

LA PROTECCIÓN LEGAL DE LOS HACKERS ÉTICOS: UNA BREVE MIRADA DESDE EL DERECHO PENAL

Rodrigo BRANCA*

Fecha de recepción: 12 de marzo de 2024

Fecha de aceptación: 9 de diciembre de 2024

Resumen

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 lo que deben estar exentos de recibir una sanción penal. Se propondrán dos soluciones posibles: una de *lege ferenda*, que implica modificar la ley actual para incluir una causa de justificación legal que proteja el trabajo de los hackers éticos, y una de *lege lata*, que involucra realizar una interpretación benévola de la ley existente que también resguarde a los hackers éticos. El núcleo de la propuesta será una comparación o paralelismo con la causa de 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

Title: *The legal protection of ethical hackers: A brief overview from a criminal law perspective*

Abstract

This work analyzes the topic of ethical hackers, explaining particularly that their actions carry an altruistic function and, therefore, should be exempt from criminal sanctions. Two possible solutions will be proposed: one of *lege ferenda*, involving amending the current law to include a legal justification that protects the work of ethical hackers, and one of *lege lata*, which entails a benevolent interpretation of existing law that also protects ethical hackers. The proposal's core will be a comparison or parallelism with the justification currently provided by positive law for the

* Magíster en Derecho Penal (UTDT). Director del Cuerpo de Investigaciones Judiciales (MPF CABA).

crime of trespassing on physical private property when the act is carried out to save a higher entity (Articles 150 and 152 CP).

Keywords: Ethical hackers – Justification – Penal code – Private property – Altruism – Punishment – Prison sentences

Sumario: I. Introducción; II. Hacking y doctrina; III. Solución I (*lege ferenda*); IV. Paralelismo. Violación de domicilio; V. Solución II (*lege lata*); VI. Conclusión; VII. Bibliografía.

I. Introducción

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 económicos¹ 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 disfrutaban del uso extremo de la tecnología, sin miedo al riesgo que esto implica, pero con altas capacidades intelectuales en esta materia.² 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”.³

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, 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.⁴ 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

¹ VÁSQUEZ, M. D., *Técnicas anti-forenses informáticas*, 2016, p. 50.

² GRADIN, Carlos, “Presentación”, en *Internet, hackers y software libre*, Fantasma, 2004, pp. 9-11.

³ HIMANEN, Pekka, *La ética del hacker y el espíritu de la era de la información*, Barcelona, Destino, 2004, p. 5.

⁴ HIMANEN, *La ética del hacker*, cit., pp. 5-6.

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.⁵

Podemos ver que 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.⁶ 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.⁷

Ahora bien, en la República Argentina el art. 153 bis del Código Penal sanciona con prisión (de 15 días a 6 meses) 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. La pena se agrava de 1 mes a 1 año de prisión si el sistema o dato informático correspondiera a un organismo público estatal o proveedor de servicios públicos o financieros.

Por otro lado, 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”;

⁵ HIMANEN, *La ética del hacker*, cit., p. 5.

⁶ GRADIN, “Presentación”, cit., p. 61.

⁷ VÁSQUEZ, *Técnicas anti-forenses informáticas*, cit., p. 50.

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”.

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

Dicho esto, 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.⁸ 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.

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 soluciones:

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.

II. Hacking y doctrina

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.⁹ Más allá de eso, también es posible afirmar que el hacking ético es una actividad que

⁸ ROIBÓN, M. M., “Reflexiones sobre el acceso ilegítimo a un sistema o dato informático”, en PARADA, R. A. (dir.), *Cibercrimen y delitos informáticos*, Ciudad Autónoma de Buenos Aires, Erreius, 2018, pp. 134-138.

⁹ ROIBÓN, “Reflexiones sobre el acceso ilegítimo a un sistema o dato informático”, cit., p. 134.

trae aparejados grandes beneficios para los sistemas informáticos y sus usuarios, ya que los hace más seguros.¹⁰ 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.

De esta forma, vemos que en definitiva los hackers éticos tienen como medio de trabajo la comisión delitos contenidos en el Código Penal argentino, 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.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.”).¹² 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.

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

¹⁰ SÁNCHEZ ÁVILA, M. Á., *Hacking ético: impacto en la sociedad*, Universidad Piloto de Colombia, 2019, pp. 7-8.

¹¹ GRADIN, “Presentación”, cit., p. 11.

¹² GUTIÉRREZ, R., RADESCA, L. C. y RIQUERT, Marcelo A., *Violación de secretos y de la privacidad*, Asociación Pensamiento Penal – Código Penal Comentado de Acceso Libre, 2013, pp. 9-11.

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.¹³ 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.

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.

En particular, 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.

Segundo, y más importante, la argumentación de GUTIÉRREZ, RADESCA y RIQUELT debería conducir, en todo caso, a una causa de justificación suprallegal (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 de lo que pasa con los casos de autorizaciones expresas del titular del bien jurídico, porque allí es la propia “víctima” quien 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

¹³ GUTIÉRREZ, RADESCA y RIQUELT, *Violación de secretos y de la privacidad*, cit., p. 10.

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,¹⁴ 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:

“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”.¹⁵

En definitiva, 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.¹⁶ Por esa razón, argumenta PALAZZI¹⁷ 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.

A pesar de que PALAZZI tiene razón en señalar que estos casos se deben resolver como causas de justificación, su argumentación no es tan robusta. 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 agresivo¹⁸ del art. 34, inc. 3º del CP, el hacker no actúa frente a un mal mayor *inminente*.

¹⁴ MORESO, José Juan, “Principio de legalidad y causas de justificación (sobre el alcance de la taxatividad)”, en *Doxa. Cuadernos de Filosofía del Derecho*, N° 24, 2001, pp. 525-545.

¹⁵ HART, H. L. A., *Castigo y responsabilidad*, Madrid, Marcial Pons, 2019, p. 54.

¹⁶ Art. 34, inc. 3º CP: “No son punibles: (...) 3º. El que causare un mal por evitar otro mayor inminente a que ha sido extraño; (...)”

¹⁷ PALAZZI, Pablo A., “Breves comentarios a los proyectos legislativos sobre delitos informáticos”, en *Revista de Derecho Penal y Procesal Penal*, Buenos Aires, Lexis-Nexis, N° 8, 2006, p. 1531.

¹⁸ CREUS, *Derecho penal. Parte general*, 3ª ed., Buenos Aires, Astrea, 1992, p. 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)

Incluso suponiendo que los intereses de seguridad informática superan esencialmente a los intereses en la intimidad de las 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 interés de seguridad cuya pérdida sea inminente. Por otro lado, ya el propio art. 34, inc. 3° 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.

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, doméstica, o bien las tareas desarrolladas por empresas de seguridad informática en la búsqueda de brindar mayor certeza o seguridad a los sistemas informáticos.

III. Solución I (*lege ferenda*)

De esta forma podemos notar que la regulación actual es insuficiente, por lo que una solución posible es la de incorporar una causa de justificación específica en el texto de la ley, que contemple la actividad de los hackers éticos. Esto podría dar mayor seguridad a su labor y otorgar mejores herramientas para la operadores judiciales, que son quienes en definitiva deben valorar, con las constancias de cada caso, si se trata de una acción de hacking ético que no merece ser sancionada o bien de una actividad de hacking criminal.

Si bien es sumamente dificultoso regular la actividad en el ciberespacio por su masividad y anonimato, han surgido distintos grupos o entidades (como la ACM¹⁹ o IEEE²⁰, que actúan de forma voluntaria) que pensaron y desarrollaron una serie de “códigos de ética” o reglas base para hacer un correcto uso de la actividad informática y la tecnología. 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.

Independientemente de que cada una de estas entidades establece reglas distintas, todas comparten una serie de principios rectores. A saber:

- evitar el daño,
- ser honesto y confiable,
- respetar la propiedad y el trabajo de los demás,
- tener responsabilidad social,
- respetar la privacidad y la confidencialidad,
- evitar la discriminación.

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.

¹⁹ Association for Computing Machinery

²⁰ Institute of Electrical and Electronics Engineers

Por ello, teniendo en consideración estos principios, es posible sostener que si se modificara el Código Penal vigente y se incorporara el siguiente apartado dentro del art. 153 bis se daría la solución al problema del hacking ético:

“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.

IV. Paralelismo. Violación de domicilio

Ahora bien, esta solución podría entrar en crisis. Siguiendo la idea de que así como se habla de “paralelismo” entre el mundo físico y el virtual, 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.

Veamos 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”.²¹ 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”.²²

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”.²³

Si bien todo ello es cierto, quienes argumenten de esta forma no han tomado en cuenta que el art. 152 CP, impone una excepción en forma de causa de justificación al delito de violación de domicilio 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”.²⁴ 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.²⁵

²¹ DONNA, Edgardo A., *Derecho penal. Parte especial*, t. IIA, 2ª ed., Santa Fe, Rubinzal-Culzoni, 2011, pp. 352-353.

²² SOLER, Sebastián, *Derecho penal argentino*, t. IV, Buenos Aires, TEA, 1992, p. 86.

²³ SOLER, *Derecho penal argentino*, cit., p. 87.

²⁴ SOLER, *Derecho penal argentino*, cit., pp. 111-112.

²⁵ DONNA, *Derecho penal. Parte especial*, cit., pp. 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 buscaran fallas de seguridad, por ejemplo, para conseguir acceso a tarjetas de crédito o información personal comprometedoras 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.

Por ello, es necesaria la incorporación al texto legal de una causa de justificación específica, parcialmente basada en nociones de necesidad, tal como sucede con la violación de domicilio clásica.

Aún si la modificación del CP no fuera posible, este argumento es el puntapié inicial para sostener que es posible hacer una interpretación del derecho vigente en un sentido más benigno

para los hackers éticos, ya que podría considerarse que sus actividades pueden ser abarcadas por la causa de justificación del art. 152 CP por medio de una interpretación analógica *in bonam partem*. Esto será explicado a continuación.

V. Solución II (*lege lata*)

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 brevemente la escasa 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”. Allí 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”.

En el análisis realizado por el tribunal interviniente, se concluyó 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.

Se trató, 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.²⁶ 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

²⁶ 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*, t. I, Madrid, Civitas, 1997, pp. 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, lo 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 (...).”

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.

VI. Conclusión

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.²⁷

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 desfase 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.²⁸

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 pérdida de datos e información. Las propuestas de

²⁷ GARCÍA, E. F., “Desafíos jurídicos interdisciplinarios de la ciberseguridad nacional: apuntes ‘de lege ferenda’”, en *Anuario de la Facultad de Derecho. Universidad de Extremadura*, N° 37, 2021, pp. 75-118.

²⁸ BORIZI CIRILLI, Fernando A., “Cibercrimen y evidencia digital: problemática probatoria”, en *Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet*, Ciudad Autónoma de Buenos Aires, Erreius, 2018, pp. 173-182.

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.

VII. Bibliografía

BORIZI CIRILLI, Fernando A., “Cibercrimen y evidencia digital: problemática probatoria”, en *Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet*, Ciudad Autónoma de Buenos Aires, Erreius, 2018, pp. 173-182.

CREUS, Carlos, *Derecho penal. Parte general*, 3ª ed., Buenos Aires, Astrea, 1992.

DONNA, Edgardo A., *Derecho penal. Parte especial*, t. IIA, 2ª ed., Santa Fe, Rubinzal-Culzoni, 2011.

GARCÍA, E. F., “Desafíos jurídicos interdisciplinarios de la ciberseguridad nacional: apuntes ‘de lege ferenda’”, en *Anuario de la Facultad de Derecho. Universidad de Extremadura*, N° 37, 2021, pp. 75-118.

GRADIN, Carlos, “Presentación”, en *Internet, hackers y software libre*, Fantasma, 2004, pp. 9-11.

GUTIÉRREZ, R., RADESCA, L. C. y RIQUERT, Marcelo A., *Violación de secretos y de la privacidad*, Asociación Pensamiento Penal – Código Penal Comentado de Acceso Libre, 2013.

HART, H. L. A., *Castigo y responsabilidad*, Madrid, Marcial Pons, 2019.

HIMANEN, Pekka, *La ética del hacker y el espíritu de la era de la información*, Barcelona, Destino, 2004.

MORESO, José Juan, “Principio de legalidad y causas de justificación (sobre el alcance de la taxatividad)”, en *Doxa. Cuadernos de Filosofía del Derecho*, N° 24, 2001, pp. 525-545.

PALAZZI, Pablo A., “Breves comentarios a los proyectos legislativos sobre delitos informáticos”, en *Revista de Derecho Penal y Procesal Penal*, Buenos Aires, Lexis-Nexis, N° 8, 2006, p. 1531.

ROIBÓN, M. M., “Reflexiones sobre el acceso ilegítimo a un sistema o dato informático”, en PARADA, R. A. (dir.), *Ciberdelitos y delitos informáticos*, Ciudad Autónoma de Buenos Aires, Erreius, 2018, pp. 134-138.

ROXIN, Claus, *Derecho penal. Parte general. Fundamentos de la estructura de la teoría del delito*, t. I, Madrid, Civitas, 1997.

SÁNCHEZ AVILA, M. Á., *Hacking ético: impacto en la sociedad*, Universidad Piloto de Colombia, 2019.

SOLER, Sebastián, *Derecho penal argentino*, t. IV, Buenos Aires, TEA, 1992.

BRANCA (2024), “La protección legal de los hackers éticos”, pp. 52-70.

VÁSQUEZ, M. D., *Técnicas anti-forenses informáticas*, 2016.