Hackers

Dal Sessantotto californiano alla rivoluzione informatica

<<Dopo tutto, se Alexander Graham Bell avesse seguito le regole della compagnia telefonica Western Union, non ci sarebbero stati telefoni. Se Jobs e Wozniak avessero creduto che la Ibm fosse l'inizio e la fine di tutto, non ci sarebbero stati personal computer. Se Benjamin Franklin e Thomas Jefferson avessero cercato di "lavorare all'interno del sistema" gli Stati Uniti non sarebbero mai nati>>

Bruce Sterling, *The Hacker crack down*

Questo volumetto, che non ha pretese di originalità ma è solo una breve introduzione ad un tema ampio e complesso, è pensato per esser compreso anche da profani o quasi profani del computer. Non so se lo leggerà e capirà anche la mia piccola Guo Irene, che ha 8 anni, ma comunque le dedico l'insegnamento fondamentale degli hackers: se sei bravo a fare una cosa, non chiederti a cosa serve. Falla e basta, il meglio possibile, e falla solo per te stesso. Se poi al mondo serve e diventi ricco, tanto meglio…sennò chissenefrega.

Chi sono mai questi hackers?

15 gennaio 1990: per tutto il pomeriggio, in gran parte degli Stati Uniti, i telefoni restarono muti. Questo gigantesco black out telefonico, uno dei più estesi della storia, fu conseguente al collasso del sistema di commutazione delle chiamate a lunga distanza della AT&T. Le autorità statunitensi puntarono immediatamente il dito contro i cosiddetti *hackers*, scatenando un'ondata di arresti e dando inizio ad una feroce politica repressiva nei loro confronti (Bruce Sterling ha raccontato magistralmente questi eventi, di fatto la prima vera guerra contro gli hackers, nel libro del 1992 *The Hacker Crackdown,* uscito poi in Italia nel 1993 col titolo *Giro di vite contro gli hackers*).

All'epoca il termine *hacker* non era diffuso come oggi, ma poco è cambiato: anche se è ora sulla bocca di tutti, di questa parola ben pochi conoscono il reale significato e altrettanto sconosciuta rimane ai più la storia di quello che, semplificando molto, potremmo definire il "movimento" degli hackers. E' almeno da quel 15 gennaio 1990 che si tende ad identificare gli hackers con criminali, basti pensare alle recentissime reciproche accuse tra Usa e Russia di utilizzare hackers al fine di portare veri e propri attacchi informatici all'antagonista, magari per creare disinformazione, rubare dati, manipolare esiti elettorali. Non solo: gli hackers vengono spesso associati, con semplicismo e superficialità, ad una serie di reati informatici in realtà molto diversi per genere e gravità, che vanno ad esempio dalla semplice pirateria (distribuzione o condivisione non autorizzata di materiale audiovisivo protetto da copyright) alle truffe online (sottrazione di dati personali o furti di denaro), fino alla creazione di supporti per la diffusione di materiale violento o pedopornografico. Cosa c'è di vero in tutto questo? Quali sono realmente i valori, gli scopi, il modo di agire di un *hacker*?

La stella che ci guida si chiama Altair

Alla fine del 1974 un certo Ed Roberts, titolare di una ditta di Albuquerque (New Mexico) chiamata Mits, che produceva principalmente orologi digitali e calcolatrici elettroniche, ebbe un'idea bizzarra: montare intorno ad un chip 8080 dell'Intel (chip che di solito veniva usato per far funzionare semafori o ascensori) un sistema di connessioni con una memoria e alcune porte di ingresso e

uscita dei dati. Questo strano oggetto, praticamente, si comportava come un computer, ma aveva due caratteristiche che lo rendevano completamente diverso da tutti i computer dell'epoca: era *piccolo* (le sue dimensioni non superavano quelle di una radio) e *non serviva a nulla*. La sua memoria-lavoro era di appena 256 bytes e, dopo averlo assemblato (veniva venduto in scatola di montaggio) si poteva procedere a inserire programmi di poche righe, il cui risultato sarebbe stato null'altro che il lampeggiamento dei led posti sulla sua parte anteriore: la risposta del computer.

A questo oggetto inutile e addirittura assurdo (chi poteva mai essere interessato a qualcosa che riproduceva nel funzionamento la logica dei computer, senza però avere alcuna delle loro effettive potenzialità?) Ed Roberts aveva dato il nome di Altair, una stella citata nella serie tv *Star Trek*. La Mits lo aveva messo in vendita a 397 dollari più spese di spedizione, un prezzo davvero incredibile se si pensa che, da solo, il chip 8080 costava normalmente 360 dollari. Roberts, tuttavia, aveva fatto una scommessa, assicurandosi una partita di 8080 alla cifra forfettaria di 75 dollari l'uno e sperando poi ovviamente di rientrare dei costi e guadagnare anche qualcosa dalla vendita degli *Altair*.

Nel gennaio del 1975 l'Altair era sulla copertina della rivista di riferimento degli hobbisti della West Coast californiana, *Popular Electronics.* Da quel momento, la Mits cominciò a ricevere anche 400 ordinazioni al giorno, e in poche settimane sul conto in banca dell'azienda (fino ad allora cronicamente in sofferenza) iniziarono ad entrare centinaia di migliaia di dollari. Gli appassionati di elettronica *adoravano* quell'inutile scatola, e nemmeno la palese falsità di molti annunci che ne accompagnarono l'uscita fermò il loro desiderio di averla subito (la Mits prometteva, ad esempio, di fornire "entro breve tempo" diverse periferiche, ma bisognerà aspettare fino al 1977 per vedere sul mercato un Altair dotato di stampante e interfaccia video). Agli acquirenti dell'Altair importava solo una cosa: poter *mettere le mani* su quell'oggetto, iniziare a lavorarci sopra per renderlo intelligente. Non si aspettavano che la Mits lo migliorasse per loro, anzi lo amavano proprio perché era grezzo e stupido, una massa informe di pongo che loro avrebbero modellato per farne un'opera d'arte.

Ed Roberts e la Mits avevano creato, con l'Altair, la base tecnologica (l'*hardware*) su cui mettere all'opera l'etica degli *hackers.* Ma gli hackers degli anni Settanta, che impareremo a conoscere meglio tra breve, costituivano in realtà la seconda generazione del "movimento": il termine *hacker* nacque all'interno del Mit (Massachusets Institute of Technology) più di vent'anni prima.

L'etica hacker

Tra la fine degli anni Cinquanta e l'inizio dei Sessanta, i computer erano mostri enormi, che occupavano intere stanze e necessitavano di sistemi di raffreddamento poderosi. L'accesso a quelle stanze era riservato a pochissimi e praticamente tutti gli studenti che arrivavano al Mit non avevano mai visto *dal vero* un computer in vita loro. Tutti però sapevano, o per lo meno intuivano, che il motivo per cui i computer venivano costruiti (nonché il motivo per cui questo tipo di tecnologia era particolarmente impiegata dai militari) era *la possibilità di possedere ed utilizzare un numero enorme di dati*. Il sogno dei più era arrivare nella *stanza dei bottoni*, diventare parte di quella ristretta casta che i computer li costruiva e li faceva funzionare; pochi altri, invece, avevano un sogno differente: *occupare la stanza dei bottoni* e trasformarla nel proprio parco giochi. Questi erano gli hackers.

Il termine *hack*, nel gergo goliardico del Mit, indicava originariamente uno scherzo o una burla particolarmente raffinati ed acuti, ma ben presto venne esteso a quelle imprese tecniche che mostrassero particolare virtuosismo o talento. Dato che l'accesso ai grandi computer del Mit era fortemente limitato per gli studenti, il problema non era soltanto *cosa* fare quando finalmente (magari alle 2 o 3 del mattino, unici orari disponibili) ci si sedeva alla consolle, ma anche *farlo in fretta*: ec-

co perché uno dei terreni su cui si sfidavano i primi *hackers* era scrivere programmi sempre più brevi a parità di prestazioni. Tra gli hackers, fin dalle origini, lo spirito di competizione fu ferocissimo ma anche molto leale: tutti dovevano avere pieno accesso allo *stato dell'arte*, perché la corsa al miglioramento non ammetteva passi indietro (il nastro perforato con le istruzioni dell'ultimo programma era sempre disponibile per chi volesse tentare di migliorarlo, nessuno si sarebbe mai sognato di tenerlo per sé o nasconderlo).

Steven Levy, che agli hackers ha dedicato un intero volume (*Hackers: gli eroi della rivoluzione informatica*, Shake, Milano, 1996) è convinto che l'*etica hacker* possa dirsi sostanzialmente già codificata nei primi anni Sessanta e che consti di sei punti fondamentali:

1)L'accesso ai computer dev'essere assolutamente illimitato e completo. Dare sempre la precedenza all'imperativo di metterci su le mani. Questa regola, che da sola potrebbe già riassumere tutte le altre, il vero hacker la applica a qualunque cosa, non soltanto al computer: qualsiasi oggetto può (e deve) essere manipolato ed eventualmente smontato per comprenderne il funzionamento ed essere poi trasformato in qualcosa di nuovo e migliore: se una persona o una legge impedisce loro di farlo, gli hackers automaticamente la detestano e si sentono autorizzati a violarla.

2)Tutta l'informazione dev'essere libera. Non ha senso scrivere tante versioni alternative di uno stesso programma: molto meglio perfezionare fino ai limiti del possibile quello che già esiste. Ovviamente, ciò implica di poter liberamente *conoscere* e *utilizzare* tutto ciò che di più avanzato viene scritto (software) o prodotto (hardware).

3)Dubitare dell'autorità. Promuovere il decentramento. Gli hackers non odiano le regole, ma odiano *le regole stupide e inutili* (in un universo di pensiero dove utile significa solo e sempre "utile al miglioramento tecnico" e mai "utile per finalità individuali") e, sopra ogni altra cosa, *odiano la burocrazia.* Non deve assolutamente esistere alcuna "autorità centrale" che filtri e padroneggi le informazioni: l'unica autorità che gli hackers rispettano è l'oggettivo ed imparziale interesse al progresso tecnologico.

4)Gli hackers dovranno essere giudicati per il loro operato, non sulla base di falsi criteri quali ceto, età, razza o posizione sociale. Questa è una logica conseguenza delle regole precedenti, sulla quale non c'è altro da dire.

5)Con un computer puoi creare arte. Per l'hacker il computer è un oggetto nel quale prendono forma la sapienza e la creatività umana. Non c'è nulla di *freddo* nei computer e, sebbene gli strumenti necessari per la loro creazione e programmazione siano discipline esatte come la matematica e la logica, l'*applicazione* di tali strumenti è multiforme e dipende esclusivamente dall'ingegno umano, inteso come insieme di valutazioni, emozioni, intuizioni. Per questo creare e perfezionare computer non è faccenda da burocrati della tecnologia, ma è appannaggio di pochi geni creativi, che non è scorretto definire artisti.

6) I computer possono cambiare la vita in meglio. Quest'ultima regola, come vedremo, diverrà pienamente operativa per gli hackers di seconda generazione. Ma anche i primi hackers del Mit intuivano che quel loro lavorare al di fuori e anche palesemente contro le regole avrebbe prodotto un miglioramento generalizzato nella vita umana, e comunque intanto aveva certamente migliorato la *loro* vita. Peter Samson, uno di quei geniali (forse il più geniale) hackers di prima generazione, disse negli anni Novanta: "L'abbiamo fatto al 30 per cento per l'amore di farlo, perché era qualcosa che potevamo fare e fare bene, e al 60 per cento per avere qualcosa che fosse a suo modo vivo, figlio nostro […] Una volta risolto un problema di errato comportamento del computer o del programma, l'hai risolto *per sempre*".

Nell'ambiente del Mit degli anni Cinquanta e Sessanta l'applicazione di questo tipo di etica portava certamente ai confini del lecito: non di rado gli hackers violavano intenzionalmente i regolamenti dell'istituto e anche la legge. C'erano vari gradi e varie sfumature nel comportamento degli hacker. In alcuni casi la trasgressione si limitava ad un utilizzo particolare e apparentemente "inutile" dei grandi computer come il Tx-0 o il successivo Pdp-1: Peter Samson, ad esempio, utilizzò nel 1962 proprio il "piccolo" Pdp-1 (rispetto al TX-0 piccolo lo era davvero, ma aveva sempre la dimensione di tre frigoriferi) per creare il primo gioco elettronico della storia, il leggendario *Spacewar*, che fece impazzire gli hackers, ma venne giudicato una stupida frivolezza dagli accademici e dai grandi produttori di computer. Nessuno, ufficialmente, poteva prenotare una sessione al Pdp-1 per giocare a *Spacewar*, ma di fatto ci fu chi passò talmente tante notti incollato a quel gioco…da scordarsi di prendere la laurea. Con *Spacewar* gli hackers si sfidarono sia per migliorare le caratteristiche del gioco, sia per primeggiare nel suo utilizzo.

Ma l'uso "distorto" (secondo il comune pensare) delle macchine non era tutto. Il *lock hacking*, ad esempio, consisteva nel forzare lucchetti o aprire porte con chiavi non proprie per accedere a stanze proibite agli studenti, mentre il *phone phreaking* (indubbiamente illegale) consisteva in una serie di pratiche volte a telefonare gratuitamente grazie a congegni quali le famose *blue box* (che riproducevano le frequenze per accedere alle linee interurbane e internazionali) o "semplicemente" rubando codici d'accesso. I sistemi telefonici avevano sempre affascinato gli hackers del Mit e, coerentemente con la propria particolare etica, molti di loro pensavano che il fatto di "capire" quei complicatissimi sistemi *anche meglio* degli ingegneri che li avevano creati, li legittimasse a servirsene per scopi sociali (libera comunicazione per tutti). Come ebbe a dire serenamente Alan Kotok, studente grassottello e letargico del Mit, mago della programmazione del Tx-0 e del Pdp-1, che aveva a lungo interrogato gli ingegneri della Western Electric durante l'estate in cui vi aveva lavorato e ne aveva capito (e carpito) i segreti: "Se c'era qualche debolezza nel sistema telefonico, un difetto di progetto col quale poter chiamare illegalmente, non mi tiravo indietro. Era un problema loro, non mio".

Un breve, intenso fuoco: il Sessantotto californiano

Tra gli hackers del Mit e la comparsa sul mercato dell'Altair si colloca quel vasto insieme di movimenti sociali e culturali che viene ricordato come Sessantotto, sebbene ovviamente copra un periodo decisamente più ampio di quel preciso anno. Negli Stati Uniti il cuore pulsante di quei movimenti fu senz'altro la California e, in particolare, l'università di Berkeley. Rispetto al Mit ci troviamo in un luogo geograficamente e anche culturalmente piuttosto distante (fu soltanto *dopo e grazie* alla seconda generazione degli hackers che la Silicon Valley divenne il cuore pulsante di una nuova rivoluzione tecnologica). Eppure non ci vuole molto a capire che il Sessantotto californiano rappresentava il brodo di coltura ideale per lo sviluppo (e che incredibile sviluppo!) dell'etica hacker.

Negli Stati Uniti il movimento del Sessantotto aveva ruotato attorno a poche, semplici, decisive questioni: la libertà di parola e di opinione, la lotta per i diritti civili dei neri, l'opposizione radicale alla guerra del Vietnam. Fu un movimento in larghissima misura studentesco e ciò non può certo stupire: la percentuale dei nati dopo la guerra che avevano accesso al mondo universitario era incomparabilmente più grande rispetto a quanto era stato per i loro genitori. E non era soltanto questo: oltre ad arrivare in maggior numero a frequentare l'università, i ragazzi e le ragazze potevano anche permettersi di rimanerci di più e non sentivano il peso di dover spendere immediatamente la propria laurea per trovare un buon impiego. L'economia era in continua crescita, non c'era nulla di più faci-

le che trovare un lavoro negli Usa degli anni Sessanta: ecco perché molti giovani potevano cambiare, durante gli studi o anche dopo la laurea, svariati lavoretti per mantenersi e rimanere a lungo in un limbo che permetteva loro di viaggiare, riflettere, divertirsi.

Prima del Sessantotto, la politica non entrava, non *doveva* entrare in alcun modo nei campus universitari. I primi movimenti radicali sorti nelle università (si pensi innanzitutto al mitico *Free Speech Movement*, nato a Berkeley nel 1964) rivendicavano innanzitutto il diritto degli studenti a poter parlare, *liberamente e pubblicamente*, di qualsiasi tematica all'interno dei campus. Il *free speech*, la libertà di parola, è d'altra parte un valore tipicamente americano: la rivolta culturale di questi ragazzi era in realtà un ritorno alle origini, un atto d'accusa verso l'ipocrisia e la falsità dei loro genitori (celeberrimo l'invito di Jerry Rubin, uno dei protagonisti del Sessantotto americano, a non fidarsi mai *di nessuno sopra i trentaquattro anni*). Il movimento non si nutriva di certezze dogmatiche, anzi veniva percepito come pericoloso proprio perché, costantemente, *seminava il* dubbio: il dubbio che la stessa dichiarazione d'Indipendenza, documento fondante dell'identità americana, fosse stata tradita prima dalla schiavitù e poi dalla discriminazione razziale; il dubbio che la supremazia del modello capitalistico americano non potesse imporsi al prezzo del sacrificio di migliaia di vite innocenti (guerra del Vietnam). Nei campus si poteva e doveva discutere di qualunque cosa, da argomenti di enorme respiro come quelli appena citati a questioni apparentemente meno essenziali come il superamento della rigida separazione degli ambienti riservati a maschi e femmine: il movimento spesso non distingueva tra sfera privata e pubblica, era insieme forma e contenuto, stile di vita e proposta socio-politica.

Il Sessantotto americano, a cui qui accenniamo soltanto con estrema superficialità, fu un fuoco intenso ma di breve durata: quando cessarono i cortei e la violenta repressione delle forze dell'ordine, quando la morte di John F. e poi di Bob Kennedy, di Martin Luther King e Malcom X mostrarono al mondo la brutalità e spietatezza della reazione, quando rifluirono le ondate di violenza nei ghetti neri delle grandi città, di quel fuoco era rimasto solo un cumulo di cenere. Ma sotto quella cenere, covava ancora qualcosa: lo spirito visionario e radicale che scatenò la corsa ad accaparrarsi l'Altair, ad esempio.

La base tecnologica per la rivolta

Dopo aver conosciuto la storia degli hackers del Mit, cominciamo ad intuire perché un oggetto come l'Altair riscosse immediatamente quel clamoroso ed imprevedibile successo. Immaginate cosa avrebbero dato personaggi come Peter Samson o Alan Kotok, disposti a forzare serrature o a prenotare per mesi sessioni di lavoro ad orari della notte impensabili al Tx-0 o al Pdp-1, per avere tra le mani un computer *piccolo*, sul quale poter operare *in qualunque momento* e *senza chiedere il permesso a nessuno*! E fate ora mente locale su un'altra questione: gli hackers al Mit erano, negli anni Cinquanta e Sessanta, una netta minoranza. Il loro spirito antiburocratico e antiautoritario cozzava con ciò che, essenzialmente, il Mit voleva essere: un'università ed un centro di ricerca avanzatissimo, ma legato a filo doppio a militari e grandi multinazionali. Gli hackers, in un certo senso, erano un corpo estraneo in quell'ambiente, dove il sogno di molti era arrivare ad indossare il perfetto, impeccabile camice bianco dei dipendenti dell'Ibm. La formazione culturale, gli interessi, i modelli di riferimento degli hobbisti californiani dei primi anni Settanta, invece, erano *perfetti* per portarli ad abbracciare l'etica hacker. Coloro che, con uno spontaneo gioco di squadra, nel giro di pochi mesi trasformarono il primo, grezzo Altair in una macchina con cui giocare, suonare e comunicare erano per la stragrande maggioranza reduci dall'esperienza del Sessantotto di Berkeley: visionari, sballati

e, soprattutto, irrimediabilmente anarchici, cercavano in quella scatoletta nient'altro che la *base tecnologica* per tentare nuovamente una rivolta sociale e culturale, dopo il fallimento di qualche anno prima.

I protagonisti

Non è possibile comprendere appieno quanto fin qui detto senza passare a parlare dei protagonisti, che non sono ovviamente solo le macchine, ma soprattutto le persone. Appena un anno prima che Ed Roberts lanciasse l'Altair, un certo Lee Felsenstein aveva fondato il *Community Memory (CM)*, una rete di attivisti che si proponeva di trasformare i computer in strumenti di relazione diretta ed informale tra le persone. Un'impresa tecno-politica perfettamente coerente con la sua biografia: nato nel 1945, figlio di un ingegnere comunista perseguitato durante il maccartismo, Felsenstein aveva studiato a sua volta ingegneria a Berkeley e, nell'inverno 1964-65, aveva militato nel *Free Speech Movement.* Nel 1968 aveva commentato per il giornale radicale *Berkeley Barb* le manifestazioni contro la chiamata di leva per la guerra in Vietnam, esprimendo opinioni favorevoli non solo verso chi "sfasciava le vetrine giuste" (non negozietti, ma banche), ma anche verso gli attentati dinamitardi contro alcuni uffici di leva.

Lee Felsenstein e i suoi amici del CM avevano avuto in prestito dall'organizzazione no-profit *Resource One* un vecchio mainframe computer, in precedenza dismesso dalla Transamerica Corporation. Questo obsoleto mostro, che richiedeva un impianto di raffreddamento da ventitré tonnellate ed occupava praticamente tutta la stanza dove Felsenstein viveva, venne collegato via telefono ad una telescrivente Model 33 donata dalla Tymshare Company, la quale fu poi posizionata nel negozio di dischi Leopold, nella zona universitaria di Berkeley. A creare il collegamento telefonico tra il "cervellone" e il "terminale stupido" fu Efrem Lipkin, un geniale hacker transfugo del Mit, che aveva abbandonato perché non sopportava la contaminazione dell'informatica con le faccende militari.

Il terminale di Leopold iniziò a funzionare come una vera e propria bacheca elettronica: la gente poteva lasciare messaggi di ogni tipo, fissare appuntamenti, vendere o barattare oggetti, ma anche regalare a chi volesse leggerli una poesia, un racconto, una riflessione politica…in piena coerenza con gli scopi della CM, insomma, quel terminale era un creatore e facilitatore di relazioni informali tra persone. E fu proprio grazie al terminale di Leopold che Lee Felsenstein incontrò Bob Marsh, personaggio con un *curriculum* non molto diverso dal suo: laureato in ingegneria a Berkeley, dedicava gran parte della propria vita all'insegnamento gratuito rivolto a bambini poveri e a coltivare una smodata passione per l'elettronica. Insieme a Gary Ingram, Marsh aveva fondato la *Processor Technology*, un'azienda a struttura socialista, dove tutti i dipendenti percepivano il medesimo stipendio di 800 dollari e che, inizialmente, produceva e vendeva componenti per l'Altair 8080.

Bob Marsh, attraverso il terminale di Leopold, assunse Felsenstein per fargli sviluppare una scheda video, che fu messa in commercio col nome di VDM-1 nel 1976; ma quello non era ancora nulla: durante lo sviluppo della VDM-1 Felsenstein e Marsh decisero che la *Processor Technology* era ormai pronta a costruire un computer completo, che venne in effetti assemblato da Felsenstein: nasceva il leggendario Sol Terminal Computer. Il nome di questa macchina era una dedica a Les Solomon, il talent scout di *Popular Electronics*, personaggio perlomeno bizzarro, che tanto per dire aveva combattuto con i sionisti di Begin in Palestina e aveva trascorso lunghi periodi di vita insieme agli indigeni dell'America Latina, prima di diventare direttore editoriale di quella rivista. La parti-

colarità del Sol, che inizialmente funzionava con la stessa scheda madre dell'Altair, era la compattezza: su un unico supporto erano stati montati tutti i componenti, compresa la tastiera e il monitor.

Felsenstein e Marsh, come già poco prima di loro Ed Roberts, non avevano un'idea precisa di ciò a cui *esattamente* l'oggetto da loro costruito sarebbe servito. Era un computer, dunque serviva a conservare ed elaborare dati, ma era anche *piccolo* e *non troppo costoso* (la prima versione costava 1350 dollari in scatola di montaggio o 1850 già montato): era un computer schierato dalla parte del popolo, uno strumento di diffusione orizzontale delle idee. John Lyle, l'eroe del romanzo fanta-anarchico *Rivolta 2100* di Robert Heinlein, adorato da Lee Felsenstein, sosteneva che *la segretezza fosse la chiave di volta di ogni dittatura.* Poter parlare liberamente di qualsiasi cosa, poter raggiungere ed essere raggiunti da un numero enorme di persone in ogni momento: questo sognavano i creatori del Sol, convinti che le battaglie politiche del decennio precedente, ad esempio sulla questione del Vietnam, fossero state perse soprattutto per l'impossibilità di smascherare le bugie e denunciare i silenzi del potere.

Ho scelto di raccontare la storia di Marsh e Felsenstein perché ha un grande valore simbolico: in essa si compì materialmente il passaggio dalla prima alla seconda generazione di hackers, dalle grandi macchine "convertite" al servizio del popolo (l'Xds-940 collegato al terminale di Leopold) al piccolo Sol. Ma anche personaggi oggi ben più conosciuti e ricordati avevano lo stesso identico spirito antiautoritario e visionario: pensiamo ad esempio a Steve Wozniak (Woz), spacciatore delle vietatissime *blue box* nei colleges di Berkeley insieme all'amico Steve Jobs, col quale poi costruirà l'Apple II, destinato ad evolversi in Macintosh.

Questi geni creativi, come molti altri semplici hobbisti (ingegneri o meno che fossero) costituirono l'ossatura di gruppi più o meno informali come il famoso *Homebrew Computer Club*, il cui scopo era far girare idee e conoscenze, ma anche scambiare hardware e software. La rivoluzione tecnologica che portò alla nascita dei personal computer non può essere ascritta a una sola persona, e nemmeno a pochi geni: essa nacque all'interno di una *comunità*, dove la condivisione era considerata un valore assoluto. Quella rivoluzione non avrebbe mai potuto realizzarsi in assenza di due condizioni molto particolari e strettamente legate a quel particolare luogo (la California) e periodo (gli anni Settanta):

1) Un atteggiamento mentale aperto alla sperimentazione senza limiti e, soprattutto, *senza precise finalità.* E' il paradosso dell'Altair: creare una cosa *prima* di sapere a cosa servirà, per il puro gusto di provarci, applicandosi poi con enorme dedizione a migliorarla, ancora una volta però non tanto per renderla *utile*, ma soprattutto *piacevole* (i primi hackers dell'Altair, come abbiamo visto, pensarono a farlo suonare, a creare dei giochi, a renderlo comunicativo: nessuno pensò di usarlo per lavorare!)

2) Una propensione smodata al rischio e alla sfida intellettuale, in una cornice tuttavia di assoluta lealtà: nella *comunità* (insisto su questo termine fondamentale) degli hackers tutti volevano primeggiare, ma nello stesso tempo tutti erano consci di aver bisogno l'uno dell'altro, perché quella tecnologia era incredibilmente complessa e nessuno, in quella fase, avrebbe mai potuto "fare da solo".

In definitiva, possiamo affermare senza ombra di dubbio che quella straordinaria rivoluzione scientifica nacque *fuori* e *contro* il sistema, intendendo con questa parola il potere industriale, accademico, politico. Questo non significa che tutti gli hackers fossero politicizzati e preparassero chissà quale sovvertimento socio-politico, anzi molti di loro di politica vera e propria non si occuparono mai. Erano però tutti apertamente, radicalmente estranei al sistema: non erano in linea di principio contrari a far soldi, sia ben chiaro (ne fecero anzi poi parecchi, come sappiamo), ma certamen-

te nessuno di loro avrebbe mai potuto lavorare per l'Ibm o per centri di ricerca governativi, perché la semplice idea di sacrificare il miglioramento alla minima regola burocratica o disciplinare sembrava loro assurda.

Bill Gates e il "casino del software"

La mentalità degli hackers diviene ancor meglio comprensibile se consideriamo lo scontro feroce che si venne a creare tra la comunità hacker e quello che ne fu considerato il primo traditore.

Correva ancora l'*anno magico*, il 1976, quando Bill Gates (un hacker che però veniva da Harvard e, come si vedrà, era parecchio interessato ai soldi) lanciò, insieme a Paul Allen, un software in linguaggio Basic per l'Altair. La novità di tale software era che fosse destinato soltanto alla vendita, con prezzi diversi a seconda che venisse acquistato da solo (500 dollari) o abbinato alla macchina (150 dollari). Naturalmente, come era stato sempre fino ad allora, furono in pochissimi ad acquistarlo: quel nastro perforato, come tantissimi altri prima di lui, iniziò ad essere copiato e modificato su larga scala, passando di mano in mano gratuitamente senza che nessuno avesse remore in proposito. Nessuno, tranne ovviamente Gates stesso, che scrisse un'infuocata *Lettera aperta sulla pirateria*, nella quale si leggeva, ad esempio: *"Chi può pensare di fare del lavoro professionale per nulla? Quale hobbista può mettere tre anni di tempo-uomo nella programmazione, trovando tutti i bug, documentare il suo prodotto e distribuirlo, il tutto gratuitamente?"* e ancora: "*La somma delle royalties ottenute dalle vendite agli hobbisti fa sì che il tempo passato a sviluppare il BASIC per l'ALTAIR sia valutato meno di due dollari all'ora. Perché questo? Voi state rubando il vostro software e la maggior parte degli hobbisti deve diventarne consapevole*."

Apparentemente, non c'è nulla di strano in quanto dice Gates, anzi le sue parole sembrano di assoluto buon senso. Ma gli hackers non potevano accettare (né accetteranno mai) questo modo di vedere le cose. Anche se molto spesso venivano scambiate attraverso il baratto, l'idea che il commercio potesse riguardare le componenti hardware era accettabile: nessuno trovava sbagliato o sconveniente vendere o comprare i pezzi di cui era materialmente fatto un computer. Ma per il software, era tutta un'altra storia. Perché il ragionamento di Gates (siete disposti a pagare l'Altair, ma non il suo software, eppure anche noi sviluppatori abbiamo lavorato, esattamente come chi ha costruito la macchina) non funzionava agli occhi degli hackers?

La risposta ha probabilmente a che fare con l'idea tipicamente novecentesca di *merce*. Nella società industriale classica novecentesca (prima della rivoluzione micro-elettronica) la *merce*, ciò che poteva esser comprato e venduto, aveva una indiscutibile dimensione materiale: era un *oggetto*. Il software ha un grado di materialità molto discutibile: quando un programma viene inserito in un computer, quella fredda macchina, quell'*oggetto*, prende vita. Il software è l'*anima* del computer, e quell'anima nasce da un sapere collettivo, da un bagaglio di conoscenze che, come l'aria o l'acqua, appartiene a tutti. Può sembrare un modo romantico e semplicistico di vedere le cose, ma la risposta sprezzante degli hobbisti alla lettera di Gates non è meno sensata della lettera stessa: avrai anche lavorato tantissime ore, caro Bill, ma sei comunque partito da un bagaglio di conoscenze pregresse, frutto di uno spontaneo gioco di squadra, un sapere che nessuno si è sognato di farti pagare. Hai fatto la tua parte, tutto qui: ora consegna il tuo lavoro e permetti a chi lo sa fare di migliorarlo.

Il dibattito inaugurato, nel mondo dei personal computer, da Bill Gates nel 1976 non è di fatto ancora terminato ed ha assunto il nome, poco elegante ma decisamente calzante di *casino del software*: ancora oggi la logica di mercato, che rende blindati i codici sorgente dei più famosi sistemi operativi a pagamento (su tutti proprio le infinite versioni di *Windows* della Microsoft di Bill Gates)

si scontra con la filosofia dell'*open source*, dove non solo i programmi sono gratuiti, ma i codici sorgente sono pubblici, aperti alle modifiche migliorative di chiunque (pensiamo ad esempio a *Linux*).

Una sottile linea di confine

Sono passati ormai più di quarant'anni dal lancio sul mercato del primo Altair. Il mondo dei personal computer da un certo punto di vista è cambiato moltissimo, ma da un altro si è fermato al 1976. Fu in quell'anno favoloso che, come abbiamo visto, questa tecnologia esplose e, insieme, precipitò dal cielo dei sogni e delle utopie al terreno del mondo reale. L'uso certamente più importante e rivoluzionario dei computer, oggi, è proprio l'unico al quale gli hackers non solo non avevano pensato, ma al quale deliberatamente non si interessavano: il computer serve a lavorare. Il computer è stato il motore della cosiddetta terza rivoluzione industriale, iniziata già nel secondo dopoguerra con un avanzamento tecnologico rapidissimo (si pensi a elettrodomestici, auto, televisioni…), ma giunta all'apice tra gli anni Ottanta del XX secolo e l'inizio del nuovo millennio.

Si potrebbero spendere ore a parlare delle applicazioni rivoluzionarie del personal computer al lavoro. Tuttavia, abbiamo sotto gli occhi in ogni momento anche la traduzione in realtà e l'enorme evoluzione dei sogni che animarono la fase aurorale della rivoluzione informatica. Il web e i social network, i forum on line, i programmi di condivisione di file audio e video…tutto quello che in generale oggi chiamiamo *la rete* è esattamente ciò che quei folli visionari californiani avevano in mente negli anni Settanta. Il computer ha creato la possibilità di mettere in comunicazione orizzontale (senza cioè passare attraverso nessuna autorità, filtro o mediazione) milioni di persone. Naturalmente ciò comporta dei rischi, perché non è sempre facile muoversi nella totale anarchia. La *rete* è spesso veicolo di violenza, abuso, comportamenti illegali. Ma attenzione: un vero hacker vi direbbe che le molte degenerazioni della *rete* sono semplicemente lo specchio delle degenerazioni della società. Un vero hacker sorriderebbe dei *parental control* (sistemi per inibire l'accesso ai minori a determinati contenuti) e schiumerebbe di rabbia di fronte ai tentativi di molti Paesi di "imbrigliare" e controllare la *rete*: condivisione *e* responsabilità possono tranquillamente andare d'accordo, in un contesto di corretta educazione al rispetto di cose e persone.

Naturalmente, questo non significa santificare gli hackers e la loro visione del mondo. Fin dalle origini, l'etica hacker è stata permeata da un gusto smodato per la sfida e la trasgressione. La lotta eterna tra grandi industrie della musica e del cinema e "pirati" informatici, ad esempio, è vissuta dalle prime come una sacrosanta crociata del libero mercato, degli onesti commercianti, contro i ladri; dai secondi come un atto di giustizia sociale: la cultura è di tutti, non può e non deve esser oggetto di mercato, specialmente di un mercato rapace che, solo per pochissimi, genera profitti incalcolabili.

Quando un'intelligenza fuori dalla media si combina al culto della trasgressione, inoltre, esiste sempre il rischio di spingersi troppo oltre e di superare quella sottile linea di confine che separa il lecito, o il tollerabile, dal puro e semplice crimine: ecco allora che l'hacker, per tornare al punto di partenza e ai fatti contemporanei, può anche rinnegare i propri principi e vendere l'anima al diavolo per pura avidità.

Tutti questi rischi esistono, è innegabile, e seppur costituiscano una degenerazione dell'etica hacker, non si può certo dire che si tratti di una degenerazione imprevista o imprevedibile. La lotta tra l'*establishment* economico e politico e gli hackers, così come quella tra hackers puri e criminali in-

formatici (chiamati sprezzantemente *crackers*) è destinata a proseguire, anzi probabilmente non avrà mai fine. Ciò non toglie, comunque, che la storia del movimento hacker sia la storia di un'impresa umana incredibilmente affascinante e che dal mio punto di vista nessun rischio, nessuna degenerazione ha finora potuto far dire che "era meglio se non fosse successo nulla".

Conclusione e breve bibliografia

Questa brevissima ricognizione nel complicato universo filosofico e sociale dei cosiddetti *hackers* si basa su pochi ma fondamentali testi (al contrario sulla parte propriamente "tecnica" della faccenda esistono moltissimi testi, ma non sono competente nell'indicarli). Chi volesse quindi addentrarsi a fondo nella mentalità e nei sogni degli hackers deve assolutamente leggere:

Steven Levy, *Hackers. Gli eroi della rivoluzione informatica,* Shake, Milano 1996

Bruce Sterling, *Giro di vite contro gli hacker. Legge e disordine sulla frontiera elettronica,* Shake, Milano, 1993

Paul Freiberger, Michael Swaine, *Silicon Valley. Storia e successo dei personal computer,* Muzzio, Padova, 1993

Marco Revelli, *Oltre il Novecento. La politica, le ideologie e le insidie del lavoro* (in particolare pagg. 91-110), Einaudi, Torino, 2001