del sistema u organización, ya que "lo que vemos entra en competencia con la versión que tenemos en nuestra cabeza"[32], es decir, nuestra propia percepción de lo creado nos dificulta detectar errores en el. Siendo por ello, mucho más fácil reconocer los errores en lo ajeno, por lo que sería más beneficioso encargar dicha tarea de detección de fallas a un terceros ajeno. Siendo poco eficiente y razonable rechazar o no incentivar el reporte de un tercero de buena fe que haya realizado una investigación en de las vulnerabilidades del sistema en cuestión.

Asimismo, tal como lo menciona el profesor Alejandro Hevia[33], en la segunda charla del Ciclo de Delitos Informáticos de la Universidad de Chile, la promoción al incentivo a reportar las brechas de seguridad viene desde hace muchos años atrás.

---

[28] Medina Rojas, E. F. (2015). *Hacking Ético: Una herramienta para la seguridad informática* (Bachelor's thesis, Universidad Piloto de Colombia). http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2932/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

[29] https://www.scielo.cl/scielo.php?pid=S0719-25842020000200001&script=sci_arttext

[30] https://www.redalyc.org/pdf/666/66612867010.pdf pp151

[31] Segunda Charla del Ciclo de Delitos Informáticos, minuto 8:50, Universidad de Chile, 2022, https://www.youtube.com/watch?v=Y-TV3oRY82U

[32] https://www.bbc.com/mundo/noticias/2014/11/141113_errores_ortografia_texto_lp

[33] Segunda Charla del Ciclo de Delitos Informáticos, minuto 20:03, Universidad de Chile, 2022 https://www.youtube.com/watch?v=Y-TV3oRY82U

Sin ir más lejos, el profesor menciona que el mismo Alfred Charles Hobbe, un importante cerrajero de su época, destacaba la importancia de testear las cerraduras, ya que en sus palabras:

"...la difusión del conocimiento es necesaria para dar juego limpio a quienes puedan sufrir por la ignorancia. Nunca se puede insistir demasiado en que el conocimiento de los hechos reales será, al final, mejor para todas las partes… seguramente a las personas honestas les interesa conocer este hecho, porque los deshonestos serán seguramente los primeros en aplicar el conocimiento en la práctica; y la difusión del conocimiento es necesaria para dar juego limpio a quienes puedan sufrir por la ignorancia…"[34]

En otras palabras, para todos los involucrados, el buscar y reportar las vulnerabilidades halladas por los hackers éticos será fructífero en la práctica, destacando que el conocimiento será beneficioso para toda comunidad, valiéndose de ella para mejorar. Entiendo además, que solos los terceros de buena fe serán los que reporten dichas fallas, en contraste que probablemente los "deshonestos" ya la poseen pero no la comunican.

Por todo lo anterior, se vuelve menester que los Estados establezcan normativas en pos de la protección de los sistemas de información, considerando que los problemas que estos sufren pueden llegar a afectar datos personales e información que las personas entregan confiando en que estarán a salvo.

Siguiendo la tendencia internacional, es que en 2022 se promulga en Chile la ley N° 21.459 que establece normas sobre delitos informáticos, posicionando a Chile como un país pionero en materia de regulación sobre ciberseguridad en Latinoamérica. Así, en 2008 se posiciona a Chile entre el top 10 de países América en gobierno electrónico (*e-government*), solo bajo Estados Unidos, Canadá y Uruguay, y por sobre países como Colombia, Argentina y Brasil[35].

En dicha ley se sanciona el delito de ataque a la integridad de los sistemas informáticos de forma que mediante la utilización de sus datos informáticos se impida su normal funcionamiento (Art 1°), el delito de acceso ilícito a un sistema informático (Art 2°), la interceptación ilícita de información (Art 3°), el ataque a la integridad de los datos

[34]A.C.Hobbs,http://www.survivorlibrary.com/library/rudimentary_treatise_on_the_construction_of_door_locks_1859.pdf pp.3

[35] United Nation E-government Survey 2018. Gearing e-government to support transformation towards sustainable and resilient societies. p. 136. Table 6.2. https://www.unescap.org/sites/default/files/E-Government%20Survey%202018_FINAL.pdf

informáticos (Art 4°) y la falsificación y receptación de los mismos (Art 5° y 6° respectivamente), y el fraude informático con el fin de obtener un beneficio económico producto del mismo (Art 7°). También se sanciona el abuso de dispositivos, programas computacionales, contraseñas, entre otros, para la perpetración del delito de ataque a la integridad de los sistemas y datos informáticos.

Además, la ley contempla situaciones agravantes y atenuantes, al igual que reglas de procedimiento especiales y definiciones de conceptos relevantes. Ahora bien, a pesar de sancionar todos los delitos mencionados, no se define qué se entiende por delito informático.

El artículo 16 de la ley N° 21.459 regula el acceso a los sistemas informáticos en el marco de las investigaciones para detectar vulnerabilidades o para mejorar la seguridad de los mismos, estableciendo que es necesario contar con la autorización del titular del sistema.

Si bien, no se menciona expresamente el hacking ético como tal, dado que solamente se hace referencia al acceso a sistemas informáticos para permitir detectar amenazas y vulnerabilidades para fortalecer dichos sistemas, podemos establecer que dicha normativa hace referencia a lo que conocemos como hacking ético. Este puede ser definido como una rama de la seguridad tecnológica dirigida a realizar un “testeo” de vulnerabiliades, dando conocimiento de ellas a la organización, de las fallas o potenciales brechas de seguridad en su sistema de almacenamiento de información[36].

De la definición anterior podemos destacar el hecho de dar conocimiento informar de las fallas o potenciales fallas como un elemento que lo vuelve “ético”. Esto porque no se relaciona con fines maliciosos, como por ejemplo, el aprovechamiento de la información a la que se pueda acceder debido a las fallas en la seguridad de un determinado sistema.

Ahora bien, este hacking puede ser evaluado desde una dualidad. Por un lado está la posibilidad de concebirlo como algo negativo, como una forma de exponer la debilidad de un sistema, considerándolo como una amenaza llevando incluso a tomar acciones legales en contra de quienes realizan las labores de investigación de ciberseguridad.

Pero a pesar de que el hacking suele asociarse a una conducta negativa, también es posible sostener que el hacking ético es beneficioso en el sentido que permite alertar el fallo

[36] CARLOS TORI,< https://nebul4ck.files.wordpress.com/2015/08/hacking-etico-carlos-tori.pdf> [Consultado: 23/07/2023]

en un sistema, lo que permite tomar acciones al respecto que permitan su correcto funcionamiento. Así, permitiría la evaluación, arreglo y mejor funcionamiento de los software. Todo lo anterior bajo el supuesto de que no se ingresa al sistema de información con la intención de causar un daño a los datos contenidos en él o de apropiarse indebidamente de ellos.

1. CÓMO CHILE HA REGULADO EL HACKING ÉTICO

1.1 LEY N° 19.223 QUE TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMÁTICA

Hablamos de la ley N° 21.459 que fue promulgada el 9 de junio de 2022, sin embargo, la historia de la ley sobre delitos informáticos es de larga data.

En 1991 comienza el interés por regular la materia, evidenciado en un Proyecto de Ley sobre Delitos Informáticos (Boletín Nº 412-07) llevado por el diputado José Antonio Viera-Gallo, motivado por querer proteger un nuevo bien jurídico formado por el desarrollo de las nuevas tecnologías y buscando evitar los posibles riesgos del mal uso de la información que contienen los sistemas informáticos.

Sostuvo el diputado que “por el actual desarrollo tecnológico de la sociedad, merece ser protegida mediante la creación de figuras delictivas nuevas, que pongan de relieve su importancia. (...) La protección de un sistema de información automatizado se realiza mediante la creación de figuras penales especiales, que evitan la necesidad de hacer interpretaciones extensivas de las tradicionales normas penales, para incluir conductas indebidas (...)”[37].

Este proyecto contaba con cinco artículos, de los cuales cuatro describen conductas constitutivas de delito y el último sostenía como agravante el ánimo de lucro en la realización de las conductas descritas. El tercer y último artículo se eliminaron durante la discusión y se agregó un nuevo artículo, resultando un proyecto de cuatro artículos. Finalmente, se publica en 1993 la ley N° 19.223 en el Diario Oficial.

[37] Historia de la Ley Nº 19.223, Tipifica figuras penales relativas a la Informática. Moción del señor Diputados José Antonio Viera Gallo Fecha 16 de julio de 1991.<https://obtienearchivo.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/4745/1/HL19223.pdf>

El modelo legislativo utilizado en esta ley fue el mismo francés en la ley, realizando un análisis fenomenológico, esto es, teniendo como foco la nueva forma de comisión de estos delitos, el fenómeno criminal y no los bienes jurídicos puestos en riesgo por ellos[38].

Estos delitos, si bien corresponden cada uno a un tipo de conducta distinta, se pueden clasificar en dos grandes figuras delictivas: sabotaje informático y espionaje informático[39]. El primero corresponde a cualquier acción que atente contra un sistema de tratamiento de información o los componentes del mismo a través de la destrucción, inutilización, obstaculización o modificación de ellos. En cambio, el espionaje informático comprende los delitos de apoderamiento, uso y conocimiento indebido de la información contenida en un sistema, esto mediante el acceso al mismo pasando por alto las barreras de seguridad que este contenga. Además, se contempla como delito acciones respecto a la utilización de esos datos obtenidos, como la revelación y difusión de ellos.

Es la categoría de espionaje informático que se encuentra el artículo 2° de esta ley que tipifica el hacking, el cual establece: “El que con el ánimo de apoderarse, usar o conocer, indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio”.

Debido a las exigencias que establece el artículo hay quienes sostienen, como Susana Hiplan, que bajo los requisitos de tipicidad subjetiva del tipo establecidos en el artículo 2°, no es posible penalizar un hacking blanco (aquél que sólo irrumpe, pero no lesiona el sistema informático, ni revela la información en él contenida)[40].

Siguiendo esta misma línea, en un análisis a la Ley N° 19.223, Becker y Viollier sostienen que basta ponerse en la situación de un tercero que realiza acciones tendientes a probar los mecanismos de seguridad de un sistema informático en búsqueda de vulnerabilidades en su código, sin la autorización de su administrador. Si este tercero es capaz de explotar una vulnerabilidad, es posible que producto de esta acción acceda necesariamente, aunque sea momentáneamente, al sistema informático, ya que su propósito inicial era, justamente, demostrar que se podría explotar al sistema para ingresar a él sin contar con las

[38] CHILE. Informe de la Comisión de Ciencias y Tecnología recaído en el Proyecto de Ley que modifica el Código Penal, con el objeto de recepcionar en los tipos penales tradicionales, nuevas formas delictivas surgidas a partir del desarrollo de la informática. Boletín Nº 3.083-07, 11 de noviembre de 2002. Disponible en: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=3083-07
[39] Chávez, Eric. Derecho Penal Parte especial. Cuarta edición, 2023.
[40] HIPLAN, SUSANA. La Ley 19.223 a 26 Años de su Promulgación. 2019.

credenciales necesarias. De no existir un apoderamiento o conocimiento indebido de la información, la conducta sería atípica. En otras palabras, aquella legislación no sancionaba el mero acceso o hackeo de un sistema informático[41]. Ahora bien, el caso contrario a lo antes señalado sería, como menciona Viollier, considerar la expresión “de forma indebida” como un sinónimo de que se realice sin haberse otorgado el consentimiento expreso, lo que limitaría el desarrollo del “hacking blanco[42].

Es así como esta ley, que, a pesar de ser bastante acotada, pasa a ser la primera regulación en relación a la ciberseguridad del país, la que además permitió poner como tema de discusión los delitos informáticos que antes no se regulaban.

Debido al paso del tiempo y al rápido desarrollo de la tecnología y el consiguiente aumento y diversificación de los delitos informáticos asociados a ello, es que esta ley prontamente requirió de una modificación, siendo unánime la conclusión que se requiere de una actualización del catálogo de delitos informáticos (...) pues las actuales carencias no sólo se radican en la falta de una tipificación moderna y eficaz, sino también en la falta de medios suficientes para desarrollar las investigaciones penales relativas a delitos informáticos.[43]

En el mismo año en que se promulga la esta ley, se presenta una moción parlamentaria sobre la protección de la vida privada, relacionado a la informática dado que sostenía que esta debía estar al servicio de las personas, con el límite de respetar justamente eso, la vida privada[44]. Esto es la evidencia de la realización de iniciativas aisladas que no se hacen cargo de la necesidad de regular conjuntamente las consecuencias que los avances tecnológicos tienen en diversas aristas como lo social y económico por lo relacionadas que están las materias, y solo se enfocan en materias específicas del derecho informático[45].

1.2 CONVENIO DE BUDAPEST Y DECRETO 83

---

[41] BECKER CASTELLARO, SEBASTIÁN; VIOLLIER BONVIN, PABLO. (2020). La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley 19.223. Revista de derecho (Concepción), 88(248), 75-112. <https://dx.doi.org/10.29393/rd248-13icsb20013> [Consultado: 23/07/2023].

[42] Viollier, Pablo. Boletín 12192-25: Delitos informáticos, Derechos Digitales, 3 de enero de 2019, <https://bit.ly/34Kwjva> [Consultado: 14/09/2023].

[43] Proyecto de ley, iniciado en mensaje de S. E. el Presidente de la República, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. Boletín Nº 12.192-25.

[44] Historia de la Ley Nº 19.628 Protección de la vida privada. 1999. Biblioteca del Congreso Nacional.

[45] Jijena Leiva, R. J. (2010). Debate parlamentario en el ámbito del derecho informático. Análisis de la ley n° 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información. Revista De Derecho - Pontificia Universidad Católica De Valparaíso, (15). <https://www.rdpucv.cl/index.php/rderecho/article/view/283>

En el plano internacional, en 2001 se realiza el Convenio de Budapest sobre Ciberdelincuencia, en adelante “El Convenio”, con el objeto de estandarizar de cierta forma las políticas penales sobre ciberdelincuencia, establecer formas de investigación y procesamiento de los delitos informáticos en armonía con las normas procesales de cada país, además de promover la cooperación internacional entre países para combatir los delitos contra los sistemas informáticos, tal como lo establece el propio convenio en el preámbulo, radicando en esto su importancia a nivel internacional.

Lo anterior debido a que los ataques cibernéticos se realizan en el ciberespacio, lo que a su vez provoca que se alteren los parámetros espacio-temporales[46]. Un ejemplo de esto es el caso de una estafa informática, en que la víctima puede encontrarse en un país A, el victimario en B y las cuentas corrientes a las que se mueven de los dineros robados en C. Recayendo ahí la importancia de la cooperación y colaboración internacional en este tipo de delitos.[47]

El Convenio fue elaborado por los países parte del Consejo de Europa, además de China, Canadá y Japón. Diversos países de Latinoamérica se hicieron parte de este, entre ellos Chile, que mediante el Decreto Supremo 83 del Ministerio de Relaciones Exteriores del 2017 promulga el Convenio de Budapest.

Dicho instrumento contó con cuatro capítulos, el primero sobre terminología en que se desarrollan diferentes definiciones, como por ejemplo, la antes mencionada de sistema informático. Además de conceptos como datos informáticos, proveedor de servicios y datos relativos al tráfico. En el segundo capítulo se abordan las medidas que deberán tomar los países que sean parte de él, lo que permite la estandarización o armonización de las normas a nivel internacional, en cuanto a derecho penal como procesal. De esa forma se pueden evitar abusos tales como el traslado del proceso a una Parte que aplique normas anteriores y sanciones menores[48].

Tal como se desarrollará más adelante, al hacerse parte de un Convenio se espera que los países cumplan con lo establecido en él, incluso si eso significa la adecuación de las leyes del país. Es por el antes mencionado Decreto 83 que Chile debe modificar la ley vigente en ese momento para cumplir con lo establecido en el Convenio de Budapest, lo que nos lleva

[46] Miró, Fernando. La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista electrónica de Ciencia Penal y Criminología.
[47] BECKER CASTELLARO, SEBASTIÁN; VIOLLIER BONVIN, PABLO. (2020). La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley 19.223. Revista de derecho (Concepción), 88(248), 75-112. <https://dx.doi.org/10.29393/rd248-13icsb20013>
[48] Convenio sobre la Ciberdelincuencia. Informe explicativo. (STE núm. 185)

a la ley N° 21.459. Siendo esto lo relevante en esta sección, ser el elemento que gatilla la modificación de la ley N° 19.223 con el fin de contar con una legislación al nivel del estándar internacional.

Ahora bien, Chile realizó algunas reservas al Convenio, la primera con respecto al artículo 4° del Convenio relativo a los ataques a la integridad de los datos que en el n° 2 estipula que las partes puedan exigir que los actos antes mencionados produzcan daños graves. Es con respecto a este n° 2 que se realiza la reserva en tanto se establece que "La República de Chile expresa, de conformidad al Artículo 4, párrafo 2, del Convenio sobre la Ciberdelincuencia, que tipificará como delitos en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves"[49].

La segunda reserva se hizo al artículo 6° del Convenio, el que trata los abusos de los dispositivos, dado que “no aplicará el párrafo 1 del mismo Artículo, en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii)"[50], esto es, no se tipificará a menos que ocurran las afectaciones señaladas.

Como tercera reserva encontramos la relativa al artículo 9° relativo a los delitos de pornografía infantil, y las últimas dos reservas se hacen al artículo 22° y 29° respectivamente. Esta última respecto a la conservación de datos informáticos almacenados, punto relevante en consideración con uno de los objetivos del Convenio, el de cooperación internacional en la persecución de los delitos informáticos, esto debido a que en virtud de ese artículo otro país podría exigirle a Chile conservar datos necesarios para una investigación criminal[51].

1.3 LEY N° 21.459 QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS Y DEROGA LA LEY N° 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST

Como ya se mencionó, el Convenio de Budapest es de suma importancia debido a que nuestra legislación tuvo que adecuarse para cumplir con las disposiciones que se

[49] Decreto 83 que promulga el Convenio sobre la ciberdelincuencia.
[50] Ibid.
[51] BECKER CASTELLARO, SEBASTIÁN; VIOLLIER BONVIN, PABLO. (2020). La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley 19.223. Revista de derecho (Concepción), 88(248), 75-112.

establecieron en él, dado que Chile se obligó a ello mediante el Decreto 83 del año 2017 del Ministerio de Relaciones Exteriores que promulga el Convenio sobre la Ciberdelincuencia.

Debido a lo anterior y al constante y acelerado desarrollo de las tecnologías es que la necesidad de actualizar la ley era evidente. Es por esto que para incorporar disposiciones y principios del Convenio de Budapest fue necesario modificar nuestra legislación y se presentó el proyecto de lo que hoy es la ley N° 21.459 que deroga la ley N° 19.223 que tipifica figuras penales relativas a la informática y modifica disposiciones del Código Penal.

Para analizar este proyecto de ley debemos tener en consideración la época de que se trata, año 2017 en que la tecnología ya llevaba años de desarrollo, lo que a la vez nos habla de la deficiencia en regulación que por años enfrentó nuestro país debido a que la ley N° 19.223 databa del año 1993. Según se señala, de conformidad a un informe presentado por la Policía de Investigaciones de Chile en abril de 2018, los delitos informáticos habrían aumentado en un 74% en el año 2017, en relación al 2016[52]. Lo anterior es relevante debido a que esa es la situación es una constante no solo respecto de esos años, sino que cada vez son más los delitos informáticos a causa de por ejemplo, la diversificación en las formas de comisión.

Una de las modificaciones a la ley N° 19.223 relevantes para analizar es la relativa al antigüo artículo 2. En la tabla N°1 se realiza la comparación del artículo 2 que establecía la antigua ley y el nuevo artículo 2 modificado en virtud de la ley N° 21.459.

Tabla N° 1. Comparación del artículo 2° de la ley N° 19.223 y el establecido en la ley N°21.459.

Artículo 2 Ley N° 19.223	Artículo 2 Ley N° 21.459
El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.	***Acceso ilícito**. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.*

[52] Boletín N° 12.192-25

	Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. *En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo*.

Fuente: Elaboración propia.

El nuevo artículo en su inciso segundo establece lo mismo que el antiguo artículo sobre el ánimo de apoderarse o usar la información, manteniendo la misma pena pero como un agravante de la pena debido a que esta aumenta en caso de cumplirse esto, y añadiendo el caso de quien divulgue la información adquirida de forma ilícita no haya sido quien la obtuvo. Si la obtención de la información y la divulgación de la misma fuere realizada por la misma persona se establece la pena de presidio menor en sus grados medio a máximo.

Esta comparación es interesante porque tal como sostienen Sebastián Becker y Pablo Viollier, en el antiguo artículo 2 la redacción del tipo exige la existencia de una predisposición subjetiva del hecho: el ánimo apoderarse o conocer indebidamente la información contenida en un sistema informático[53]. Sobre lo mismo, Escalona sostiene que el incluir un elemento subjetivo junto con uno objetivo no sería una técnica legislativa recomendable “no sólo porque mezcla los planos objetivo y subjetivo a nivel comisivo, sino porque podría llevar a pensar que quien actúa sin autorización no necesariamente lo hace de manera deliberada e ilegítima”[54]. Artículo que además genera problemas de interpretación para quienes consideran per se delictiva la conducta del acceso no

[53] BECKER CASTELLARO, SEBASTIÁN; VIOLLIER BONVIN, PABLO. (2020). La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley 19.223. Revista de derecho (Concepción), 88(248), 75-112. <https://dx.doi.org/10.29393/rd248-13icsb20013> [Consultado: 16/07/2023].

[54] Mayer, Laura; Vera, Jaime. El delito de espionaje informático: Concepto y delimitación. Revista Chilena de Derecho y Tecnología. 2020.

autorizado, porque debe satisfacerse este elemento subjetivo, lo cual se vuelve problemático en la medida que involucra conceptos que generan debates por la doctrina[55].

Es relevante esto en relación al hacking ético dado que bajo este supuesto, de no existir ese ánimo mencionado, no se sanciona el trabajo de los expertos en ciberseguridad que se dedican a la detección de vulnerabilidades de sistemas informáticos, tal como se mencionó en el punto 1.1 de esta investigación. En el proyecto de ley este punto se modifica con la incorporación de la frase “El que indebidamente acceda a un sistema informático”, dejando de lado la intención de la persona que realice dicha acción. Ahora bien, sabemos que finalmente la redacción del artículo fue otra, resultando una disposición que sanciona a quien sin autorización o que excediendo la que posee accede al sistema informático donde el ánimo del que ya se ha hablado se contempla como una agravante de la pena.

De lo anterior podemos concluir que el resultado del proceso mencionado fue la penalización del hacking ético, dado que el artículo 2° de la ley N° 21.459 finalmente penaliza el mero ingreso a un sistema informático, incluso aunque se realice de buena fe como lo haría un investigador especializado.

Lo anterior puede ser visto como una falencia de la legislación dado que en la redacción del artículo en la nueva ley podría haberse considerado una excepción en el caso de tratarse de hacking ético, esto considerando que fue un tema debatido durante la discusión del proyecto de la ley actual.

Ahora bien, los delitos informáticos no admiten comisión culposa por la naturaleza de los mismos: los conocimientos necesarios para llevar a cabo un delito informático impiden que haya una imprevisión por parte del sujeto activo respecto del significado de su conducta y sus consecuencias[56], lo que nos lleva a sostener que la exigencia del dolo en la redacción del artículo no fue vista como algo que cambie el hecho de que la intromisión sin autorización constituye un delito por vulnerar intereses o bienes jurídicos, idea que se desarrollará más adelante en la sección 1.2 del Capítulo II sobre los eximentes de responsabilidad penal.

[55] Escalona, Eduardo. El hacking no es (ni puede ser) delito. 2004. Revista Chilena de Derecho Informático. 4. p.151.
[56] Moscoso, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista Chilena De Derecho Y Tecnología, 3(1). p.22.

1.4 PROYECTO DE LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN

Este proyecto se desarrolla en conjunto con distintos Ministerios; el Ministerio Secretaría General de la Presidencia, Ministerio de Ciencia, Tecnología, C e I, Ministerio de Defensa Nacional, Ministerio de Economía, Fomento y Turismo, Ministerio de Energía, Ministerio de Hacienda, Ministerio de Justicia y de Derechos Humanos, Ministerio de Minería, Ministerio de Relaciones Exteriores, y por último el Ministerio de Transporte y Telecomunicaciones.

Mediante el Boletín N° 14.847-06 del 2 de marzo de 2022[57] se presentó el proyecto de ley, iniciado en Mensaje del ex Presidente Sebastián Piñera, para ser ingresado a tramitación el 15 de marzo de 2022.

En el artículo 1° se estableció que el objeto de la ley era establecer la institucionalidad, principios y normativa que permitan regular las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; además de establecer requisitos mínimos que permitan prevenir y dar respuesta de incidentes de ciberseguridad[58]". Artículo que posteriormente ha sido modificado, por lo cual la tabla N° 2 a continuación contiene cambios realizados a modo de comparación.

Así como este artículo, varios han corrido la misma suerte, sufriendo modificaciones. Otro cambio relevante es la que sufrió el título IV, al que incluso se le cambia el encabezado, donde se contempla el deber de informar las vulnerabilidades e incidentes de ciberseguridad, lo que nos lleva a sostener que protegía la figura del hacking ético. Esto debido a que puede ser entendido como una ayuda, una figura que contribuye a lo que pretende regular este proyecto de ley, lo que hubiera contribuido a dejar atrás trabas que representa la ley N° 21.459 para el hacking ético.

[57] CHILE. Proyecto de ley, iniciado en Mensaje del ex Presidente de la República, señor Sebastián Piñera Echeñique, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14.847-06, 2 de marzo de 2022. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06
[58] Idem.

Tabla N°2. Comparación de modificaciones realizadas al artículo 1 en el Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

Artículo 1° presente en el Boletín N° 14.847-06 (2 de marzo de 2022).	**Artículo 1° presente en Oficio de Ley a Cámara Revisora (26 de abril de 2023).**	**Modificación al artículo 1° realizada en el Oficio del Presidente de la República (N°103-371), mediante el cual formula indicaciones al proyecto.**
Objeto. *La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permiten estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los órganos del Estado así como los deberes de las instituciones privadas que posean infraestructura de la información calificada como crítica y, en ambos casos, los mecanismos de control, supervisión y de*	Objeto. *La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.* *Para los efectos de esta ley, se entenderá por*	Se elimina la frase: *No se aplicarán las disposiciones de esta ley a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital.*

responsabilidad por la infracción de la normativa.	*Administración del Estado a los ministerios, las delegaciones presidenciales regionales y provinciales, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, las Fuerzas de Orden y Seguridad Pública y los órganos y servicios públicos creados para el cumplimiento de la función administrativa. Los órganos autónomos constitucionales se ajustarán a las disposiciones de esta ley que así lo señalen. <u>No se aplicarán las disposiciones de esta ley a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital.</u>* *La institucionalidad de la ciberseguridad velará por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias, que comprende la adopción de las medidas necesarias e*	

	idóneas para garantizar la integridad, confidencialidad, disponibilidad y resiliencia de la información que contengan sus redes y sistemas informáticos, incluyendo las herramientas de cifrado.	

Fuente: Elaboración propia basada en: Boletín N° 14.847-06, Oficio de Ley a Cámara Revisora (26 de abril de 2023) y Oficio del Presidente de la República (N°103-371).

Este proyecto es de especial relevancia porque modifica la regulación del hacking ético. En primer lugar crea la Agencia Nacional de Ciberseguridad, servicio público que dentro de sus funciones destacan el asesoramiento al Presidente de la República en lo relativo a la ciberseguridad y la fiscalización tanto de instituciones privadas como de los órganos de la Administración del Estado en lo relativo a ciberseguridad.

Además, en el artículo 3 aprobado por el Senado se contemplan principios rectores a tener en consideración al momento de aplicar la ley. Dicho artículo contemplaba 8 principios: el de responsabilidad, protección integral, confidencialidad de los sistemas de información, integridad de los mismos, de disponibilidad en el sentido de estar accesibles para su uso, control de daños que exige tomar las medidas necesarias a tiempo para evitar lamentar un problema de mayor envergadura, por último el principio de cooperación con la autoridad y la especialidad de la sanción.

Siguiendo la línea de las modificaciones, el artículo 46 contenido en el título X “De las modificaciones a otros cuerpos legales” del texto sugerido que dice relación con el artículo 2 de la Ley N° 21.459 incorpora una modificación a dicho artículo a modo de eximente de responsabilidad penal.

El artículo señala que “*No será objeto de sanción penal el que, realizando labores de investigación en seguridad informática, hubiere incurrido en los hechos tipificados en el inciso primero, siempre que se cumplan las siguientes condiciones:*
1) Haber reportado el acceso y las vulnerabilidades de seguridad detectadas en su investigación al responsable de las redes y sistemas informáticos afectados, en forma

inmediata y a más tardar en el momento en que alerte a la Agencia Nacional de Ciberseguridad;
2) Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia Nacional de Ciberseguridad;
3) Que el acceso no haya sido realizado con el ánimo de apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, ex filtración o destrucción de datos, y
4) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad.
Tampoco será objeto de sanción penal la persona que comunique a la Agencia información sobre una vulnerabilidad potencial de la que haya tomado conocimiento en su contexto laboral o con ocasión de la prestación de sus servicios, ni se considerará que ha incumplido con ello su obligación de secreto profesional."[59].

Esto significa, sin dudas, una protección legal al hacking ético y según Alejandro Hevia, las condiciones que exige hacen casi imposible que se utilice el hacking ético para cubrir accesos ilícitos realizados por ciberdelincuentes[60].

Por lo anterior es que esto constituye un gran avance en la regulación informática en nuestro país, no solo en cuanto al hacking ético, sino que para la ciberseguridad en general porque tal como se señala en el Informe de la Comisión de Hacienda sobre el proyecto de ley, este "crea un modelo de gobernanza que promueve la gestión de riesgos y la implementación de estándares de ciberseguridad, para mejorar la prevención, contención, resolución y respuesta de incidentes y ciberataques"[61]. Siendo esto un paso importante hacia la protección de los sistemas de información y por consiguiente de los derechos de los usuarios de los mismos.

---

[59] Oficio de ley a Cámara Revisora. 26 abril de 2023. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06

[60] Informe de la Comisión de Seguridad Ciudadana recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14.847-06 (S). 27 noviembre de 2023. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/informes.aspx?prmID=15344&prmBOLETIN=14847-06

[61] Informe de la Comisión de Hacienda, recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14.847-06

A inicios de diciembre del presente año, se presentó el primer informe de la Comisión de Hacienda recaído en este Proyecto de Ley donde se señala que fueron aprobados por unanimidad de los presentes (a excepción del artículo 2 transitorio) todos los artículos.

2. LA AUTORIZACIÓN COMO REQUISITO

Se ha mencionado antes el consentimiento, y al respecto, en el artículo 2 de la Ley N° 21.459 se tipifica el acceso ilícito a sistemas informáticos, y se establece que "sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales…"[62]. Esto nos lleva al requisito esencial que se contempla para poder realizar el hacking ético de forma lícita, el consentimiento, esto es, la autorización expresa del titular del sistema informático.

Entonces, la prohibición de acceder a un sistema establecida por la ley se puede dar por dos supuestos. El primero en el caso de no existir la autorización, ya sea por la ausencia de la misma o por exceder los límites de ella, y el segundo caso por la violación de las barreras técnicas, lo que haría que esta redacción funcione tanto para sistemas abiertos, en que no existen las barreras técnicas para controlar el acceso y por consecuencia, se cuenta con la autorización, como para los sistemas cerrados en que si existen estas barreras[63].

La especificación que se realiza con respecto a la forma en que el consentimiento debe ser otorgado, esto es de forma expresa, excluye la posibilidad de que se pueda hacer de forma tácita, por ejemplo, pudiendo simplemente no iniciar ninguna acción ante la detección de una intromisión al sistema de información. Cuestión que genera dudas, dado que si el propio encargado del sistema decide no judicializar el asunto y acepta la ayuda de quien alerta las vulnerabilidades, ¿por qué alguien más debería sancionar dicha acción?

---

[62] Ley N° 21.459, Artículo 2, establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

[63] Navarro-Dolmestch, R. (2023). La autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos. https://d1wqtxts1xzle7.cloudfront.net/105727397/navarro-libre.pdf?1694711256=&response-content-disposition=inline%3B+filename%3DLa_autorizacion_como_causal_de_atipicida.pdf&Expires=1701624707&Signature=MU04NPFl0fLfOzEJbD4sOC65IVVEkujLPFLN40Ml1AERi8YtmHauteKLQ0yTjbMFaTaPi~fM4~i97ez89CvobHzFjnlw10KLTRuzF7Ca77MpFKZsSELX9i5GVxm~LvmMw1yR4qsDkIN~7A4v~-SXx8tfpF4COzTrL3QMSdrqOwnNMbBDdQwVjgw3Lwe29bCK76LVl1MDFTugm3QTbVHDhPB8vn36oUwprvjpdWwvg3ar7vAmy3OukG3o0nJIFk5n4iY0PTr70E-YfKNXO4GKX4QZf0Tu2ygBlET8sohkRxc--5EfAJy-itpDcHnZ9o6YLLtssyEWsMXErp7ChffGrQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Entonces, la falta de autorización desaparecerá sólo en caso de manifestación expresa o, a lo menos, exteriorizada de tal voluntad por la víctima[64]. Siendo aquello la línea divisoria para lograr diferenciar entre un delito y el hacking ético como rama de la seguridad tecnológica dirigida a prevenir, erradicar, estabilizar y contraatacar vulnerabilidades de software o de hardware[65].

Esta autorización se entiende que debe ser anterior a la realización de la conducta, dado que una otorgada de forma posterior no excluiría la ilicitud de la misma, pero que a pesar de esto, en el supuesto de que se haya llevado el caso ante la justicia, esta autorización posterior podría llevar a un acuerdo reparatorio[66].

Debido a lo anterior es que en caso de omitirse este requisito estaríamos frente a una conducta establecida como delito por la ley y de esta forma es la autorización expresa la que permite que no se configure el delito dado que es la manifestación de acuerdo del titular del sistema informático con respecto a la intromisión al mismo por parte de un *white hacker.*

De acuerdo con lo anterior, parece carecer de importancia el fin con que se realiza el hacking ético dado que en todos los casos se exige el consentimiento expreso, no siendo relevante si el hacking se realiza de buena fe con la mera intención de detectar vulnerabilidades del sistema como podría ser el caso del experto informático que, para estar al día en sus conocimientos, “practica” acceso a soportes lógicos para detectar vulnerabilidades y fortalezas de sistemas ejecutados por otros[67]. Esto porque el ánimo exigido no tiene nada que ver con la producción de un resultado dañoso sobre la información[68].

El objetivo de analizar el elemento del consentimiento es precisamente, estudiar la problemática que gira en torno a él, dado que genera discusión en el sentido de que por una

---

[64] Escalona, Eduardo. El hacking no es (ni puede ser) delito. 2004. Revista Chilena de Derecho Informático. 4 , 149-167.
[65] ALAIN EDUARDO RODRÍGUEZ LLERENA, Herramientas fundamentales para el hacking ético, Revista Cubana de Informática Médica 2020, <https://www.medigraphic.com/pdfs/revcubinfmed/cim-2020/cim201j.pdf> [Consultado: 15/07/2023], p.117.
[66] Canal Uchilederecho. Ciclo de charlas sobre derecho informático. Nueva ley de delitos informáticos y principales aspectos para su implementación. 4 de mayo de 2022 [archivo de video], minuto 54:27. https://www.youtube.com/watch?v=Y-TV3oRY82U
[67] Escalona, Eduardo. El hacking no es (ni puede ser) delito. 2004. Revista Chilena de Derecho Informático. 4 , 149-167.
[68] Moscoso, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista Chilena De Derecho Y Tecnología, 3(1). p.33.

parte se puede entender como un limitante al desarrollo del hacking ético y por otra parte encontramos la postura que defiende la criminalización de esta herramienta.

Con respecto a la primera postura en contra de la criminalización del hacking ético, esto estaría justificado por el principio de "respeto histórico al ámbito legal de lo prohibido", del que se deduce que no puede ni debe criminalizarse conductas que carecen de la entidad suficiente para ser normativamente consideradas delictuales[69]. Lo anterior porque si penalizamos, por ejemplo, el mero acceso al sistema de información, se le está imponiendo una pena, y por lo tanto, asignando un riesgo a una conducta que por sí sola no lesiona un bien jurídico, sino que llega a provocar el daño en el caso de consumarse.

Esta segunda postura a favor de la criminalización del hacking ético postula que el acceso a un sistema informático, a pesar de ser sin intención de generar un daño al mismo o a la información en él contenida, debe ser penalizado de todas formas debido a que se ponen en riesgo los datos e información que son de tal importancia que no merece la pena arriesgarse a que exista dicho riesgo. Además, estas motivaciones que antes se creían eran de aprendizaje y demostración de habilidades, han cambiado para hoy ser la comisión de delitos que antes se realizaban de forma tradicional[70].

Otro argumento a considerar para defender esta postura es el cómo afecta a empresas o instituciones el que se acceda a sus sistemas de información sin contar con la autorización, en la medida que se ve perjudicada la imagen de estos al demostrar que en definitiva los datos que entregan los usuarios no está del todo segura bajo su administración.

La ley N° 21.459 en su artículo 16° trata la autorización y establece: "Autorización e Investigación Académica. 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".

Este artículo lo que hace es establecer nuevos casos de atipicidad además de lo señalado en el artículo 2. El primer supuesto es en el marco de investigación de vulnerabilidades y el segundo, mejorar la seguridad del sistema[71].

---

[69] Ibid, p.160.
[70] Ibid.
[71] Navarro-Dolmestch, R. (2023). La autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos, p. 11.

Lo cual es de gran avance para nuestra legislación, ya que como se mencionó anteriormente, antes de que empezara a regir dicha ley, nuestra legislación no contaba con ninguna referencia al hacking ético, principalmente debido su fecha de publicación en 1993, cuando el internet contaba con un incipiente avance en nuestro país. Es por eso que esta normativa viene a subsanar un vacío legislativo, que en nuestra época hiper digitalizada es de gran importancia, debido principalmente a su función preventiva contra ataques cibernéticos, la cual nos permitirá identificar qué incidentes podrían ocurrir antes de que sucedan y, posteriormente, reparar o mejorar el sistema, de forma tal que se eviten estos ataques[72].

Cabe destacar que en derecho comparado, específicamente en el caso de España, tampoco se definió el hacking ético y se realiza la misma especificación que hace nuestra legislación, la necesidad de acceder con autorización de los titulares de los datos o programas informáticos[73], estableciendo también al hacking ético como un delito si se realiza sin ella. Ello en razón de una búsqueda para el endurecimiento de penas contra ciberdelincuentes.

Ahora bien, entendemos que, tal como se mencionó anteriormente, la ley N° 21.459 es un avance en cuanto a la regulación del hacking ético sobre todo si consideramos que antes no era mencionado. Pero de igual forma es relevante destacar, que si bien se hizo referencia a él, no se definió claramente ni se enmarcaron requisitos claros y concisos que se debían cumplir para ser afecto a dicha definición. Dejando graves vacíos que son perjudiciales para toda la comunidad, ya que si una persona detecta e informa sobre un fallo de sistema de una organización, en la actualidad, correrá el riesgo de ser sancionado por cometer un delito. Asimismo, tampoco se aclaró que si bajo el contexto de una mera investigación, su notificación deberá realizarse en un plazo determinado o si dicha investigación debe ser demostrada o notificada de alguna manera formal.

Requisitos como el consentimiento, notificación oportuna de brecha, confidencialidad, el no daño al sistema y un objetivo legítimo, son a nuestro entender, de total importancia para permitir e incentivar el uso de esta herramienta de investigación de brechas de seguridad, siempre bajo un contexto matizado y responsable para con los usuarios, propietarios e

[72] ALAIN EDUARDO RODRÍGUEZ LLERENA, Herramientas fundamentales para el hacking ético, Revista Cubana de Informática Médica 2020, <https://www.medigraphic.com/pdfs/revcubinfmed/cim-2020/cim201j.pdf> [Consultado: 15/07/2023], pp. 121

[73] Artículo 197 del Código Penal español.

investigadores de dichos sistemas informáticos. Todo lo cual, nos permite determinar que se dejó de nuevo un vacío en esta materia.

Si bien, como parte de la doctrina sostiene, la exigibilidad de la autorización expresa podría limitar la realización de hacking ético, hay que considerar que el Derecho Penal no tiene que promover determinadas conductas de ciberseguridad por sobre otras dado que no es esa su función, y por lo tanto, la razón de tipificar esta conducta es proteger uno o más bienes jurídicos que se ponen en riesgo con la realización del mismo.

CAPÍTULO II. CONSIDERACIONES DEL DERECHO PENAL

1.1. ¿MERECE REPROCHE PENAL?

Es importante reiterar, que hoy en el siglo XXI, los avances tecnológicos han conquistado diferentes ámbitos de la vida moderna. Surgiendo en consecuencia, nuevos fenómenos delictivos y nuevas formas de cometer los viejos delitos[74], especialmente, a través de sistemas o redes informáticas de transmisión e intercambio de datos por Internet[75], la llamada cibercriminalidad. La cual, si bien en nuestra legislación no tiene una definición propiamente tal, existe un acuerdo aceptado, que "trata de un término que hace referencia a un conjunto de actividades ilícitas cometidas al amparo del uso y el abuso de las tecnologías de la información y la comunicación, poniendo en peligro o lesionado intereses o bienes jurídicos de naturaleza individual, o bien, amenazando la seguridad de los sistemas sociales"[76]. Por lo cual, para algunos autores como Héctor Álvarez Fortte, lo hace un tema ineludible para el derecho penal. Efectivamente la defensa del bien jurídico otorga una base al sistema punitivo, la dota de sustento y permite que este realmente castigue a sus trasgresores cuando se han vulnerado derechos dignos de ser protegidos penalmente[77]

Asimismo, se debe entender dicho precepto bajo un contexto de un fenómeno generalizado, que da cuenta de la creencia de que el derecho penal todo lo soluciona[78]. Desconociendo circunstancias que pueden hacer que el peligro desaparezca, o bien que sea posible enfrentarlo eficazmente con otro tipo de reacciones como la autorregulación, la persecución de la responsabilidad civil o hasta la creación de una institucionalidad administrativa (normas, responsabilidad, órgano fiscalizador). Sosteniendo incluso, bajo la opinión del autor Nicolás Oxman[79], que no es suficiente con prevenir estos hechos ya sea a través del pago de indemnizaciones civiles a los titulares, sanciones administrativas u otros medio de

---

[74] Regional y Subregional Andina, R. J. (s/f). *Corpus Iuris Regionis*. Unap.cl.pp. 101 https://www.unap.cl/prontus_unap/site/docs/20180425/20180425122950/corpus_iuris_9.pdf

[75]Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". *Revista de Derecho*, *41*, 211–262. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007#footnote-35037-5

[76] Idem

[77]Héctor Álvarez Fortte, https://www.unap.cl/prontus_unap/site/docs/20180425/20180425122950/corpus_iuris_9.pdf pp.109

[78] Moscoso, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista Chilena De Derecho Y Tecnología, 3(1). p.74 <https://doi.org/10.5354/0719-2584.2014.32220>

[79] https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007#footnote-35037-6

prevención y educación ciudadana, ya que no resulta ser lo bastante disuasorio para no cometer ataques contra intereses o derechos constitucionales.

Por lo cual, bajo dicho escenario nuestro legislador ha optado por disposiciones penales para demarcar límites precisos en pos de lograr un entorno seguro en la red. Redactando dichas normas, como se ha dicho y se desarrollará más adelante, bajo acuerdos internacionales para así lograr una uniformidad entre fronteras, con el objetivo de facilitar su persecución y debido a complejidad operativa, impidiendo así incrementar los niveles de impunidad.

Con ello ya comprendido, nos podemos preguntar ¿porque en una ley especial?. Si bien es una discusión antigua, nos ayudará a comprender mejor la historia misma de nuestra legislación en esta materia.

En relación a dicha pregunta surgieron diferentes corrientes en el tratamiento de delitos informáticos propiamente tales. Por un lado, una "corriente postula tratar los delitos informáticos como una nueva pequeña rama del Derecho penal, este es el modelo fenomenológico. La segunda corriente, intenta integrar el tema de los delitos informáticos en el campo ya regulado por el Derecho penal, introduciendo solo las modificaciones o ampliaciones legislativas necesarias en los tipos penales tradicionales, de manera tal de poder comprender en ellos la ejecución de los tipos por medio de mecanismos informáticos"[80]. Cabe señalar que, difícilmente se encontrarán países que adhiera puramente[81] a alguna de las corrientes.

En la actualidad, con la Ley N° 21.459, podemos afirmar que, si bien, el legislador intentó sistematizar los delitos informáticos, se optó por la primera corriente, perdiendo la oportunidad de tratar a los delitos informáticos, en este caso al acceso ilícito, de una forma orgánica. Prefiriendo la actualización de una norma especial y creando una nueva serie de figuras penales relativas a la informática. Opción la cual otras legislaciones no siguieron, punto el cual se desarrolla más adelante. Optado por introducir modificaciones en el ordenamiento penal general, de manera tal de abarcar aquellas conductas que, por vía de la informática, podían afectar bienes jurídicos ya protegidos[82].

---

[80] Regional y Subregional Andina, R. J. (s/f). *Corpus Iuris Regionis*. Unap.cl.pp 104, https://www.unap.cl/prontus_unap/site/docs/20180425/20180425122950/corpus_iuris_9.pdf

[81] Magliona, Claudio y Lopez, Macarena, Delincuencia y Fraude Informático:81 Derecho comparado y Ley Nº19.223, Editorial Jurídica de Chile, pp81

[82] Regional y Subregional Andina, R. J. (s/f). *Corpus Iuris Regionis*. Unap.cl.pp 102 https://www.unap.cl/prontus_unap/site/docs/20180425/20180425122950/corpus_iuris_9.pdf

Asimismo, en opinión de la autora Laura Mayer, dicha corriente permitirá dar respuesta sistemáticamente y razonablemente adecuadas, desde un punto penológico[83] y sistemático, dado que una aproximación fenomenológica eventualmente lleva a problemas de legitimación y coherencia normativa[84].

En relacion a esto último, España se inclinó por asociar comportamientos constitutivos de delitos informáticos a otras conductas que lesionan o ponen en peligro algún bien jurídico ya protegido por la legislación penal general[85]. Ejemplo de ello, es que se agregó en el apartado de descubrimiento y revelación de secretos ya existente dentro del Código Penal Español, el artículo *197 BIS* donde se tipifica el acceso ilícito.

La misma forma de abordar este tema es la que tomó Alemania a través de la Segunda Ley contra la Criminalidad Económica e Italia con la Ley 547 de 1993[86].

1.2. BIEN JURÍDICO PROTEGIDO

"Toda pena, dice el gran Montesquieu, que no se deriva de la absoluta necesidad, es tiránica; proposición que puede hacerse más general de esta manera: todo acto de autoridad de hombre a hombre que no se derive de la absoluta necesidad, es tiránico"[87].

Como sostiene Beccaria, debe existir una necesidad para establecer una norma, llevado al caso concreto, se requiere un motivo para tipificar ciertas conductas, esto considerando que tipificar una conducta corresponde al medio punitivo más grave, en cuanto restrictivo de derechos fundamentales básicos, sólo estará materialmente legitimada cuando pretenda la

---

[83] Seminario Virtual: La regulación chilena de los delitos informáticos, Pontificia Universidad Catolica, minuto 47:23 https://www.youtube.com/watch?v=AKN6s8tJI-g&t=1505s

[84] CHILE. Informe de la Comisión de Ciencias y Tecnología recaído en el Proyecto de Ley que modifica el Código Penal, con el objeto de recepcionar en los tipos penales tradicionales, nuevas formas delictivas surgidas a partir del desarrollo de la informática. Boletín Nº 3.083-07, 11 de noviembre de 2002. Disponible en: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=3083-07

[85] https://www.unap.cl/prontus_unap/site/docs/20180425/20180425122950/corpus_iuris_9.pdf , pp104

[86] CHILE. Informe de la Comisión de Ciencias y Tecnología recaído en el Proyecto de Ley que modifica el Código Penal, con el objeto de recepcionar en los tipos penales tradicionales, nuevas formas delictivas surgidas a partir del desarrollo de la informática. Boletín Nº 3.083-07, 11 de noviembre de 2002. Disponible en: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=3083-07

[87] Beccaria, Cesare. Tratado de los delitos y las penas. P.19

protección de bienes básicos para la vida de las personas en sociedad y, además, sólo si ese objetivo no puede lograrse de otro modo[88].

Por lo que esta limitación de establecer que el Derecho Penal sólo castiga ataques a bienes jurídicos se trata de un planteamiento político-criminal que tiene como objetivo limitar el uso del Derecho Penal a situaciones en que sea estrictamente necesaria su intervención[89], y es debido a esto que el catálogo de intereses que subyace al Derecho penal nuclear se encuentra integrado por la vida, la salud, la libertad, la propiedad y el honor[90].

Si bien no existe una única definición del concepto de bien jurídico, esto se debe a que no se trata de algo estático. Una de las definiciones es la que establece Roxin al sostener que son circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema social global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del propio sistema[91].

Entonces, los bienes jurídicos o intereses protegidos serán distintos dependiendo la sociedad y la cultura de la que se trate, y del sistema de valores filosóficos y políticos que la inspiren[92]. Es así que el bien pasa a ser llamado bien jurídico cuando el interés de su titular es reconocido como social o moralmente valioso por el legislador[93].

En ese sentido, Etcheberry sostiene que el interés es la posición de un sujeto frente a un bien, y bien es todo aquello que puede satisfacer una necesidad humana, material o idea (individual o social)[94].

En base a esto podemos sostener que el interés que se protege con esta norma es el de esa persona que vela por el correcto funcionamiento del sistema, quien coordina, autoriza y gestiona todo lo que ocurre en él. Es por esto que para sancionar una acción, en este caso el hacking ético sin autorización expresa, esta debe lesionar uno o más bienes jurídicos, a tal punto que se limite la libertad individual para evitar que ocurran esas vulneraciones.

---

[88] Rodríguez, Samuel. ¿Ha de cumplir el bien jurídico protegido una función de garantía o legitimadora del Derecho Penal? Hacia una búsqueda de la legitimidad material de las normas penales. Revista de Derecho, Universidad San Sebastián. 2017. P.159.
[89] Mir, Santiago. Bien jurídico y bien jurídico-penal como límites del Ius puniendi, 1989/1990, p.205.
[90] Mayer, Laura y Fernandes, Inês. La estafa como delito económico. p. 187.
[91] Roxin, Claus. Derecho Penal, parte general. Tomo I. Fundamentos, la estructura de la teoría del delito. P.56
[92] Etcheberry, Alfredo. Derecho Penal parte general, Tomo I. Tercera edición. P.29.
[93] Ibid.
[94] Ibid.

Lo anterior se refiere a los bienes jurídicos que se protegen mediante el Derecho Penal, intereses que se ven amparados producto de la prohibición de una conducta por la ley y es en este contexto, que el interés del titular de un sistema informático surge con el desarrollo de la tecnología, incrementando la necesidad de su protección debido al veloz avance del internet, lo que conlleva más instancias de vulnerabilidad.

Es por esto que en el caso de comisión del delito, es el titular del sistema la víctima del mismo, pudiendo tratarse de una persona natural o jurídica, a pesar de que en términos generales –como acontece respecto de muchos otros delitos–, la identidad de la víctima es secundaria para la ejecución de un delito informático. En ese sentido, el autor más bien está pendiente de descubrir vulnerabilidades en un sistema informático cualquiera o en un determinado sistema informático, mediante el que pueda llegar a afectar a cualquier individuo[95].

Por esto, surge entonces la pregunta sobre cuál es esta necesidad o motivo que lleva a establecer en el artículo 16° de la ley N° 21.459 como requisito la autorización expresa para realizar de forma lícita el hacking ético en el marco de la investigación académica, y en caso de que se realice contraviniendo esta norma establecer la pena de presidio menor en su grado mínimo o una multa.

Ahora bien, en lo relativo a los delitos informáticos es posible distinguir dos teorías, estrechamente vinculadas con la forma que adopta (o debería adoptar) la tipificación de dichos delitos[96].

La primera teoría sostiene que el bien jurídico que se pretende tutelar con la creación de estas figuras delictuales es uno específico, uno propiamente informático. Esto permite hacer una diferencia con los bienes jurídicos implicados en los demás delitos que contiene el Código Penal, lo que lleva a explicar el hecho de que se regulan en leyes especiales y no las contenga dicho catálogo de delitos, evidencia de esto es la Ley N° 19.223, en cuyo proyecto de ley se sostuvo que este tenía por finalidad proteger este nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan[97].

---

[95] Mayer, Laura. Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos.
[96] Mayer, Laura. “El Bien Jurídico protegido en los Delitos Informáticos”. Revista Chilena de Derecho, Vol. 44, Nº 1, Chile, Pontificia Universidad Católica de Chile, 2017.
[97] Historia de la Ley Nº 19.223, Tipifica figuras penales relativas a la Informática.

Lo anterior no está exento de críticas y sería el primer error de la Ley N° 19.223 al identificar un bien jurídico amplio en términos de cualidades de la información como aquel interés socialmente protegido dado que no puede ser uno planteado en términos genéricos y que no otorgue ningún elemento de distinción en torno a otros objetos materiales, de aquellos protegidos por los tipos penales tradicionales[98].

Ese bien jurídico señalado por la ley N° 19.223 encontraría su razón debido a las características propias de los delitos informáticos, lo que explicaría entonces el surgimiento de un bien jurídico autónomo consistente en la integridad, confidencialidad y disponibilidad de los sistemas informáticos y de los datos contenidos en ellos[99].

Estos conceptos son los que Allan Friedman y Peter Singer establecen como los tres objetivos en materia de seguridad de la información, llamándola la "tríada *CIA*" por las siglas en inglés de las palabras: *Confidentiality, Integrity, Availability*. La primera referida a mantener la privacidad de los datos, considerando los datos sensibles que permitan revelar detalles importantes sobre relaciones de los individuos o empresas, esto a través de herramientas como el cifrado y códigos de acceso. La integridad tiene que ver con que los datos que se contengan en el sistema de información no se alteren o modifiquen sin la debida autorización, y por último la disponibilidad en relación a que se pueda hacer uso del sistema tal como se previó[100].

Es tal la importancia de estos objetivos que el Convenio sobre Ciberdelincuencia sostiene que es su objetivo al señalar que es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos[101].

A su vez, esta primera postura puede subdividir en dos variantes dependiendo de si se sostiene que se trata de un bien jurídico específico pero común a todos los delitos informáticos o si cada cual afecta un bien en particular, el que igualmente sería específico de esta clase de delitos. En el primero de los casos, el propio proyecto de ley N° 19.223 establecería ese bien específico y común siendo la calidad, pureza e idoneidad de la información. Estos términos utilizados llevan a la interrogante sobre qué procedimiento o

[98] Moscoso, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista Chilena De Derecho Y Tecnología, 3(1). p.15.
[99] Bascur, Gonzalo y Peña Rodrigo. Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Primera parte. Revista de Estudios de la Justicia. 2022, p.4.
[100] Singer, Peter & Freidman, Allan. Cybersecurity and Cyberwar. Oxford, Reino Unido, Oxford University Press, 2014, p. 35.
[101] Preámbulo del Convenio de Budapest.

según qué criterios es posible sostener que una información es de calidad, pureza o idoneidad[102], lo cual vuelve problemática la cuestión acerca de la terminología usada.

En cuanto a la segunda tesis, esta sostiene que no se trata de un bien jurídico especial, sino que serían los mismos bienes jurídicos tradicionales los que se ven afectados por los delitos informáticos. Consiguientemente, según este planteamiento, la diferencia entre un delito informático y otros delitos sería meramente de forma y no de fondo[103].

En base a lo anterior, los bienes jurídicos tradicionales que pueden destacarse son la privacidad, y en cuanto a la información y datos propiamente tales contenidos en los sistemas informáticos, la confidencialidad y la propiedad de estos. Tal como sostiene Mayer, en base a esta postura, el elemento informático de los delitos del mismo nombre es la forma en que se afectan estos bienes jurídicos tradicionales, la antes llamada forma de comisión y no el hecho de que tutelan intereses distintos de esa índole.

1.2.2 AFECTACIÓN DE BIENES JURÍDICOS PARTICULARES

Hasta ahora se ha hablado del hacking ético como una herramienta de la ciberseguridad propendiendo generar un beneficio para los involucrados, pero puede ser analizado desde otra perspectiva, la amenaza de hacking ético.

La frase "*el normal funcionamiento, total o parcial, de un sistema informático*" del artículo 1 de la ley N° 21.459 corresponde al bien jurídico protegido con la tipificación de los delitos que dicha ley contiene, pero esta clase de delitos son pluriofensivos, es decir, este no es el único bien que afectan y que, por lo tanto, se buscan proteger[104].

Además, de la mano de la discusión antes planteada sobre si debía hablarse de un bien jurídico informático propio de esta clase de delitos o que estos involucran en definitiva bienes jurídicos tradicionales, y sosteniendo la segunda postura es que podemos hablar, por ejemplo, de la privacidad.

[102] Mayer Lux, Laura. "El Bien Jurídico protegido en los Delitos Informáticos".
[103] Ibid, p.6.
[104] Chávez, Eric. Derecho Penal Parte Especial. Cuarta Edición, 2023.

Ahora bien, tal como se señaló anteriormente, no se trata de sostener que solamente se atenta contra estos bienes jurídicos, como la privacidad, intimidad o el patrimonio, sino que se ven involucrados diversos intereses colectivos[105].

A. PRIVACIDAD

La privacidad deriva del derecho a la libertad[106] y está consagrada en la Declaración Universal de los Derechos Humanos[107] y en el Pacto Internacional de Derechos Civiles y Políticos de 1966[108].

Nuestra Carta Fundamental consagra derechos esenciales, entre ellos el derecho a la protección de la vida privada y la protección de los datos personales como establece en su artículo 19 N°4.

Tal como se señaló con anterioridad, los delitos informáticos pueden amenazar bienes jurídicos tradicionales y la privacidad no es la excepción a ello. Evidencia de esto es que, por ejemplo, España decidió incorporar en el Código Penal, precisamente, en el capítulo de delitos contra la intimidad, las conductas constitutivas de hacking[109].

Con respecto a esto, el Código Penal en el Título Tercero de los crímenes y simples delitos que afectan a los derechos garantizados por la Constitución, establece delitos que atentan contra la vida privada y pública de las personas. En específico el artículo 161 A enumera diversas acciones a desarrollarse en un recinto privado y establece una pena, esto a modo de protección de la privacidad de las personas.

Podríamos entonces hacer el símil entre lo anterior y el delito del hacking ético realizado sin consentimiento, dado que en ambos casos se ve vulnerada la privacidad aunque esto sea

---

[105] Magliona Claudio, Macarena López. Delincuencia y fraude informático. Derecho Comparado y Ley N° 19.223, Editorial Jurídica de Chile,1999, p.66.

[106] Porto Macedo, R., (2002). Privacidad, mercado e información. Cuestiones Constitucionales, (6),135-151. ISSN: 1405-9193. https://www.redalyc.org/articulo.oa?id=88500606

[107] Artículo 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. Disponible en: https://www.un.org/es/about-us/universal-declaration-of-human-rights

[108] Artículo 17: 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. Disponible en: https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[109] Álvarez Fortte, H. (2009). Los delitos informáticos. Corpus Iuris Regionis: Revista Jurídica Regional y Subregional Andina, 9(9), pp. 101-128.

realizado de distinta forma, atendida la clase de delitos de la que se trata. Esta analogía es muy útil, entrar en una casa o computadora sin autorización, aún con buenas intenciones, puede llevar a consecuencias no deseadas y lo mismo puede ocurrir con el hacking dado que muchos sistemas pueden resultar dañados accidentalmente por intrusos ignorantes o descuidados[110].

1.3. EXIMENTES DE RESPONSABILIDAD PENAL

Ahora bien, como el hacking ético es tratado en el contexto de los delitos informáticos es que debemos adentrarnos en el derecho penal propiamente tal.

Al tratarse de la tipificación del hacking ético bajo el supuesto de no contar con autorización expresa, es que tenemos que entender que estamos frente al Ius Puniendi, entendido como como la facultad que tiene el Estado para castigar, el cual se limita a través de, por ejemplo, el principio de legalidad.

Así como el Estado tipifica conductas, también puede establecer circunstancias modificatorias de responsabilidad penal, entendidas como situaciones de naturaleza accidental, con existencia marginal a la estructura del tipo penal que toman en cuenta para la determinación de la pena[111], dentro de las cuales encontramos las atenuantes, agravantes y las eximentes de responsabilidad.

Las dos primeras circunstancias son las que permiten disminuir la pena establecida para una conducta típica y las agravantes, al contrario, llevan a la imposición de una pena más alta. En cambio, las eximentes de responsabilidad penal, entendidas como circunstancias que permiten al autor de un delito quedar exonerado de responsabilidad, tal como lo dice su nombre, lo eximen de responsabilidad. Entonces, si sostenemos que no se le hace responsable por realizar un acto establecido como delito en el Código Penal o en alguna ley especial, podemos sostener de igual forma que se está permitiendo realizar esa conducta cuando concurra alguna circunstancia específica.

En base a lo señalado en la sección anterior, debido a que el fin con que se realiza el hacking ético carece de importancia debido a que se exige el consentimiento expreso en cualquier caso, es que no es considerado como un eximente de responsabilidad penal, por

[110] Vásquez, Miguel. Técnicas anti-forenses informáticas. Córdoba. 2016. p.50
[111] Garrido, Mario. Derecho penal. Parte general. Tomo I, p.181.

ejemplo, el hecho de ingresar a un sistema sin la intención de apropiarse indebidamente de la información que éste contiene con el cometido de causar daño.

Lo anterior y considerando que el hacking ético es una práctica que puede ser beneficiosa para la ciberseguridad, nos lleva a la pregunta y posición contraria a la antes señalada sobre si debieran existir eximentes de responsabilidad por la comisión del delito del hacking ético sin autorización, así como las eximentes de responsabilidad criminal que establece el Código Penal para otros delitos, como son el caso del loco o demente, la fuerza irresistible o el cumplimiento de un deber, cargo u oficio, por nombrar algunas.

En relación a esto, si sostenemos que no sería relevante la presunta buena fe o falta de intención maliciosa con respecto al tratamiento de los datos encontrados en un sistema, no es posible hablar de eximentes de la responsabilidad por tales motivos. Lo anterior dado por el hecho de que la mera intromisión al sistema por sí sola ya es constitutiva del delito.

Un elemento importante para hablar de una exculpante de la responsabilidad penal es el riesgo socialmente permitido, dado que existen riesgos que pueden ser tolerados sin necesidad de tipificarlos. Entonces el riesgo permitido es la determinación de la relevancia típica de una conducta a partir de la demarcación de los límites del ámbito de competencia del agente[112]. Un caso que ejemplifica un riesgo tolerado es el de la venta de automóviles, el hecho de que estos circulen por las calles es un riesgo, más aún si transitan a altas velocidades, pero no por eso se prohíbe la venta y circulación de los mismos en las calles[113].

Ahora bien, en el campo de la informática no resulta sencilla la determinación del conjunto de conductas socialmente aceptables o, más bien, la línea divisoria constituida por el riesgo permitido, debido a que particularmente en este ámbito confluyen un sinnúmero de intereses contrapuestos en juego[114].

Esto es lo que hace que el también llamado hacking blanco sea objeto de discusión en torno a su criminalización, habiendo adeptos a la penalización de esta figura sosteniendo que el mero acceso indebido constituye un peligro de daño para los datos procesados y la antesala

[112] Caro, José. Algunas consideraciones sobre el riesgo permitido en el Derecho Penal. Forseti, Revista de Derecho, volúmen 12, N°18, Lima 2023. p. 48.
[113] Idem, p.45.
[114] Moscoso, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista Chilena De Derecho Y Tecnología, 3(1). p.37.

para la comisión de otros delitos de mayor gravedad[115] y detractores que estiman que no se produce efectivamente el daño.

Ahora bien, nuestra legislación se hace referencia al requisito de autorización en la ley N° 17.336 sobre Propiedad Intelectual, la cual establece en su artículo 71 Ñ que: "*Las siguientes actividades relativas a programas computacionales están permitidas, sin que se requiera autorización del autor o titular ni pago de remuneración alguna: …. c) Las actividades que se realicen sobre una copia obtenida legalmente de un programa computacional, con el único propósito de probar, investigar o corregir su funcionamiento o la seguridad del mismo u otros programas, de la red o del computador sobre el que se aplica. La información derivada de estas actividades sólo podrá ser utilizada para los fines antes señalados*".[116]

Podríamos inferir entonces, que sería un eximente de responsabilidad del delito informático tipificado en el artículo 197.3 del Código Penal, permitiendo el acceso a programas computacionales sin autorización expresa en virtud de la intención de mejorar el funcionamiento o seguridad del sistema informático.

Lo cual, notoriamente se contrapone a lo que se pretendía legislar en la ley N° 21.459, tal como lo manifestó el Honorable Diputado señor Fuenzalida en la sesión complementaria de fecha 2 de marzo de 2022 de la Comisión Mixta[117], donde por unanimidad se establece que no se está de acuerdo con legislar en dicha Ley, un eximente de responsabilidad en favor de investigaciones de vulnerabilidades o correcciones de seguridad, ya que se cree que podría ser un subterfugio para crackers que estén cometiendo efectivamente un delito informático.

Ahora bien, dado que se trató de un debate, no todos estuvieron de acuerdo con no incorporar una eximente de responsabilidad penal a los que desarrollaran el hacking ético. Hay quienes sostenían que sería beneficioso incorporar esta excepción específica dado los beneficios propios del hacking ético, en virtud de su función de búsqueda de vulnerabilidades y notificación coordinada de ellas, que permite a los responsables de

---

[115] Idem, p.42.

[116] CHILE. Ley N° 17.336 sobre Propiedad Intelectual. Diario Oficial de la República de Chile, Agosto de 1970. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=28933&idParte=8636844&idVersion=

[117] Sesión complementaria de fecha 2 de marzo de 2022 transmitida por TV Senado en que la Comisión Mixta dedicó al estudio del proyecto Ley N° 21.459*: <https://tv.senado.cl/tvsenado/comisiones/mixta/mixta/comision-mixta-boletin-n-12192-25-delitos/2022-03-02/101517.html>* [Consultado: 15/07/2023].

sistemas informáticos, proveedores de servicios, organismos públicos, etc. cerrar las brechas, blindar los sistemas y contribuir a un ecosistema digital más seguro.[118]

Mientras que por otro lado, otros, entre ellos el Ministerio del Interior, sostenían que no era factible dado que la actividad de estos investigadores de vulnerabilidades de sistemas perjudica las potestades que tiene el dueño o administrador del sistema sobre el mismo.

Finalmente, la decisión fue de no incorporar esta excepción en la ley N° 21.459 lo que conlleva, como sostiene el profesor de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, señor Alejandro Hevia Angulo, que dicha sanción legal sea utilizada como un mecanismo de censura, ya que el acceso ilícito sin salvaguardias legales para la investigación y búsqueda de vulnerabilidades han sido usadas para intentar silenciar la investigación en ciberseguridad[119].

Significado, la pérdida de la posibilidad de ejercicio de un agente que podía llegar a informar sobre vulnerabilidades informáticas a diferentes organismos del mercado, tanto privados como públicos, que ahora por temor a amenazas legales preferirán callar antes de revelar fallos de seguridad, por temor a represalias legales que dichos organismos pudieran realizar para proteger su reputación.

Siendo más fácil para un organismo aceptar que se cometió un delito a aceptar un informe de investigadores, en que se estipule una falla de seguridad que fácilmente le pudiera costar clientes, legitimidad contra su competencia o prestigio.

En relación a lo anterior, es interesante analizar las indicaciones que se realizaron en su etapa de Proyecto de Ley, Boletín N° 12.192-25. En particular al respecto del artículo 16 de la derogada ley N° 19.223, algunos Senadores mediante una indicación a dicho artículo intentaron establecer una excepción al agregar un inciso que establecía que quienes realizaran investigación con el fin de detectar las vulnerabilidades del sistema informático y que, al momento de encontrarlas notificarán de inmediato a la autoridad a cargo de dicho sistema, no estarían sujetos a la sanción establecida en el mismo artículo. A pesar de los intentos por incorporar esta modificación, no fue acogida en el proyecto.

---

[118]Informe de la comisión de futuro, ciencias, tecnología, conocimiento e innovación recaído en el proyecto de ley que establece normas sobre delitos informáticos, deroga la Ley n° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. <https://www.camara.cl/verDoc.aspx?prmID=23303&prmTIPO=INFORMEPLEY> [Consultado: 16/07/2023], p.24.
[119] Ibid, p.14.

Esto es algo que sostiene igualmente Daniel Álvarez en el ciclo de Charlas sobre Delitos Informáticos organizado por la Universidad de Chile, en que señala que elaborar un capítulo sobre el procedimiento de notificación de las vulnerabilidades en que se establezcan las etapas, forma de hacerlo y ante qué autoridad, podría ser una mejora importante como eximente de responsabilidad penal[120].

Así, tampoco fue acogida la indicación referida a exigir como requisitos de la misma ley en su artículo 2, que el acceso ilícito al sistema informático debiera ser realizado de forma deliberada e ilícita, sumado a que debía ser superando una medida de seguridad o medida técnica. Fracasando con esto los intentos por proteger la figura del hacking ético.

[120] Canal Uchilederecho. Ciclo de charlas sobre derecho informático. Nueva ley de delitos informáticos y principales aspectos para su implementación. 4 de mayo de 2022 [archivo de video], minuto 46:36. https://www.youtube.com/watch?v=Y-TV3oRY82U

CAPÍTULO III. ACCESO ILÍCITO EN EL DERECHO COMPARADO Y DIRECTRICES INTERNACIONALES.

Uno de los puntos polémicos, es la redacción del concepto de acceso ilícito, ya que ello definirá cuando el acto de evaluar vulnerabilidades de un sistema informático pasará a ser un acto ilegal. Es por ello, por lo que pasaremos en primera instancia a comparar definiciones entre la legislación internacional y la nuestra.

1. EL CONVENIO SOBRE LA CIBERDELINCUENCIA DEL CONSEJO DE EUROPA, EL LLAMADO CONVENIO DE BUDAPEST

Tal instrumento se presenta como la respuesta legal del siglo XXI ante la presencia y auge de las conductas criminales[121] en el ciberespacio. Dicha normativa es de gran relevancia, ya que ha impulsado el debate en diversas legislaciones. Generando que diversos ordenamiento jurídicos la acojan, buscando su actualización legislativa, que les permita afrontar dicho fenómeno que afecta las redes informativas a nivel transnacional.

Como se ha mencionado anteriormente, en el 2017 el Ministerio de Relaciones Exteriores mediante el Decreto 83 promulga el Convenio de Budapest, entrando en vigencia el 28 de agosto del mismo año. Con ello, nuestro país pasó a formar parte del instrumento internacional más relevante en materia de cibercrimen, junto con asumir una serie de deberes que derivan del Convenio[122]. Su principal objetivo es el desarrollo de una política criminal común frente a la ciberdelincuencia, mediante la homologación de los conceptos fundamentales y del tratamiento de la legislación penal, sustantiva y procesal, así como del establecimiento de un sistema rápido y eficaz de cooperación internacional.[123]

A la luz de lo anterior, Chile se comprometió a modificar su legislación en búsqueda de cumplir estándares internacioanles y lograr una armonización legislativa. Siendo por ello, de gran relevancia el análisis del Convenio ya que fue nuestra piedra angular en nuestra actual legislación respecto al cibercrimen.

---

[121] Lobo, M. M., Gil, S. V. H., & Aguirre, A. M. G. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: estudio comparativo. *Revista de ciencias sociales - Universidad del Zulia. Facultad de Ciencias Económicas y Sociales*, *29*(2), pp.358, https://dialnet.unirioja.es/servlet/articulo?codigo=8920556

[122] Mayer Lux, L., & Vera Vega, J. (2022). La falsificación informática: ¿un delito necesario? *Revista chilena de derecho y tecnología*, *11*(1), *pp.262, https://rchdt.uchile.cl/index.php/RCHDT/article/view/65299*

[123] *Historia de La Ley, Biblioteca del Congreso Nacional,* Consulado: el 11 de diciembre de 2023, https://www.bcn.cl/historiadelaley/historia-de-la-ley/vista-expandida/8018/

Ahora bien, cabe señalar que el Convenio de Budapest, en su **Artículo 2°**, ubicado en el Titulo 1 (Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas infromaticos), de la seccion 1º (Derecho penal sustantivo), del Capital II (Medidas que deberan adoptarse a nivel naciaonal), si bien no nombra el hacking etico, mandata a sancionar el acceso ilicito:

"*Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos* ***u*** *otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático."*

En base a ello, nuestra legislación mediante la **Ley N° 21.459** en su **Artículo 2**°, nos entrega una definición acceso ilícito:

"*El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.*

*Si el acceso fuera realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático****,*** *se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.*

En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo".

Estableciendo así 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[124]. Causando con dicha regulación, el cierre o al menos una limitación considerablemente en la posibilidad de excluir del castigo punitivo a aquellos comportamientos que puedan englobarse dentro de la noción de *hacking* ético.[125] Lo cual,

[124] Navarro-Dolmestch, Roberto (2023), L*a autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos, Revista Chilena de Derecho y Tecnologia, 12(1),*pp1, https://rchdt.uchile.cl/index.php/RCHDT/article/view/67546/74234

[125] Laura Mayer Lux y Jaime Vera Vega, Revista de Ciencias Penales Sexta Época, Vol. XLVIII, Número 3 (2022), pp278.

es un gran avance desde la **Ley 19.223,** que fue derogada el 22 de junio del año 2022, específicamente respecto a su **Artículo 2º**, que estipulaba lo siguiente:

"El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio."

Notándose en ello, que la antigua ley imponía un elemento excesivamente subjetivo, debido a la estipulación de requerir ánimo de apoderarse o conocer indebidamente la información contenida en un sistema informático. Significando la no tipificación del hacking ético, resultando que en la práctica no sancionara el mero acceso[126]. Pero generando a su vez, una barrera para la persecución penal al *cracking*, ya que en términos probatorios, era muy complejo probar que junto a la acción se producía esta intención criminal. Aquello debido a que la parte acusante le correspondía probar que efectivamente sí existió un ánimo de apropiarse o conocer indebidamente la información, no presuponiendo esta por el solo hecho de haber accedido al sistema.[127] Dificultando la diferenciación entre hacker ético y el ciberdelincuente[128], causando trabas en la persecución criminal a delitos realizados en el ciberespacio.

Dicha barrera fue subsanada con la actual Ley N° 21.459, ya que está no sujeta la acción tipificada a un elemento subjetivo, estableciéndose dicho ánimo "malicioso" como un mero agravante penal en su inciso siguiente, ya que en aquel inciso si se estipula el "ánimo de apropiarse o usar". Debiendo destacar que en su tercer inciso se redactó una figura calificada ya que requiere la divulgación.

Estando aquello acorde a lo mandatado por el Convenio de Budapest, ya que tal como se mencionó, este busca sancionar el acceso ilícito. Castigando la simple entrada o penetración de un sistema protegido sin autorización[129], Siendo esta última distinción muy relevante para los white-hackers, es decir, aquellos individuos que accedieron al sistema

---

[126] BecKer, Sebastián y vioLLier, Pablo. "La implementación del Convenio de budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley No 19.223", en *Revista de Derecho Universidad de Concepción*, vol. 88, No 248 (2020), <https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-591X2020000200075 >

[127] Idem

[128] ¿Cuál Es La Diferencia Entre Un Hacker ético Y Ciberdelincuente?: Las Caras Opuestas De La Ciberseguridad (2022, junio 30), *CronUp Ciberseguridad*, https://www.cronup.com/cual-es-la-diferencia-entre-un-hacker-etico-y-ciberdelincuente-las-caras-opuestas-de-la-ciberseguridad/

[129] Bascur, G., & Peña Sepúlveda, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. *Revista de estudios de la justicia*, *37*, pp.9, https://doi.org/10.5354/0718-4735.2022.67885

con el único propósito de probar su sistema de seguridad y detectar algún tipo de vulnerabilidad[130], ya que el legislador chileno ha optado por castigar todo acceso no autorizado a un sistema informático[131], causando que se tipifique el hacking ético sin una autorización, pero permitiendo dicha práctica con la autorización del administrador del sistema.

Siendo importante señalar, que el Convenio redacta el Artículo 2° con dos requisitos copulativos que deben cumplirse para formarse el delito, estos son: acceso **deliberado e ilegítimo**. En primer lugar, del término "deliberado" podemos inferir que se refiere a un acto intencionado o voluntario y no un mero accidente.

Aquello último, es especificado en el Informe Explicativo del Convenio de Ciberdelincuencia, en el cual se estipula que los redactores del convenio acuerdan que el significado exacto del término "deliberado" debería ser interpretado conforme a las leyes de cada país. Con todo ello, dicha redaccion permite proteger a las personas en casos atípicos o accidentales, como por ejemplo: en una sección de un sitio web que se encuentra abierta (en el sentido que no cuenta con medidas de seguridad, como una contraseña u otro similar), pero que para entrar exige que el usuario marque en una casilla una declaración señalando que pertenece a una determinada institución y que, por lo tanto, goza de acceso al sistema. Si el tercero accede al sistema habiendo mentido sobre su filiación institucional, a pesar de no haber superado ninguna barrera técnica ni un mecanismo de seguridad, el acceso todavía podría considerarse típico, puesto que la persona no se encontraba autorizada para acceder al mismo.[132]

Lo anterior, es apoyado por el Informe Explicativo al Convenio de Ciberdelincuencia del Consejo Europea, ya que menciona que dicha redacción proviene desde un enfoque amplio respecto de lo que constituye el delito contenido en el Artículo Nº 2, especificando que suscita controversias respecto a situaciones en que la mera intrusión no crea un peligro, o

---

[130] Becker, Sebastián y Viollier, Pablo. "La implementación del Convenio de budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley Nº 19.223", en *Revista de Derecho Universidad de Concepción*, vol. 88, Nº 248 (2020), <https://revistas.udec.cl/index.php/revista_de_derecho/article/view/2185/3155> [Consultado: 9/10/2023]. pp89.

[131] Bascur, G., & Peña Sepúlveda, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. *Revista de estudios de la justicia*, *37*, pp.13, https://doi.org/10.5354/0718-4735.2022.67885

[132] Idem, pp.91[Consultado: 15/08/2023]

cuando incluso los actos de piratería han dado lugar a la detección de “agujeros” y puntos débiles de los sistemas de seguridad.[133]

Asimismo, el informe aclara que dichas controversias han llevado a que los países tomen enfoques más restrictivos, para evitar estas. Situación en la cual el mismo Informe, aclara que ambas opciones son válidas. Entregando incluso opciones para que las partes agreguen términos que maticen sus normativas: infracción de las medidas de seguridad; intención especial de obtener datos informáticos; otras intenciones dolosas que justifiquen la responsabilidad penal, o la exigencia de que el delito se haya cometido en relación con un sistema informático que esté conectado de forma remota a otro sistema informático.[134] Reflejando que si bien el Convenio, se inclina por un enfoque más amplio, incentiva a los países a modificar la terminología para que esta se adecue a su normativa interna.

Por otro lado, el término “ilegítimo” se puede entender en relación a que busca sancionar actos no autorizados por el titular o actos no exceptuados por la ley. Es decir, englobando aquellas circunstancias en que el tercero actúe sin derecho o no estando amparado por circunstancias exculpantes[135]. Reflejando con ello, que el acceso ilícito no es siempre punible *per se,* sino que puede llegar a ser un acto legal o justificado, no sólo en aquellos casos en que corresponde aplicar una defensa legal clásica, como el consentimiento, la defensa propia o la necesidad, sino también cuando otros principios o intereses conducen a la exclusión de la responsabilidad penal (por ejemplo, a efectos del cumplimiento de la ley, con fines académicos o con propósitos de investigación)[136].

---

[133] *Convenio Sobre La Ciberdelincuencia Protocolo Sobre La Xenofobia y El Racismo Segundo Protocolo Adicional Relativo al Refuerzo de la Cooperación y de la Divulgación de Pruebas Electrónicas Convenio sobre la Ciberdelincuencia Protocolo Sobre la Xenofobia y el Racismo Segundo Protocolo Adicional Relativo al Refuerzo de la Cooperación y de la Divulgación de Pruebas Eléctricas (2023),* Informe explicativo y notas de orientación, Consejo de Europa, pp.52 *t*https://Www.Coe.Int/Documents/8475493/202017550/Prems+015123+Esp+2023+Convention+Cybercrimininalité+Web+A5.Pdf/A6b85c77-C79a-Ef99-4d66-48351c1b48fc?T=1678890134243

[134] *Convenio Sobre La Ciberdelincuencia Protocolo Sobre La Xenofobia y El Racismo Segundo Protocolo Adicional Relativo al Refuerzo de la Cooperación y de la Divulgación de Pruebas Electrónicas Convenio sobre la Ciberdelincuencia Protocolo Sobre la Xenofobia y el Racismo Segundo Protocolo Adicional Relativo al Refuerzo de la Cooperación y de la Divulgación de Pruebas Eléctricas (2023),* Informe explicativo y notas de orientación, Consejo de Europa, pp.52 *t*https://Www.Coe.Int/Documents/8475493/202017550/Prems+015123+Esp+2023+Convention+Cybercrimininalité+Web+A5.Pdf/A6b85c77-C79a-Ef99-4d66-48351c1b48fc?T=1678890134243

[135] Becker, Sebastián y Viollier, Pablo. “La implementación del Convenio de budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley Nº 19.223”, en *Revista de Derecho Universidad de Concepción*, vol. 88, Nº 248 (2020), <https://revistas.udec.cl/index.php/revista_de_derecho/article/view/2185/3155> [Consultado: 9/10/2023]

[136] *Convenio Sobre La Ciberdelincuencia Protocolo Sobre La Xenofobia y El Racismo Segundo Protocolo Adicional Relativo al Refuerzo de la Cooperación y de la Divulgación de Pruebas Electrónicas Convenio sobre la Ciberdelincuencia Protocolo Sobre la Xenofobia y el Racismo Segundo Protocolo Adicional Relativo al Refuerzo de la Cooperación y de la Divulgación de Pruebas*

En otras palabras, del Convenio de Budapest se inclina por requisito que protegen a las personas que hayan accedido al sistema informático por error, por mero accidente o bajo una motivación de investigación. Pudiendo ser vez una puerta para permitiría el acceso a "hackers éticos", evitando así su criminalización, extendiéndose bajo la percepción que existen circunstancia exculpantes. Ayudando a resolver las tensiones entre la disponibilidad y el libre intercambio de la información, por una parte, y la necesidad de establecer límites y sanciones[137], optándose por castigar exclusivamente una forma *cualificada* de ingreso ilícito y no cualquier acto de ingreso ilegal[138].

Línea la cual, si bien Chile no siguió textualmente, más si se inspiró en ella. Esto ya que por un lado, no permite ampliamente la técnica de ciberseguridad, de hacking ético, debido al riesgo que supondría para la privacidad de la información encontrada en los sistemas informáticos y la legitima voluntad de exclusión de esta por parte de los titulares de un sistema[139].

Pero en paralelo, se permite el instrumento de hacking ético, mediante una autorización expresa del titular del sistema informático, en que se desee ejercer esta prueba para identificar vulnerabilidades. Debiendo comprender de forma armónica el Artículo 2 de la Ley 21.459, con el **Artículo 16** de la misma Ley, que estipula: *"Autorización e Investigación Académica. 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."*

Sin embargo, al entender que se cuenta con una autorización solo si media una autorización expresa, el eximente pierde su funcionalidad. Confundiendo otra vez al hacker ético y el ciberdelincuente, gracias a que se establece como único criterio de diferenciación que el primero desarrolla su actividad bajo la autorización del titular del sistema informático, olvidando aquellas diferencias y objetivos que ponen a ambos actores en lados opuestos de

---

Eléctricas (2023), Informe explicativo y notas de orientación, Consejo de Europa, pp.161, https://www.coe.int/documents/8475493/202017550/PREMS+015123+ESP+2023+Convention+Cybercrimininalité+WEB+A5.pdf/a6b85c77-c79a-ef99-4d66-48351c1b48fc?t=1678890134243

[137] Mayer Lux, L., & Vera Vega, J. (2020). El delito de espionaje informático: concepto y delimitación. *Revista chilena de derecho y tecnología*, *9*(2), pp 238, https://www.scielo.cl/pdf/rchdt/v9n2/0719-2584-rchdt-9-2-00221.pdf

[138]Bascur, G., & Peña Sepúlveda, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. *Revista de estudios de la justicia*, *37*, pp.9,pp11, https://doi.org/10.5354/0718-4735.2022.67885

[139] Idem, pp.11

la moneda[140]. Evidenciando que en la actualidad dicha conducta que en un principio no sería tolerable, solo bajo la ciertas circunstancia de una autorización expresa será permitida por nuestro legislador.

Finalmente, se puede concluir que la redacción propuesta por el Convenio de Budapest resulta más prudente y adecuada en lo que respecta a la tipificación del delito de acceso informático, buscando un equilibrio entre el establecimiento de requisitos que describen rigurosamente la conducta típica y una flexibilidad que facilite la labor de los organismos persecutores del delito[141]. Resultando en una redacción con un enfoque más general y permitiendo la alternativa facultativa de exigir requisitos adicionales que faciliten su regulación y persecución a los diferentes países que adhirieron al convenio. Caso que fue el de Chile, debido a que como se mencionó, incorporamos el requisito de infringir medidas de seguridad.

2. Comparación de normativas: en relación con otros modelos comparados del hacking ético

El presente punto, tiene por objetivo evidenciar las diferentes formas en el que el derecho comparado ha regularizado las acciones constitutivas a de hacking ético o en contra sensu, a actuaciones constitutivas a acceso ilícito. Generando distintos métodos para regularizar o sancionar dichas actuaciones, mostrándonos también como los distintos pies incorporaron a su normativa interna el Convenio de Budapest. Esencialmente se eligieron los siguientes países por su cercanía en la formación de nuestro sistema jurídico o por sus revolucionarios métodos para enfrentar el ataque cibernético.

Asimismo se busca evidenciar los diferentes métodos para protegerse del ciberataque, logrando diferenciar ordenamientos que consideran que los delitos relativos a los sistemas informáticos no presentar alguna particularidad, considerando incluso que el computador es simplemente un instrumento para la comisión de los delitos tradicionales[142]. O en cambio, ordenamientos que consideran que frente a la delincuencia informática es de considerar que

---

[140] ¿Cuál Es La Diferencia Entre Un Hacker ético Y Ciberdelincuente?: Las Caras Opuestas De La Ciberseguridad (2022, junio 30), *CronUp Ciberseguridad*, https://www.cronup.com/cual-es-la-diferencia-entre-un-hacker-etico-y-ciberdelincuente-las-caras-opuestas-de-la-ciberseguridad/

[141] Becker Castellaro, S., & Viollier Bovin, P. (2020). La Implementación Del Convenio De Budapest En Chile: Un Análisis A Propósito Del Proyecto Legislativo Que Modifica La Ley 19.223. *Revista de Derecho (Concepción)*, *88*(248), 75–112, https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-591X2020000200075

[142] Magliona, Claudio y Lopez, Macarena, Delincuencia y Fraude Informático: Derecho comparado y Ley Nº19.223, Santiago, Editorial Jurídica de Chile, 1999, pp.81

es necesaria una nueva legislación[143], ya sea modificando la legislación vigente o estableciendo nuevas figuras sancionatorias, caso el cual nuestro país siguió.

A. LEGISLACIÓN ESPAÑOLA

Con independencia de la relevancia que hoy toma la ciberseguridad, el acceso ilícito a un sistema informático no fue tipificado en España hasta 2010. Concretamente fue introducido en el Código Penal español a través de la reforma operada por la Ley Orgánica 5/2010[144]. En consecuencia de las contraídas obligaciones internacionales que España ratificó mediante el Convenio de Budapest, así como respecto a la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005[145]. Promovidas por la necesidad de "llegar a un enfoque común respecto de los elementos constitutivos de las infracciones penales, estableciendo delitos comunes de acceso ilegal a un sistema de información intromisión ilegal en el sistema e intromisión ilegal en los datos"[146].

Significando que se adquiere una obligación de adecuar la legislación interna para aumentar esfuerzos contra la comisión de delitos informáticos, que en gran medida pueden ser cometidos y afectar simultáneamente a diferentes países. En otras palabras, dicha armonización era necesaria porque en estos comportamientos, podemos encontrar una nota que le añade un especial grado de peligrosidad: su conexión internacional o transfronteriza, de modo que sus actuaciones pueden ir más allá de un ámbito geográfico concreto.[147]

Posteriormente, modificada en su redacción y ubicación sistemática por la Ley Orgánica 1/2015, de 30 de marzo del año 2015, reubicando el tipo penal previsto, hasta dicha

---

[143] Idem

[144]Sánchez-Escribano, M. I. M. (2023). *El delito de acceso ilícito a un sistema informático: aspectos relativos a su regulación e interpretación*. ARANZADI/CIVITAS, https://books.google.es/books?hl=es&lr=&id=3UWxEAAAQBAJ&oi=fnd&pg=PT4&dq=acceso+il%C3%ADcito+España+tesis+&ots=jlQGjRmMnO&sig=wiby6LdTPZgenK5JCiw9S-_2wPU#v=onepage&q&f=true

[145] Boletín Oficial Del Estado, España, Miércoles 23 de junio de 2010, sec I. pag 54817 .https://www.boe.es/eli/es/lo/2010/06/22/5/dof/spa/pdf

[146]Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, Diario Oficial de la Unión Europea, https://www.boe.es/doue/2005/069/L00067-00071.pdf

[147]Ángeles, M., & Martín, R. (s/f). *Los Ataques Contra Los Sistemas Informáticos: Conductas De Hacking. Cuestiones Político-Criminales*. Revistajuridicaonline.com. Recuperado el 11 de noviembre de 2023,pp.191, https://www.revistajuridicaonline.com/wp-content/uploads/2009/09/26_7_los_ataques_contra_los_sistemas_.pdf

reforma, en el Art. 197.3, que sanciona el acceso ilegal a sistemas de información, también conocido como allanamiento o intrusismo informático[148]. Dicha reforma fue impulsada por las directrices establecidas por la Directiva de la Unión Europea Nº 40/2013[149], relativa a los ataques contra los sistemas informáticos. Esta tenía el objetivo, tal como lo señala en su considerando primero, de lograr establecer normas mínimas relativas a definiciones de infracciones penales como sanciones aplicables a ataques de ciberseguridad. Introduciendo así, la conducta de acceso ilícito como un delito autónomo en el Código Penal. Subsanando carencias legislativas que eran necesarias gracias a la gran dependencia de las nuevas tecnologías tanto a nivel social como económico.

Quedando formulado de la siguiente manera: *"Código Penal Español, Título X: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, Capítulo I: Del descubrimiento y revelación de secretos,* ***Artículo 197 BIS:*** *1. El que por cualquier medio o procedimiento,* ***v****ulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años."*

La actual redacción del artículo, se enmarca en los parámetros entregados por el Artículo 3 de la Directiva Europea Nº 40/2013, manteniendo la doble exigencia para la tipicidad de la conducta[150].Estableciendo que: "*Los Estados miembros adoptarán las medidas necesarias para que, cuando haya sido realizado intencionalmente, el acceso sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal cuando se haya cometido con violación de una medida de seguridad, al menos en los casos que no sean de menor gravedad*".[151] Es decir, el acceso ilegítimo debe realizarse sin autorización y vulnerando las medidas de seguridad establecidas para impedirlo. En razón

---

[148] Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, Doctrina de la Fiscalía General del Estado, pp.8 https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf

[149] Directiva 2013/40/Ue Del Parlamento Europeo y Del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, Diario Oficial de la Unión Europea, del 14.8.2013, pp.1 https://www.boe.es/doue/2013/218/L00008-00014.pdf

[150]Fiscalía General del Estado, España, Circular 3/2017.[Consultado:15/08/2023] <https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf >pp.9

[151] Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de Agosto de 2013 relativa A Los Ataques Contra Los Sistemas De Información Y Por La Que Se Sustituye La Decisión Marco 2005/222/JAI del Consejo [Consultado: 15/08/2023] <https://www.boe.es/doue/2013/218/L00008-00014.pdf > pp.12

de ello, la legislación española ha acordado que en concordancia a nuestra legislación, establece dos requisitos copulativos para definir el acceso ilícito a un sistema informático.

En primer lugar, se hace referencia al requisito de "**vulnerar el sistema de seguridad**", entendiéndose ello "cuando los datos…sufren un incidente de seguridad que da lugar a la violación de la confidencialidad, disponibilidad o integridad de los datos"[152]. Siendo ello relevante, debido a que pone entredicho lo que podría entenderse como vulnerabilidad, por ejemplo una vulneración puede ser adivinar la contraseña de correo de un cercano. Dicho lo cual, en nuestra legislación también ocurre debido a que la Ley 21.459, se menciona: "superando barreras técnicas o medidas tecnológicas de seguridad". Hecho que exige una propiedad objetiva de la acción típica cuya función es caracterizar objetivamente su ilicitud[153]. Circunstancia que cumple el rol para acreditar el interés inequívoco del titular en orden a mantener el secreto (o libertad de exclusión) sobre sus datos[154].

Siendo sumamente relevante para materia de hacking blanco, ya que criminaliza el mero acceso, gracias a que el término "vulnerar el sistema de seguridad" puede ser definido como una acción que suponga evadir alguna barrera de seguridad, logrando así acceder al sistema, significando con ello que se tipifique, en una primera instancia, al hacking ético. Esto debido a como se ha mencionado, el hacking ético se refiere a un acceso indebido sin la intención de producir un resultado dañoso que generalmente será con ánimo de diversión o motivado por un desafío intelectual.[155]

En segundo lugar, el requisito faltante para configurar el delito es el acceso "***sin estar debidamente autorizado"***. Si bien, no se describe cómo esta debe realizarse, el Artículo 2 letra d Directiva Europea Nº 40/2013, define el termino de "sin autorizacion" como "un comportamiento que incluye el acceso, la interferencia o la interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o

---

[152]Comision Europea, ¿Qué es una violación de la seguridad de los datos y qué deberíamos hacer en caso de sufrir una?, [En linea]**,** <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_es#:~:text=Una%20violación%20de%20la%20seguridad%20de%20los%20datos%20se%20produce,o%20integridad%20de%20los%20datos > [Conusltado: 15/08/2023]

[153] Bascur, G., & Peña Sepúlveda, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. *Revista de estudios de la justicia*, *37, pp.10, https://rej.uchile.cl/index.php/RECEJ/article/view/67885*

[154] Bascur, G., & Peña Sepúlveda, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. *Revista de estudios de la justicia*, *37, pp.10, https://rej.uchile.cl/index.php/RECEJ/article/view/67885*

[155] Moscoso Escobar,Romina, La Ley 19.223 en general y el delito de *hacking* en particular (2014),Revista Chilena De Derecho y Tecnología, 3(1), pp33, https://rchdt.uchile.cl/index.php/RCHDT/article/view/32220/34154

no permitido por el Derecho nacional"[156]. Siguiendo con lo normado en anteriormente en el 2005 en el Artículo 1 de la Decisión Marco 2005/222/JAI del Consejo[157]. Lo cual, en nuestra actual legislación dicha definición no ocurre, dejando espacio a la interpretación.

Ahora bien, en vinculación del el Artículo 3 de la Directiva Europea núm. 40/203o, los considerandos 16º y 17º de Directiva 40/2013/UE, destacan especialmente la necesidad de constatar que la actividad se realiza con un propósito delictivo, indicando con ello que deberían quedar al margen de una posible responsabilidad penal aquellos supuestos en que la persona desconocía que el acceso no estaba autorizado o cuando, en el marco de una relación laboral o contractual, la conducta observada únicamente supone la infracción de políticas de usuario o el incumplimiento de las normas organizativas sobre utilización de los sistemas de información de la empresa[158]. Es decir, la Directiva comprendió que puede generarse caso atípicos que no es lo ideal la persecución penal, estableciendo un factor clave, la intencionalidad. Hecho que no ocurre en Chile, ya que expresamente se autoriza la persecución penal en el caso de que dicha autorización sea sobrepasada, permitiendo que en casos como en un contrato de servicios de hacking ético con una empresa experta, se pueda buscar consecuencias penales, opción la cual desde un punto de vista de criterio jurídico mayoritario debería ser resguardado como último ratio. [159]

B. LEGISLACIÓN ARGENTINA

En Argentina con el objetivo de regular los efectos que conllevan las nuevas tecnologías en la comisión de delitos, se promulgó el 24 de junio de 2008, la Ley Nº 26.388. La cual incorporó el **Artículo 153 bis** al Código Penal, el dispone lo siguientes:

"*Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a* ***sabiendas accediere por cualquier medio, sin la***

---

[156]Raúl Carnevali Rodríguez,Derecho Penal Como Ultima Ratio. Hacia Una Política Criminal Racional [En linea], SciELO Chile, <https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122008000100002 >pp.12

[157] https://www.boe.es/doue/2005/069/L00067-00071.pdf pp2.

[158] Directiva 2013/40/Ue Del Parlamento Europeo Y Del Consejo De 12 De Agosto De 2013, Relativa A Los Ataques Contra Los Sistemas De Información Y Por La Que Se Sustituye La Decisión Marco 2005/222/Jai Del Consejo [Consultado: 15/08/2023] <https://www.boe.es/doue/2013/218/L00008-00014.pdf >pp.9

[159] Raúl Carnevali Rodríguez,Derecho Penal Como Ultima Ratio. Hacia Una Política Criminal Racional [En linea], SciELO Chile, <https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122008000100002 >pp.12

debida autorización o excediendo la que pose*a, a un sistema o dato informático de acceso restringido.*

*La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financiero*s."[160]

Antes que todo, hay que comprender que por "dato informático" se entiende a la unidad mínima de información sometida a tratamiento informático o automatizado. Y, por "sistema informático", al dispositivo aislado o conjunto de dispositivos interconectados que aseguran, mediante la ejecución de un programa o software, el tratamiento automatizado de datos[161]. Siendo relevante ya que, nos aclara que la acción típica no diferencia en el grado de acceso que se generó, bastando con un acceso a la unidad mínima de información de algún agente.

Asimismo, el tipo penal bajo análisis tiene una aplicación subsidiar[162], lo cual no sucede en Chile, ya que expresamente se menciona que "si no resultare un delito más severamente penado", lo cual resuelve un gran punto de relevancia, ya que en palabras de Reyna, «el *hacking* tiende a generar comportamientos de mayor daño; el *hacker* (intruso) no se complace con la conducta delictiva inicial, intenta analizar su capacidad técnica personal agotando las posibilidades de obtención de información; así, el *hacker* modificará progresivamente su accionar hasta concluir realizando actos de sabotaje o espionaje informático[163]. Puedo llegar a formarse una relación concursal entre otros los delitos informáticos, así como con el acceso no autorizado con figuras tradicionales[164]. En nuestra legislación, dicha situación es resuelta mediante la figura del concurso de delitos.

Por ello, se asimila en gran medida a lo normado por la legislación española y chilena ya que sanciona el mero acceso, sin requerir ninguna acción adicional. Ello indica, que no es necesario realizar alguna acción "maliciosa" o negativa al agente titular de dicha información, sin necesitar para sancionar al sujeto que realice por ejemplo una publicación, interferencia o manipulación en dicha información, significando la tipificación el hacking

---

[160] Codigo Penal De La Nacion Argentina, http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#19

[161] Linares, M. B. (2020). Delitos informáticos en el Código penal argentino. *Revista chilena de derecho y ciencia política*, *11*(2), https://dialnet.unirioja.es/servlet/articulo?codigo=8758428

[162] Idem pp.131

[163] Moscoso Escobar,Romina, La Ley 19.223 en general y el delito de *hacking* en particular (2014),Revista Chilena De Derecho y Tecnología, 3(1), pp186, https://rchdt.uchile.cl/index.php/RCHDT/article/view/32220/34154

[164] Idem, pp.49

ético. Como se ha mencionado anteriormente, aquello también sucede en Chile, gracias a que el acceso no autorizado es un delito de mera actividad, pues el tipo no exige la verificación de ningún resultado al margen de las acciones descritas[165] , por el artículo Nº 2 de la ley N° 21.459.

Con este último párrafo, el legislador incrementa la escala penal de la figura legal básica por considerar que el acceso en perjuicio de un sistema o dato informático de un organismo público estatal, o de un proveedor de servicios públicos o financieros, configura un supuesto que merece una protección penal especial .[166]

C. LEGISLACIÓN BELGA

En el último tiempo Bélgica ha recibido un exponencial número de ataques cibernéticos, llegando a considerarlos, riesgos prioritarios nacionales[167]. Por lo cual, a nivel estatal se ha propuesto abogar por un ciberespacio abierto, libre y seguro[168]**.** En respuesta de ello, Bélgica desarrolló una política pública para enfrentar los ciberataques.[169]

Ahora bien, hay que mencionar que en su Código Penal se encuentra regulado el acceso no autorizado a sistemas informáticos:

"***Artículo 550-bis: § 1****. Quien, sabiendo que no está autorizado para ello, acceda a un sistema informático o lo mantenga, será castigado con prisión de tres meses a un año y multa de veintiséis a cinco mil francos o uno de estas sanciones únicamente.*

Si el delito a que se refiere el apartado 1 se comete con intención fraudulenta, la pena de prisión será de seis meses a dos años.

§ 2. Quien, con intención fraudulenta o con ánimo de lucro, exceda su capacidad de acceso a un sistema informático, será castigado con prisión de seis meses a dos años y multa de veintiséis francos. o una de estas sanciones solamente"[170]

---

[165] Moscoso Escobar,Romina, La Ley 19.223 en general y el delito de hacking en particular (2014),Revista Chilena De Derecho y Tecnología, 3(1), pp47 https://rchdt.uchile.cl/index.php/RCHDT/article/view/32220/34154

[166] idem

[167] El mercado de la ciberseguridad en Bélgica (2021),Oficina Económica y Comercial de la Embajada de España en Bruselas,pp.5 https://www.icex.es/content/dam/es/icex/oficinas/024/documentos/2022/01/documentos-anexos/DOC2021896736.pdf

[168] Idem

[169] Idem

[170] Código Penal de Bélgica (traducido)

Reflejando la misma línea normativa, que otros países Europeos han seguido, al tipificar todo acceso no autorizado o todo acceso que sobrepase dicha autorización. Sancionando más duramente al agente que accede con una intención "maliciosa", al estipular la terminología de "intención fraudulenta".

Ahora bien, Bélgica nos presenta un gran avance respecto a la materia de hacking ético, graciasa que el 25 de diciembre del 2022, publicó en su Boletín Oficial la Ley de protección de las personas que denuncien violaciones del derecho de la Unión o del derecho nacional observadas dentro de una persona jurídica en el sector privado, la cual entró en vigor el 15 de febrero de 2023. Si bien, no contiene ningún artículo que lo defina, establece condiciones que deben ser cumplidas para que el actuar de los hackers éticos, incluso sin consentimiento del titular, no sea sancionada por el Artículo 550-bis de su Código Penal. En otras palabras, desde el 2023, Bélgica se legalizó e incluso en ausencia del consentimiento, el llamado "hacking ético"[171]. Cambiando así, el estatus jurídico del hacking ético en Bélgica, ya que en estos momentos una persona física o jurídica está autorizada a investigar organizaciones en Bélgica en busca de posibles vulnerabilidades de ciberseguridad, incluso si no han dado su consentimiento para dichas investigaciones[172]. Ello bajo la autorización del Art 49 de la llamada Ley de Protección de Denunciantes[173], concretamente en su Capítulo Nº 8, Sección 8: Reformas a la Ley de 7 de abril de 2019 que establece un marco para la seguridad de las redes y sistemas de información de interés general para la seguridad pública:

"Art. 62/1. § 1. Sin perjuicio de la aplicación de la ley de 28 de noviembre de 2022 sobre la ***protección de las personas que denuncien violaciones*** *del Derecho de la Unión o del Derecho nacional observadas en una entidad jurídica del sector privado,* ***cualquier persona física o jurídica podrá informar al CSIRT nacional de la existencia de una vulnerabilidad*** *potencial en el sentido del artículo 6. , 34°.*

---

https://etaamb.openjustice.be/fr/loi-du-28-novembre-2000_n2001009035.html

[171] Asesoría Técnica Parlamentaria, Modelos de Ciberseguridad en la Experiencia Internacional, Agosto del 2023, Biblioteca del Congreso Nacional. pp5

[172] Somers, C., Vranckaert, K., & Drechsler, L. (2023, mayo 3). *Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity?* CiTiP Blog; CiTiP KU Leuven. https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/

[173] *Are you ready for the new Belgian whistleblower protection rules?* (s/f). Clifford Chance. Recuperado el 11 de diciembre de 2023, https://www.cliffordchance.com/insights/resources/blogs/regulatory-investigations-financial-crime-insights/2023/01/are-you-ready-for-the-new-belgian-whistleblower-protection-rules.html

Asimismo, esta disposición se entiende sin perjuicio de las disposiciones legales sobre protección de las personas que denuncien violaciones del Derecho de la Unión o nacional observadas en el seno de una persona jurídica del sector público.
El informe se realiza por escrito, según el procedimiento detallado en el sitio web nacional del CSIRT…"

Cabe mencionar que la misma ley, define qué entiende por "vulnerabilidades" en su Art.48: "*34° "vulnerabilidad": una debilidad, susceptibilidad o defecto de un activo, o de una red y un sistema de información que puede ser explotado por una ciberamenaza en el sentido del artículo 2, punto 8), del Reglamento (UE) 2019 /881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre ENISA (Agencia de Ciberseguridad de la Unión Europea) y la certificación de ciberseguridad de las tecnologías de la información y las comunicaciones, y por el que se deroga el Reglamento (UE) n.º 526/2013 (Reglamento de Ciberseguridad)".*

Por ende, se legaliza el hacking ético pero no se le entrega una carta blanca [174] o un libre actuar, sino que se les regulariza, ya que se les liga con la obligación y/o limitación de cumplir con las condiciones copulativas, para que su su actuar siga estando en el marco de la ley. Condiciones las cuales la misma ley especifica en su Art 50:

"... **Art. 62/2. § 1**. En el marco del procedimiento previsto en el artículo 62/1, los autores del informe no cometen delito por los hechos necesarios para el informe, siempre que:
1° que actuaron sin intención fraudulenta o de causar daño;
2° han informado a la organización responsable del sistema, proceso o control del descubrimiento de una vulnerabilidad potencial, lo antes posible, y a más tardar, en el momento de informar al CSIRT nacional
3° que no actuaron más allá de lo necesario y proporcionado para verificar la existencia de una vulnerabilidad;
4° que no hayan hecho pública información relativa a la vulnerabilidad descubierta, sin el acuerdo del CSIRT nacional…"

La primera condición,hace referencia a la definición misma del hacking ético, ya que su trabajo se basa en principios y estándares éticos que promueven la seguridad digital y la protección de datos[175]. Demostrando su diferenciación de los ciberdelincuentes,

[174] Somers, C., Vranckaert, K., & Drechsler, L. (2023, mayo 3). *Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity?* CiTiP Blog; CiTiP KU Leuven, https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/
[175] https://www.ufv.es/cetys/blog/que-es-el-hacking-etico/

remarcando por lo mismo un claro límite en referencia a ellos, ya que de otra forma, pasaría a aplicar el Art 550 Bis Apartado 3º Nº 3, el cual especifica que el que cause daño, incluso sin quererlo, al sistema informático en cuestión, será castiga con pena de prisión de uno a tres años y multa de veintiséis francos belgas a cincuenta mil francos o una sola de estas penas. Procurando por ello, que la prueba de vulnerabilidades nunca afecta de forma negativa al funcionamiento del organismo testeado. Demostrando así, que situaciones como la la extorsión[176] al solicitar un pago para revelar posibles vulnerabilidades encontradas, está totalmente prohibido.

Por otro lado, la segunda condición, refleja el requisito de publicidad de la vulnerabilidad encontrada, estando en correlación la principal función y objetivo que persiguen los hacking éticos y el motivo por el cual el Estado Belga ha optado por legalizarlo. Dicha notificación deberá ser realizada tanto al organismo al que se le hizo esta prueba de barreras de seguridad como a CSIRT. Esta última se refiere al Equipo de Respuesta ante Incidentes de Seguridad Informática Belga.

En cuanto a la tercera condición impuesta, busca limitar las acciones ejercidas por los hackers, a aquellas actividades que sean estrictamente necesarias, con el objetivo de notificar una vulnerabilidad de ciberseguridad[177]. Es decir, marca su campo de acción, estableciendo que el hackeo es producido en pro de un objetivo y no por un mero trabajo recreativo. Por ende, condición se infringe por ejemplo, si una vulnerabilidad se puede descubrir con medios menos intrusivos que los elegidos por el hacker ético[178].

Como último, su cuarta condición hace referencia al requisito de confidencialidad que requieren los hackers al ejercer su actividad, requisito el cual es de gran importancia ya que frecuentemente están en contacto con datos sensibles, debiendo proteger el derecho a la intimidad y privacidad de los usuarios.

---

[176] Cetys, U. F. V. (2023, septiembre 5). *¿Qué es el hacking ético?* Formación profesional Universidad Francisco Vitoria, https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/

[177] Cetys, U. F. V. (2023, septiembre 5). *¿Qué es el hacking ético?* Formación profesional Universidad Francisco Vitoria, https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/

[178] idem

Tabla Nº3: Comparación de la normativa mencionada, para una mayor claridad y compresión.

País	Normativa
España	***Artículo 197 BIS: 1º.*** *El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.*
Argentina	**Artículo 153 bis:** *Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido*
Bélgica	**A*rtículo 550-bis: § 1.*** *Quien, sabiendo que no está autorizado para ello, acceda a un sistema informático o lo mantenga, será castigado con prisión de tres meses a un año y multa de veintiséis a cinco mil francos o uno de estas sanciones únicamente.*
Chile	**Artículo 2°.-** Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Fuente: elaboración propia.

3. JURISPRUDENCIA NACIONAL E INTERNACIONAL

A continuación se hará referencia a una serie de casos que reflejarán los distintos desarrollos jurisprudenciales. En este punto se hará referencia principalmente a los países anteriormente mencionados.

A. ORTMANN, GASPAR ARIEL S/ AVERIGUACIÓN DE DELITO, JUZGADO CRIMINAL Y CORRECCIONAL FEDERAL Nº 11, CAUSA CFP 8143/2019 DEL DÍA 20 DE NOVIEMBRE DE 2020, ARGENTINA

El 03 de septiembre de 2019, Gaspara Ariel Ortmann, un cliente del Banco de la Nación Argentina y especialista en seguridad informática y desarrollo de software, ingresó a la plataforma de HomeBanking del mismo Banco, mediante su autentificación con sus propias credenciales. Pero gracias a técnicas específicas para detectar vulnerabilidades en sistemas informáticos, modificó a su favor la cotización del dólar dentro de su navegador[179]. Llevando a cabo él mismo múltiples transacciones de compraventa de dólares, adquiriendo los mismos a una cotización de $5,695 (cuando la real era de $56,95), y luego vendiéndolos a $530,50 (cuando la real era de $53,05)[180]. Ello para demostrar que efectivamente si existia una vulnerabilidad en la plataforma,HomeBanking del Banco Nación que permitía a los usuarios modificar el precio del dólar estadounidense sin que el sistema de seguridad del banco verificara el precio[181].

Luego de dicha detección, Gaspar Ortmann intentó revelar esta vulnerabilidad a los funcionarios de seguridad del banco, comunicándose por correo electrónico, LinkedIn, y Whatsapp[182]. Pero al no tener respuesta, el 23 de octubre de 2019 entregó físicamente una carta al Banco, el cual contenía capturas de pantalla de las transacciones que había llevado a cabo que demostraban la vulnerabilidad[183]. Asimismo, en ella se estipula expresamente

---

[179] Gamen, S. A. (2020, diciembre 11). *Caso Gaspar Ariel Ortmann, otra sentencia a favor del hacking ético,Consulatado el 21 de de Octubre de 2023,* https://www.perfil.com/noticias/opinion/sebastian-gamen-caso-gaspar-ariel-ortmann-otra-sentencia-a-favor-del-hacking-etico.phtml

[180] Sentencia del Juzgado Nacional en lo Criminal y Correccional Federal Nº. 11, Argentina, CFP 8143/2019, pp.1, https://www.pensamientopenal.com.ar/system/files/2021/03/fallos49634.pdf

[181] La persecución de la comunidad de la seguridad informática en América Latina, Agosto del 2021, accessnow.org, Consulado el 20 de octubre de 2023, pp.8, https://www.vialibre.org.ar/wp-content/uploads/2021/08/persecusion-latam-seguridad-digital.pdf

[182] Idem.

[183] Idem.

que: “no tengo *intenciones de usar ese dinero ni quiero tener problemas, decidí dejarlo en mi cuenta sin tocar nada”*[184].

Asimismo, don Cristian Patti, Gerente de Seguridad Informática y Prevención de Fraudes de la firma Red Link S.A., desarrolladora y operadora de la plataforma de Home banking del Banco de la Nación Argentina, estipula en su declaración testimonial, que el acusado efectivamente si utilizo un programo especializado para modificar el punto decimal de la cotización que se le mostraba al cliente al momento de efectuar la operación de compraventa de dolares[185], dejando constancia que el programa fue instalado en su computadora personal y no en el servidor de la Red Link, sin afectar así al sistema en general.

Pero pese a las buenas intenciones de Gaspara Ortmann, este fue procesado penalmente por su actuar. Siendo el caso desestimado el 30 de noviembre de 2020. En dicho fallo se explica que no se consideró como un acceso ilícito al sistema de HomeBanking ya que el acusado había ingresado con sus propias credenciales, había comunicado lo antes posible la vulnerabilidad encontrada, y que segun lo señalado por los mismo responsables de las áreas técnicas del Banco de la Nación Argentina y de Red Link S.A., el acusado no había generado daños en los servidores de Red link ni en el funcionamiento de la plataforma en cuestión. Destacando que, el sistema operado por Red Link, presentaba previamente, por sí mismo, una deficiencia en materia de seguridad que fue descubierta y utilizada por Gaspara Ortmann, por lo que la misma no fue generada por el nombrado[186]. Estipulando expresamente que no se configuraría el delito del Art 153 Bis del Código Penal Argentino, al no haberse accedido indebidamente a ningún sistema informático.

Dicho resultado del caso, refleja que para nuestro país vecino, el requisito de autorización es cumplido al ingresar con las credenciales propias del usuario previamente autorizado para utilizar la plataforma, incluso si dicha autorización no fue con el objetivo que el usuario pusiera prueba las barreras de seguridad de esta mismo. Lo cual, deja el precedente que dicho actuar no es considerado como una forma de exceder la autorización entregada por el titular del sistema, sin lo cual se podría configurar el delito de acceso ilícito del Art 153 Bis del Codigo Penal Argentino.

---

[184] Sentencia del Juzgado Nacional en lo Criminal y Correccional Federal Nº. 11, Argentina, CFP 8143/2019, pp.7, https://www.pensamientopenal.com.ar/system/files/2021/03/fallos49634.pdf
[185] Sentencia del Juzgado Nacional en lo Criminal y Correccional Federal Nº. 11, Argentina, CFP 8143/2019, pp.4 https://www.pensamientopenal.com.ar/system/files/2021/03/fallos49634.pdf
[186] Idem, pp 10.

En consecuencia su legislación se inclina por la preferencia de la buena fe y el haber obrado en pos del interés público, permitiendo ejercer sus conocimientos técnicos especializados, bajo el límite de actuar con la máxima diligencia posible y no generar daños al sistema intervenido. Estableciendo un precedente a favor de la investigación de seguridad y la revelación de vulnerabilidades[187].

Asimismo, establece un precedente a favor de la investigación de seguridad y la revelación de vulnerabilidades[188]. Demostrando la reiterada criminalización de hacking ético pero también la relevancia que tiene los hacking éticos en la actualidad, llegando a ser requeridos por diversas empresas, para identificar fallas en sus protecciones.

B. SENTENCIA PENAL Nº*267/2020,JUZGADO DE LO PENAL Nº 12 DE VALENCIA, REC 498/2019,* DE 24 DE SEPTIEMBRE DE 2020, ESPAÑA

El 12 de abril de 2017, dos estudiantes de la Universidad de Valencia, Severino y Carlos Jesús, realizaron múltiples accesos fraudulentos a las cuentas de usuario de una serie de profesores del Doble Grado de Administración de Empresas e Ingeniería en Tecnologías y Servicios de la Telecomunicación.[189] Dicho acceso fue realizado, gracias al uso de las credenciales (usuario y contraseña)[190] de sus propios profesores, pudiendo acceder a sus cuentas de correo y su intranet, así como para acceder a la aplicación de notas[191], logrando con ello cambiar y mejorar sus notas en más de cinco materias.

Aquello fue posible, ya que ambos estudiantes colocaron en las sales de clases donde se impartía su carrera un dispositivo Keylogger (detectado el 2 de febrero de 2018) susceptible de captar las pulsaciones de los teclados de los ordenadores utilizados por los profesores[192].

Con lo cual, ambos acusados fueron condenados como responsables tanto por el delito de falsedad documental, como del delito de acceso ilícito a un sistema infromatico. Siendo

---

[187] La persecución de la comunidad de la seguridad informática en América Latina,Agosto del 2021, accessnow.org, Consulado el 20 de octubre de 2023, pp.8, https://www.vialibre.org.ar/wp-content/uploads/2021/08/persecusion-latam-seguridad-digital.pdf
[188] Idem
[189] Sentencia Penal Nº*267/2020,Juzgado De Lo Penal Nº 12 de Valencia, Rec 498/2019,* de 24 de Septiembre de 2020, España, pp.2, https://www.poderjudicial.es/search/AN/openDocument/4f1dcca959c56f45/20201001
[190] Idem
[191] idem
[192] Idem

sancionados con las penas de prisión de veintiún meses y un día, y multa de nueve meses y un día con una cuota diaria de 6 euros.

Aquello es de suma relevancia, ya que nos deja apreciar que el legislador español sanciona el mero acceso a un sistema vulnerando las medidas de seguridad y sin estar autorizado para ello, sin que se exija que dicha conducta permita, de lugar, o posibilite en alguna forma el conocimiento de información de carácter íntimo o reservado[193]. Lo cual, es crucial, ya que da cuenta que el bien jurídico protegido no es simplemente la intimidad de la persona. Por lo contrario, ratifica que dicho tipo penal no se enmarca en la protección de un solo bien jurídico en específico. Sino que es un delito pluriofensivo,por lo que atentan contra diversos bienes jurídicos, a saber, la propiedad, la intimidad, etc[194]. Tal como importante parte de la doctrina chilena lo señala.[195]

Por otro lado, podemos señalar que el legislador español entendió como medida de seguridad, toda aquella que se haya establecido con el propósito de impedir el acceso al sistema, independiente de su solidez o complejidad[196]. Es decir, el requisito de vulnerar una medida de seguridad, puede ser cumplido vulnerando su clave de acceso, ya que esta se entiende como un barrera técnica de seguridad que al ser conseguida de mal forma y sin la autorización del titular, a través de un medio informático, como en este caso gracias al dispositivo Keylogger, configura el ilícito.

---

[193] Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, Doctrina de la Fiscalía General del Estado, pp.3-4**,** https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf

[194] Idem

[195]Doctrina que lo apoya: Contreras Clunes, A. (2003). Delitos informáticos: Un importante precedente. *Ius et Praxis*, *9*(1), pp. 515–521, https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122003000100023, y Magliona, Claudio y Lopez, Macarena, Delincuencia y Fraude Informático: Derecho comparado y Ley Nº19.223, Santiago, Editorial Jurídica de Chile, 1999, pp.64-65.

[196] Linde, E., & Contreras Fresneda, S. (2021, abril 16). *Delito de hacking y comentario de sentencia*. Legaltoday.com; Legal Today, https://www.legaltoday.com/practica-juridica/derecho-penal/penal/delito-de-hacking-y-comentario-de-sentencia-2021-04-16/

C. Sentencia del Cuarto Tribunal Oral en lo Penal de Santiago del 2 de septiembre de 2009, RIT 135-2009, RUC 0700879841-3, Chile

Entre los meses de agosto y noviembre de 2007, Gino Rojas Tillemann[197], logró acceder al portal de comercio electrónico denominado Chilecompra, en el cual logró ingresar en forma reiterada y automatizada, mediante un mecanismo que permitió la suplantación de la calidad de comprador, accediendo directamente a conocer el cuadro comparativo de cientos de miles de ofertas cerradas y decenas de ofertas abiertas en estado de publicadas, de muy distintos rubros[198]. Para ello, accedio ilícitamente a los números identificatorios, los cuales no son de acceso público, y que le permitieron ingresar al registro del cuadro comparativo de las ofertas indebidamente[199]. El Señor Gino logró acceder ilícitamente a un número de cotizaciones que alcanza aproximadamente a 333.871. Por lo cual, el tribunal lo sentencia al delito de acceso ilicito, contemplado en aquella época en el artículo 2° de la Ley N° 19.223, siendo sancioando a presidio menor en su grado mínimo a medio.

La sentencia se concentra más que nada en las cuestiones referidas a la superación de las barreras informáticas que impiden el acceso de cualquiera a la información contenida en un sistema informático[200]. Siendo un claro ejemplo de cómo tipificó la conducta el legislador chileno a futuro, sancionado el menor acceso. Estableciendo que con el mero acceso no autorizado y vulneración de barreras de seguridad ya existía un daño al titular.

Asimismo, con lo anterior y con el número de reiteraciones cometidas por el Señor Gino, podemos señalar clramente que fue una conducta totalmente voluntaria y no resultado de un error. Lo cual, lo diferencia rápidamente del actuar de un hacking ético ya que este

---

[197] Cuarto Tribunal Oral en la Penal, 2 de septiembre de 2009, RIT 135-2009, https://oficinajudicialvirtual.pjud.cl/ADIR_871/penal/documentos/docCausaPenal.php?dtaDoc=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwczpcL1wvb2ZpY2luYWp1ZGljaWFsdmlydHVhbC5wanVkLmNsIiwiYXVkIjoiaHR0cHM6XC9cL29maWNpbmFqdWRpY2lhbHZpcnR1YWwucGp1ZC5jbCIsImlhdCI6MTcwMjI2MzgwMSwiZXhwIjoxNzAyMjY3NDAxLCJkYXRhIjoicndIaHYyVlZiZHJDdUNKd214cWZpb2kyXC9cLzVoQVdXajN2Qk9ZMFN3SGp0aFUxcTltMWVtaE9odUtyZVFyd2Uwd1g3WldFXC9kQTJDUmNcLzVEN2RvMG5tTVdvN3hsS1I5bmJ5UUxNYndWVUlLVVFOazB6STZ6c1BKWVNQeDVjQXpwIn0.ciyoJkdv4ANeGFTb88CuWK0feRYOLNuBT0Ntf_U-QeE

[198] Medina Schulz, Gonzalo, Estructura típica del delito de intromisión informática,Revista Chilena De Derecho Y Tecnología,Vol.3 Nº 1(2014), Recuperado el 11 de diciembre de 2023, pp.83, https://rchdt.uchile.cl/index.php/RCHDT/article/view/32221/34152

[199] Cuarto Tribunal Oral en la Penal, 2 de septiembre de 2009, RIT 135-2009, https://oficinajudicialvirtual.pjud.cl/ADIR_871/penal/documentos/docCausaPenal.php?dtaDoc=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwczpcL1wvb2ZpY2luYWp1ZGljaWFsdmlydHVhbC5wanVkLmNsIiwiYXVkIjoiaHR0cHM6XC9cL29maWNpbmFqdWRpY2lhbHZpcnR1YWwucGp1ZC5jbCIsImlhdCI6MTcwMjI2MzgwMSwiZXhwIjoxNzAyMjY3NDAxLCJkYXRhIjoicndIaHYyVlZiZHJDdUNKd214cWZpb2kyXC9cLzVoQVdXajN2Qk9ZMFN3SGp0aFUxcTltMWVtaE9odUtyZVFyd2Uwd1g3WldFXC9kQTJDUmNcLzVEN2RvMG5tTVdvN3hsS1I5bmJ5UUxNYndWVUlLVVFOazB6STZ6c1BKWVNQeDVjQXpwIn0.ciyoJkdv4ANeGFTb88CuWK0feRYOLNuBT0Ntf_U-QeE

[200] Estructura típica del delito de intromisión informática,Revista Chilena De Derecho Y Tecnología,Vol.3 Nº 1(2014), Recuperado el 11 de diciembre de 2023, pp.83, https://rchdt.uchile.cl/index.php/RCHDT/article/view/32221/34152

ingresa a un sistema informático con el propósito de identificar y corregir vulnerabilidade[201], no de dañar o utilizar dichas vulnerabilidades a su favor.

Aquello, es rescatado por legislaciones como la de Bélgica, permitiendo que dicha diferenciación sea mucho más notoria y fácil de identificar, gracias a un listado de requisitos que permite clasificar la conducta a la de un hacker ético (Art. 62/2. § 1). Bajo dicha legislación, la conducta en cuestión no le corresponde ser excluida en la denominación de hacking ético, ya que no cumple con que la conducta sea relizada sin una intención fraudulenta o de causar daño, y no haber informado a la organización responsable del sistema lo antes posible. En aquello último, nuestro país aún no ha logrado avanzar, ya que en la actualidad solo contamos con dos requisitos copulativos que de cumplirse nos señalan que será una conducta tipificada. Además si bien, contamos con un eximente de responsabilidad, en el Art 16 de la Ley N° 21.459, este quedó profundamente incompleto y confuso. Debido a que es nada razonable que un eximiendo de responsabilidad de una conducta en que no se cuenta con autorización, exija una autorización expresa.

[201] ¿Cuál Es La Diferencia Entre Un Hacker ético Y Ciberdelincuente?: Las Caras Opuestas De La Ciberseguridad (2022, junio 30), *CronUp Ciberseguridad*, https://www.cronup.com/cual-es-la-diferencia-entre-un-hacker-etico-y-ciberdelincuente-las-caras-opuestas-de-la-ciberseguridad/

CONCLUSIONES

En razón de lo desarrollado en esta investigación y en el contexto en que la sociedad actual se mueve digitalmente, podemos concluir que es necesario hacerse cargo de la realidad en que diariamente se recolectan, tratan, almacenan y se transmiten grandes cantidades de datos a través de sistemas informáticos.

La masificación y accesibilidad del uso de las nuevas tecnologías ha provocado que la seguridad en los sistemas de información sea de gran importancia a nivel mundial, ya que tal situacion ha generado nuevos riesgos y ataques contra bienes jurídicos social y penalmente relevantes[202], como es la intimidad de la vida privada, la libertad informática o llegando a tener incluso relación con la propiedad privada, ya que en la actualidad todos los datos bancarios pueden ser blanco de ataques cibernéticos.

Entendido ello, surge la necesidad de estandarizar en alguna medida las políticas de persecución penal sobre ciberdelincuencia. Pero así como se deben legislar nuevos tipos penales o adecuar los anteriores, concluimos que es necesario complementarlos con una normativa procesal que entregue recursos que permitan realizar investigaciones eficaces atendidas las especiales características de la ciberdelincuencia[203], ya que el hacking ético es una de las formas de detección de vulnerabilidades, actividad que promueve la necesaria protección de los sistemas informáticos debido a que ninguno es totalmente seguro o impenetrable, y al rápido y continuo avance y actualizaciones que se generan en los programas informáticos.

Es por esta razón que se desarrolla esta investigación, con el objetivo de poner en la palestra el hacking ético como herramienta utilizada en el desarrollo de la ciberseguridad, debido a su rápida respuesta en los avances que continuamente se genera en los sistemas informáticas ya su gran fardo de efectividad en la hora de detectar brechas. Así como este ve reducido su campo de acción mediante la exigibilidad de la autorización expresa como requisito.

---

[202] Informe de la comisión de futuro, ciencias, tecnología, conocimiento e innovación recaído en el proyecto de ley que establece normas sobre delitos informáticos, deroga la Ley n° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.<https://www.camara.cl/verDoc.aspx?prmID=23303&prmTIPO=INFORMEPLEY > [Consultado: 16/07/2023], pp.2

[203] Idem, pp.4

En base a lo expuesto en la investigación es que pudimos evidenciar las posturas en la discusión respecto de la autorización expresa, en cuanto a si debiera ser o no un requisito, o si debiera ser exigible sólo en algunos escenarios, debiendo existir una excepción a la regla general. Concluyendo que si bien el consentimiento es un requisito para el desarrollo legal del hacking ético, éste debería ser matizado para permitir la excepción legal de responsabilidad que permita proteger el trabajo de los investigadores que desarrollan el hacking ético, siempre en un contexto de investigación, a la vez que esto permitiría dejar de limitar y penalizar esta herramienta de detección de vulnerabilidades.

Lo anterior, además nos lleva a considerar que, a pesar de que se ha avanzado en las leyes sobre ciberdelincuencia, falta por desarrollarlas de forma que se vele por la seguridad de los sistemas de información y en definitiva, por la sociedad misma, como lo sería la incorporación de la excepción a la exigibilidad del consentimiento antes señalada.

BIBLIOGRAFÍA

ÁLVAREZ-VALENZUELA, DANIEL, Y HEVIA ANGULO, ALEJANDRO. (2020). Protección legal para la búsqueda y notificación de vulnerabilidades de ciberseguridad en Chile. Revista chilena de derecho y tecnología, 9(2), 1-4. <https://dx.doi.org/10.5354/0719-2584.2020.60658>

ÁNGELES, M., & MARTÍN, R, *Los Ataques Contra Los Sistemas Informáticos: Conductas De Hacking. Cuestiones Político-Criminales*. Revistajuridicaonline.com. Disponible en: https://www.revistajuridicaonline.com/wp-content/uploads/2009/09/26_7_los_ataques_contra_los_sistemas_.pdf

Are you ready for the new Belgian whistleblower protection rules? (s/f). Clifford Chance. Recuperado el 11 de diciembre de 2023. Disponible en: https://www.cliffordchance.com/insights/resources/blogs/regulatory-investigations-financial-crime-insights/2023/01/are-you-ready-for-the-new-belgian-whistleblower-protection-rules.html

BASCUR, G., & PEÑA SEPÚLVEDA, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. Revista de estudios de la justicia, 37. Disponible en: https://doi.org/10.5354/0718-4735.2022.67885

BASCUR, GONZALO Y PEÑA, RODRIGO. Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Primera parte. Revista de Estudios de la Justicia. 2022. P.4.

BECKER CASTELLARO, SEBASTIÁN, Y VIOLLIER BONVIN, PABLO. (2020). La implementación del convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley 19.223. Revista de derecho (Concepción), 88(248), 75-112. <https://dx.doi.org/10.29393/rd248-13icsb20013> [Consultado: 16/07/2023]

BECKER CASTELLARO, S., & VIOLLIER BOVIN, P. (2020). La Implementación del Convenio de Budapest en Chile: Un Análisis a Propósito del Proyecto Legislativo que Modifica la Ley 19.223. Revista de Derecho (Concepción), 88(248), 75–112. Disponible en: https://doi.org/10.29393/rd248-13icsb20013

BARRIOS, VERÓNICA Y VARGAS, ANDREA. Convenio sobre la Ciberdelincuencia: Convenio de Budapest (2018). <https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf>[Consultado: 14/07/2023].

BRANCA, R. (2023) “La protección legal de los hackers éticos: una mirada desde el derecho penal” [Tesis de maestría. Universidad Torcuato Di Tella]. Repositorio Digital Universidad Torcuato Di Tella <https://repositorio.utdt.edu/handle/20.500.13098/11981>

CARLOS TORI, https://nebul4ck.files.wordpress.com/2015/08/hacking-etico-carlos-tori.pdf, [Consulatdo: 23/07/2023]

CARO, JOSÉ. Algunas consideraciones sobre el riesgo permitido en el Derecho Penal. Forseti, Revista de Derecho, volúmen 12, N°18, Lima 2023. pp.41-66 <http://190.119.238.140/index.php/forseti/article/view/2167/1683>

CHÁVEZ, ERIC. Derecho Penal Parte especial. 2023. <https://app-vlex-com.uchile.idm.oclc.org/#sources/37897>

CONTRERAS CLUNES, A. (2003). Delitos informáticos: Un importante precedente. *Ius et Praxis*, *9*(1), 515–521. Disponible en: https://doi.org/10.4067/s0718-00122003000100023

ESCALONA, EDUARDO. El hacking no es (ni puede ser) delito. 2004. Revista Chilena de Derecho Informático. 4 , 149-167.

ETCHEBERRY, ALFREDO. Derecho Penal parte general, Tomo I. Tercera edición. P.29.

GAMEN, S. A. (2020, diciembre 11). *Caso Gaspar Ariel Ortmann, otra sentencia a favor del hacking ético*. Perfil. Disponible en: https://www.perfil.com/noticias/opinion/sebastian-gamen-caso-gaspar-ariel-ortmann-otra-sentencia-a-favor-del-hacking-etico.phtml

Historia de la Ley Nº 19.223, Tipifica figuras penales relativas a la Informática, <https://obtienearchivo.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/4745/1/HL19223.pdf> [Consultado: 12/07/2023]

Historia de La Ley Nº 21.459 , Biblioteca Nacional del Congreso. Disponible en: https://www.bcn.cl/historiadelaley/historia-de-la-ley/vista-expandida/8018/

HIPLAN, SUSANA. La Ley 19.223 a 26 Años de su Promulgación. 2019 <https://repositorio.uchile.cl/bitstream/handle/2250/173119/La-ley-N%C2%B019223-a-26-a%C3%B1os-de-su-promulgacion.pdf?sequence=1> [Consultado: 23/07/2023]

Indicaciones recaídas en el proyecto de ley, en primer trámite constitucional, que establece normas sobre delitos informáticos, deroga la ley n° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.

Informe de la Comisión De Futuro, Ciencias, Tecnología, Conocimiento e Innovación Recaído, en el proyecto de ley que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, <https://www.camara.cl/verDoc.aspx?prmID=23303&prmTIPO=INFORMEPLEY> [Consultado:16/07/2023]

Informe de la Comisión de Hacienda, recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14.847-06 <https://www.camara.cl/legislacion/ProyectosDeLey/informes.aspx?prmID=15344&prmBOLETIN=14847-06> [Consultado: 22/07/2023]

LINARES, M. B. (2020). Delitos informáticos en el Código penal argentino. Revista chilena de derecho y ciencia política, 11(2), 122–144. https://dialnet.unirioja.es/servlet/articulo?codigo=8758428

LINDE, E., & CONTRERAS FRESNEDA, S. (2021, abril 16). Delito de hacking y comentario de sentencia. Legaltoday.com; Legal Today. https://www.legaltoday.com/practica-juridica/derecho-penal/penal/delito-de-hacking-y-comentario-de-sentencia-2021-04-16/

LOBO, M. M., GIL, S. V. H., & AGUIRRE, A. M. G. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: estudio comparativo. Revista de ciencias sociales - Universidad del Zulia. Facultad de Ciencias Económicas y Sociales, 29(2), 356–372. https://dialnet.unirioja.es/servlet/articulo?codigo=8920556

Magliona, Claudio y López, Macarena. Delincuencia y fraude informático. Derecho Comparado y Ley N° 19.223, Editorial Jurídica de Chile,1999, p.66.

MAYER LUX, LAURA. “El Bien Jurídico protegido en los Delitos Informáticos”. Revista Chilena de Derecho, Vol. 44, Nº 1, Chile, 2017. <https://dx.doi.org/10.4067/S0718-34372017000100011>

MAYER, LAURA Y VERA, JAIME. El delito de espionaje informático: Concepto y delimitación. Revista Chilena de Derecho y Tecnología. 2020. <https://www.scielo.cl/pdf/rchdt/v9n2/0719-2584-rchdt-9-2-00221.pdf> [Consultado: 14/09/2023]

Mayer Lux, L., & Vera Vega, J. (2022). La falsificación informática: ¿un delito necesario? *Revista chilena de derecho y tecnología*, *11*(1), 261–286. Disponible en: https://doi.org/10.5354/0719-2584.2022.65299

MAYER, LAURA Y FERNANDES, INÊS. La estafa como delito económico. pp.187. <https://app-vlex-com.uchile.idm.oclc.org/#search/jurisdiction:CL+content_type:4/afectaci%C3%B3n+al+derecho+de+propiedad+por+delitos+inform%C3%A1ticos/vid/estafa-delito-economico-648790361>

MEDINA SCHULZ, GONZALO, Estructura típica del delito de intromisión informática,Revista Chilena De Derecho Y Tecnología,Vol.3 Nº 1(2014), Recuperado el 11 de diciembre de 2023, pp.83, https://rchdt.uchile.cl/index.php/RCHDT/article/view/32221/34152

Mir, Santiago. Bien jurídico y bien jurídico-penal como límites del Ius puniendi, 1989/1990, p.205.

MIRÓ, FERNANDO. El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. 2012, pp. 1-41 <https://www.marcialpons.es/media/pdf/9788415664185.pdf> [Consultado: 12/11/2023]

MOSCOSO, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista Chilena De Derecho Y Tecnología, 3(1). p.15 <https://doi.org/10.5354/0719-2584.2014.32220>

NAVARRO-DOLMESTCH, R. (2023). La autorización como causal de atipicidad en el delito de acceso ilícito a un sistema informático en la legislación chilena de delitos informáticos. Disponible en: <https://d1wqtxts1xzle7.cloudfront.net/105727397/navarro-libre.pdf?1694711256=&response-content-disposition=inline%3B+filename%3DLa_autorizacion_como_causal_de_atipicida.pdf&Expires=1701624707&Signature=MU04NPFl0fLfOzEJbD4sOC65IVVEkujLPFLN40Ml1AERi8YtmHauteKLQ0yTjbMFaTaPi~fM4~i97ez89CvobHzFjnlw10KLTRuzF7Ca77MpFKZsSELX9i5GVxm~LvmMw1yR4qsDkIN~7A4v~-SXx8tfpF4COzTrL3QMSdrqOwnNMbBDdQwVjgw3Lwe29bCK76LVl1MDFTugm3QTbVHDhPB8vn36oUwprvjpdWwvg3ar7vAmy3OukG3o0nJIFk5n4iY0PTr70E-YfKNXO4GKX4QZf0Tu2ygBlET8sohkRxc--5EfAJy-itpDcHnZ9o6YLLtssyEWsMXErp7ChffGrQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA>

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming”. Revista de Derecho, 41, 211–262. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007#footnote-35037-5

PORTO MACEDO, R., (2002). Privacidad, mercado e información. Cuestiones Constitucionales, (6),135-151. ISSN: 1405-9193. https://www.redalyc.org/articulo.oa?id=88500606

REGIONAL Y SUBREGIONAL ANDINA, R. J. (s/f). *Corpus Iuris Regionis*. Unap.cl.pp 104, https://www.unap.cl/prontus_unap/site/docs/20180425/20180425122950/corpus_iuris_9.pdf

ROXIN, CLAUS. Derecho Penal, parte general. Tomo I. Fundamentos, la estructura de la teoría del delito.

RODRÍGUEZ LLERENA ALAIN EDUARDO, Herramientas fundamentales para el hacking ético, Revista Cubana de Informática Médica 2020, <https://www.medigraphic.com/pdfs/revcubinfmed/cim-2020/cim201j.pdf> [Consultado: 15/07/2023].

RODRÍGUEZ, SAMUEL. ¿Ha de cumplir el bien jurídico protegido una función de garantía o legitimadora del Derecho Penal? Hacia una búsqueda de la legitimidad material de las normas penales. Revista de Derecho, Universidad San Sebastián. 2017. P.159. <https://app-vlex-com.uchile.idm.oclc.org/#search/jurisdiction:CL+content_type:4/funci%C3%B3n+derecho+penal/vid/cumplir-bien-juridico-protegido-705175173>

SANDRA MILENA CASTRO CUBILLOS, White hat: Hacking étic, <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2679/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y > [Consultado: 23/07/2023]

SÁNCHEZ-ESCRIBANO, M. I. M. (2023). El delito de acceso ilícito a un sistema informático: aspectos relativos a su regulación e interpretación. ARANZADI/CIVITAS. Disponible en: https://books.google.es/books?hl=es&lr=&id=3UWxEAAAQBAJ&oi=fnd&pg=PT4&dq=acceso+il%C3%ADcito+España+tesis+&ots=jlQGjRmMnO&sig=wiby6LdTPZgenK5JCiw9S-_2wPU#v=onepage&q&f=true

SOMERS, C., VRANCKAERT, K., & DRECHSLER, L. (2023, mayo 3). Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity? CiTiP Blog; CiTiP KU Leuven. Disponible en: https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/

OXMAN, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del “phishing” y el “pharming”. *Revista de Derecho*, *41*, 211–262. https://doi.org/10.4067/s0718-68512013000200007

VIOLLIER, PABLO. Boletín 12192-25: Delitos informáticos, Derechos Digitales, 3 de enero de 2019, <https://bit.ly/34Kwjva> [Consultado: 14/09/2023].

LEGISLACIÓN Y NORMATIVA

CHILE. Código Penal. 12 de noviembre de 1974. Disponible en: https://bcn.cl/3gqj6

CHILE. Decreto 83 del Ministerio de Relaciones Exteriores que promulga el Convenio sobre la Ciberdelincuencia. 27 de abril de 2017. Disponible en: https://bcn.cl/2yv71

CHILE. Ley Nº 19.223 que tipifica figuras penales relativas a la informática. Diario Oficial de la República de Chile, Santiago, Chile. 7 de junio de 1993. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=30590&buscar=ley%2B19223

CHILE. Proyecto de ley, iniciado en Mensaje del ex Presidente de la República, señor Sebastián Piñera Echeñique, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14.847-06. Disponible en:

https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06

CHILE. Proyecto de ley, iniciado en mensaje de S. E. el Presidente de la República, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. Boletín Nº 12.192-25. 25 de octubre de 2018. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=12509&prmTIPO=INICIATIVAZ

CHILE. Proyecto de Ley sobre Delito Informático. Boletín Nº 412-07, Agosto de 1992. Disponible en https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=2167&prmBOLETIN=412-07

CHILE. Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14847-06. 15 de marzo de 2022. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06

CHILE. Informe de la Comisión de Ciencias y Tecnología recaído en el Proyecto de Ley que modifica el Código Penal, con el objeto de recepcionar en los tipos penales tradicionales, nuevas formas delictivas surgidas a partir del desarrollo de la informática. Boletín Nº 3.083-07, 11 de noviembre de 2002. Disponible en: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=3083-07

CONSEJO DE EUROPA, *Convenio Sobre La Ciberdelincuencia Protocolo Sobre La Xenofobia Y El Racismo Segundo Protocolo Adicional Relativo Al Refuerzo De La Cooperación Y De La Divulgación De Pruebas Electrónicas Convenio Sobre La Ciberdelincuencia Protocolo Sobre La Xenofobia Y El Racismo Segundo Protocolo Adicional Relativo Al Refuerzo De La Cooperación Y De La Divulgación De Pruebas Electrónicas*. Disponible en: https://www.coe.int/documents/8475493/202017550/PREMS+015123+ESP+2023+Convention+Cybercrimininalité+WEB+A5.pdf/a6b85c77-c79a-ef99-4d66-48351c1b48fc?t=1678890134243

ESPAÑA, Boletín Oficial Del Estado, Miércoles 23 de junio de 2010. Disponible en: https://www.boe.es/eli/es/lo/2010/06/22/5/dof/spa/pdf

SITIOS WEB

CETYS, Universidad Francisco de Vitoria, (2023, septiembre 5). ¿Qué es el hacking ético? Formación profesional UFV. Disponible en: https://www.ufv.es/cetys/blog/que-es-el-hacking-etico/

CRONUP (2022, junio 30). ¿Cuál Es La Diferencia Entre Un Hacker ético Y Ciberdelincuente?: Las Caras Opuestas De La Ciberseguridad. CronUp Ciberseguridad. Disponible en: https://www.cronup.com/cual-es-la-diferencia-entre-un-hacker-etico-y-ciberdelincuente-las-caras-opuestas-de-la-ciberseguridad/

Senado. Comisión de Economía conoció detalles del ciberataque del BancoEstado. Disponible en: https://www.senado.cl/noticias/ciberseguridad/comision-de-economia-conocio-detalles-del-ciberataque-del-bancoestado

Cybersecurity & Infrastructure Security Agency. Disponible en: https://www.cisa.gov/coordinated-vulnerability-disclosure-process

Ciclo de charlas sobre derecho informático [archivo de video], minuto 10:40. Canal Uchilederecho. Disponible en: https://www.youtube.com/watch?v=Y-TV3oRY82U