Question
Periodismo / Comunicación
ISSN 1669-6581

¿Qué es ser hacker?
Nelson Scariot Esquivel
Question/Cuestión, Nro.71, Vol.3, abril 2022
ISSN: 1669-6581
URL de la Revista: https://perio.unlp.edu.ar/ojs/index.php/question/
IICom -FPyCS -UNLP
DOI: https//doi.org/10.24215/16696581e661

¿Qué es ser hacker?

What is being a hacker?

Nelson Scariot Esquivel
Licenciado en Comunicación Social, Facultad de Ciencia Políticas y Sociales, Universidad Nacional de Cuyo
Argentina
nelsonscariot96@gmail.com
https://orcid.org/0000-0003-1316-6037

Resumen

Este artículo está basado en el primer capítulo de mi tesina de grado *La cultura hacker como filosofía de vida en la era del capitalismo cibernético. Una aproximación al caso en Mendoza* (Scariot, 2020). Aquí buscamos responder a la pregunta: ¿qué es ser hacker? Para responderla, es necesario un recorrido por el origen del término, comprender su tergiversación a lo largo del tiempo a manos del poder hegemónico, y analizar la diferencia entre hackers y crackers. Esto nos llevará a precisar, ampliar y resignificar el concepto *hacker* como aquella

persona que difiera, crea, comparte y expresa su pasión creativa libremente en pos del bien común.

Palabras claves: hacker, génesis hacker, cracker

Abstract

This article is based on the first chapter of my dissertation Hacker culture as a philosophy of life in the era of cyber capitalism. An approach to the case in Mendoza. Here we seek to answer the question: what is being a hacker? To answer it, it is necessary to go through the origin of the term, understand its misrepresentation over time at the hands of the hegemonic power, and analyze the difference between hackers and crackers. This will lead us to specify, expand and re-signify the hacker concept as a person who differs, creates, shares and expresses their creative passion freely in pursuit of the common good.

Keywords: hacker, hacker genesis, cracker

Introducción

En primer lugar, es pertinente realizar un breve resumen de mi tesina de grado *La cultura hacker como filosofía de vida en la era del capitalismo cibernético. Una aproximación al caso en Mendoza* (Scariot, 2020). Esta se conforma de tres capítulos. En el primero buscamos comprender el significado de lo que implica ser hacker, remontándonos a los orígenes del término y explorar lo que motiva su accionar. En el segundo nos centramos en las comunidades hackers, intentando interpretar sus valores, ética y acciones. Por último, en el tercer capítulo, indagamos el aspecto político, revolucionario y filosófico de la cultura hacker.

Para iniciar este recorrido, primero es pertinente referirnos al aspecto semántico de la palabra hacker. En relación a esto, los medios de comunicación suelen referirse a los/as hackers como criminales informáticos/as que roban identidades y vacían cuentas bancarias, entre otros actos de vandalismo. Resulta que el término adecuado para este tipo de personas es *cracker*. De hecho, ser hacker implica más que saber de computadoras o delinquir. Se puede ser hacker en cualquier área de conocimiento. Así, Leonardo Da Vinci, Jorge Luis

Borges o Simone de Beauvoir, entre otros/as, pueden ser considerados/as hackers. Porque hackear es construir, diferir, compartir. Ser hacker conlleva un conjunto de prácticas y valores encaminados a liberar nuestra "pasión creativa" (Himanen, 2004) en pos del bien común.

Para comprender esta idea con exactitud, es necesario precisar y ampliar el término hacker para luego resignificarlo. Es fundamental explorar el origen del concepto y su tergiversación a manos de las grandes compañías de hardware y software, los medios de comunicación hegemónicos y los gobiernos de las potencias.

Este análisis nos permite definir qué es la cultura hacker y cómo se manifiesta en la provincia de Mendoza. A nivel provincial damos cuenta de dos casos de manifestaciones hackers, la revista digital *Tribuna Hacker* y el movimiento software libre de Mendoza. Comprender los valores y ética de la cultura hacker nos abre a definir lo que podemos denominar: *filosofía hacker*.

Con estos objetivos, para el desarrollo de esta investigación utilizamos tres métodos de recolección de información. Por un lado, analizamos elaboraciones teóricas sobre cultura hacker. Por el otro, aplicamos entrevistas en profundidad con referentes de esta comunidad en la provincia de Mendoza. Finalmente, empleamos la observación participante como instrumento de recopilación de datos complementario de la entrevista en profundidad.

Las entrevistas en profundidad fueron realizadas con personas vinculadas a la cultura hacker en Mendoza: el movimiento software libre provincial y la revista digital *Tribuna Hacker*. En el caso del movimiento software libre entrevistamos a Sergio, Ingeniero electrónico y coordinador provincial del Festival Latinoamericano de Instalación de Software Libre (FLISoL); y a Julia, ingeniera en sistemas de información, desarrolladora de software, investigadora y docente universitaria. También forma parte del movimiento software libre y es referente del grupo R-Ladies. En el caso de *Tribuna Hacker* entrevistamos a Matías, periodista, programador y director del medio digital. Es pertinente aclarar que por cuestiones de anonimato, no utilizamos el nombre real de los entrevistados y la entrevistada.

Respecto al método de observación participante, este constó de una intervención en el Festival Latinoamericano de Software Libre 2019 que se llevó a cabo en la Universidad

Tecnológica Nacional (sede Mendoza) en abril de 2019, en el cual exploramos las acciones y discursos expresados por organizadores, expositores y participantes del encuentro. Y el análisis de algunas notas periodísticas elaboradas por *Tribuna Hacker*.

Por último, a luz de lo indagado en este trabajo de investigación, hay diferentes argumentos para pensar que la filosofía hacker puede considerarse una alternativa sólida frente a la lógica capitalista. El conocimiento tecnológico de los/as hackers sobre el cual se sostiene este modelo mercantil y el conjunto de valores, ética y acciones de la filosofía hacker constituyen motivos concretos para explorar este fenómeno.

¿Qué es ser hacker?

¿Son los/a hackers criminales informáticos/as que pueden ingresar a nuestra cuenta bancaria y extraer todo nuestro dinero? ¿Son capaces de vulnerar la seguridad de nuestros celulares y computadoras para extorsionarnos y hacer lo que nos pidan? En realidad esta es una concepción errada de qué es ser hacker. Para comprender con mayor precisión su significado tenemos que remontarnos a su origen.

Entender el surgimiento de la cultura hacker, nos permite comprender porqué corporaciones de hardware y software, gobiernos y medios de comunicación modificaron el concepto original de lo que implica ser hacker para transformarlo en sinónimo de criminal y terrorista. A partir de esta estigmatización, la comunidad hacker estableció el término *cracker*, aquellas personas que utilizan sus conocimientos informáticos para dañar a terceros por vandalismo y/o beneficio personal. En cambio, el comportamiento de los hackers está impulsado por una serie de valores y una ética que están muy lejos de la criminalidad cibernética y el ciberterrorismo.

No obstante, es conveniente derribar el mito de que los hackers únicamente son genios/as informáticos/as. De hecho, se puede ser hacker en cualquier campo de conocimiento. Es posible hackear los códigos normativos de la ciencia, la política, el deporte, el lenguaje, la educación y cualquier forma de manifestación. Ya sea como Sergei Eisenstein en la cinematografía siendo pionero en la técnica del montaje o como Mahatma Gandhi practicando la desobediencia civil no violenta como método de acción política. Así, ser hacker

es repensar la realidad en todas sus expresiones a favor del bien común. Idealmente el hackeo debe tener valor social, aunque promover la libre expresión de nuestra creatividad, también es ser hacker. Siguiendo esta visión, toda persona puede ser hacker.

En efecto, para precisar y ampliar que implica ser hacker es pertinente conocer su origen, sus valores y ética, y los actores involucrados en su modificación semántica.

Génesis hacker

Podemos establecer tres antecedentes hackers que confluyeron y dieron origen a la cultura hacker tal como la definiremos a lo largo de esta tesis. Los/as hackers aficionados/as, los/as ocupantes de las redes y los/as académicos/os (Gradin, 2004).

Los/as hackers aficionados/as o *hobbyists* fueron aquellos/as radioaficionados/as de la década de 1920. Entusiastas argentinos/as y estadounidenses modificaron el hardware radiofónico y le dieron una nueva función a una herramienta que nació como instrumento militar. Entretenimiento e información fueron esas nuevas funciones. Progresivamente el hackeo radiofónico de Enrique Susini y el de los/as estadounidenses desembocó en la radio como medio masivo de comunicación. El origen de este servicio de información y entretenimiento fue un hackeo. Se modificaron diversas piezas del aparato radiofónico militar para darle una nueva función. Se trató de un experimento motivado por la curiosidad, actitud clave en todo hackeo.

Luego nos encontramos con el hackeo de redes telefónicas, grupo denominado *phreakers.* Alberto Quian (2016) explica que los/as *phreakers* nacieron en la década de 1950, vinculados al estudio, la exploración y la experimentación de sistemas de telecomunicaciones, principalmente de equipos y sistemas de redes telefónicas. En este sentido, Matías, director de *Tribuna Hacker,* amplía su origen:

> Arrancaron formalmente en el 57´, con el Capitán Crunch (John Thomas Draper, también conocido como Capitán Crunch, es un programador y exphreaker estadounidense). El capitán Crunch tenía un sobrino ciego (Joe Engressia) de 8 años que se da cuenta que silbando el teléfono, el teléfono se ponía en modo

> terminal. En ese momento, los *phreakers* llevaban 30 años queriendo dominar el sistema telefónico de Estados Unidos, que es el primer monopolio natural del mundo. Entonces, ¿qué hace Estados Unidos? Regula la telefonía a través de un sistema integrado y todo se hacía a través del teléfono. Los *phreakers* sabían que si controlaban el teléfono, controlaban el sistema. Entonces pasaron 27 años tratando de encontrar la *Blue Box*, una máquina capaz de controlar el sistema telefónico. El sobrino del Capitán Crunch le dice: "Che tío, cuando silbo el teléfono hace unos ruidos raros y después puedo llamar a cualquier lado gratis". Y efectivamente era así. En la frecuencia 2600 Hz se producía el error y el niño este había logrado silbar en esa frecuencia. Entonces, el Capitán Crunch había logrado modificar un silbato que venía en unos cereales en 1957 y publica cómo modificar el silbato para poder hablar gratis. Esa es la primera *Blue Box*, un tipo con un sobrino ciego que llevaba 20 años buscando una solución a poder operar en el sistema y se da cuenta que un silbato que venía en los cereales Capitán Crunch, de ahí su apodo, les iba a permitir eso. Todo este movimiento, técnicamente no son hackers, son *phreakers*. (Matías, *Tribuna Hacker*)

Este movimiento exploró el hacking de redes telefónicas, permitiendo llamadas gratuitas y conexiones de comando a escala internacional que se suponía solo debían conocer las empresas de telefonía. Progresivamente, estas compañías adoptaron interruptores controlados por computadoras. Entonces los/as *phreakers* trasladaron el hacking de redes telefónicas electromecánicas a las redes digitales. Un nueva forma de hackeo se avecinaba (Gradin, 2004).

El tercer antecedente son los/as hackers académicos/as. En realidad, sus hackeos van más allá de lo estrictamente académico, pero surgen en la esfera universitaria. Eric Steve Raymond (2002), afirma que la cultura hacker nació en 1961, año en que el MIT (Instituto de Tecnología de Massachusetts) adquirió la primera PDP-1, la primera computadora de la *Digital Equipment*. El Club de Tecnología de Trenes a Escala del MIT adoptó la máquina como su juguete predilecto e inventó herramientas de programación, argot y toda una cultura a su alrededor que persiste hasta la actualidad. Estos/as informáticos/as fueron los primeros en acuñar el término *hacker* para autodenominarse y describir sus actividades.

Según este antecedente, la figura del hacker surgió, en lo estrictamente técnico, con la aparición de la informática, la expansión de la computación interactiva, la interrelación entre universidades y el florecimiento de las redes cibernéticas.

Los diversos avances tecnológicos de la década de 1960 en adelante, impulsaron y acompañaron la génesis del/la hacker, que desde el principio manifestó un espíritu por la libre creación de software, donde los/as hackers exploraban su imaginación. Estos/as *programadores auténticos/as* expresaban su espíritu juguetón, es decir, su creatividad por medio de la creación de software. Lo distintivo en esta creación de programas informáticos era y es el proceso. Los/as hackers compartían su diseño con otros programadores, sin restricciones. Se trató de trabajo en equipo, de cooperación y solidaridad. Es por esta razón que los/as hackers quieren que el código fuente de todo programa sea abierto, porque esto permite que otros puedan editar y mejorar el programa.

Ahora bien, ¿por qué considerar estas tres experiencias como impulsoras de la cultura hacker tal como la planteamos en este trabajo? En principio porque modificaron lo existente y le dieron una nueva función a sus creaciones, una con valor social. Los/as hackers de la radiodifusión convirtieron un aparato militar en un servicio de información y entretenimiento; los/as *phreakers* encontraron la forma de permitirle a toda la población acceder libremente a un servicio monopolizado; y los/as hackers académicos modificaron el software expandiendo sus funciones mediante el trabajo en equipo y la solidaridad.

La curiosidad, la experimentación, el espíritu autodidacta, liberar y compartir información, la cooperación, la solidaridad y el valor social de los hackeos son algunos de los valores que podemos observar en estos antecedentes hackers que dan vida a la actual cultura hacker. Una que busca que sus hackeos mejoren la vida de la sociedad en conjunto. Una cuya hackeos deben ir más allá del aspecto económico. De hecho, la cultura hacker manifiesta un estilo de vida que rechaza la mercantilización de su pasión creativa. Para los/as hackers, la creatividad debe ser libre de toda imposición del poder estatal y económico. En resumen, expresar libremente nuestra “pasión creativa”, como la define Himanen (2004), fue la premisa que dio origen a los hackers.

Definiciones del hacker

Para lograr una definición adecuada y acabada de la cultura hacker, y también para precisar el término hacker, es relevante aclarar ciertas cuestiones. El/la hacker no es un/a criminal informático/a, en ese caso no estamos refiriendo al/la *cracker*. Pero esta "confusión" es el resultado de intereses gubernamentales y empresariales que cuentan con el apoyo de los medios de comunicación.

Lo que nos proponemos en este apartado es determinar qué no es y qué sí es un hacker. Por esta razón, realizamos un breve recorrido histórico desde el momento en que se creó la palabra hacker hasta el momento en que comenzó a pervertirse el término, y las razones de tal perversión.

Qué no es un/a hacker: el ataque de empresas, gobiernos y medios de comunicación

Actualmente el término hacker es utilizado para referirse, principalmente, a los/as criminales informáticos/as, como resultado del uso masivo establecido por los medios de comunicación a partir de la década de 1980. La estigmatización de los/as hacker beneficia a gobiernos y a poderes privados en dos sentidos: por un lado, para determinar qué es normal en el mundo informático haciendo creer que un/a ciudadano/a de bien es todo lo que el/la hacker no es; por otro, para justificar la seguridad, la vigilancia y el castigo (Quian, 2016). Para Himanen (2004) esto obligó a la comunidad hacker a crear el término *crackers*, que designa a aquellas personas que utilizan sus conocimientos informáticos para delinquir sin más motivación que el beneficio personal o incluso por malicia. Como amplía en su testimonio, Matías afirma que "un *cracker* va a ser hacker en la medida en que logre una auditoria, pero cuando perpetúa un ataque, es un *cracker*. La gente que utiliza sus conocimientos en contra de otra es miserable y no la considero hacker". De modo que el ethos hacker está muy lejos de la idea que ha calado en la opinión pública. Desde sus propios medios, los hackers han intentado explicar al mundo, con poco éxito, su genuino carácter y sus valores (Quian, 2016).

Richard Stallman afirma que el significado del hacking comenzó a pervertirse a principios de los ´80, cuando los medios de comunicación detectaron la existencia de los/as hackers pero se centraron solo en un aspecto: subvertir la seguridad informática para acceder a otras computadoras. Pero es incorrecto considerar que ser hacker implica únicamente romper la seguridad. Además, cuando el/la hacker corrompe el sistema de seguridad de una

computadora no lo hace por vandalismo, lo hace para mejorar el sistema informático y compartirlo libremente con otras personas (Quian, 2016). Stallman explica que el concepto del/la hacker como aquel que penetra ilegalmente en los sistemas de seguridad es una confusión impulsada por los medios de comunicación: "Nosotros, los hackers, nos negamos a reconocer esta acepción y seguimos utilizando este término para describir a alguien que ama la programación y disfruta explorando nuevas posibilidades" (2004:20).

Asimismo, el autor niega que la cultura hacker, por medio de su actitud rebelde y desafiante de los sistemas de seguridad, busque llevar a cabo una revolución. Para él, los/as hackers no buscan hacer una revolución o cambiar el mundo, simplemente quieren lucir su inteligencia juguetona, como lo puede hacer un poeta al escribir (Quian, 2016). Esto será algo que discutiremos en el Capítulo III, donde interrogamos sobre el potencial revolucionario del hacker en la era del capitalismo cibernético.

Volviendo al tema de este apartado, Quian (2016) explica que la criminalización de los/as hackers creada por los poderes estatales, esparcida por los medios masivos de comunicación e inoculada en la población, se basa en una arbitraria identificación de los miembros de esta comunidad con los/as *crackers*, aquellos/as usuarios/as destructivos cuyo objetivo es crear virus e introducirse en otros sistemas. Los/as hackers, a diferencia de los/as *crackers*, utilizan sus habilidades tecnológicas para realizar intervenciones orientadas a solucionar crisis en sus entornos.

Según el *Jargon File,* el diccionario del argot hacker, el término *cracker* fue creado por los/as hackers en 1985 para defenderse del mal uso periodístico de la palabra hacker. Su uso denotaba el rechazo de esta comunidad al robo y al vandalismo *cracker*. Esto no implica que los/as hackers se abstengan de introducirse en sistemas sin permiso, pero siempre debe realizarse con un espíritu juguetón y curioso, y por razones justificadas que no conlleven destrucción o daño (Quian, 2016).

Para Eric Raymond, muchos/as periodistas han sido engañados/as sobre el concepto del/la hacker y lo han confundido con lo que es de hecho el/la *cracker*. Tal artimaña ha sido articulada por los aparatos del poder gubernamental y las grandes corporaciones tecnológicas, incumbidas en criminalizar a una comunidad que cuestiona su hermetismo y un modelo

comercial privativo y opresor que deja al usuario en manos de la tecnología, en la más absoluta ignorancia e indefenso, y a la sociedad en general, limitada por barreras técnicas, legales o institucionales que impiden la reutilización y mejoras comunitarias (Quian, 2016).

La confusión generada sobre qué implica ser hacker y la estigmatización de esta comunidad ha sido alentada por las autoridades. Simbólico es el discurso pronunciado por el presidente Bill Clinton del 22 de enero de 1999 en la *National Academy of Sciences* en Washington DC, titulado "*Keeping America Secure for the 21st Century"*. En dicha alocución, "Clinton identificó a los hackers como una nueva amenaza ciberterrorista para la seguridad nacional equiparable a la del terrorismo, en general, y a la del bioterrorismo, en particular" (Quian, 2016: 110). Por medio de ese discurso, Clinton no sólo robusteció la criminalización de la cultura hacker identificada con cualquier delito informático, sino que también declaró oficialmente la guerra a los/as hackers como enemigos del Estado y asentó las bases de una nueva Red de redes controlada y vigilada por el Estado-nación, bajo el pretexto de la seguridad nacional y pública.

De esta forma, el gobierno de Estados Unidos, entre otros gobiernos, mancomunados con empresas y medios de comunicación, deformaron el concepto hacker otorgándole una connotación negativa. Actualmente, para el público en general, la palabra hacker es sinónimo de criminal o ladrón. Pero queda claro que el/la hacker no es eso: la criminalización del/la hacker es intencional y con evidentes intereses gubernamentales y empresariales. La persecución de los/as hackers es una buena excusa para aumentar el control y vigilancia de las personas en internet. Las empresas colaboran en esto para obtener beneficios en sanción de leyes que profundizan el monopolio de hardware y software privativos. Copyright, patentes, derechos de autor, propiedad intelectual son algunos ejemplos.

Sin embargo, no solo los medios de comunicación han esparcido el concepto erróneo del/la hacker como un/a criminal informático/a, sino también instituciones académicas de gran trayectoria y prestigio colaboran con este error forzado. La Real Academia Española y el Diccionario Oxford son algunas de ellas. El Diccionario de la Real Academia Española, en su actualización al 2019, aplica el término hacker en las siguientes dos acepciones (RAE):

1. m. y f. Inform. Pirata informático.

> 2. m. y f. Inform. Persona con grandes habilidades en el manejo de computadoras, que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.

En lengua inglesa, el *Oxford Dictionary* da cuenta de las siguientes acepciones para la palabra hacker (Quian, 2016: 74)

> 1. Una persona que usa una computadora para obtener acceso no autorizado a datos.
>
> 1.1. Un entusiasta y hábil programador o usuario de computadoras.
>
> 2. Una persona o cosa que machetea o corta bruscamente.

Si bien ambos reconocen la habilidad informática del hacker, sus definiciones reducen y connotan negativamente el concepto del hacker, considerándolo principalmente un pirata informático, es decir, un *cracker*. Esto, además, da cuenta de que instituciones de gran prestigio y trayectoria académica reproducen el concepto del hacker como *cracker*. En consecuencia, la población tiende a repetir este concepto erróneo de qué es, verdaderamente, el hacker.

Qué es un/a hacker: hacia una defensa y valorización de la cultura hacker

A partir de 1960, un grupo de programadores/as del MIT (Instituto de Tecnología de Massachusetts) autodenominados/as hackers, establecieron como algunos de sus principios fundamentales analizar, resolver problemas, desarrollar su intelecto y ofrecer el fruto de su trabajo intelectual para el bien común (Himanen, 2004).

De acuerdo al *Jargon File,* los/as hackers son personas que se dedican a programar creativamente y que comparten sus trabajos con la comunidad, considerando un deber ético elaborar software libre, facilitar el acceso a la información como también a los recursos de computación (Himanen, 2004). Por ejemplo, Matías afirma que ser hacker es una capacidad inherente al ser humano, tal como la curiosidad: “No se puede ser hacker si no sos curioso”, afirma el periodista, que tiene una buena opinión sobre ellos/as, pues se define como tal: “Me defino como un hacker porque soy una persona curiosa a la que le gusta ponerse objetivos y le

gusta alcanzarlos. Me gusta experimentar, me gusta investigar, me gusta ver si puedo mejorar las cosas". Y aclara que hay gente que no considera hacker, como un/a *lamer* (sujetos que penetran ilegalmente en los correos de las personas) que se integra al concepto de *cracker*.

Por su parte, para Emmanuel Goldstein, hacker y ex editor de la revista *2600*, hackear es aprender libremente. Afirma que la cultura hacker desafía a la cultura de masas alienante y a las creencias sistémicas de que una persona emancipada que practique plenamente su libertad individual es una amenaza para el sistema. Y esta es la razón que empuja a los poderes del Estado a condenar socialmente a los/as hackers y a someterlos/as a redadas gubernamentales, persecución selectiva, vigilancia y a la histeria de masas (Quian, 2016). Julia, integrante del movimiento software libre en Mendoza, coincide con esta visión y afirma que un hacker es alguien que construye y colabora. Según ella, es un término que tiene una connotación negativa y que está fuertemente vinculado con la informática y con lo intangible, y es por esa razón la dificultad para saber qué es un hacker y qué hace. Considera que los medios de comunicación lo definen como un/a delincuente y que por ello sería bueno utilizar el término "hacking ético" para diferenciar a hackers y *crackers*. Julia también se considera una hacker y explica el por qué:

> Me defino como una hacker porque es un término muy amplio. Yo creo que muchas personas somos hackers, aunque no nos denominemos hackers. No se usa debido a la connotación negativa que tiene el término. Para diferenciar, se está usando mucho el término *maker*: alguien que construye o que participa en hackatones. En Mendoza se hace el hackatón. Pero hay todo un drama con los hackatones, depende mucho cómo se lleve adelante. Muchas veces se hacen hackatones muy competitivos. Hay muchos que son por dinero. (Julia, movimiento software libre Mendoza)

Para Sergio, ingeniero electrónico y referente del movimiento software libre en Mendoza, hackers son personas marcadas por valores como la curiosidad, el aprendizaje y la ética "buena o correcta" en sus actos de hacking: "Contrario a la creencia popular o que los medios han impuesto que es alguien malo, para mí el hacker es alguien que resuelve algo muy complejo en el ámbito de la tecnología. Esta sería la definición real". Sin embargo, Sergio no se considera un hacker: "No soy hacker, pero trato de fomentar la actividad hacker, más en el

ámbito universitario-tecnológico. Me parece que es algo que se debe desarrollar, que genera muchísimos conocimientos y que inspira mucho más que la formación formal académica". Además, afirma que como ingeniero electrónico ha hackeado hardware y que por lo tanto no se considera un hacker informático. Si ampliamos el concepto de hacker más allá de la informática, es pertinente afirmar que Sergio es de hecho un hacker. Ya que promueve algunos valores de la cultura hacker a través del movimiento software libre y porque realiza hackeos de hardware.

Podemos observar en las opiniones de los y la entrevistada, diferentes formas de concebir que implica ser hacker. Por esta razón, para lograr un consenso y mayor precisión, exponemos las ocho acepciones del *Jargon File* (cit. en Quian, 2016: 73):

> 1. Una persona que disfruta explorando los detalles de los sistemas programables y cómo estirar sus capacidades, a diferencia de la mayoría de los usuarios, que prefieren aprender sólo lo mínimo necesario. RFC1392, el Glosario de los Usuarios de Internet, útilmente amplifica esto como: una persona que se deleita en tener un profundo conocimiento del funcionamiento interno de un sistema, ordenadores y redes informáticas en particular.
>
> 2. Quien programa con entusiasmo (incluso obsesivamente) o disfruta de la programación en lugar de teorizar acerca de la programación.
>
> 3. Una persona capaz de apreciar el valor del hackeo.
>
> 4. Una persona que es buena programando rápidamente.
>
> 5. Un experto en un programa informático en particular, o una persona que con frecuencia trabaja usando cierto programa. Por ejemplo, «un hacker de Unix programador en C».
>
> 6. Un experto o un entusiasta de cualquier tipo. Uno puede ser un hacker de la astronomía, por ejemplo.
>
> 7. Aquel que disfruta el reto intelectual de superar o eludir creativamente limitaciones.

> 8. [Obsoleta] Un intruso malicioso que trata de descubrir información sensible entrometiéndose en algún sistema. Por lo tanto, hackers de contraseñas, hackers de acceso a redes. El término correcto para este sentido es cracker.

Las primeras cinco definiciones del *Jargon File* dan cuenta de qué es un/a hacker informático. Pero como explicamos al comienzo, uno de nuestros objetivos es ampliar y precisar este concepto para luego resignificarlo. Eso es lo que hacen las acepciones 6 y 7, que se refieren más a la actitud que una persona puede tener frente al acontecer de la vida, que al talento en un campo disciplinario en particular. Aunque, si bien las definiciones del *Jargon File* son válidas, no incluyen el aspecto político y filosófico que caracteriza el accionar hacker. Igualmente, a partir de las diferentes visiones expuestas, podemos aproximarnos a dar una definición nueva de qué es el/la hacker.

No obstante, antes es preciso exponer una categorización del/la hacker, según su ética y su accionar político. Nos referimos a la distinción entre hackers de "sombrero gris, blanco y negro" (Soria Guzmán, 2016). El color de su "sombrero" nos da la pauta de su ética e ideología. Esta categorización nos ayuda a integrar el aspecto político en el accionar del/la hacker y empezar a entender la filosofía hacker como tal.

Irene Soria Guzmán (2016) afirma que desde fines de 1990, se implantaron los calificativos "hacker de sombrero blanco" y "hacker de sombrero negro", en principio definidos en torno de si cada individuo/a es fundamentalmente "bueno/a" o "malo/a". El/la hacker de sombrero blanco es aquel sujeto/a que nunca vulneraría la seguridad de un sistema con espíritu malicioso, para ganancia personal o sin la autorización de sus propietarios/as. Si lo hiciera, nos estaríamos refiriendo al/la hacker de sombrero negro. En este caso, estamos hablando del/la *cracker*, retratado en noticias y películas como un/a potencial "genio/a maligno/a".

Surgió, posteriormente, el concepto de hacker de "sombrero gris", el equivalente a un híbrido entre los/as hackers de sombrero blanco y de sombrero negro. Un/a hacker de sombrero gris puede actuar por fuera de los límites legales, pero con "buenas intenciones". Generalmente no atacan por intereses personales o con intenciones destructivas, aunque en el curso de sus logros informáticos pueden realizar acciones que son consideradas delito (Soria

Guzmán, 2016). En su testimonio, Matías coincide con esta categorización, aunque añade un aspecto a la explicación:

> Los sombreros es la mejor forma de guiarte. Pero para mí por un lado están los que desarrollan ingeniería social y los que desarrollan ataques, como romper un vidrio. La ingeniería social busca ver cómo abrir el vidrio sin romperlo. Si sabés cómo abrirlo, sabés cómo cerrarlo. Si lo rompés, tenés que cambiarlo. A nivel genérico tenés los de sombrero blanco que hacen que el mundo sea peor colaborando con las corporaciones. Los de sombrero negro obtienen beneficios personales haciéndole mal a la gente. Y estamos los de sombrero gris, que tenemos motivaciones políticas y que a veces cobramos o no por nuestro trabajo, de acuerdo al tiempo que dispongamos. (Matías, *Tribuna Hacker*).

En coincidencia con lo anterior, Sergio establece dos grandes categorías de hackers: "el ético y el no ético". En realidad es preciso aclarar, desde un punto de vista semántico, que no existen dos tipos de hackers. Lo que existe es el/la hacker que no actúa con malicia y el/la *cracker*, que sí tiene un espíritu malicioso o destructivo. En este sentido, Sergio describe al/la *cracker* así:

> Es el que viola una licencia privativa para que el software pueda ser usado por otros usuarios. Algunos autores definen al *cracker* como un rebelde, pero están en contra de su accionar, no por cuestiones éticas de robarle datos a una corporación sobre qué hacen con nuestras computadoras, el problema para ellos es que para hacer algo revolucionario real se debe promover el uso del software libre. No romper un software privativo para que lo pueden usar todos, ahí no estás transformando nada digamos. Estás continuando con el uso del software privativo, y no fomentando el uso del software libre que sería realmente lo revolucionario. (Sergio, movimiento software libre Mendoza)

Si bien la diferenciación del comportamiento del/la hacker a través de sombreros es esclarecedora, conlleva un error semántico. En realidad no existen diferentes tipos de hackers, solo existe un tipo de hacker. Por supuesto, no siempre se van a cumplir todos los valores que convierten a un/a hacker en hacker, pero una persona que vulnera un sistema informático para

beneficio personal es un/a *cracker*, y una persona que mejora el sistema de vigilancia de un organismo estatal que espía a la población o colabora en mantener la estructura desigual del mundo, no es hacker, podemos afirmar que es un/a tecnócrata o alguien "funcional al sistema". Por eso, la categorización de hackers según su sombrero no es correcta en cuanto terminología, pero sí en contenido, ya que nos ayuda a entender quién sí es y quién no es un hacker de acuerdo a sus motivaciones ideológicas.

Aproximación final: ¿Da Vinci fue un hacker?

Para continuar con la ampliación y precisión del concepto hacker, nos resulta pertinente el ejemplo utilizado por Matías. Para él, el artista renacentista Leonardo Da Vinci fue un hacker en su tiempo:

> Hay un estudio español que se llama Almeida y asociados, un estudio de abogados hackers, que plantea, y yo coincido en esto, que Da Vinci fue un hacker en su tiempo. Los hackers, el tipo de hacker que soy yo, buscamos desafíos, buscamos resolver cosas, nos preguntamos si podemos saltar esa pared y probamos. Nuestro objetivo no es hacerle daño a las personas, es saltar la pared. ¡Me metí en una caja de seguridad! ¡Uh, mirá! ¡Pude! Me voy, listo. No voy chorear nada. (Matías, *Tribuna Hacker*)

Siguiendo esta visión, ser hacker implica una actitud y una serie de valores, no debemos centrarlo únicamente al campo informático. Como explica McKenzie Wark (2006) hackers son aquellas personas que producen nuevos conceptos, nuevas percepciones, nuevas sensaciones. Pero los/as hackers no solo hackean el código del lenguaje informático, también hackean el de la poesía, el de la música, el de las matemáticas, cualquier lenguaje puede ser hackeado, es decir, repensado. Hackear es diferir. Los/as hackers crean la posibilidad de un nuevo mundo. O al menos de nuevas cosas, creaciones de todo tipo, expresiones que pueden escapar de toda categorización mercantil.

En cualquier área disciplinaria el/la hacker puede extraer información y producir nuevas posibilidades para el mundo: "Hackear es expresar conocimiento en cualquiera de sus formas.

El conocimiento hacker implica, en su práctica, una política de información libre, de aprendizaje libre, el regalo del resultado en una red punto a punto" (41).

El/la hacker es alguien que difiere. Hacker es proyectar la virtualidad de lo presente. Los/as hackers quieren ser libres para hackear por hackear, libre y continuamente para crear múltiples futuros. Por eso Da Vinci, como también Albert Einstein, Pablo Picasso, Simone de Beauvoir, Sergei Eisenstein, Frida Kahlo, Jorge Luis Borges, John Lennon, Mahatma Gandhi, Martin Luther King, Marie Curie y la lista puede continuar, son hackers, porque crearon algo nuevo, hackearon lo existente para construir la posibilidad de una nueva realidad. Hackear es construir. Esa creación puede envolver algo novedoso o distinto, con valor social, idealmente con valor social, pero el solo hecho de revelarse ante el orden de las cosas es ser hacker. A partir de allí construir algo que desafíe la estructura ordinaria de la realidad. Esa actitud está marcada por la curiosidad, pero también compartir esa creación para que otros puedan seguir construyendo en una cadena infinita de expresiones. Así, ser hacker es diferir, construir, compartir y expresar nuestra pasión creativa libremente.

Referencias bibliográficas

Acevedo Musto, R. (20 de marzo de 2018). 7 claves para entender el escándalo de Facebook y Cambridge Analytica. InfoBae. Recuperado en https://www.infobae.com/

BBC News Mundo (1 de mayo de 2019). Condenan a Julian Assange, el fundador de WikiLeaks, a 50 semanas de cárcel. Recuperado en https://www.bbc.com/

Brezina, Natalia (1 de junio de 2020). Anonymous anunció que revelará los crímenes de la policía de Minneapolis. La Izquierda Diario. Recuperado en https://www.laizquierdadiario.com/

Comité Invisible (2016) A nuestros amigos. Buenos Aires, Argentina. Hehkt Editorial.

Davies, Harry (11 de diciembre de 2015).Ted Cruz utiliza una empresa que obtuvo datos de millones de usuarios involuntarios de Facebook. The Guardian. Recuperado en https://www.theguardian.com/

Festival Latinoamericano de Software Libre (2019). Recuperado en https://flisol.info/

Gradin, Carlos (Comp.) (2004). Internet, hackers y software libre. Argentina. Editorial Fantasma.

Himanen, Pekka (2004). La ética del hacker y el espíritu de la era de la información. Barcelona, España. Destino.

Hopenhayn, D. (18 de abril de 2018). Martin Hilbert y el escándalo de Facebook: “Estamos atacando los síntomas, pero no la enfermedad”. The Clinic. Recuperado en https://www.theclinic.cl/

Kleiner, Dmytri (2019). El manifiesto telecomunista. Recuperado en https://endefensadelsl.org

Levis, Diego (2009). La pantalla ubicua: televisores, computadoras y otras pantallas. Buenos Aires, Argentina. La Crujía.

Masse, F. (2 de septiembre de 2019). Diez frases geniales de Einstein… que nunca dijo. Milenio Diario. Recuperado en https://www.milenio.com/

Padilla, Margarita (2012). El kit de la lucha en Internet. Madrid, España. Traficantes de Sueños.

Partido Interdimensional Pirata (2019). Recuperado en https://partidopirata.com.ar/

Perry, York. (30 de julio de 2020). Cuidado: hacker encuentra fallo en Zoom para robar cualquier contraseña. FayerWayer. Recuperado en https://www.fayerwayer.com/

Quian, Alberto (2016). Impacto mediático y político del activismo hacker en la sociedad red. Estudio de caso: WikiLeaks (Tesis doctoral). Universidad Carlos III de Madrid, España.

Ramirez-Escudero, Daniel. (11 de julio de 2020). Hacker roba 336 Bitcoin de un exchange de criptomonedas y se da a la fuga. BeInCrypto. Recuperado en https://es.beincrypto.com/

Raymond, Eric (1999). La catedral y el bazaar. Recuperado en http://biblioweb.sindominio.net/telematica/catedral.html

Raymond. Eric (2002). Breve Historia de la Cultura Hacker. Recuperado en https://www.oreilly.com/openbook/opensources/book/raymond2.html.

Sadoul, George (1977). Historia del Cine Mundial. México. Siglo XXI.

Scariot, Nelson (2020). La cultura hacker como filosofía de vida en la era del capitalismo cibernético. Una aproximación al caso en Mendoza (Tesis de grado). Universidad Nacional de Cuyo, Mendoza, Argentina.

Serra, A. (20 de abril de 2019). El caso Snowden: historia del genio cyber que traicionó a su patria y huyó a Rusia protegido por Putin. InfoBae. Recuperado en https://www.infobae.com/

Soria Guzmán, Irene (2016). Ética hacker, seguridad y vigilancia. México. Universidad del Claustro de Sor Juana.

Srnicek, Nick (2018). Capitalismo de plataformas. Buenos Aires, Argentina. Caja Negra.

Stallman, Richard (2004). Software libre para una sociedad libre. Madrid. Traficantes de Sueños.

Tiqqun (2016). La hipótesis cibernética. Buenos Aires, Argentina. Hehkt Editorial.

Traficantes de Sueños (2020). Recuperado en https://www.traficantes.net/

Tribuna Hacker (2019). Recuperado en https://www.tribunahacker.com.ar/

Villatoro, G. (5 de febrero de 2018). El joven alvearense que fabrica prótesis gratis tendrá a disposición 10 impresoras 3D. Diario Los Andes Online. Recuperado en https://www.losandes.com.ar/

Wark, McKenzie (2006). Un manifiesto hacker. Barcelona, España. Alpha Decay.