La protección legal de los hackers éticos: una mirada desde el derecho penal

Autoría: Branca, Rodrigo Nahuel
Año de defensa de la tesis: 2023

UNIVERSIDAD TORCUATO DI TELLA

ESCUELA DE DERECHO

MAESTRÍA EN DERECHO PENAL

La protección legal de los hackers éticos: una mirada desde el derecho penal

BRANCA RODRIGO NAHUEL
LEGAJO:19P1123
DNI: 36687591

TUTOR: Leandro Dias

Firma tutor

FECHA DE PRESENTACIÓN (17 - 2 - 2023)

La protección legal de los hackers éticos: una mirada desde el derecho penal.

Rodrigo Branca

RESUMEN

En la presente monografía se analizará la temática de los Hackers éticos. Se explicará, en particular, que existe una función altruista de las acciones que estos llevan a cabo. Por consiguiente, el autor del presente propondrá la necesidad de una modificación en el Código Penal, que regule una causa de justificación para estos sujetos, con el fin de que el artículo 153 bis CP no castigue con pena de prisión a los hackers éticos. El núcleo de la propuesta será una comparación o paralelismo con la causa justificación que el derecho positivo actualmente prevé para el delito de violación a la propiedad privada física cuando el hecho se realiza para salvar a un bien de mayor entidad (artículos 150 y 152 CP).

Palabras Clave

Hackers éticos; Causal de justificación; Código Penal; Propiedad Privada; Altruismo; Pena; Prisión.

ABSTRACT

This paper will analyze the issue of ethical hacking. It will be explained that there is an altruistic function regarding the actions that they carry out. For these reasons, the author of this article will propose an amendment to the Criminal Code, regulating a justification for hackers who commit the offense regulated in article 153 bis CP. The core argument will be a comparison or parallelism with the usual lesser evil justification in cases of trespassing (articles 150 and 152 CP).

Keywords.

Ethical hackers; Justification; Penal Code; Private Property; Altruism; Punishment; Prison sentences.

INDICE

I. INTRODUCCIÓN.

1. Hackers Éticos y Crackers.

Vivimos en la era de la información y la comunicación, donde cualquier ser humano, desde casi cualquier lugar del planeta, puede conectarse a internet y comunicarse en directo con alguien del otro lado del mundo. Un estudio reciente demostró que hay casi 5000 millones de personas que tienen acceso a Internet, sin mencionar que el acceso a Internet ya es considerado, por algunas voces, como parte de un derecho humano inviolable[1], irrenunciable y fundamental para las personas del mundo (Galeano, 2022). Para que esto suceda, simplemente es necesario contar con un dispositivo electrónico que sea capaz de conectarse a internet y que posea un micrófono, pantalla, parlantes y una cámara de video. Características que tiene prácticamente cualquier teléfono móvil moderno. Esto es conocido como "hardware". Pero además, deberá contar con un sistema operativo que le permita al ser humano operar e interactuar con ese dispositivo electrónico y sus componentes físicos, mediante un lenguaje de programación. A esto lo conocemos como "software". En otras palabras, el hardware es el conjunto de elementos físicos que constituyen un sistema informático y el software el conjunto de programas o rutinas que les permiten a las personas darle ordenes al sistema informático y que éste realice una función predeterminada (Cottino, 2009, págs. 15-16) .

Esto quiere decir que cualquier persona que sea capaz de darle órdenes a un dispositivo informático, podría ejecutar cualquier tipo de función, o básicamente, hacer con él lo que se le antoje. Para evitar esto, los especialistas en informática crearon un conjunto de medidas de seguridad o barreras que le impiden al usuario que no cuente con los permisos necesarios (como una contraseña), hacer lo que quiera con el sistema. Estas medidas las conocemos como "ciberseguridad" o seguridad informática (Llamas, 2021). Bancos, empresas, personas particulares y hasta los estados del mundo operan hoy en día a través de sistemas informáticos conectados a internet, por lo que sin una de estas

[1] Así lo entendió el Consejo de Derechos Humanos de la Organización de Naciones Unidas el 27/06/16 al suscribir la resolución A/HRC/32/L.20. La cual puede ser revisada en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf (Español) – (consultado el 1/12/2022). (ONU, 2016)

medidas de seguridad podría ver comprometida su privacidad y hasta su correcto funcionamiento.

Estos programas o softwares pueden ser de propiedad privada, como pueden ser de propiedad pública. También conocidos como "software libre" o "software privado". La principal diferencia entre ambos es que el código fuente[2] es de acceso público en los casos de software libre, pudiendo ser modificado y alterado por cualquier persona; por el contrario el software privado es de acceso restringido. Un ejemplo sería el sistema operativo Linux, basado en software libre y su contraparte, el sistema operativo Windows, el cual es cerrado, mediante medidas de seguridad informática, que impiden a las personas acceder al código fuente (Gradin, 2004, págs. 10-11).

Ahora que tenemos claro cómo están compuestos los sistemas informáticos, vamos a hablar sobre quienes este trabajo está basado: los "hackers". Es probable que toda persona que lea este texto, alguna vez haya escuchado la palabra hacker, a la cual se la asocia rápidamente con sujetos con una finalidad siniestra, cuyo propósito es el de irrumpir en los sistemas informáticos y cuentas de usuarios sin autorización de sus dueños para causar daños o hasta obtener beneficios económicos (Vásquez, 2016, pág. 50). Hoy en día se entiende como hackers a personas ligadas a usos ilegales de la tecnología, específicamente en la violación de la protección de las computadoras y las redes privadas. Y suelen ser asociados a la imagen que aparece en las noticias, las películas, series, etc.: adolescentes que disfrutan del uso extremo de la tecnología, sin miedo al riesgo que esto implica, pero con altas capacidades intelectuales en esta materia (Gradin, 2004, págs. 9-11). Pero en este trabajo no nos vamos a referir a ellos como "hackers". Las personas descriptas anteriormente son simplemente criminales o "cibercriminales", como se los denomina hoy en día. También en algunos textos se los puede identificar como "crackers" (Himanen, 2004, pág. 5).

El filósofo finlandés Pekka Himanen concede una mirada distinta y se refiere a los hackers como personas que se caracterizan por ser expertos o entusiastas que les apasiona su trabajo. Pueden ser actores, chefs, médicos o cualquier otra profesión,

[2] El código fuente es el conjunto archivos con instrucciones escritas por una persona (programador) en un lenguaje de programación determinado, que sirve para compilar un programa para que pueda ser utilizado de forma directa por el usuario. https://tecnologia-facil.com/que-es/que-es-codigo-fuente/ (consultado el 1/12/2022)

siempre y cuando sean apasionados por lo que hacen y busquen ir más allá de sus conocimientos para superar las dificultades y barreras. Inclusive sin tener nada que ver con las computadoras (Himanen, 2004, págs. 5-6). Siguiendo ese pensamiento, podemos definir que un hacker informático es aquél que tiene pasión y conocimientos sobre la programación de los sistemas informáticos y en cuya naturaleza está el hecho de encontrar la forma de superar las barreas que las tecnologías modernas le imponen. También son personas que creen que la información debe ser pública y abierta a todos como un bien común, facilitando el acceso a la información y a los recursos informáticos (Himanen, 2004, pág. 5).

De esta forma, vemos como dentro de la naturaleza de los hackers informáticos está implícito el hecho de buscar superar las medidas de seguridad informática y acceder a los sistemas informáticos de forma ilegítima, en algunos casos. Pero no tenemos que confundirlos con los crackers o cibercriminales. Existen profesionales informáticos que ingresan sin autorización a un sistema informático privado, pero con una intención altruista y beneficiosa para la sociedad (Gradin, 2004, pág. 61). Por ejemplo, para descubrir vulnerabilidades y colaborar para su corrección y fortalecimiento. Esto es, si realizan una operación de intromisión a una propiedad informática privada, en vez de ser un ilícito, sería considerado un servicio a la comunidad. A estos sujetos se los conoce como “hackers éticos”, ya que cómo vimos, sus motivaciones no son las de cometer delitos, sino más bien las de hallar vulnerabilidades en los sistemas informáticos y poder subsanarlas, creando sistemas más robustos. Se cree que la palabra “ético” anula aquellas connotaciones negativas que implica el hacking, ya que en definitiva los hackers éticos utilizan técnicas maliciosas, pero de una manera profesional para tratar de mejorar la seguridad de los sistemas. (Vásquez, 2016, pág. 50)

2. Marco legal

Es fácil darse cuenta como la proliferación y masividad de los dispositivos informáticos, hicieron que algunos tipos penales que solamente eran pensados en el mundo físico también ocurran en este nuevo el universo virtual creado gracias a los avances de la tecnología (estafas, daños, accesos ilegítimos, entre otros), por lo que los

estados han tenido que amoldar sus leyes internas para incluir estos nuevos "ciberdelitos" o delitos informáticos.

Pese a ello, aún hoy en día, existe una discusión doctrinaria sobre la definición y el concepto de "delitos informáticos" o "ciberdelitos". Ésta misma radica en considerar si hay o no ciberdelitos verdaderos, o si en realidad se trata de delitos comunes con ciertas particularidades[3]. Específicamente en la República Argentina esta discusión no parece ser tan importante ya que, conforme la ley vigente, los delitos informáticos no poseen un régimen jurídico especial, más allá de que en algunas jurisdicciones haya fiscalías especializadas en investigar ciberdelitos[4] (Temperini, 2018, págs. 54-55). Si bien no hay una definición legal sobre el término, el Gobierno de la Nación Argentina los define como *"conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas".* Es decir que estos consisten en diversas situaciones dañosas como "estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing" (Gobierno de la Nación Argentina, 2022).

Por su parte, es necesario entonces definir el lugar en donde se podrían llevar a cabo este tipo de delitos; en este caso se hablaría del ciberespacio. Este es entendido como un área intangible, a la cual, todos pueden acceder por medio de una computadora con acceso a internet, desde cualquier lugar del mundo. Para la comisión de ciberdelitos, los "ciberdelincuentes" utilizan medios informáticos tales como internet, dispositivos móviles (computadoras, teléfonos, etc.), entre otras cosas (Gobierno de la Nación Argentina, 2022). Como es de esperarse, el ciberdelito puede aparecer a partir del uso de cualquiera de las plataformas virtuales que se manejan en el día a día; pero, sobre todo, a partir de sitios no seguros, contraseñas que no cumplen las reglas mínimas de seguridad, entre otros. Los ciberdelitos más comunes son los que se cometen por medio del uso de programas maliciosos que se desarrollan con la intención de "borrar, dañar, deteriorar,

[3] Para un mejor entendimiento del debate, véase Temperini (2018), págs. 54-55

[4] El Ministerio Público Fiscal de la CABA creó en el año 2012 la primera fiscalía especializada en delitos informáticos. También existe, en el ámbito de la Procuración General de la Nación, la UFECI (Unidad Fiscal Especializada en Ciberdelincuencia) creada en el año 2015. Córdoba, Salta y Chubut son otras de las jurisdicciones que también poseen organismos específicos para la investigación de estos delitos en particular.

hacer inaccesibles, alterar o suprimir datos informáticos sin tu autorización y con fines económicos y de daño" (Gobierno de la Nación Argentina, 2022).

Estas apreciaciones no son algo característico únicamente de la República Argentina. Por el contrario, tienen lugar en un marco de normativa internacional. En especial, en la "Convención Contra la Ciberdelincuencia del Consejo de Europa (Convención de Budapest)" (2001), donde en un primer artículo se definen palabras claves tales como sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico. Seguidamente, en la misma convención, se establecen las medidas que deben adoptarse nivel nacional. Como primera cuestión en el Título 1 se trata los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. De esta forma pasa a abarcar, el "acceso ilícito"[5], la "interceptación ilícita"[6], los "ataques a la integridad de los datos"[7], los "ataques a la integridad del sistema"[8] y el "abuso de los dispositivos"[9]. Luego, en el Título 2, se detallan los delitos informáticos, haciendo referencia a la "falsificación informática"[10] y el "fraude informático"[11]; posteriormente, se mencionan los "delitos relacionados con el contenido" (Título 3), donde se hallan los "delitos relacionados con la pornografía infantil"[12]. Seguido de estos están los "delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines"[13].

En cuanto a la normativa nacional concreta, basada en las directivas internacionales mencionadas anteriormente, debe decirse que, en la Argentina en 2008 se tipificaron o adecuaron una serie conductas previstas en el Código Penal Argentino, para poder amoldarse a estos nuevos tiempos, mediante la sanción de la Ley 26.388[14]. En lo

[5] Art. 2. Convenio sobre la ciberdelincuencia del Consejo de Europa
[6] Art. 3. Convenio sobre la ciberdelincuencia del Consejo de Europa
[7] Art. 4. Convenio sobre la ciberdelincuencia del Consejo de Europa
[8] Art. 5. Convenio sobre la ciberdelincuencia del Consejo de Europa
[9] Art. 6. Convenio sobre la ciberdelincuencia del Consejo de Europa
[10] Art. 7. Convenio sobre la ciberdelincuencia del Consejo de Europa
[11] Art. 8. Convenio sobre la ciberdelincuencia del Consejo de Europa
[12] Art. 9. Convenio sobre la ciberdelincuencia del Consejo de Europa
[13] Art. 10. Convenio sobre la ciberdelincuencia del Consejo de Europa
[14] Pablo A. Palazzi destaca que el CP, redactado en el siglo pasado y aprobado en la década del veinte, respondía a otra era tecnológica y que si bien a lo largo de los años se habían hecho modificaciones y reformas parciales, el problema de la criminalidad informática requería de una reforma general en la materia debido a sus características: magnitud de los daños, naturaleza global e internacional de esta clase de delitos, facilidad para cometerlos y las dificultades para la investigación. También destaca los hechos históricos que motivaron a los legisladores a proponer las reformas legislativas que incluyeran esta nueva modalidad criminal: en 1998 la página web oficial del Poder Judicial de la Nación fue atacada y se colocó una imagen

que a este trabajo importa veremos este tipo de delitos bajo el "Título V. Delitos contra la libertad. Capítulo III. Violación de secretos y de la privacidad".

En particular, en el art. 153 CP se habla de la violación de, entre otras cosas, comunicaciones electrónicas, así como de su apoderamiento, incluso cuando no estuviesen cerradas, o de su supresión o desvío a personas a las que no estaban dirigidas. También están contemplados los casos de intercepción o captación de comunicaciones electrónicas o telecomunicaciones que provengan de cualquier sistema privado o de acceso restringido. Para todos estos casos la pena es de 15 días a 6 meses de prisión. Si, además, el autor del delito comunica o publica el contenido de la comunicación electrónica, la pena pasa de 1 mes a 1 año de prisión. En estos casos, además se establece una multa de 1.500 a 100.000 pesos argentinos.

En el artículo siguiente, más precisamente en el artículo 153 bis CP, se establece una pena a un "ciberdelito" relevante para la presente investigación. Es en esta figura que se sanciona a quien accede ilícitamente, o excediendo a una autorización concedida, a un sistema informático privado, por cualquier medio y a sabiendas de que su acceso está restringido. En este caso, la prisión será de 15 días a 6 meses. Pero si el sistema o dato informático correspondiera a un organismo público estatal o proveedor de servicios públicos o financieros, la pena será de 1 mes a 1 año de prisión.

Por último, en el artículo 157 bis, se castigan con 1 mes a 2 años de prisión los siguientes casos de quien:

1. "A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales";

2. "Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley".

---

recordando el asesinato del fotógrafo José Luis Cabezas, hecho que fue declarado atípico en el año 2002; o bien cuando en el año 2006 se desató una polémica sobre la violación de correos electrónicos de varios periodistas y jueces, cuando hasta el momento los correos electrónicos no eran equiparados ni protegidos como la correspondencia física, generando un vacío legal. Para un mayor detalle sobre los antecedentes históricos y las intenciones legislativas que llevaron a la sanción de la Ley 26.388 (Palazzi, Los Delitos Informáticos en el Código Penal, 2016, págs. 3-22).

3. “Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales”.

Dicho lo anterior, podemos ver que si nos guiamos exclusivamente por la letra de la ley, nuestro ordenamiento penal no distingue entre un cracker o cibercriminal y un hacker ético, por más fin altruista que tenga su acción. Esto es así, ya que el art. 153 bis CP castiga el simple hecho de acceder a un sistema informático ajeno sin autorización, o excediendo los límites de la autorización concedida, quedando comprendida cualquier acción de hacking (Roibón, 2018, págs. 134-138). Esto es extraño, porque cuando nos referimos a la violación de la propiedad privada física de un inmueble, es decir, al delito de violación de domicilio —previsto en el art. 150 CP— la ley sí establece una causa de justificación y permite la violación de la propiedad privada ante una situación de peligro que generará un beneficio —art. 152 CP—. Sin embargo, una conducta equivalente, pero llevada a cabo en el “mundo virtual” en principio sería siempre un ilícito punible según el Código Penal Argentino. En el siguiente apartado se explicará la hipótesis de trabajo y las posibles soluciones al problema planteado.

II. OBJETIVO DEL TRABAJO Y ACTUALIDAD DEL TEMA

1. Objetivo del trabajo

Como vimos hasta ahora, el hacking —en cualquiera de sus variables— podría ser considerado un delito dentro de la República Argentina, ya sea dentro de los términos del art. 153 bis o del 157 bis del CP (Roibón, 2018, pág. 134). Más allá de eso, también es posible afirmar que el hacking ético es una actividad que trae aparejados grandes beneficios para los sistemas informáticos y sus usuarios, ya que los hace más seguros (Sánchez Avila, 2019, págs. 7-8). Esta es la postura que se adoptará en el presente trabajo. El objetivo general de este trabajo consiste en contestar la siguiente pregunta: ¿se debe eliminar la pena que establece el CP en los casos de hackers éticos, debido a los beneficios altruistas que traen aparejados?

A modo de adelanto, se dirá que la respuesta es afirmativa y para ello se van a proponer dos caminos. Estos son:

1. una modificación del Código Penal en el artículo 153 bis, incorporando una causal de justificación para estos casos;

2. una interpretación benévola de la norma con su redacción actual.

2. La necesidad de proteger a los hackers éticos mediante una causa de justificación.

A continuación se buscará plasmar de forma clara la hipótesis de trabajo, así como también justificar la idea mediante ejemplos que hagan entender, de forma inequívoca, la diferencia entre un hacker y un hacker ético que actúa con fines altruistas. A su vez, explicaré por qué la forma de materializar esta propuesta es mediante una modificación de la redacción actual del Código Penal.

Los hackers éticos, como fue explicado anteriormente, tienen como medio de trabajo la comisión delitos contenidos en el Código Penal argentino y en las convenciones internacionales, pero con objetivos que están alejados de lo delictivo. Se puede pensar a los hackers como artistas informáticos o tecnológicos que sienten, en algún punto, orgullo por las obras que llevan a cabo a través de sus conocimientos y destrezas (Gradin, 2004, pág. 11). No obstante, desde un punto de vista meramente legal, las actividades de los hackers sin dudas cumplirían el tipo al menos del art. 153bis del CP: su actividad justamente consiste en acceder ilícitamente a un sistema informático (privado, pero también eventualmente público) y con dolo de acceder a un sistema restringido. La redacción de la disposición, entonces, está en tensión con la función social beneficiosa que pueden cumplir los hackers éticos.

De todos modos, en la doctrina se ha intentado resolver el problema al señalar que estas conductas serían atípicas. Según lo analizado por Gutiérrez, Radesca y Riquert, las acciones de los hackers éticos serían atípicas dentro del delito penado en el artículo 153bis del CP. Se plantearía así una excepción al principio de la inviolabilidad de las comunicaciones, porque se entiende que el "derecho protegido" no es un concepto absoluto ("autorizaciones judiciales para su acceso en curso de una investigación penal, o por razones de seguridad, o por cumplimiento efectivo del ejercicio de un deber derivado de la patria potestad, etc.") (Gutiérrez, Radesca, & Riquert, 2013, págs. 9-11).

Entonces, incluso si no se contase con una autorización previa, los hackers éticos podrían realizar estas conductas, en virtud de esta excepción a la regla.

Otras causas de atipicidad vinculadas a este delito se refieren al acuerdo del usuario o sujeto pasivo o al cumplimiento del deber a través de un mandato judicial fundado en una investigación que se encuentra en proceso en diversas situaciones tales como:

"que autorice el acceso a la información que pueden brindar los programas digitales de telefonía celular, generalmente utilizados a nivel comercial para facturación, con el objetivo de ubicar a una determinada persona, independientemente de la comunicación que entable, su itinerario en virtud de la información de antena, la activación de GPS, etc." (Gutiérrez, Radesca, & Riquert, 2013, pág. 11).

Por supuesto que estos casos no son relevantes para el análisis de los hackers éticos, que justamente actúan sin el acuerdo del titular y sin una orden judicial o equivalente. Lo que estaría en juego con esta excepción, entonces, es una ponderación entre la necesidad de protección de la intimidad y la de obtener beneficios tangibles en cuestiones de seguridad. Cuando el hackeo es realizado con la intención de facilitar formas de trabajo a ingenieros informáticos, detectar situaciones de riesgo en diversos sistemas o software y solucionarlas, existencia de programa maligno y su posterior eliminación, pruebas de sistemas de bloqueo, entre otras situaciones que incluyen a estos hackers éticos, esta ponderación daría como resultado un balance a favor de obtener los beneficios en materia de seguridad. Lo decisivo entonces sería el motivo con el que se accede al sistema, no la forma de acceso (Gutiérrez, Radesca, & Riquert, 2013, pág. 10). En otras palabras, podemos inferir en base a lo dicho por los autores, que las situaciones penadas por ley, como las exceptuadas en la doctrina, no hacen referencia a la forma en la que se hackeo el sistema, sino al por qué.

A su vez, se ha dicho que "*[e]l tipo no distingue la forma de intrusismo, de modo que el acceso bien puede realizarse mediante la utilización de los datos concernientes al sujeto pasivo, es decir, como si el autor fuera en realidad el legítimo usuario del sistema, o aprovechando las deficiencias de los procedimientos de seguridad del sistema o en*

alguno de sus procedimientos" (Gutiérrez, Radesca, & Riquert, 2013, pág. 10)[15]. Continúan diciendo los autores que tal circunstancia descripta implica una razón de uso que permite excluir del tipo los casos de los programadores o "hackers éticos", que acceden mediante el hecho de poder abrir claves o puertos en una computadora o red informática, con herramientas de software dedicadas a tal fin para el testeo y con el objetivo de resguardar, restablecer o mejorar el sistema.

No obstante, el problema de esta postura es que, primero, va directamente en contra de lo que dice la ley en el art. 153bis del CP. La ley no establece esa excepción al alcance de la regla de forma expresa, sino que la conducta prohibida se encuentra especificada sin una excepción de esta clase. Entonces, ya desde el vamos se parte de un déficit en la argumentación que no es reconocido por los autores en cuestión. Como se ha mencionado, se trata de una intrusión o acceso ilegítimo a un sistema informático determinado, ya que el tipo delictivo exige la vulneración o afectación del derecho a la privacidad y confidencialidad, la cual se reduce a dos aspectos esenciales de la vida de toda persona: "la exclusividad y la intimidad". La conducta típica se traduce en el acceso a un sistema o dato informático, existiendo una limitación o restricción en cuanto a la posibilidad de acceder o tomar conocimiento de este.

Los ejemplos adicionales que brindan los autores, basados en una *autorización* del titular, sí son causas de atipicidad, debido a que la ley expresamente hace mención de eso con la cláusula "sin la debida autorización o excediendo la que posea". En este sentido, el elemento subjetivo requiere que el autor del hecho tenga conocimiento del acto que está cometiendo, es decir que está realizando un acceso ilegal al sistema o dato en concreto, el cual mantiene un acceso limitado para el público en general, debiendo mediar además una voluntad o intencionalidad de realizar tal trasgresión. No caben dudas de que el hacker ético tiene conocimiento y voluntad de acceder al sistema informático sin la debida autorización del sujeto, por lo que el elemento subjetivo estaría perfeccionado. Pero esto no es un impedimento para afirmar que, igualmente, su labor altruista trae aparejada grandes beneficios y que por ello la ley no debería sancionarlo a través de una causa de justificación. Entonces, si la conducta o el acto realizado se llevara adelante mediando el consentimiento o la autorización del dueño de una red o sistema informático

[15] Véase también (Morosi & Viera, 2011, pág. 531).

determinado, existe o media una autorización formal del propio "ofendido", que impide el cumplimiento del elemento del tipo legal que requiere que la intromisión se realice "*sin la debida autorización o excediendo la que posea*" (Buompadre, 2009, pág. 713). Así, "en la medida en que la falta de autorización debida es un elemento normativo del tipo, el acuerdo previo con terceros legitima el accionar y directamente elimina el tipo objetivo sistemático. La autorización puede ser formulada de cualquier forma aunque, por lo general, cuando se trata de un permiso previo, se entiende traducida en un contrato de prestación de servicios de seguridad informática" (Gutiérrez, Radesca, & Riquert, 2013, pág. 9)[16].

Segundo, y más importante, la argumentación de Gutiérrez, Radesca y Riquert debería conducir, en todo caso, a una causa de justificación supralegal (es decir, no escrita en la ley), y no a una causa de atipicidad. Una causa de atipicidad se produce cuando por alguna razón ya la conducta prohibida o mandada ni siquiera es realizada *prima facie*, por ejemplo, porque el bien jurídico protegido (o el "fin de la norma") no ha sido afectado. Sin embargo, en los casos de conductas de "white hacking", es casi una obviedad que el bien jurídico protegido ha sido afectado: el hacker *sí* ingresa en el ámbito protegido por el bien jurídico, esto es, en el ámbito de intimidad de la víctima. Por tanto, se trata de una conducta en principio prohibida y que merece ser castigada. A diferencia, nuevamente, de lo que pasa con los casos de autorizaciones expresas del titular del bien jurídico, porque allí es la propia "víctima" abre su esfera de derechos ante el supuesto autor. Es lo mismo que sucede, por ejemplo, en el delito de hurto: si A está de acuerdo en que su compañero B se lleve la lapicera que tiene en el escritorio de la oficina y B, sabiéndolo, se la lleva, entonces se trata de una conducta atípica, por falta de afectación al bien jurídico "propiedad".

Este problema no es visto por los autores, debido a que argumentan con el lenguaje de las excepciones. Estas últimas son justamente la que caracteriza a las causas de justificación que, en cierto sentido, son excepciones a reglas aplicables, (Moreso, 2001, págs. 525-545) y *no* a las causas de atipicidad. Así, ya señalaba Hart con claridad lo siguiente sobre la estructura de las causas de justificación, a partir del ejemplo clásico de la legítima defensa:

[16] Véase también (Sáez Capel & Velciov, 2008, págs. 733-735)

"Matar en defensa propia es una excepción a la regla general que hace punible el dar muerte a alguien; se admite porque la política, dentro de las finalidades u objetivos que, en general, justifican el castigo del homicidio (p. ej., la protección de la vida humana), no incluyen casos como estos" (Hart, 2019, pág. 54).

Por consiguiente, la argumentación de los autores debería ser considerada una causa de justificación. De hecho, cuando señalan que en casos así se produce una ponderación entre intereses de seguridad de la generalidad y los intereses de la víctima en la intimidad, están recurriendo a la argumentación característica del estado de necesidad justificante agresivo (prototipo de causa de justificación basada en ponderaciones) del artículo 34, inc. 3º del CP[17]. Por esa razón, argumenta Palazzi (Breves comentarios a los proyectos legislativos sobre delitos informáticos, 2006, pág. 1531) que el hacker queda amparado, en una situación de necesidad en lo que respecta a su accionar, donde muchas veces resulta necesario comprometer la confidencialidad de los sistemas o archivos hackeados, con el fin de lograr el bien mayor. Este autor señala también al fenómeno de la ingeniería inversa como contemplado dentro de este supuesto de ética hacker, la cual tiene la finalidad de tomar un producto existente e investigarlo rompiendo con la privacidad de su composición para conocer esta última y su funcionalidad; de esta forma se estaría violando la propiedad intelectual, pero con un fin lícito y ético (Palazzi, Breves comentarios a los proyectos legislativos sobre delitos informáticos, 2006, pág. 1531)

A pesar de que Palazzi tiene razón en señalar que estos casos se deben resolver como causas de justificación, su argumentación no es convincente. El hacker ético no se encuentra en una situación de necesidad, o al menos no en sentido estricto. Desde el punto de vista del estado de necesidad justificante agresivo[18] del art. 34, inc. 3º del CP, el hacker no actúa frente a un mal mayor *inminente*. Incluso suponiendo que los intereses de seguridad informática superan esencialmente a los intereses en la intimidad de las

[17] Art. 34, inc. 3° CP: "No son punibles: (…) 3º. El que causare un mal por evitar otro mayor inminente a que ha sido extraño; (…)"

[18] Creus (Derecho Penal. Parte General. 3° edición, 1992, pág. 323) dice: "Es la situación en que se encuentra un sujeto en la que, como medio -'necesario'- para evitar la pérdida de bienes jurídicos propios (o de un tercero en determinados casos), **ataca** un bien jurídico extraño de menor entidad que el que trata de salvar." (el destacado me pertenece)

personas concretas, el peligro de afectación a los intereses de seguridad todavía no es actual. En ese sentido, una violación a la seguridad informática (diferente a la realizada por el propio hacker ético) podría suceder en el futuro cercano, lejano, o no suceder nunca. En ese sentido, difícilmente pueda decirse que una conducta típica de white hacking salvaguarde un intereses de seguridad cuya pérdida sea inminente. Por otro lado, ya el propio art. 34, inc. 3º del CP señala que quien actúa en estado de necesidad debe ser "extraño" al mal mayor inminente. Así, el hacker ético que "descubre" una vulnerabilidad es quien en cierto sentido ha creado ese mal mayor, derivado de una violación a los sistemas de protección, previamente no reconocida.

A su vez, Palazzi destaca que "las conductas de testeo de seguridad de falencias de redes informáticas (ethical hacking) en el marco de investigación académica, casera o empresaria, muchas veces serían realizadas con consentimiento de la víctima, interesada en la detección de errores para su subsanación" (Palazzi, 2008, pág. 1217). Dado que en estos casos la víctima *no* brinda su consentimiento expreso, a lo sumo podría hablarse de un consentimiento presunto o uno hipotético. El presunto queda fuera de lugar, porque en estos casos el hacker ético *puede* preguntarle a la víctima si autoriza la conducta, pero por razones prácticas decide no hacerlo. Es decir, existe la posibilidad fáctica de consultar a las víctimas (a diferencia de lo que sucede, por ejemplo, en una operación médica de urgencia a favor de alguien inconsciente), por lo que no puede hablarse de un consentimiento presunto del titular del bien jurídico "intimidad". Solo quedaría a disposición un "consentimiento hipotético", en el sentido de que si la víctima hubiese sabido que un hacker está ingresando a su esfera de intimidad informática, de todos modos habría consentido, debido a que le interesa proteger su seguridad futura. Sin embargo, no solo la figura del consentimiento hipotético se encuentra muy discutida en la doctrina, sino que además difícilmente pueda afirmarse algo así. No es difícil suponer que muchas personas no consentirían en que un tercero ingrese a sus cuentas de correo electrónico o a sus bases de datos, incluso si eso fuese realizado con fines altruistas. Por consiguiente, una causa de justificación (o de atipicidad, dado el caso, a partir del ya mencionado elemento de la autorización) basada en la noción del consentimiento no puede abarcar los casos de white hacking.

Esto significa que la causa de justificación que ampare a los hackers éticos no puede buscarse sin más en el estado de necesidad o en el consentimiento. Más bien, se

requiere una causa de justificación específica, quizá parcialmente basada en nociones de necesidad, tal como sucede con la violación de domicilio clásica. En definitiva, el interrogante que se plantea la doctrina gira en torno a la posibilidad de admitir al "ethical hacking o a las tareas que —mediante herramientas de software dedicadas a tal fin— desarrollan los expertos en seguridad informática para determinar las eventuales falencias de las redes" como una circunstancia o comportamiento exento de la prohibición establecida por el propio art. 153 bis CP. Ello en función de que la noción de hacking ético involucra una amplia gama de actividades como puede ser el caso de la realización de tareas de investigación académica, domestica, o bien las tareas desarrolladas por empresas de seguridad informática en la búsqueda de brindar mayor certeza o seguridad a los sistemas informáticos.

3. Actualidad de la cuestión.

Eric Raymond establece que: "*La cultura hacker no tiene líderes, pero tiene héroes culturales, ancianos de la tribu, historiadores y portavoces*" (Raymond, 2001). Y estas obras pueden beneficiar a la sociedad de un modo notable. Un ejemplo se dio en los años 70, cuando un grupo de hackers pudo desarrollar las técnicas de criptografía avanzada que copiaron del ejército de EEUU. Esto se realizó por medio del diseño de programas que garantizan la privacidad de las comunicaciones electrónicas. A partir de esto, si bien el programa es positivo para el refuerzo del cumplimiento del derecho a la privacidad en contra del abuso de obtención de información del gobierno estadounidense, el mismo ejército de ese país lo prohibió en su exportación (Gradin, 2004, pág. 11). La difusión de estos programas obtenidos del ejército estadounidense, al estar de forma gratuita y con el código abierto, logró que se pudiera obtener un nuevo nivel de seguridad mundial y este se estableciera de forma standard. La "iniciativa personal", la "autogestión de proyectos" nacidos en las necesidades locales o personales, beneficiando a la sociedad en general son características propias de estos hackers (Gradin, 2004, pág. 11). Otro caso es el de Linus Torvalds, quien en el año 1991 programó un sistema operativo que luego sería conocido como Linux, que fue luego distribuido gratuitamente a lo largo del mundo para su utilización por todo aquel que lo necesitara (Gradin, 2004, pág. 11).

En Argentina la cuestión resulta extremadamente actual a partir de la aparición de un caso notorio de un hacker ético. Un joven llamado Santiago López, con 19 años de edad a la fecha del 4 de marzo de 2019, alcanzó a percibir la suma de 1 millón de dólares por descubrir los errores informáticos de empresas como Twitter, Verizon, otras empresas privadas y también al propio gobierno de Estados Unidos de América (BBC News Mundo, 2019). Su trabajo se conoce como "bug-bounty hacker" en inglés o "cazarrecompensas en internet" o "hacker de sombrero blanco" en español. Este consiste en aumentar la seguridad en las redes a nivel mundial, detectando problemas y errores de software, así como programa maligno, antes de que hackers con malas intenciones lo logren hacer (BBC News Mundo, 2019). Muchas de las empresas a nivel mundial están dispuestas al pago de sumas de dinero altas para los hackers que tengan estas habilidades y busquen ocupar estos trabajos. Algunas de esas empresas son Facebook, Google, Apple, Yahoo, Nintendo, Lufthansa, General Motors y otras más, igual o más grandes que las mencionadas; así como diversas instituciones (BBC News Mundo, 2019).

Al 4 de marzo de 2019, López había ya encontrado más de 1.600 errores informáticos o "bugs", lo que protegió a millones de personas que navegan las redes, de posibles ataques cibernéticos. Su trabajo depende directamente de la empresa Hacker One, la cual tiene su base situada en la Ciudad de San Francisco, EEUU, que contiene millones de hackers éticos trabajando alrededor del mundo. Se estima que estos obtienen un promedio de entre US$ 50 y US$ 500.000 por dos horas de trabajo. Según el comentario esbozado por Luke Tucker (director de la empresa mencionada), "la percepción sobre los hackers está cambiando" (BBC News Mundo, 2019).

Tal como en la doctrina se entiende que los hackers éticos son personas extraordinarias, que no se encuentran normalmente, sino que en su mayoría son los hackers maliciosos los que se hayan a menudo en el día a día. Se ha de entender que el mundo de los hackers es una cuestión constantemente cambiante, por lo que la sociedad misma va avanzando en los diversos pensamientos sobre el tema y regulando la cuestión de acuerdo con esos cambios. En este marco, una solución por medio de una causal de justificación de lege ferenda, es decir, mediante una propuesta de reforma del derecho vigente, encuentra su razón de ser, puesto que de esta forma se pueden comenzar a regular las acciones de estos individuos que tienen intenciones nobles.

Por otra parte, en el caso en que no sea posible lograr el remedio planteado en el párrafo anterior, es decir una reforma legislativa del derecho, igualmente es posible afirmar como solución alternativa, que una interpretación del derecho vigente —que veremos más adelante— podría beneficiar directamente a los activos en esta profesión. Esto tendría la ventaja de que la propuesta de interpretación podría alcanzar tanto a los hackers éticos actuales, como a los futuros.

III. ARGUMENTOS EN CONTRA DE UNA CAUSA DE JUSTIFICACIÓN

Esta parte del trabajo tiene como objetivo plantear un contraargumento a la hipótesis propuesta. Para ello se formulará la idea de que, así como se habla de "paralelismo" entre el mundo físico y el virtual en el primer apartado, sería posible argumentar una analogía estructural entre los tipos penales de violación de domicilio y de acceso ilícito a un sistema informático. Así, las conductas de white hacking generarían situaciones indeseadas, cómo por ejemplo que individuos —con fines también altruistas— prueben las seguridades de los domicilios particulares (ventanas, puertas, cerraduras, etc.) y eso es algo que intuitivamente no se debería permitir: ya el mero hecho de que alguien ingrese sin autorización, por ejemplo, a las casillas de email, de privados, genera peligros considerables que deberían ser desalentados.

Comencemos por el delito clásico de violación de domicilio. Dentro del Capítulo segundo del CP, se tipifica en los artículos 150 al 152, la violación del domicilio. Donna comparte con Creus y Núñez que el bien jurídico protegido por la norma es la intimidad al decir: "Se trata de proteger al domicilio como ámbito de intimidad del sujeto pasivo. No hay lugar con mayor reserva y donde se daba respetar más rigurosamente el derecho a la privacidad que el domicilio" (Donna, 2011, págs. 352-353). Soler, por su parte, refiere que estos delitos protegen la libertad de las personas, y que ese es un concepto amplio y polimorfo, por lo que incluye a la violación de domicilio y al allanamiento irregular. Dice: "importa considerar a la libertad personal proyectada alrededor de la persona física (…) dotándola de cierto derecho a la soledad o a la intimidad, en virtud del cual se reconoce al individuo el poder de excluir a otro individuos de cierto lugar." (Soler, 1992, pág. 86).

En el primer artículo mencionado se pena con prisión de 6 meses a 2 años al que ingrese en la "morada" ajena o en otros similares casos, contra la voluntad expresa o presunta de quien pueda excluirlo. Seguidamente, en el artículo 151, la misma pena será impuesta, en conjunto con inhabilitación especial en el mismo plazo, a los funcionarios públicos o agentes de las autoridades, que allanen domicilios sin los requisitos que impone la ley. Soler manifiesta que "para nuestro orden jurídico, la tutela del domicilio tiene importancia constitucional, art. 18: el domicilio es inviolable. Esta declaración tiene el sentido de fijar limitaciones al ejercicio del poder de los órganos del Estado (…) por el cual se dispone que una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación. Pero es evidente que puesto ese derecho en tan alta jerarquía, no solo habría de valer contra los órganos del Estado sino contra cualquier particular." (Soler, 1992, pág. 87)

Finalmente, en el artículo 152, se impone una excepción en forma de causa de justificación y es que estas penas no serán aplicadas si el ingreso sea para evitar un mal mayor tanto para los moradores como para un tercero, ni tampoco si lo hiciese como el cumplimiento de un deber de humanidad o para prestar auxilio a la justicia. Al respecto dice Soler "El mal al cual la ley se refiere es un mal de cualquier naturaleza, siempre que sea grave. (…) Por último, si se recuerda el caso tercero de excepción al ingreso en morada ajena, es decir, cuando de ella parten clamores, se verá el sentido de la ley al referirse al deber de humanidad." (Soler, 1992, págs. 111-112). Donna indica con respecto al art. 152, que pareciera ser una repetición de la causa de justificación prevista en el art. 34 inc. 3° —estado de necesidad—, pero que sin embargo, existen diferencias fundamentales: no se exige que el mal que se trata de evitar sea inminente ni tampoco que sea extraño al sujeto. Respecto del "deber de humanidad" dice que se entiende a toda conducta orientada a la salvaguarda de bienes jurídicos valorados por la cultura humana, cumpliendo con un deber humanitario quien intenta salvar la vida o evitar el sufrimiento de un animal o resguardar el medio ambiente (Donna, 2011, págs. 396-399).

Dado que los artículos siguientes, referidos a conductas de violación a la intimidad en el mundo digital, no está presente la causa de justificación del art. 152 del CP, entonces se podría decir que en realidad no corresponde su aplicación. No solo por razones legales, sino también y especialmente porque sería más importante preservar la intimidad de los posibles afectados, que lograr alguna clase de fin superior basado en la idea de seguridad.

Es entonces que siguiendo con este análisis, este detenta en que toda aquella persona que actúe de esta forma, infringiendo límites electrónicos o digitales, sin importar sus intenciones ni tampoco sus objetivos o finalidades en el accionar, deberían ser penados según lo establecido por la ley.

Sin embargo, no se les aplican las mismas excepciones que se aplican a la violación de domicilio art. 150, 152 y 155 CP; por lo que los hackers informáticos que buscan cumplir con una función meramente ética o "White Hat" no tienen la posibilidad de salir ilesos de una situación que cumpla con las características del artículo 153 bis del CP. El argumento de la protección de la intimidad de las personas potencialmente afectadas no sería tomado en serio si se prohibieran estas conductas, por la siguiente razón. Si realmente lo que interesa es proteger a terceros de violaciones a su intimidad, entonces los hackers éticos lo que hacen es *proteger* a esos terceros de afectaciones futuras mucho más graves y no-éticas. En ese sentido, si se impidiesen estas conductas de white hacking, por ejemplo a través del efecto disuasivo del castigo, entonces las potenciales víctimas quedarían más desprotegidas frente a las posibles conductas de hackers con habilidades similares que buscasen fallas de seguridad, por ejemplo, para conseguir acceso a tarjetas de crédito o información personal comprometedora con fines de extorsión.

De esta forma podemos ver la injusticia plasmada en la normativa, en la jurisprudencia y en la doctrina; donde nadie se refiere a la desventaja que sufren estas personas que bajo un formato electrónico o digital de trabajo buscan hacer el bien para la protección de la privacidad y la seguridad de los usuarios en todas las plataformas electrónicas y digitales. Esto, a su vez, se plasma en una injusticia contra los propios titulares del derecho a la intimidad, ya que el actuar preventivo y, posteriormente, retributivo, contra hackers éticos en última instancia deja a los terceros a merced de las conductas de otros hackers no-éticos.

Es en base a esto que se plantearán dos soluciones prácticas para eliminar finalmente esta injusticia. Primeramente, se buscará que se genere una reforma legislativa que exceptúe a estas personas de forma rigurosa, de las penas establecidas en el CP; en segundo lugar, se desarrollará una interpretación del derecho vigente en un sentido más benigno para los hackers éticos, estableciendo que sus actividades no se encuentran dentro

de las previsiones del art. 153 bis y pueden ser abarcadas por la causa de justificación del art. 152 CP por medio de una interpretación analógica *in bonam partem*.

IV. PROPUESTA CONCRETA DE LEGE FERENDA Y DE LEGE LATA

1. Cuestión previa: Código de Ética

Ya habiéndose abordado la temática sobre las cuestiones éticas del asunto que este trabajo plantea, muchos grupos (como la ACM[19] o IEEE[20], que actúan de forma voluntaria) han desarrollado códigos que emplean ciertas reglas en el mundo de la computación. Estos códigos no son creados para certificar un nivel de responsabilidad o experiencia dentro de la comunidad, sino que sientan las bases para la orientación y análisis de ciertos problemas concernientes a la ética en cuanto a la actividad informática se refiere. Si se quisiese establecer una causa de justificación para casos de hacking ético, entonces la conducta de estos hackers debería ser llevada a cabo según estas reglas éticas que se verán a continuación.

El código de ética elaborado por la IEEE, y aprobado en 1990, abarca aspectos que, si bien están centrados en la seguridad informática, no es el único elemento que abarca, principalmente porque esta organización no se enfoca únicamente en ingenieros informáticos o profesionales de la computación, sino que también otras ramas de la ingeniería electrónica y demás (Institute of Electrical and Electronics Engineers, 1990). Algunas de las normas éticas más destacables establecidas por la IEEE son:

"1. A aceptar responsabilidad en la toma de decisiones de ingeniería consistentes con la seguridad, la salud y el bienestar del público, y revelar con prontitud los factores que puedan poner en peligro al público o al medio ambiente.

2. A evitar conflictos de interés reales o supuestos siempre que sea posible, y dar a conocer a las partes afectadas cuando existan.

4. A rechazar el soborno en todas sus formas.

[19] Association for Computing Machinery
[20] Institute of Electrical and Electronics Engineers

5. A mejorar la comprensión de la tecnología, su aplicación adecuada y sus posibles consecuencias.

9. A evitar dañar a otros, sus propiedades, reputación o puesto de trabajo mediante acción falsa o maliciosa." [21]

En cambio, la ACM elaboró un código de ética que mantiene tres pilares principales para sus miembros: imperativos morales generales a seguir, responsabilidades profesionales, y principios de liderazgo profesional (Association for Computing Machinery, 2018). Este código de ética posee importantes principios éticos a destacar:

"1.1 Contribuir a la sociedad y al bienestar humano, reconociendo que todas las personas son partes interesadas en la Informática.

1.2 Evitar el daño.

1.3 Ser honesto y confiable.

1.4 Ser justo y tomar medidas para no discriminar.

1.5 Respetar el trabajo necesario para producir nuevas ideas, inventos, trabajos creativos y artefactos informáticos.

1.6 Respetar la privacidad.

1.7 Respetar la confidencialidad."[22]

Por otro lado, Vásquez (Técnicas anti-forenses informáticas, 2016, pág. 52) destaca que el Computer Ethics Institute (CEI) es una organización sin fines de lucro, cuyo fin es la investigación y educación, animando a considerar distintos aspectos éticos dentro de las actividades informáticas. Así es cómo se establecieron los "Diez Mandamientos de Ética Informática" del CEI:

"I. No usarás una computadora para dañar a otras personas.

[21] Puede descargarse la versión completa y en español del Código de Ética del IEEE en la web: https://edu.ieee.org/ec-ups/wp-content/uploads/sites/266/CODIGO_DE_ETICA_IEEE.pdf (consultado el 25/1/23)

[22] Es posible observar la versión completa y en español del Código de Ética y Conducta Profesional de ACM en la web: https://www.acm.org/code-of-ethics/the-code-in-spanish (consultado el 25/1/23)

II. No interferirás con el trabajo de la computadora de los demás.

III. No has de husmear en los archivos de otras personas.

IV. No usarás una computadora para robar.

V. No usarás una computadora para dar falso testimonio.

VI. No has de copiar o utilizar software propietario por el que no has pagado.

VII. No usarás los recursos informáticos de otras personas sin autorización o compensación adecuada.

VIII. No has de adueñarte de la propiedad intelectual de otras personas.

IX. Piensa en las consecuencias sociales del programa que estas escribiendo o el sistema que estás diseñando.

X. Usarás siempre una computadora de manera que asegure consideración y respeto por tu prójimo."

De esta forma, muchas organizaciones como las mencionadas, generaron dentro de sus propios códigos, ciertas máximas en común y en conjunto que de forma similar entablaron las bases para la utilización adecuada de los medios informáticos para no incurrir en delitos ni daños a ninguna persona o entidad (Vásquez, 2016).

En principio, estas cuestiones normativas internas, además de las leyes vigentes, actualmente en cuanto al cibercrimen son los principios y bases sentadas hoy en día para una convivencia que permita la inclusión del hacking ético en la comunidad. Si se siguiesen esas reglas, entonces podría excepcionalmente considerarse la conducta de los hackers éticos como amparadas por una causa de justificación.

2. Propuesta de lege ferenda.

Como se mencionó con anterioridad, la regulación actual es ciertamente insuficiente, por lo que es necesario que las reformas legislativas de tamaña importancia para el tema sean realizadas con rapidez. Sobre todo, luego de haber enfrentado una

pandemia que agudizó los ciberataques (estafas, robo de datos por medio del ingreso a plataformas de reuniones, etc.), la intensificación de ciberataques domésticos y en el entorno empresarial, incluso a nivel estatal. Todo ello da la gran pauta de la necesidad urgente de la construcción de un ordenamiento que regule de forma actualizada y en constante renovación a medida que surgen los cambios, para prevenir y sancionar los ciberataques y sus consecuencias (García, 2021, págs. 75-118).

Pero regresando a las cuestiones que atañen al hacking ético, uno de los problemas que mayor relevancia toma, es la necesidad de organización del proceso de lo que se conoce como "testeo por hacking ético" o "test de penetración". Esta prueba permite realizar un examen de seguridad que identifica y saca a la luz las vulnerabilidades del sistema empleado, simulando un ataque y advirtiendo las vetas que permitirían el ingreso de ciberataques

La organización necesaria que se nombró en el anterior párrafo puede darse en diferentes etapas, según el método aportado por Giannone (Investigación en Progreso: Método de Inclusión de Hacking Ético en el Proceso de Testing de Software., 2016, págs. 252-254):

1. Primero, la planificación, donde se documenta y modela el planeamiento de las pruebas que se llevarán a cabo en el software a intervenir.
2. Luego, la ejecución, cuando una vez realizada la prueba, se ordena y fundamenta la realización de un software libre de vulnerabilidades.
3. Finalmente, la etapa de mantenimiento del sistema, con el objeto de someter de manera periódica el software desarrollado y libre de debilidades.

Teniendo en cuenta el desarrollo realizado a lo largo del presente trabajo, debe entenderse como fundamental la posibilidad de incluir un apartado concreto en el Código Penal (Art. 153 bis), que recepte el trabajo realizado y entendido como hacking ético, donde independientemente del acceso ilícito a un sistema informático, éste no tiene otra finalidad más que la de hallar vulnerabilidades que ponen en peligro la integridad del sistema informático en su conjunto, para luego dar aviso a su titular y que sean remediadas. Observemos que en el caso de que la vulnerabilidad sea detectada por un hacker no ético, éste podría aprovecharse de ella para obtener información sensible,

privada o bien para cometer otros delitos como daño informático, secuestro de información, defraudaciones, entre otros.

La pregunta a realizar sería "¿Condenaríamos al sujeto activo por este hecho?". Cuando el comportamiento desplegado solo puede resultar beneficioso para la sociedad o bien para el propio denunciante. Restringiendo tal conducta lo único que se haría es la de generar una vulnerabilidad de los sistemas de información y se tendrían noticias de un acceso informático restringido una vez que este hubiera ocurrido y no hubiera solución posible para el bien jurídico protegido. Ahora bien, si debe existir una norma que establezca una causa de justificación, esta debe ser clara con relación a la distinción entre lo que se entiende por "intrusismo informático" punible y la actividad desplegada por muchas personas cuyo trabajo consiste en probar sistemas de seguridad y acceso con fines puramente "éticos".

Diferentes son los supuestos donde el acceso se realiza con un fin estricto de obtener determinada información para "defraudar, extorsionar, obtener ventajas económicas y otro sin fin de circunstancias" y la conducta desplegada se constituye como la antesala para cometer otro delito diferente. Se ha manifestado que el acto de "hacking" representa un sinfín de variables, las cuales derivan en una problemática de difícil sanción por parte de la ley penal, toda vez que se ha dicho que esta conducta, por su insignificancia, se encuentra fuera de los límites de intervención del poder punitivo (Gutiérrez Francés, 1996, págs. 1163-1184).

Tampoco se puede, en aquellos supuestos como el caso de análisis, imponer determinados tipos penales donde la distinción entre la idea de libertad y la restricción que quiere imponerse queda sujeta a la mera esfera subjetiva de la persona que realiza el hecho típico, teniendo como base el sistema en un mecanismo de capacidad probatoria donde además del delito en sí mismo se exige la trasgresión a los secretos de acción privada (arts. 73 y 153 del Código Penal) y esencialmente la capacidad de impulsar la acción penal recae sobre personas que no tendrán conocimiento alguno de que sus sistemas informáticos se han visto vulnerados, salvo cuando vean en la red su información privada. Si la idea esencial consiste en proteger la información o datos sensibles de las personas, resulta necesario analizar y contemplar diferentes variables y factores, en función de que los usuarios son las personas con mayor vulnerabilidad en cuanto a sus

datos e información privada, la cual se encuentra expuesta a numerosos hechos ilícitos, ya que los sistemas informáticos se encuentran al resguardo en algunos supuestos por leyes de protección y por otros la información confidencial de las empresas por normativas en concreto. En este punto debe decirse que a un hacker le resultará más atractivo trasgredir un sistema llamativo o con gran cantidad de información que la información de un particular concreto, salvo que tenga conocimiento de la existencia de datos sensibles del sujeto de los cuales pueda obtener un provecho, por lo cual buscará obtener tal información y de esa manera caerá fuera de los límites del mero acceso o intrusismo.

Conforme lo señalado, resulta esencial determinar los supuestos donde terceras personas que no resultan ser los propios usuarios de los datos y la información comprometida, deberían tener la posibilidad de tomar acceso a estos por razones de seguridad. Se trata de casos en los que el objetivo último es el de brindar facilidades al personal o profesionales idóneos para el manejo de sistemas o expertos en programación y seguridad informática para poder identificar y reparar las falencias a nivel de seguridad de los sistemas informáticos. En la realidad, frente al supuesto o amenaza de un posible daño al sistema, el acceso a los datos se produce en general mediando permiso de su dueño o titular de la red que se encuentra vulnerada. Sin perjuicio de ello, podría el profesional ver protegida su situación cuando medie un caso de necesidad especial y análogo al del art. 152 del CP. De ese modo, se sacrificaría la intimidad en pos de evitar un daño mayor como puede ser la perdida de datos sensibles. A su vez, debería mediar una intención directa de evitar un mal mayor a la seguridad informática. Como dice Palazzi, debería tratarse de una conducta “cuyo objetivo es obtener información técnica a partir de un producto accesible al público, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado. Los productos más comunes que son sometidos a ella son los programas de ordenador y los componentes electrónicos (…). El bien jurídico protegido por la figura que estudiamos (art. 153 bis, Cód. Penal) es la privacidad y la confidencialidad de un espacio informático. Por ende, (…) está claro que cualquier intento de utilizar esta figura para frenar un acto de ingeniería inversa legítimo no debería tener recepción judicial. ” (Palazzi, 2016, págs. 109-111).

En síntesis, teniendo en cuenta los diferentes puntos de vista de la doctrina, este autor cree conveniente realizar la siguiente incorporación al articulado vigente en el "Código Penal":

"No será punible quien, con el fin de evitar un perjuicio grave para los usuarios y/o a los propietarios, accediera éticamente a un sistema informático ajeno, en el marco de una investigación de vulnerabilidades informáticas aficionada o académica.

Para la determinación de si se trata de un comportamiento ético, se deberán tener en cuenta todos los siguientes factores: 1) ausencia de modificaciones del sistema informático; 2) puesta en conocimiento de la vulnerabilidad hallada al propietario del sistema informático en un plazo máximo de 24 hs e insistencia ante la falta de respuesta por parte del propietario en las siguientes 72 hs; 3) ausencia de maniobras de ocultamiento del acceso por parte del autor; 4) ausencia de apoderamiento de datos privados"**.**

Así, en definitiva, lo que se pretende es justificar aquella conducta que no tenga que ver con un ilícito, sino más bien desarrollar actividades tendientes a generar una mejora o beneficio a los sistemas informáticos, como puede ser las tareas descriptas en el ejercicio del Hacking ético.

3. Propuesta de lege lata.

Ahora bien, si no resulta factible o no existen avances sobre la posibilidad de introducir modificaciones a la norma tal y cual se encuentra escrita a la actualidad, resulta necesario analizar diferentes opciones o estrategias para la realización de una interpretación benévola de la norma. Esto deberá ser realizado a los fines de justificar el accionar de los denominados hackers éticos en cada caso concreto para evitar injusticias.

Para abordar esta cuestión, resulta valedero desmenuzar la jurisprudencia Argentina aplicable a la materia. Así, puede citarse el fallo "Ortmann, Gaspar Ariel s/ averiguación de delito – Juzgado Criminal y Correccional Federal Nro. 11 Causa CFP 8143/2019 del día 20 de noviembre de 2020" o la resolución en la Causa "MPF 83322".

Empiécese por lo primero, el 1 de diciembre del año 2019 el "Juzgado Federal Nro. 11 de la Ciudad Autónoma de Buenos Aires" decidió el sobreseimiento del Sr. Gaspar Ortmann, especialista en seguridad informática. En cuanto a los hechos del caso, el acusado fue denunciado por haber ingresado a la plataforma de home banking del Banco de la Nación Argentina, la cual era manejada por la firma Red Link. Con su acceso, autenticó sus credenciales necesarias y a partir de la implementación de técnicas y conocimientos específicos pudo identificar una falencia en el sistema informático y a partir de ello "modificó a su favor la cotización del dólar dentro de su navegador".

Resulta esencial resaltar que no existió ningún daño a los sistemas informáticos involucrados, cuestión que hubiese derivado en la aplicación de otro tipo penal. Los cambios realizados por el acusado fueron realizados únicamente mediante la utilización de su computadora personal mediante la cual ingresó a su usuario personal de home banking, por lo que específicamente se vieron afectadas las operaciones y transacciones realizadas desde su propia sesión y no el sistema en su conjunto. Otra cuestión para resaltar radica en que el Sr. Ortmann es cliente de la entidad denunciante desde el año 2017, y que la vulnerabilidad del sistema informático fue descubierta desde su propio usuario, pero bien podría haberla realizado cualquier cliente del banco con acceso a home banking.

Por último, no se determinó que hayan existido transferencias de dinero o cualquier otro tipo de actividad tendiente a restringir o afectar el recupero de los fondos, como así tampoco existió algún tipo de conducta que tenga por objeto "objeto encubrir, enmascarar y/o dificultar el rastreo de la procedencia y origen de dichas operaciones". Dato no menor es que fue el propio Ortmann quien alertó a la entidad bancaria de los sucesos producidos, lo cual dejó de manifiesto la verdadera intención que tenía el agente, esto es alertar y poner en conocimiento de la entidad bancaria de la existencia de deficiencias en su sistema de seguridad informático y no la realización de un acto de defraudación o estafa mediante la utilización de herramientas tecnológicas.

En el análisis realizado por el tribunal interviniente, los mismos concluyen que "sobre este punto, debe destacarse que más allá del error técnico descubierto y utilizado por ORTMANN, Red Link cuenta con múltiples controles que le permiten detectar este tipo de operaciones anómalas, por lo que las maniobras investigadas en ningún momento

tuvieron posibilidad de ser concretadas sin ser descubiertas por los distintos sistemas de seguridad de dicha empresa, circunstancias que difícilmente pudo haber desconocido ORTMANN dada su expertise en la materia.- Lo expuesto hasta aquí, demuestra que el encartado en ningún momento intentó ocultar su responsabilidad por lo sucedido, sino que por el contrario, siempre estuvo en su voluntad realizar las operaciones y que luego se supiera que había sido él quien las había llevado a cabo, todo ello con la intención de demostrar la vulnerabilidad del sistema operado por Red Link.-"

Otra cuestión fundamental en el análisis resulta del hecho de que "A ello, debe agregarse que incluso algunas de las operaciones de compraventa de dólares cuestionadas fueron realizadas en detrimento patrimonial del propio encausado, lo que también evidencia que la intención del nombrado no estaba dirigida a causar un perjuicio patrimonial a las arcas del Banco de la Nación Argentina, sino a probar las debilidades del sistema informático antes aludido.". Así, queda descartada cualquier motivación o intención de provocar un perjuicio a un tercero, mediante el acceso a determinado sistema informático, quedando al descubierto la verdadera intención de poner de manifiesto las flaquezas que mantenía el sistema de seguridad.

Así en el presente caso, no existió daño alguno en cuanto a que el error ya formaba parte del sistema operativo, ni medió acceso restringido toda vez que el agente uso sus propias credenciales. Se trata, entonces, de un caso de hacking ético, en el que no existe ninguna clase de intención de cometer un daño (que vaya más allá de la violación a la "intimidad") o defraudación sino que respeta los códigos de ética, informa y da cuenta de las vulnerabilidades que encuentra a su paso. Por tanto, un caso así debe quedar impune y el tribunal correctamente ha considerado que esta conducta no ha de ser castigada, aunque sin reconocer una causa de justificación como la que aquí se propondrá.

Por otro lado, el Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires, en el marco de la causa MPF 83322, también arribó a una solución similar a la mencionada. En cuanto a los hechos se investigó que un grupo de personas habría accedido ilícitamente al sistema informático de la empresa "Grupo MSA S.A" y alteraron su normal funcionamiento. De la investigación se pudo comprobar que efectivamente se había accedido remotamente al sistema informático de la empresa, mediante técnicas de penetración informática, desde un domicilio en la República Argentina.

Además, las tareas periciales llevadas a cabo en el sistema informático afectado concluyeron que el autor había accedido unas 91 veces al sistema y que además había creado un evento "PWNED". El perito destacó que "el concepto 'PWNED' en términos de informática, significa que el pequeño (una persona) encuentra una vulnerabilidad a un grande (una empresa), donde se utiliza colocar una bandera (como símbolo) para informar que el sistema desarrollado por la empresa es vulnerable. Esta bandera no genera ningún daño o alteración al normal funcionamiento del sistema informático en cuestión". Finalmente, la fiscalía terminó realizando una novedosa interpretación de la norma y desechó la acusación por entender que si bien se pudo acreditar que el autor accedió al sistema informático de la empresa, no lo hizo de manera indebida ni causó daño alguno, sino que por el contrario, lo hizo para avisar a la firma de que el sistema de seguridad era vago y podía ser vulnerado con facilidad.

Es cierto que esta interpretación se encuentra en línea con lo propuesto en este trabajo y por ello es posible afirmar que aun no pudiendo lograr la modificación de la ley penal a fin de incluir una causal de justificación que excluya la responsabilidad de los hackers éticos, es posible interpretar la ley vigente de forma benévola para igualmente otorgar protección jurídica a este grupo de individuos. No obstante, no es cierto que el autor haya ingresado *debidamente* al sistema, sino que lo esencial de su actividad es el haber actuado sin una autorización. Por consiguiente, resulta equívoco señalar que la conducta es atípica. Más bien, lo que la fiscalía ponderó de forma positiva fue el descubrimiento de fallas de seguridad, algo que valdría más que una vulneración no dañina a la intimidad del titular del bien jurídico. Esa forma de argumentar es característica, nuevamente, de una causa de justificación, no de una de atipicidad.

La forma de solucionar adecuadamente estos casos según el derecho vigente es el de sencillamente aplicar analógicamente a estos casos la causa de justificación del art. 152 del CP. Esto parecería un poco extraño, porque la ley no establece esta causa de justificación para los delitos que aquí resultan relevantes, por un lado. Por otro, porque los penalistas solemos ver con desconfianza las analogías, debido al principio de legalidad en su faceta *lex stricta*. Sin embargo, esta maniobra es perfectamente posible. Respecto de la ausencia de una causa de justificación expresa para estos casos, es sabido que los permisos legales, debido a que rigen *a favor de imputado*, pueden surgir no solo de la ley. De hecho, muchas causas de justificación surgen del derecho consuetudinario. La más

usual es, sin ir más lejos, la del consentimiento justificante, ya que a pesar de no estar reconocida expresamente en la ley, es considerada un caso clásico de justificación, al menos según la opinión dominante[23]. Respecto de la analogía, también es sabido que la analogía prohibida es la analogía *contra reo*. En cambio, cuando se recurre a analogías a favor del imputado, no hay ningún problema de legalidad, siempre y cuando se brinden buenas razones para realizar esa interpretación. Si lo que se ha señalado en este trabajo es cierto, sería injusto castigar a los hackers éticos, entonces existe una buena razón para aplicar analógicamente el art. 152 del CP.

V. CONCLUSIÓN

Existe un debate social y político que condiciona las propuestas de regulación debido a que la masividad de herramientas tecnológicas actuales da paso a acciones que invaden libertades públicas. No obstante, las herramientas desarrolladas no son del todo negativas, ya que desde el aporte del hacking ético se cuenta con posibilidades tecnológicas de anticipación a los ciberataques, incluso de contraataque para revelar vulnerabilidades de los propios cibercriminales. Es justamente en esta situación donde se deben situar las esferas de propuestas de reformas para la regulación del hacking ético, legalizando los métodos de seguridad, adecuando la normativa necesaria que permita aplicar la ley penal con terminologías especializadas para su comprensión y adaptándose a los principios de legalidad, proporcionalidad, y legítima defensa que eviten las consecuencias últimas de ciberataques graves contra las autoridades nacionales, y personas individuales (García, 2021, págs. 75-118).

[23] Si bien existe una discusión del consentimiento como causa de justificación o como causa de atipicidad, lo cierto es que la opinión dominante se apoya en la primera. Sobre esto menciona Roxin (Derecho Penal. Parte General. Fundamentos de la estructura de la teoría del delito. Tomo I, 1997, págs. 512-513): "La opinión hoy dominante distingue, (…) entre el acuerdo y consentimiento. El acuerdo actúa excluyendo la tipicidad. Ello entra en consideración en los tipos en que la acción típica presupone ya conceptualmente un actuar contra o sin la voluntad del lesionado. (…) Por el contrario, el consentimiento en sentido estricto, cuando es presentado por el portador del bien jurídico, sólo tendría el efecto de justificación, pero no el de excluir la realización del tipo. (…) Según esta opinión, el consentimiento excluye sólo la antijuricidad, cual se funda la mayoría de las veces en que en el consentimiento descansaría una renuncia al bien jurídico que tendría fuerza justificante desde el punto de vista jurídico-consuetudinario como consecuencia del derecho de autodeterminación individual (…).

Es necesario que se adecue la visión del ordenamiento jurídico de modo que la regulación de este tipo de actividades derive en los efectos que la ciberseguridad a nivel nacional necesita. Más aún, teniendo en cuenta la terminología especializada, la tipificación de los delitos cibernéticos que clarifiquen la comprensión de la línea que traza el cibercrimen con lo permitido. Y esto no se trata de una cuestión de tecnicismos, sino de que se debe suprimir la inseguridad jurídica que califica conductas ilegales. Aunque el contenido jurídico no es el principal problema al momento de establecer estas terminologías, sino más bien la significancia de estas: el constante avance de técnicas dentro de la informática abre posibilidades de delitos diferenciados con conductas legales en mínimos detalles. El trabajo de los juristas que deben realizar calificaciones en los ciberataques se enfrenta a siglas, modismos, silogismos y palabras que son difícilmente entendibles para quienes no son especialistas, y que imposibilitan la conversión o traslado de términos adaptables a lo jurídico procesal (García, 2021, págs. 75-118).

En cuanto a la cuestión de tratamiento trasnacional de conductas delictivas y los ataques desde el extranjero, sería de vital importancia un tratamiento al nivel de la comunidad internacional y de las autoridades competentes del Derecho Penal Internacional, ya que muchas de las actividades no son comprendidas como actos lo suficientemente graves como para perseguirse internacionalmente, sino con las potestades nacionales de cada uno de los Estados en cuestión. Existen diversos obstáculos procesales a la hora de investigar y enjuiciar a lo que tan difícilmente logra tener una tangibilidad que desde el anonimato causa los daños graves dentro de la seguridad nacional, pública y privada. Dentro de estos contratiempos de aplicación del Derecho Internacional Público, se destaca la difícil aplicación en sentido estricto del principio de proporcionalidad como complementario al principio de necesidad, dado que la desigualdad de medios es parte inseparable de la guerra en el ciberespacio (García, 2021, págs. 75-118).

Muchos ámbitos del ordenamiento jurídico deben tomar direcciones para que las normas vigentes sobre delitos informáticos y ciberseguridad sean mayormente efectivas. Ya se ha hecho hincapié en el desfasaje existente entre las normas actuales y el avance tecnológico que recorren dos caminos diferentes con velocidades sumamente distintas, y en las terminologías que deberán adaptarse a las tipificaciones penales (Borizi Cirilli, 2018, págs. 173-182).

Como también se mencionó a lo largo de este trabajo, no es tarea sencilla juzgar delitos informáticos. Desde la parte administrativa que corre con las investigaciones pertinentes a este tipo de violaciones, no cuentan con las especificaciones ni los equipos necesarios para ello, sobre todo teniendo en cuenta la seriedad de este tipo de delitos. Las legislaciones han avanzado respecto a las leyes y penas aplicables a las categorías delictivas informáticas, pero muchas veces quedan atrasadas por la evolución constante de esta materia y sus innumerables variables, en consecuencia, los daños económicos, las violaciones a privacidad y la perdida de datos e información. Las propuestas de regulación deben acompañarse de especialistas capacitados de la misma forma que los cibercriminales, para dar fe de los avances necesarios a realizarse en las legislaciones a medida que los cambios sean imprescindibles para evitar y entender las penas y sanciones que deberán aplicarse a cada caso.

Ahora bien, en base a lo visto es posible concluir que la inclusión del hacking ético, el proceso de testing de softwares y test de penetración en los sistemas actuales permiten que las políticas de seguridad y los controles lleguen a garantizar la protección incluso total de la información y los datos. Los códigos de ética informática son herramientas esenciales para tener referencia del profesionalismo de los hackers éticos, con los principios que evidencien la importancia de poder evitar delitos desde la moralidad y conocimiento de la ley, la responsabilidad y el respeto por los accesos a la información privada. Nuevamente, las figuras delictivas y los especialistas que ayudan a prevenir y combatir este tipo de conductas son, ni más ni menos, dos caras de una misma moneda, que necesita retroalimentarse de las actividades del otro para poder continuar con su accionar.

Es por lo que a la hora de analizar la letra fría de la norma que sanciona el acceso indebido a los sistemas informáticos, debe valorarse la conducta del agente, en función de que no toda persona que accede a un determinado sistema informático lo hace con el objetivo de ocasionar un daño o en contra de la autorización de su titular. Entonces, resulta necesario que el ordenamiento jurídico contemple verdaderas excepciones a la regla y conceda a los operadores judiciales las herramientas necesarias para poder valorar o discriminar cada caso en concreto, facultando la posibilidad de discernir la intencionalidad o las consecuencias que se derivan de los actos realizados por el hacker. Esto se podría realizar a partir de una causa de justificación expresa en la ley, lo que

requeriría una reforma legal. Pero también se podría lograr mediante una aplicación analógica del art. 152 CP a los casos de hacking ético.

BIBLIOGRAFÍA

Association for Computing Machinery. (2018). *Código de Ética y Conducta Profesional de ACM.* Obtenido de https://www.acm.org/code-of-ethics/the-code-in-spanish

BBC News Mundo. (4 de Marzo de 2019). Santiago López, el millonario hacker adolescente argentino que ganó US$1 millón descubriendo errores informáticos. *BBC News Mundo*, págs. https://www.bbc.com/mundo/media-47416402.

Borizi Cirilli, F. A. (2018). Cibercrimen y evidencia digital: problemática probatoria. En *Cibercrimen y Delitos Informáticos. Los nuevos tipos penales en la era de internet.* (págs. 173-182). Ciudad Autónoma de Buenos Aires: Erreius.

Buompadre, J. E. (2009). *Tratado de derecho penal. Parte especial.* Ciudad Autónoma de Buenos Aires: Astrea.

Consejo de Europa. (23 de noviembre de 2001). *Convenio sobre la Ciberdelincuencia*. Obtenido de Covnenio de Budapest: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Cottino, D. (2009). *Hardware desde cero.* Banfield - Argentina: Users.

Creus, C. (1992). Derecho Penal. Parte General. 3° edición. Buenos Aires: Astrea.

Donna, E. A. (2011). *Derecho penal: parte especial. Tomo IIA. 2° Edición.* Santa Fe: Rubinzal-Culzoni.

Galeano, S. (27 de enero de 2022). El número de usuarios de internet en el mundo crece un 4% y roza los 5.000 millones (2022). *Marketing Commerce*. Obtenido de https://marketing4ecommerce.net/usuarios-de-internet-mundo/

García, E. F. (2021). Desafíos jurídicos interdisciplinares de la ciberseguridad nacional: Apuntes “de lege ferenda”. . *Anuario de la Facultad de Derecho. Universidad de Extremadura, 37*, 75-118.

Giannone, A. (2016). Investigación en Progreso: Método de Inclusión de Hacking Ético en el Proceso de Testing de Software. *Revista Latinoamericana de Ingeniería de Software, 4*(6), 252-254.

Gobierno de la Nación Argentina. (junio de 2022). *Ciberdelitos* . Obtenido de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito#:~:text=Se%20considera%20ciberodio%20a%20la,videos%20de%20actividad%20sexual%20expl%C3%ADcita.

Gradin, C. (2004). Presentación. En C. Gradin, E. S. Raymond, R. Stallman, M. Vidal, J. Gilmore, C. Ferrer, . . . B. Joy, *Internet, Hackers y Software libre.* Fantasma.

Gutiérrez Francés, M. (1996). El intrusismo informático (Hacking): ¿Represión Penal Autónoma? *Informática y Derecho: Revista iberoamericana de derecho informático*, 1163-1184.

Gutiérrez, R., Radesca, L. C., & Riquert, M. A. (2013). *Violación de secretos y de la privacidad.* Asociación Pensamiento Penal - Código Penal Comentado de Acceso Libre.

Hart, H. L. (2019). *Castigo y Responsabilidad.* Madrid: Marcial Pons.

Himanen, P. (2004). *La Ética Del Hacker Y El Espíritu De La Era De La Información.* Barcelona: Destino.

Institute of Electrical and Electronics Engineers. (1990). *Código de Ética del IEEE -versión en español-.* Obtenido de https://edu.ieee.org/ec-ups/wp-content/uploads/sites/266/CODIGO_DE_ETICA_IEEE.pdf

Llamas, J. (7 de octubre de 2021). *Seguridad informática*. Obtenido de Economipedia.com: https://economipedia.com/definiciones/seguridad-informatica.html

Moreso, J. J. (2001). Principio de Legalidad y Causas de Justificación. (Sobre el alcance de la taxatividad). *Doxa. Cuadernos de Filosofía del Derecho* , 525-545.

Morosi, G. E., & Viera, M. (2011). Comentario al art. 153". En A. J. D'Alessio, *Código Penal de la Nación. Comentado y Anotado.* Buenos Aires: La Ley.

ONU, C. d. (27 de junio de 2016). Obtenido de https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf

Palazzi, P. A. (2006). Breves comentarios a los proyectos legislativos sobre delitos informáticos. *Revista de Derecho Penal y Procesal Penal. D'Alessio y Bertolino, Lexis-Nexis, Bs.As., N° 8*, 1531.

Palazzi, P. A. (2008). Análisis de la ley 26388 de reforma al Código Penal en materia de delitos informáticos. En A. J. D'Alessio, & P. Bertolino, *Revista de Derecho Penal y Procesal Penal. N° 7.* Buenos Aires: Lexis Nexis.

Palazzi, P. A. (2016). *Los Delitos Informáticos en el Código Penal.* Ciudad Autónoma de Buenos Aires: Abeledo Perrot.

Raymond, E. S. (2001). *Cómo convertirse en hacker. Traducción por Miquel Vidal.* Obtenido de https://biblioweb.sindominio.net/telematica/hacker-como.html

Roibón, M. M. (2018). Reflecciones Sobre el Acceso Ilegítimo a un Sistema o Dato Informático. En R. A. Parada, *Cibercrimen y Delitos Informáticos.* Ciudad Autónoma de Buenos Aires: Erreius.

Roxin, C. (1997). Derecho Penal. Parte General. Fundamentos de la estructura de la teoría del delito. Tomo I. Madrid: Civitas.

Sáez Capel, J., & Velciov, C. (2008). Comentario al art. 153bis. En D. Baigún, & E. Zaffaroni, *Código Penal. Tomo 5.* Buenos Aires: Hammurabi.

Sánchez Avila, M. Á. (2019). *Hacking Ético: Impacto en la Sociedad.* Univesidad Piloto de Colombia.

Soler, S. (1992). *Derecho Penal Argentino, Tomo IV.* Buenos Aires: TEA.

Temperini, M. (2018). Delitos Informáticos y Cibercrimen: Alcances, Conceptos y Características. En R. A. Parada, *Cibercrimen y delitos informáticos.* Ciudad Autónoma de Buenos Aires: Erreius.

Vásquez, M. D. (2016). *Técnicas anti-forenses informáticas.*