



## Etica hacker?

Marco Ciurcina  
StudioLegale.it  
Via San Quintino n. 32, Torino, Italia

### Abstract

Negli anni in cui si sviluppano le tecnologie digitali, sorgono gruppi di persone che si definiscono *hacker*. Oggi il termine *hacker* viene utilizzato per identificare persone collegate alle tecnologie digitali con significati diversi.

Quando gli *hacker* interagiscono e formano un gruppo sociale, si organizzano intorno a valori etici: l'etica sociale di quel gruppo. Ci si domanda se esista un modo univoco di intendere l'espressione "etica *hacker*" come elemento caratterizzante i sistemi sociali, tecnologici e culturali che fanno riferimento al termine *hacker*. Si osserva come esistano diversi modi di intendere l'etica *hacker* e come le radici dei valori etici dei gruppi di *hacker*, a volte, dipendono da caratteristiche antropologiche e da fenomeni culturali profondamente radicati nella nostra storia e più antichi dell'*hacking* tecnologico.

### Hacker Ethics?

As digital technologies developed, groups of people calling themselves hackers arose. Today the term *hacker* is used to identify people connected to digital technologies with different meanings.

When hackers interact and form a social group, they organize themselves around ethical values: the social ethics of that group. The question is whether there is only one way of understanding the expression "*hacker ethics*" as a characterizing element of the social, technological and cultural systems that refer to the term *hacker*. It is observed that there are different ways of understanding *hacker* ethics and that the roots of the ethical values of *hacker* groups sometimes depend on anthropological characteristics and cultural phenomena deeply rooted in our history and more ancient than technological *hacking*.

Published 21 August 2020

Correspondence should be addressed to Marco Ciurcina, StudioLegale.it, Via San Quintino n. 32. Email: [ciurcina@studiolegale.it](mailto:ciurcina@studiolegale.it)

*DigitCult, Scientific Journal on Digital Cultures* is an academic journal of international scope, peer-reviewed and open access, aiming to value international research and to present current debate on digital culture, technological innovation and social change. ISSN: 2531-5994. URL: <http://www.digitcult.it>

Copyright rests with the authors. This work is released under a Creative Commons Attribution (IT) Licence, version 3.0. For details please see <http://creativecommons.org/licenses/by/3.0/it/>



## Introduzione

Il termine hacker è molto comune nelle comunità di persone che si occupano di tecnologie digitali e di internet. Eppure, spesso, il termine viene inteso con sfumature diverse. Se poi si guarda al modo in cui viene inteso nei media, le sfumate differenze di significato diventano profonde dissonanze; così, a seconda dei casi, l'hacker può essere il losco figuro che viola sistemi informativi con intenti criminali oppure l'attivista motivato da ragioni ideali e che, a volte, si sacrifica per il bene dell'umanità.

### Hacking, hacker e tecnologia

La parola *hack*, in inglese, ha diversi significati. Per esempio è *hack* l'atto di tagliare a pezzi con l'accetta (*hack* è anche il nome dello strumento); o anche, il gestire con successo un'attività<sup>1</sup>.

Da tempo, e ancora oggi, al MIT di Boston la parola *hack* è utilizzata per riferirsi ad attività varie e a scherzi che dimostrano abilità e intelligenza<sup>2</sup>; l'esplorazione non autorizzata di tetti e tunnel è una pratica che già negli anni '20 veniva definita *hacking*<sup>3</sup>. Ma è negli anni '60 che l'uso delle parole *hack*, *hacking*<sup>4</sup> e *hacker* inizia ad essere più direttamente associata a chi svolge attività legate ai computer e al software. In quegli anni, negli Stati Uniti, a partire dal MIT di Boston, si iniziano a formare gruppi di persone che condividono la passione per i computer e si definiscono espressamente *hacker*<sup>5</sup>.

Secondo Levy (Levy 2002) il primo nucleo di persone che dà forma alla cultura *hacker* nel nuovo senso del termine (attività legate a computer e/o software) si costituisce dopo gli anni '50 nel quadro del *Tech Model Railroad Club*<sup>6</sup>, l'associazione studentesca presso il MIT fondata nel 1946<sup>7</sup>. In quel contesto *hacker* è "qualcuno che applica l'ingegnosità per creare un risultato intelligente, chiamato "hack". L'essenza di un "hack" è che viene fatto rapidamente e di solito non è elegante. Raggiunge l'obiettivo desiderato senza cambiare il design del sistema in cui è incorporato. Nonostante sia spesso in contrasto con il design del sistema più grande, un hack è generalmente abbastanza intelligente ed efficace."<sup>8</sup>.

Nel Laboratorio d'Intelligenza Artificiale del MIT<sup>9</sup>, frequentato anche da Richard M. Stallman<sup>10</sup>, autore della definizione di "software libero"<sup>11</sup>, la cultura *hacker* trova un altro centro di sviluppo molto importante.

Successivamente, mentre i computer e il software si diffondono, la cultura *hacker*<sup>12</sup> penetra e si radica nelle comunità di appassionati di computer e software che si formano negli Stati Uniti d'America. È doveroso citare l'*Homebrew Computer Club*<sup>13</sup>, un gruppo informale di appassionati di computer e amanti del "fai da te" che iniziò a riunirsi a Menlo Park nel 1975. Negli anni '80 si diffondono gruppi di *hacker* che, mano a mano che gli anni passano, condividono la passione per il software in ambiti sempre più vari.

Stephen Levy nel suo libro "*Hackers. Gli eroi della rivoluzione informatica*" (Levy 2002) offre una ricostruzione dettagliata delle vicende e delle persone che hanno caratterizzato il sorgere e lo sviluppo della cultura *hacker* dalle origini ai primi anni '80<sup>14</sup>. La prima edizione del libro si chiude con il capitolo "*L'ultimo dei veri hacker*" dedicato a Richard M. Stallman. Richard M. Stallman nel

<sup>1</sup> Vedi <https://www.merriam-webster.com/dictionary/hack>

<sup>2</sup> Vedi [https://en.wikipedia.org/wiki/Hacks\\_at\\_the\\_Massachusetts\\_Institute\\_of\\_Technology](https://en.wikipedia.org/wiki/Hacks_at_the_Massachusetts_Institute_of_Technology)

<sup>3</sup> Vedi [https://en.wikipedia.org/wiki/Room\\_and\\_tunnel\\_hacking](https://en.wikipedia.org/wiki/Room_and_tunnel_hacking)

<sup>4</sup> Vedi <https://it.m.wikipedia.org/wiki/Hacking>

<sup>5</sup> Vedi <https://en.wikipedia.org/wiki/Hacker> e <https://it.wikipedia.org/wiki/Hacker>

<sup>6</sup> Vedi [https://en.wikipedia.org/wiki/Tech\\_Model\\_Railroad\\_Club](https://en.wikipedia.org/wiki/Tech_Model_Railroad_Club)

<sup>7</sup> Vedi <https://web.archive.org/web/20060503072049/http://tmrc.mit.edu/hackers-ref.html>

<sup>8</sup> Vedi <https://web.archive.org/web/20060503072049/http://tmrc.mit.edu/hackers-ref.html>

<sup>9</sup> Vedi [https://en.wikipedia.org/wiki/MIT\\_Computer\\_Science\\_and\\_Artificial\\_Intelligence\\_Laboratory](https://en.wikipedia.org/wiki/MIT_Computer_Science_and_Artificial_Intelligence_Laboratory)

<sup>10</sup> Vedi [https://it.wikipedia.org/wiki/Richard\\_Stallman](https://it.wikipedia.org/wiki/Richard_Stallman)

<sup>11</sup> Vedi <http://www.gnu.org/philosophy/free-sw.it.html>

<sup>12</sup> Vedi [https://en.wikipedia.org/wiki/Hacker\\_culture](https://en.wikipedia.org/wiki/Hacker_culture) e [https://it.wikipedia.org/wiki/Cultura\\_hacker](https://it.wikipedia.org/wiki/Cultura_hacker)

<sup>13</sup> Vedi [https://en.wikipedia.org/wiki/Homebrew\\_Computer\\_Club](https://en.wikipedia.org/wiki/Homebrew_Computer_Club)

<sup>14</sup> La prima edizione del libro è del 1984.

1983 lancia il Progetto *GNU*<sup>15</sup>, con l'intento di sviluppare un sistema operativo in software libero, e nel 1989 scrive la prima versione della licenza *copyleft*<sup>16</sup> GNU General Public License (detta anche GNU-GPL)<sup>17</sup>.

Il diffondersi del software libero segna un passaggio importante nella storia della cultura *hacker*. Le licenze di software libero permettono agli utenti di accedere al codice sorgente consentendo di usare il programma, studiarlo, modificarlo e distribuirlo: favoriscono l'accesso all'informazione che è un elemento centrale nella cultura *hacker*. Mano a mano che si diffondono, le licenze di software libero diventano sempre più conosciute e si dimostrano strumenti efficaci per creare fiducia tra le persone coinvolte (i membri dei progetti di sviluppo e i terzi utilizzatori) e, col trascorrere del tempo, sempre più comunità di sviluppatori si organizzano per collaborare nello sviluppo di software che distribuiscono con una licenza di software libero.

Il crescente diffondersi di internet accelera il processo di organizzazione delle comunità di *hacker* che sviluppano software libero: nel tempo, si raffinano tecnologie che favoriscono lo sviluppo collaborativo del software (sistemi che permettono il controllo delle versioni, la segnalazione di bug, ecc.) in modi coerenti col principio del libero flusso dell'informazione, al cuore della cultura *hacker*. Diventa quindi sempre più facile organizzare la collaborazione di gruppi di persone intorno ad attività di sviluppo di software e lo sviluppo di software libero si dimostra un'attività naturalmente idonea ad aggregare gruppi di *hacker*.

Nel 1998 un gruppo di appassionati fonda la *Open Source Initiative*<sup>18</sup> con lo scopo dichiarato di evitare l'enfasi sugli aspetti etici del software libero che, a loro dire, ostacola la comprensione e l'uso del software libero da parte dell'industria informatica. Utilizzano quindi l'espressione "*open source*" e adottano la *Open Source Definition*<sup>19</sup>. L'espressione *Open Source* enfatizza il requisito dell'accesso al software in formato anche sorgente: l'*Open Source Initiative* mette in sordina gli aspetti etici e punta l'attenzione sul modello di sviluppo del software.

Nel sito del progetto GNU è pubblicato un elenco di licenze che rispettano i criteri della definizione di software libero<sup>20</sup> e in quello dell'*Open Source Initiative* un elenco di licenze<sup>21</sup> che soddisfano i criteri dell'*Open Source Definition*. Anche se le due definizioni sono formulate in modo diverso, hanno lo stesso obiettivo: identificare le licenze che favoriscono l'uso, la condivisione, lo studio e la modifica del software. È un dato di fatto che gli elenchi di licenze compatibili con le due definizioni sono in gran parte coincidenti (fatta eccezione per alcuni casi)<sup>22</sup>.

Col trascorrere degli anni, l'uso dei computer e le comunità di sviluppo di software libero si diffondono nel mondo. Si moltiplicano quindi i gruppi di persone che si definiscono *hacker* e si organizzano intorno a specifici interessi e obiettivi. Questi gruppi sono partecipati in ambiti sociali, culturali e territoriali sempre più lontani dal luogo d'origine della cultura *hacker*. Nel tempo quindi sono sempre più numerosi e vari i gruppi di persone che, nutrendosi della parola iconica originaria, fanno propria la definizione di *hacker*, reinterpretandola e adattandola alle circostanze e al contesto nel quale si trovano.

Intanto si moltiplicano i casi nei quali degli *hacker* commettono degli illeciti che, col crescere di valore delle attività svolte mediante sistemi informativi, diventano sempre più rilevanti: l'"*intenzionale cecità*" delle origini<sup>23</sup> si fa strada in alcune comunità *hacker* ed è causa del "giro di vite contro gli *hacker*" descritto da Sterling nel suo libro (Sterling 2004) che racconta vicende che si svolgono nei primi anni '90. La nuova figura dell'*hacker* criminale (da molti definito *cracker*, per distinguerlo dall'*hacker*) si è ormai fatta spazio nei media e ancora oggi quest'accezione è quella prevalente per il grande pubblico.

<sup>15</sup> Vedi <https://en.wikipedia.org/wiki/GNU>

<sup>16</sup> Sono *copyleft* le licenze che includono una clausola per la quale chi modifica e redistribuisce il software licenziato secondo la licenza *copyleft* è tenuto a distribuire la versione modificata secondo i termini della stessa licenza o di altra compatibile. La parola "*copyleft*" esprime un gioco di parole.

<sup>17</sup> Alla quale è seguita una seconda versione del 1991 e una terza del 2007.

<sup>18</sup> Vedi <http://www.opensource.org>

<sup>19</sup> Vedi [http://www.opensource.org/docs/definition\\_plain.php](http://www.opensource.org/docs/definition_plain.php)

<sup>20</sup> Vedi <https://www.gnu.org/licenses/license-list.html>

<sup>21</sup> Vedi <https://opensource.org/licenses>

<sup>22</sup> Vedi [https://en.wikipedia.org/wiki/Comparison\\_of\\_free\\_and\\_open-source\\_software\\_licenses#Approvals](https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses#Approvals)

<sup>23</sup> Levy ricorda il *Midnight requisitoring committee* del *Tech Model Railroad Club*, preposto ad organizzare attività notturne di reperimento dei componenti necessari allo svolgimento delle attività del club (Levy, 2002, p. 35).

Così si arriva ai nostri giorni nei quali, in astratto, è *hacker* chi è capace di usare i sistemi informativi con grande perizia, ma, in concreto, quando si usa il termine *hacker* ci si riferisce a figure diverse a seconda dei casi e del contesto. Per i media *mainstream* è *hacker* il losco figura che viola sistemi informativi con intenti criminali o il membro di *Anonymous* (un gruppo internazionale di attivisti decentralizzato che mette in atto azioni di attacco cibernetico<sup>24</sup>). Molti *hacker* sono motivati da ragioni ideali, come Richard M. Stallman<sup>25</sup> o Aaron Swartz<sup>26</sup>. Alcuni *hacker* hanno consapevolmente compiuto atti illegali perché ritenevano giusto farlo per il bene della società. Per esempio, Julian Assange<sup>27</sup>, il creatore del progetto *Wikileaks*<sup>28</sup>, che sul finire degli anni ottanta è membro di un gruppo di *hacker* noto come *International Subversives* (“Sovversivi internazionali”) con lo pseudonimo di “Mendax”. Ancora, Edward Snowden<sup>29</sup>, l’autore delle rivelazioni sulle pratiche di sorveglianza di massa dell’NSA, che nel suo libro (Snowden 2019) dedica un capitolo a spiegare cosa intende per “essere *hacker*”.

La figura dell’*hacker* nel tempo ha ottenuto visibilità in ambiti sociali sempre più vari e oggi ci sono molti gruppi che scelgono di qualificarsi *hacker* e che svolgono attività in ambiti molto lontani dalle comunità che diedero origine alla figura dell’*hacker* descritto da Levy, come per esempio gruppi di appassionati del “fai da te” in agricoltura<sup>30</sup>.

È certo che sono frutto dalle idee condivise nelle comunità *hacker* alcune scelte importanti che hanno determinato la storia dell’informatica. Richard M. Stallman dice “*Questa è la base per il movimento del software libero - l’esperienza che ho avuto, la vita che ho vissuto al laboratorio di intelligenza artificiale del MIT - per lavorare sulla conoscenza umana e non ostacolare l’ulteriore utilizzo di nessuno e diffondere ulteriormente la conoscenza umana*”<sup>31</sup>. Steve Jobs e Steve Wozniak, fondatori della Apple Computer Company (ora Apple Inc.)<sup>32</sup>, erano tra i fondatori dell’*Homebrew Computer Club* e Steve Wozniak attribuisce a quegli incontri l’ispirazione per progettare l’Apple I<sup>33</sup>.

## Storia dell’etica hacker

In questo articolo si utilizza la nozione di etica nel senso di insieme di norme e valori di un gruppo di persone, o etica sociale. L’etica sociale di un gruppo costituisce il collante di quel gruppo ed è una mediazione delle etiche soggettive dei suoi membri, frutto delle dinamiche d’interazione tra i componenti del gruppo. A volte l’etica sociale di un gruppo prende la forma di un documento (codice di deontologia, manifesto, o altro); ma i documenti di questo tipo possono non riflettere in modo accurato l’etica sociale del gruppo al quale si riferiscono, soprattutto quando non cambiano nel tempo.

La cultura *hacker* è poliedrica e si evolve nel tempo; è inevitabile che l’etica *hacker* segua la stessa sorte. Dalle articolate vicende delle comunità *hacker* discendono idee diverse su cosa si debba intendere per etica *hacker*<sup>34</sup>. Da comunità diverse, composte da persone diverse, con un retroterra culturale diverso e lontane nel tempo, derivano inevitabilmente insiemi etici (norme e valori) almeno parzialmente diversi.

Per approfondire la nozione di etica *hacker* nei luoghi in cui la cultura *hacker* è nata, è utile iniziare ricordando la *Hacking Etiquette* (galateo dell’*hacking*), riprodotta in un cartello presente

<sup>24</sup> Vedi [https://en.wikipedia.org/wiki/Anonymous\\_\(group\)](https://en.wikipedia.org/wiki/Anonymous_(group))

<sup>25</sup> Vedi [https://it.wikipedia.org/wiki/Richard\\_Stallman](https://it.wikipedia.org/wiki/Richard_Stallman)

<sup>26</sup> Vedi [https://en.wikipedia.org/wiki/Aaron\\_Swartz](https://en.wikipedia.org/wiki/Aaron_Swartz)

<sup>27</sup> Vedi [https://it.wikipedia.org/wiki/Julian\\_Assange](https://it.wikipedia.org/wiki/Julian_Assange)

<sup>28</sup> Vedi <https://it.wikipedia.org/wiki/WikiLeaks>

<sup>29</sup> Vedi [https://it.wikipedia.org/wiki/Edward\\_Snowden](https://it.wikipedia.org/wiki/Edward_Snowden)

<sup>30</sup> Vedi per esempio Farm Hack, una comunità internazionale che si propone lo sviluppo e la condivisione di strumenti per un’agricoltura basata sulla condivisione delle conoscenze e sulla ricerca collaborativa (<https://farmhack.org>).

<sup>31</sup> Vedi <https://www.gnu.org/gnu/rms-lisp.html>

<sup>32</sup> Vedi [https://en.wikipedia.org/wiki/Apple\\_Inc](https://en.wikipedia.org/wiki/Apple_Inc)

<sup>33</sup> Vedi [https://en.wikipedia.org/wiki/Homebrew\\_Computer\\_Club#cite\\_ref-6](https://en.wikipedia.org/wiki/Homebrew_Computer_Club#cite_ref-6)

<sup>34</sup> Vedi [https://en.wikipedia.org/wiki/Hacker\\_ethic](https://en.wikipedia.org/wiki/Hacker_ethic) e [https://it.wikipedia.org/wiki/Etica\\_hacker](https://it.wikipedia.org/wiki/Etica_hacker)

all'ingresso del *Ray and Maria Stata Center* del MIT, che riporta undici regole sviluppate dalla comunità *hacker* studentesca<sup>35</sup>:

1. *Sta' attento: la tua sicurezza, la sicurezza degli altri e la sicurezza di chiunque tu stia hackerando non dovrebbero mai essere compromesse.*
2. *Sii sottile: non lasciare alcuna prova che tu sia mai stato lì.*
3. *Lascia le cose come le hai trovate, o meglio.*
4. *Se trovi qualcosa di rotto, chiama F-IXIT [il numero interno per segnalare problemi alle infrastrutture].*
5. *Non lasciare danni.*
6. *Non rubare nulla.*
7. *La forza bruta è l'ultima risorsa degli incompetenti.*
8. *Non hackerare sotto l'effetto di alcool o droghe.*
9. *Non far cadere oggetti (da un edificio) senza personale di terra.*
10. *Non hackerare da solo.*
11. *Soprattutto, fa' uso del tuo buon senso*<sup>3</sup>.

La comunità *hacker* studentesca del MIT è centrata sugli aspetti goliardici dell'essere *hacker* e svolge attività non necessariamente legate a computer e software. Ma il documento è utile per avere contezza del retroterra culturale nel quale prende forma la nozione di *hacker* più specificamente connessa alle tecnologie informatiche.

Stephen Levy nel suo libro centrato sulle vicende delle prime comunità *hacker* informatiche (Levy, 2002) offre una descrizione dell'etica *hacker* che ha certamente contribuito a rendere popolare l'idea che esista un'etica *hacker*. Nella prefazione (Levy 2002, 9) così sintetizza l'etica *hacker*: "È una filosofia di socializzazione, di apertura, di decentralizzazione e del mettere le mani sulle macchine a qualunque costo, per migliorarle e per migliorare il mondo".

Nel secondo capitolo del suo libro (Levy 2002, 34-42) approfondisce i principi dell'etica *hacker* che descrive come segue.

"L'accesso ai computer - e tutto ciò che potrebbe insegnare qualcosa su come funziona il mondo - dev'essere assolutamente illimitato e completo. Dare sempre precedenza all'imperativo di metterci su le mani!"; l'*hacker* deve seguire il suo istinto di correggere i difetti e migliorare le cose (computer e software, innanzitutto).

"Tutta l'informazione deve essere libera"; quando un *hacker* risolve un difetto o migliora un sistema, quella soluzione deve essere a disposizione di tutti.

"Dubitare dell'autorità. Promuovere il decentramento"; la burocrazia (industriale, governativa o universitaria) e qualunque sistema che impedisce l'accesso all'informazione va guardato con sospetto.

"Gli *hacker* dovranno essere giudicati per il loro operato, e non sulla base di falsi criteri quali ceto, età, razza o posizione sociale"; gli *hacker* sono meritocratici e questo beneficia la comunità *hacker* nel suo complesso.

"Con un computer puoi creare arte"; un programma non è apprezzato solo per la sua funzionalità, ma anche per la sua estetica e, per esempio, la capacità di scrivere un programma per svolgere una funzione nel minor numero possibile di righe è ammirata.

"I computer possono cambiarti la vita in meglio"; gli *hacker* credono che i computer possono migliorare la vita a se stessi e a tutti gli esseri umani.

*The Conscience of an Hacker* scritto l'8 gennaio 1986<sup>36</sup> dal giovane Loyd Blankenship<sup>37</sup> (Mentor 1986), poco dopo il suo arresto, indica gli elementi principali dell'etica *hacker* (socialità, rifiuto dell'autorità, uguaglianza, curiosità e accesso all'informazione) e, allo stesso tempo, offre spunti per osservare più da vicino l'altro lato della medaglia: il percorso psicologico che può avvicinare l'*hacker* all'atto criminale.

Il libro di Pekka Himanen (Himanen 2003) ha il merito di arricchire la prospettiva sul tema dell'etica *hacker* (che per l'autore è incentrata su passione, impegno, creatività e gioia nella creazione) individuandovi i semi di un'etica del lavoro che sfida l'etica del lavoro protestante. A

<sup>35</sup> Vedi <https://web.archive.org/web/20150710113854/http://studentlife.mit.edu/mindandhandbook/policies/hacking>

<sup>36</sup> Vedi <http://phrack.org/issues/7/3.html>

<sup>37</sup> Che si firma The Mentor; vedi [https://it.m.wikipedia.org/wiki/The\\_Mentor](https://it.m.wikipedia.org/wiki/The_Mentor)

distanza di 20 anni si iniziano a vedere alcuni cambiamenti interessanti alla luce dell'intuizione di Himanen. Oggi molte industrie informatiche distribuiscono software libero, usano sistemi per la gestione dello sviluppo collaborativo del software pensati da e per le comunità di software libero e fanno dell'interazione con le comunità di sviluppatori un obiettivo esplicito<sup>38</sup>. È interessante osservare che Steve Balmer, ex CEO di Microsoft, nel 2001 affermava "Linux è un cancro che si attacca a tutto ciò che tocca nel senso della proprietà intellettuale"<sup>39</sup> mentre nel 2014 Satya Nadella, attuale CEO di Microsoft, dichiarava "Microsoft ama Linux"<sup>40</sup>. È certo che l'industria del software ha imparato a lavorare secondo le regole del software libero e ad utilizzarlo per trarne profitto, anche se non si può dire che il processo abbia completamente esaurito il suo percorso o che l'intuizione di Himanen sia una predizione avverata: se l'etica del lavoro protestante sarà superata dall'interazione con l'etica *hacker* lo potremo giudicare tra un po' di tempo.

Eric Raymond, uno dei fondatori dell'*Open Source Initiative*<sup>41</sup>, collega in modo esplicito l'*open source* e la sua azione alla cultura *hacker*<sup>42</sup>. In effetti, l'idea di software libero è centrata su scelte etiche. Dice Richard M. Stallman: "Il mio lavoro sul software libero è motivato da un obiettivo ideale: diffondere la libertà e la cooperazione. Voglio incoraggiare la diffusione del software libero sostituendolo al software proprietario che proibisce la cooperazione, e quindi rendere la nostra società migliore."<sup>43</sup>

È quindi interessante rilevare che lo stesso Stallman rifiuta di collegare il software libero a supposti valori etici *hacker* e contesta l'idea che dei principi etici siano al cuore dell'essere *hacker*. "Concordo con la persona che ha affermato che non esiste un'etica hacker, ma piuttosto un'estetica hacker"<sup>44</sup>, dice. Ancora, definisce l'*hacking* come l'attività di "esplorare i limiti di ciò che è possibile in uno spirito di giocosa intelligenza"<sup>45</sup>. La posizione di Stallman è che essere *hacker* non implica necessariamente avere una specifica etica. Pare quindi che Stallman non concordi con Raymond quando questi afferma che Stallman abbia la pretesa "di definire e guidare la comunità degli hacker con la bandiera del software libero"<sup>46</sup>. È però vero che gruppi di persone

<sup>38</sup> Ad oggi, la penetrazione del software libero non è invece ugualmente efficace nelle istituzioni pubbliche, anche se negli ultimi anni si iniziano a percepire i segni d'un cambiamento in corso.

<sup>39</sup> Vedi [https://www.theregister.com/2001/06/02/balmer\\_linux\\_is\\_a\\_cancer/](https://www.theregister.com/2001/06/02/balmer_linux_is_a_cancer/)

<sup>40</sup> Vedi [https://www.theregister.com/2014/10/20/microsoft\\_cloud\\_event/](https://www.theregister.com/2014/10/20/microsoft_cloud_event/)

<sup>41</sup> Vedi <http://www.opensource.org>

<sup>42</sup> Si ricordano gli articoli *How To Become A Hacker* (vedi <http://www.catb.org/~esr/faqs/hacker-howto.html>), *A Brief History of Hackerdom* (vedi <http://www.catb.org/~esr/writings/hacker-history/>) e *The Revenge of the Hackers* (vedi <http://www.catb.org/~esr/faqs/hacker-revenge.html>). Eric Raymond è anche stato editore del *Jargon File* (vedi <http://www.catb.org/jargon/>), una raccolta di termini gergali utilizzati da varie sottoculture *hacker*.

In particolare, nell'articolo *How To Become A Hacker*, al paragrafo *Historical Note: Hacking, Open Source, and Free Software*, scrive:

"L'etica e la comunità degli hacker, come li ho descritti qui, precedono di molto l'emergere di Linux dopo il 1990; sono stato coinvolto per la prima volta intorno al 1976 e le sue radici sono facilmente rintracciabili nei primi anni '60. Ma prima di Linux, la maggior parte dell'*hacking* avveniva su sistemi operativi proprietari o su una manciata di sistemi nostrani quasi sperimentali come gli ITS del MIT che non venivano mai distribuiti al di fuori delle loro nicchie accademiche originali. Mentre c'erano stati alcuni tentativi precedenti (pre-Linux) di cambiare questa situazione, il loro impatto era nella migliore delle ipotesi molto marginale e limitato alle comunità di veri credenti dedicati che erano minuscole minoranze anche all'interno della comunità degli hacker, figuriamoci rispetto al mondo più vasto di software in generale.

Ciò che ora viene chiamato "open source" risale alla comunità degli hacker, ma fino al 1985 era una pratica popolare senza nome piuttosto che un movimento consapevole con teorie e manifesti collegati. Questa preistoria terminò quando, nel 1985, l'astuto hacker Richard Stallman ("RMS") tentò di dargli un nome: "software libero". Ma il suo atto di denominazione era anche un atto di rivendicazione; ha attaccato un bagaglio ideologico all'etichetta "software libero" che gran parte della comunità di hacker esistente non ha mai accettato. Di conseguenza, l'etichetta "software libero" è stata fortemente respinta da una sostanziale minoranza della comunità degli hacker (specialmente tra quelli associati a BSD Unix) e utilizzata con riserve serie ma silenziose dalla maggior parte del resto (incluso me stesso)."

<sup>43</sup> Vedi <https://www.fsf.org/licensing/essays/pragmatic.html>

<sup>44</sup> Vedi <https://www.gnu.org/philosophy/rms-hack.html>

<sup>45</sup> Vedi l'articolo *On hacking* alla pagina <https://stallman.org/articles/on-hacking.html>

<sup>46</sup> Nell'articolo di Eric Raymond (citato alla nota 22) *How To Become A Hacker*, al paragrafo *Historical Note: Hacking, Open Source, and Free Software*, si legge:

che si definiscono *hacker* e si riconoscono nel valore della libertà dell'informazione si organizzano intorno allo sviluppo di software libero / open source.

## Etica o etiche hacker?

Restano aperte alcune domande. Il rispetto delle norme è un valore dell'etica *hacker* o in certi casi è accettabile violare alcune norme? Che ruolo gioca nella nozione di etica *hacker* il fine di conseguire il bene per la società? Esiste un'etica *hacker* o esistono modi diversi di intendere l'espressione "etica *hacker*"?

Certamente la commissione di un illecito non è universalmente riconosciuta come di per sé idonea a causare la violazione dell'etica *hacker*, come dimostrano le vicende di Julian Assange e Edward Snowden. I due *hacker* hanno deliberatamente violato delle norme, almeno quelle di certi paesi, ma non per questo hanno subito un grave danno di reputazione, per lo meno nella gran parte delle comunità *hacker*. Ma certi comportamenti illeciti, perlomeno per certe comunità *hacker*, non sono accettabili e la loro violazione può determinare la stigmatizzazione del loro autore, almeno da parte di molti membri delle comunità *hacker*.

L'atteggiamento nei confronti del rispetto delle regole è un punto rispetto al quale le etiche sociali di diversi gruppi di *hacker* si differenziano. Ci sono gruppi che includono il rispetto delle norme tra i loro principi etici. Sono un chiaro esempio di ciò i gruppi di *hacker* che sviluppano software libero: le licenze di software libero funzionano proprio perché si basano sul rispetto delle norme (di diritto d'autore, ecc.), che rendono efficaci le stesse licenze. Ma ci sono gruppi che hanno posizioni diverse sul punto. Alcuni ritengono accettabile la violazione delle norme per realizzare il bene della società. Altri ritengono accettabile il comportamento dell'*hacker grey hat*<sup>47</sup>: colui il quale accede a un sistema illegalmente ma senza produrre danni.

Conforta in queste conclusioni il contenuto della voce etica *hacker* contenuta nel *Jargon File*<sup>48</sup>, edito da Eric Raymond:

*"1. La convinzione che la condivisione di informazioni sia un potente bene positivo e che sia un dovere etico degli hacker condividere le proprie competenze scrivendo codice open source e facilitando l'accesso alle informazioni e alle risorse informatiche ove possibile.*

*2. La convinzione che il cracking dei sistemi per divertimento ed esplorazione sia eticamente corretto fintanto che il cracker non commette furti, atti vandalici o violazione della riservatezza.*

*Entrambi questi principi etici normativi sono ampiamente, ma non universalmente, accettati tra gli hacker. La maggior parte degli hacker sottoscrive l'etica hacker nel senso 1, e molti agiscono su di essa scrivendo e distribuendo software open source. Alcuni vanno oltre e affermano che tutte le informazioni dovrebbero essere libere e che qualsiasi controllo proprietario delle stesse è negativo; questa è la filosofia alla base del progetto GNU.*

*Il senso 2 è più controverso: alcune persone ritengono che l'atto stesso del cracking non sia etico, come lo scassinare ed entrare. Ma la convinzione che il cracking "etico" escluda la*

---

*"Nonostante queste riserve, la pretesa di RMS di definire e guidare la comunità degli hacker con la bandiera "software libero" tenne ampiamente fino alla metà degli anni '90. Fu seriamente messa in discussione solo dall'ascesa di Linux. Linux ha dato allo sviluppo open source una casa naturale. Molti progetti pubblicati in termini che ora chiameremmo open source migrati da Unix proprietari a Linux. La comunità intorno a Linux è cresciuta in modo esplosivo, diventando molto più grande ed eterogenea della cultura degli hacker pre-Linux. RMS tentò risolutamente di cooptare tutta questa attività nel suo movimento di "software libero", ma fu contrastato sia dalla diversità esplosiva della comunità Linux sia dallo scetticismo pubblico del suo fondatore, Linus Torvalds. Torvalds continuò a usare il termine "software libero" per mancanza di alternative, ma pubblicamente respinse il bagaglio ideologico di RMS. Molti hacker più giovani hanno seguito l'esempio.*

[omissis]

*Il termine "open source", tuttavia, non era ancora emerso; non lo farebbe fino all'inizio del 1998. Quando lo fece, la maggior parte della comunità degli hacker lo adottò nei sei mesi successivi; le eccezioni erano una minoranza ideologicamente legata al termine "software libero". Dal 1998, e in particolare dopo circa il 2003, l'identificazione di "hacking" con "sviluppo open source (e software libero)" è diventata estremamente vicina. Oggi c'è poco senso nel tentativo di distinguere tra queste categorie e sembra improbabile che cambi in futuro."*

<sup>47</sup> Vedi [https://en.wikipedia.org/wiki/Grey\\_hat](https://en.wikipedia.org/wiki/Grey_hat)

<sup>48</sup> Vedi <http://www.catb.org/jargon/html/H/hacker-ethic.html>

*distruzione almeno modera il comportamento delle persone che si considerano cracker "benigni"...*

*La manifestazione più sicura di entrambe le versioni dell'etica hacker è che quasi tutti gli hacker sono attivamente disposti a condividere trucchi tecnici, software e (dove possibile) risorse informatiche con altri hacker. Enormi reti cooperative come Usenet, FidoNet e Internet stesso possono funzionare senza controllo centrale grazie a questa caratteristica; entrambi fanno affidamento e rafforzano il senso di comunità che può essere la risorsa immateriale più preziosa per gli hacker."*

La stessa voce etica *hacker* del *Jargon File* è anche utile per gettare luce sulle altre domande formulate sopra. Alla domanda su quale sia il ruolo che gioca nella definizione dell'etica *hacker* l'obiettivo di conseguire il bene per la società il *Jargon File* risponde che è sufficiente condividere conoscenze e codice sorgente, facilitando l'accesso alle informazioni "ove possibile" ma dà atto che per alcuni è necessario massimizzare quest'obiettivo: sull'interpretazione del termine "possibile" si distribuisce la gamma di posizioni assunte dalle diverse comunità *hacker* sul punto. Alla domanda se esista una sola etica *hacker* la risposta del *Jargon File* è negativa. Ci sono diversi modi di intendere l'etica *hacker*: la definizione ammette opzioni diverse sia rispetto alla condivisione delle informazioni che rispetto al *cracking* dei sistemi informativi. Su questo parrebbe quindi esservi convergenza tra gli esponenti principali del mondo del software libero e dell'*open source*: l'etica *hacker* non è univoca. Le divergenze iniziano subito dopo: secondo Eric Raymond ne esistono diverse varianti, secondo Richard M. Stallman non ne esiste nemmeno una e più che di etica *hacker* si deve parlare di estetica *hacker*.

## Le radici delle etiche *hacker*

Considerando la varietà di contesti (sociali, culturali, spaziali e temporali) nei quali è stata adottata la denominazione *hacker* è utile domandarsi da dove originano gli elementi delle etiche adottate dai diversi gruppi di appassionati di tecnologie informatiche che si formano nel mondo, a partire dagli anni '50 e '60 negli Stati Uniti.

Proprio per la varietà di contesti nei quali si sono manifestati, è ragionevole ritenere che i principali valori delle etiche *hacker* siano manifestazione, nelle specifiche circostanze, di valori più profondi che ne sono elementi costituenti e fattori generativi, che hanno traiettorie più antiche e che trovano nel tempo vettori di trasmissione fino ai nostri giorni.

Per esempio, l'idea che l'informazione e la conoscenza devono essere libere è antica e trova radici nel pensiero greco, nell'idea di Accademia, come luogo nel quale maestri e allievi condividono spazio e tempo per insegnare e imparare. L'idea è migrata fino ai nostri giorni attraverso la secolare storia delle università, nelle quali, appunto, l'idea della libertà della conoscenza è stata l'unico modello etico di riferimento fino a quando, a partire dagli anni '90, ha iniziato ad insinuarsi nelle università la possibilità di privatizzare i risultati dell'attività di ricerca<sup>49</sup>. Probabilmente non è un caso che le prime comunità *hacker* si siano sviluppate in ambito accademico.

D'altro canto, le metodologie di lavoro collaborativo raffinate nel tempo dalle comunità *hacker* che sono basate sul principio di libertà d'informazione e si concretizzano nella possibilità per tutti di testare, individuare errori e proporre correzioni, sono figlie del metodo scientifico che raccoglie ancora una volta l'eredità del pensiero greco (Russo 2017) e, attraverso il recupero operato nel rinascimento, giunge fino a noi attraverso i secoli. In questa prospettiva è anche interessante collegare i ragionamenti di Himanen sulla nuova etica del lavoro che emergerebbe nelle comunità *hacker* (Himanen 2004), con le riflessioni di Zerzan sulle caratteristiche dell'uomo cacciatore-raccogliitore che vive in comunità di eguali, dedica gran parte del suo tempo ad attività creative e ludiche ed è incline alla collaborazione (Zerzan 2004) o l'analisi condotta da Tomasello sull'origine della morale umana, che permette il formarsi di gruppi in grado d'esercitare un'intenzionalità collettiva (Tomasello 2016).

<sup>49</sup> Si fa risalire le origini di questa contaminazione culturale tra accademia e privatizzazione della conoscenza all'adozione del Bayh Dole Act nel 1980 negli Stati Uniti d'America (vedi [https://en.wikipedia.org/wiki/Bayh%E2%80%93Dole\\_Act](https://en.wikipedia.org/wiki/Bayh%E2%80%93Dole_Act)); oggi il modello si è diffuso in molte parti del mondo.

L'inclinazione per la socializzazione e la collaborazione, lo spirito giocoso dell'essere *hacker*, il rifiuto dell'autorità e il favore per la decentralizzazione, in un certo senso, restituiscono la possibilità di interagire con successo in comunità tra pari ricreando le condizioni sociali nelle quali vivevano i nostri antenati fino a 10.000 anni fa, prima che la società agricola ingabbiasse gli esseri umani in strutture gerarchiche e di potere: si potrebbe dire che l'*hacker* è l'uomo cacciatore-raccogliatore che ritorna. In questo senso offre spunti suggestivi il lavoro di Tomasello che descrive le caratteristiche di cognizione e socialità unicamente umane (Tomasello 2019). Probabilmente, i valori *hacker* rispondono ad istanze antropologiche che le strutture della società agricola e industriale non soddisfano pienamente e che nel contesto delle reti telematiche trovano spazio per manifestarsi in nuovi modi che si dimostrano efficienti ed efficaci.

## Conclusioni

La parola *hacker* ha indubbiamente avuto successo: negli ultimi decenni è utilizzata in misura crescente per descrivere uno spazio culturale nel quale agiscono persone e valori etici, a volte così distanti tra loro che è legittimo domandarsi se esista un'etica *hacker*.

Certamente esistono diverse etiche *hacker* nel senso sociale del termine (etica sulla quale si fonda un gruppo di persone) che hanno tratti in comune ma che possono divergere anche radicalmente. Socializzazione e libertà dell'informazione e della conoscenza sono il denominatore comune delle diverse etiche *hacker*: un insieme che mette in comunicazione gruppi disomogenei. Questi valori comuni sono figli di idee e valori molto più antichi della cultura *hacker*, che dipendono da caratteri profondamente radicati nella natura e nelle culture umane.

## References

- Berlinguer, Marco. *Commons, Markets and Public Policy*, Transform! ePaper, January 2020, [https://www.transform-network.net/fileadmin/user\\_upload/2020-01-commons\\_3.pdf](https://www.transform-network.net/fileadmin/user_upload/2020-01-commons_3.pdf)
- Ciurcina, Marco. "Licenze di software libero ed altre licenze libere: codice genetico di beni comuni digitali." *DigitCult | Scientific Journal on Digital Cultures 2.1* (2017). Available at <http://digitcultnew.lim.di.unimi.it/index.php/dc/article/view/26>. DOI <https://doi.org/10.4399/97888255045142>
- Coleman, Gabriela. *Coding freedom: the ethics and aesthetics of hacking*. Princeton University Press, 2013. Available at <http://gabriellacoleman.org/Coleman-Coding-Freedom.pdf>
- Evangelista, Rafael. *Beyond machines of loving grace: Hacker culture, cybernetics and democracy*. Edições Sesc, Coleção Democracia Digital, 2018.
- Himanen, Pekka. *L'etica hacker e lo spirito dell'età dell'informazione*. Feltrinelli, 2003.
- Levy, Steven. *Hackers. Gli eroi della rivoluzione informatica*. Shake Editore, 2002.
- Russo, Lucio. *La rivoluzione dimenticata. Il pensiero scientifico greco e la scienza moderna*. Feltrinelli, 2017.
- Snowden, Edward. *Errore di sistema*. Milano: Longanesi & C., 2009.
- Sterling, Bruce. *Giro di vite contro gli hacker*. Shake Editore, 2004.
- The Mentor. "The Conscience of an Hacker." *Phrack 7* (1986). Available at <http://phrack.org/issues/7/3.html#article>
- Tomasello, Michael. *Diventare umani*. Milano: Raffaello Cortina Editore, 2019.
- Tomasello, Michael. *Storia naturale della morale umana*. Milano: Raffaello Cortina Editore, 2016.
- Zerzan, John. *Primitivo attuale. Il rifiuto della civiltà*. Roma: Stampa Alternativa, 2004.