L’hacking tra etica e diritto

di Giovanni Ziccardi

Giovanni Ziccardi, Avvocato, è Professore di Informatica Giuridica presso la Facoltà di Giurisprudenza dell’Università degli studi di Milano.

The_Truth@hc-mag.com

Quando si abbassano le luci in sala, e l’oratore, con mosse rapide e consumata esperienza, estrae dal cilindro le magiche parole ‘etica’, o ‘etico’, la platea di solito ammutolisce. Il tecnico-informatico solleva lo sguardo dal portatile sul quale stava lavorando e ascolta in silenzio, un po’ stupito ma anche incuriosito da quei termini, in attesa di una qualche, nuova, rivelazione filosofica. Il filosofo seduto al suo fianco, invece, sorride, e si guarda intorno un po’ supponente: si crede il vero e unico padrone del significato di quelle parole. Il giurista, di solito seduto in fondo alla sala, sente correre un brivido lungo la schiena, e pensa a tutti quei comportamenti contrari alla legge che possono essere compiuti sotto la bandiera dell’etica. Ultimo, ma non ultimo, lo spettatore che ha un po’ la coscienza sporca, solitamente in piedi, e vicino all’uscita: riprende il colorito, accenna ad un sorriso, si siede anche lui insieme agli altri e si sente un po’ più pulito dentro, persino più pulito degli avvocati...
Chi frequenta conferenze e seminari specialistici, sa bene che l’hacking è uno di quegli argomenti dove il termine ‘etica’ viene sciorinato con più frequenza dei crash di un ben noto sistema operativo, ed è utilizzato in ogni contesto e in ogni salsa.
Si parla di ‘etica hacker’ per individuare una sorta di decalogo di comportamenti del ‘buon hacker’, i dieci comandamenti che dovrebbero guidarne le mosse, il riferimento morale delle sue azioni. Si parla, poi, di ‘hacking etico’ per individuare attività di hacking che si rifarebbero a determinate regole - a volte non si capisce bene stabilite da chi e, soprattutto, con quale autorità – e che servono sovente a cercare di connotare in un’ottica positiva azioni al confine tra il lecito e l’illecito.
Questo riferimento ad un’etica ‘superiore’, scritta o non scritta che sia, è poi più frequente, nel mondo hacker, durante i momenti di crisi con il sistema, di voglia di ribellione, di contrasto aperto con l’ordinamento costituito, con il Legislatore, con determinati e ben individuati gruppi di potere.
Nel momento, però, in cui si chiede a un hacker – ‘vero’, ‘falso’, ‘bianco’, ‘nero’ o ‘riciclato’ che sia – quali siano i principi etici che muovono il suo agire, le risposte che si hanno sono, di solito, differenti, confuse, originate da un misto di letture, di ‘sentiti dire’, di nozioni tramandate da amici o parenti.
Può allora essere interessante, in questa sede, cercare di capire in che rapporto la cosiddetta ‘etica hacker’ – ovvero quei principi, codificati e non, cui la maggior parte degli hacker si ispirano, o si dovrebbero ispirare – si pone con il diritto e, in generale, con la società, e come si è evoluta ed è mutata in rapporto al cambiamento della società stessa.

Un’etica hacker o tante etiche hacker?

Se si interpella un hacker storico – ad esempio Steve Wozniak – e gli si chiede in che cosa consista l'etica hacker, ci dirà che, in quasi cinquant'anni di attività di hacking, sono state definite tante, diverse 'etiche', strettamente condizionate ai tempi, alle leggi, ai comportamenti, alle tecnologie. E questo è normale e comprensibile: l'etica è comportamento, l'etica è legata al mondo esterno, a come il mondo si evolve, ma è legata anche alle mode, alle percezioni di alcuni fatti da parte di alcuni gruppi, alle reazioni a certe situazioni esterne. Vedremo, però, che alcuni principi di base si sono tramandati, e costituiscono una sorta di 'zoccolo duro' dell'etica hacker.
Seguendo l'opera e gli scritti di Richard Stallman, da molti considerato 'l'ultimo, vero hacker', si nota innanzitutto che tutte le sue azioni sono mosse da un senso morale rigoroso.
L'amore per il computer, per le tecnologie, per il codice, proprio ed altrui, porta a considerare quasi un'eresia il danneggiamento di un sistema informatico o di un programma.
Le teorie alla base dell'etica di Stallman e degli hackers della 'vecchia scuola' si rifanno all'idea di hacking come ricerca pura, un'idea nata negli ambienti universitari negli anni Cinquanta e Sessanta.
In questi anni l'hacking era inteso come ricerca, a volte esasperata, che mirava a conoscere sempre più di una macchina, di un sistema, di un programma, o a risolvere problemi tecnici concreti che si presentavano nei laboratori di ricerca.
Questa prima etica vede come padri The Woz stesso, Stallmann, John Draper (aka Captain Crunch). Le regole etiche sono focalizzate sulla costruzione di piccoli oggetti elettronici, sullo spingere la tecnologia del computer oltre ogni limite, su un hacking inteso da un punto di vista scientifico, legittimo. Le sfide tipiche che gli hacker portavano al sistema erano quelle di utilizzare meno righe di codice o meno componenti hardware degli altri hacker.
Nasce, in questo contesto, anche l'idea che le informazioni debbano essere libere e condivise, che debbano essere risorse gratuite per tutti, che le strutture informatiche e le informazioni correlate non siano di proprietà esclusiva dei governi.
Quattro, allora, i fondamenti dell'etica, per la vecchia scuola: idee, cuore, cultura, rispetto.
Già in questa prima fase di hacking storico, e in un quadro normativo fatto di poche, e inadeguate leggi, si cominciano a prospettare i primi rapporti turbolenti tra comportamenti considerati conformi a un modo di intendere una attività (etica hacker) e il diritto.
Le blue box che permettono di ingannare i centralini telefonici, o gli hacker che vanno a 'sbirciare' all'interno di codici proprietari, nonostante le previsioni contrarie indicate sui contratti di licenza, per adattare tali programmi a certe situazioni, cominciano a sollevare i primi problemi giuridici.
Ancora non si prospettano, in questa fase, problematiche giuridiche correlate all'attacco alla sicurezza, alle informazioni o ai servizi informatici.
E' presente, in questo periodo, una sorta di cultura del rispetto dell'informazione e del sistema.
Si propugna la necessità che tutti abbiano un accesso aperto alle informazioni, che il mondo informatico sia fatto di risorse che siano libere da alcun vincolo, ma nel caso ci si imbatta in un sistema o in un codice chiuso, piuttosto che romperlo si preferisce non utilizzarlo o, addirittura, crearne uno simile ma libero.

L’evoluzione dell’etica hacker.

Chi studia l’evoluzione dell’hacking e ‘salta’ dagli anni Cinquanta ai giorni nostri, nota dei cambiamenti sensibili.
Internet e la sua diffusione hanno rovesciato il mondo dell’hacking come un calzino. Il novanta per cento delle azioni di hacking segnalate dai quotidiani riguardano azioni che tendono al blocco dell’accesso alle informazioni – si pensi agli attacchi dDoS – o alla distruzione/deterioramento di dati e di risorse informatiche, quali defacements e creazione/diffusione di virus e worms.
Il passaggio, allora, è stato abbastanza brusco: da un accesso libero alle informazioni, e difesa dell’habitat informatico dai potenti e dalla censura, come regole etiche di base dell’hacking storico, ad azioni di blocco dell’accesso alle informazioni e danneggiamento dei sistemi informatici, come regole di base di ciò che viene ‘spacciato’, da stampa, televisioni e anche studiosi, come hacking del ventesimo secolo.
Diversi anni orsono, Allen Ginsberg, grande poeta della beat generation, fu intervistato da un giornalista italiano, Paolo Mastrolilli, a proposito del fenomeno hacker. Ginsberg disse al giornalista che gli hacker facevano col computer quello che i poeti della beat generation cercavano di fare con la penna. L’etica, in questo caso, prendeva allora le forme della difesa della libertà, del rifiuto della centralità, della negazione della censura, della difesa della democrazia.
Eric Corley (aka Emmanuel Goldstein) è solito individuare, nei suoi scritti e nei suoi programmi radiofonici, alcuni precetti su cui si reggeva l’etica e l’impegno dei primi hackers e che identifica ancora oggi, secondo lo storico hacker, l’essenza dell’etica hacker.
Per prima cosa l’accesso ai computer e a qualsiasi cosa che possa insegnare il ‘funzionamento’ del mondo in generale, non solo tecnologico, deve essere illimitato e totale. Poi tutte le informazioni devono essere libere. Non bisogna fidarsi mai dell’autorità e occorre promuovere la decentralizzazione. Infine scopo degli hackers è cambiare la vita in meglio tramite il computer.
Utile spunto per cercare di capire le basi dell’etica hacker può essere la consultazione del documento ‘The Jargon File’, che definisce gli hacker come persone che programmano con entusiasmo, che ritengono che la condivisione delle informazioni sia un bene di formidabile efficacia e che sia un dovere etico condividere le competenze scrivendo free software e facilitando l’accesso alle informazioni e alle risorse di calcolo ogni qualvolta sia possibile.

E il diritto dove lo mettiamo?

Che il rapporto tra diritto, autorità e hacking non sia mai stato un rapporto sereno, è un segreto di Pulcinella. Ma di chi è la colpa, se una colpa ci può essere? Di un diritto informatico, e non solo, ingiusto, che criminalizza anche comportamenti che in realtà non dovrebbero essere sanzionati? Probabile: il diritto dell’informatica si è sempre caratterizzato per essere poco ‘giusto’ e molto più rispettoso di interessi di parte o corporativi che dei diritti fondamentali dell’individuo. O la colpa è dell’autorità che, alcuni sostengono, ha sempre criminalizzato di default il mondo hacker? Probabile

anche quello, si pensi alle gigantesche retate che negli anni novanta hanno portato a poco o nulla. O la colpa è degli hackers stessi, che non si rendono conto – o fanno finta di non rendersi conto – che certi comportamenti portati in nome di una fantomatica etica sono palesemente contrari alla legge, legge che dovrebbero ben conoscere? Probabile anche quello, si pensi a chi insiste a voler giustificare comportamenti assolutamente gratuiti, unicamente finalizzati all'attacco ai sistemi o in palese violazione della privacy altrui come comportamenti leciti.
La situazione è allora un po' caotica: o è colpa di tutti, o di nessuno, o come direbbe un avvocato, siamo in presenza di un concorso di colpa.
La questione di fondo è che, in realtà, per il mondo giuridico, la soluzione al problema, ovvero l'analisi del rapporto tra etica hacker – o, comunque, comportamenti diffusi nel mondo hacker – e diritto, è molto semplice.
Basta comprendere, o smettere di far finta di non comprendere, che il diritto altro non è che un fenomeno in buona misura normativo (ovvero un insieme di norme, di regole) che convive con altri fenomeni normativi quali possono essere la morale, il costume e l'etichetta, ma che non è allo stesso livello.
Qual'è la differenza fondamentale? Che il diritto, in rapporto alla morale e agli altri fenomeni, compresa l'etica hacker o l'etichetta di rete, si contraddistingue per il fatto di essere il sistema normativo prevalente, con l'ausilio della forza, presso una popolazione e su un territorio determinati. La morale è invece quel sistema normativo che, secondo una o più persone, deve prevalere su qualsivoglia altro sistema. In questo caso non rileva la prevalenza di fatto, ma rileva la credenza delle persone. Diritto e morale possono avere qualsiasi contenuto, e possono essere divergenti.
In conclusione, ognuno di noi è libero di chiamare diritto ciò che preferisce, o sostenere che qualcosa non è diritto se non ha certe caratteristiche auspicabili sotto un punto di vista etico-politico.
Ognuno di noi è libero di dire che le informazioni debbono essere libere, che i sistemi informatici non debbono essere protetti ed è quindi legittimo abbattere le barriere informatiche, che i documenti tecnici delle compagnie telefoniche, soprattutto di quelle pubbliche, devono essere svelati per la sicurezza del cittadino, che il reverse engineering è lecito in ogni caso perché mira a diffondere la conoscenza, che il port scan è lecito anche se, in quella occasione, non serve a nulla se non a verificare un'eventuale porta aperta per entrare nel sistema, che il war driving è lecito perché i pacchetti che galleggiano nell'etere sono, come dicevano gli hippies nella San Francisco degli anni Settanta, di proprietà dell'universo.
Possiamo dire quello che vogliamo, siamo liberi di dare definizioni che corrispondono alla nostra morale, ovvero ai comportamenti che pensiamo siano da tenere, e ne abbiamo tutti i diritti. Possiamo dire ciò che vogliamo, ma i problemi reali nascono quando si ha a che fare con coloro che hanno autorità, con chi ha il potere, in una società, circa l'attribuzione del nome 'diritto'.
E, di solito, i problemi sorgono nei confronti di quattro categorie di soggetti: di chi emana il diritto (Legislatore e altre autorità di governo); di chi interpreta, ovvero spiega, il significato del diritto (studiosi e pratici del diritto); di chi, con la forza, fa in modo che si ubbidisca alle direttive emesse, ovvero al diritto (giudici, funzionari della p.a., apparati militari dello stato); di chi, infine, influisce sulle prime tre categorie, ovvero i gruppi di interesse.

Per il giurista, dicevo, la soluzione è semplice: ogni comportamento, compresi quelli che vengono a costituire la base dell'etica hacker, deve essere valutato sempre e comunque in rapporto al diritto vigente.
Non si può giustificare come lecito un comportamento che è previsto come vietato o illecito da una norma giuridica o, meglio, si può giustificare nel proprio pensiero, nella propria mente, nella propria convinzione, ma tutto viene riportato a realtà quando interviene il diritto, ovvero le regole che nella nostra società vengono rese efficaci con la forza.

L'etica hacker del nuovo millennio.

Riprendendo le fila del discorso, e cercando di disegnare un'etica hacker del nuovo millennio che sia da un lato rispettosa dei principi originari degli hacker della vecchia scuola e dall'altro che conviva con un quadro normativo per molti versi desolante, ovvero leggi e leggine che spingono in una direzione di censura, di tutela di interessi di parte e non dell'interesse pubblico, penso che si possano evidenziare spunti di riflessione interessanti.
Un'etica hacker che unisce i principi bel evidenziati dal poeta Allen Ginsberg (difesa della libertà, del rifiuto della centralità, della negazione della censura, della difesa della democrazia) con le teorie dell'hacker storico Emmanuel Goldstein (accesso libero all'informazione e alle tecnologie, diffidare dell'autorità, promuovere la decentralizzazione, cambiare in meglio la qualità della vita tramite l'uso del computer) può ben coesistere con un ordinamento giuridico. Con conflitti, problemi, dibattiti, ma può convivere.
Il panorama del vero hacking oggi, ovvero di quell'hacking che mira realmente ai fini esposti sopra, tutti finalizzati a un progresso culturale e scientifico, è un panorama molto interessante.
I 'gruppi', nell'era di Internet, stanno facendo tanto. Si pensi ai movimenti del software libero e dell'open source. Si pensi ai gruppi di studiosi che lavorano nei settori della sicurezza, della crittografia, della firma digitale, e all'eccellente lavoro di disclosure che tanti hacker seri stanno facendo, anche in Italia, per rendere noti al pubblico – soprattutto se questo pubblico è un cittadino che deve utilizzare determinati servizi informatici garantiti dallo Stato – difetti di programmazione, o problemi di sicurezza. Si pensi a chi combatte realmente il potere per fare in modo che le informazioni circolino il più possibile, ma sempre nel rispetto dei diritti e delle volontà altrui. Si pensi, al contrario, agli hacker che lottano perché tutti possano proteggere, ovvero mantenere segrete, le proprie informazioni, grazie alla tecnologia. Si pensi ai tanti 'cani da guardia' che, giorno dopo giorno, testano la sicurezza di sistemi e di software che hanno funzioni critiche.
L'etica hacker del nuovo millennio deve anche puntare, a mio avviso, sulle potenzialità di diffusione dell'informazione che Internet oggi offre. Mai si è avuto un mezzo di libertà talmente potente, un mezzo che, se usato bene, può realmente aiutare i nuovi hackers a perseguire quei principi etici, e rigorosi da un punto di vista morale, che già animavano i primi geni informatici.
Il successo sarà dato da una chiusura del cerchio. Può sembrare assurdo, in un settore tecnologico come il nostro - dove l'evoluzione si misura in giorni - parlare di un recupero di principi di cinquant'anni fa. Ma il recupero di vecchi valori si fa sempre

quando non ci si riconosce nei valori attuali, quando la sicurezza, nei periodi di crisi culturale, giuridica, o degli ordinamenti, si recupera guardando al passato e imparando dai nostri padri, pescando nella nostra cultura.
L'hacking ha passato un brutto periodo, negli anni Ottanta e Novanta, che ha mutato la considerazione dell'opinione pubblica su questo termine. E ci siamo stancati, ad ogni conferenza, di sentire studiosi che impiegano i primi quindici minuti del loro speech per spiegare, a un timorato pubblico, la differenza tra crackers, hackers, malicious hackers, virus writers, criminali e simili.
Il termine hacker non ha un significato, come non l'hanno gli altri termini che ho elencato prima. L'hacking non è mai stato, nella sua essenza, un termine, una definizione. E' puro spirito, è uno stato mentale, è una nozione che nel corso degli anni si è evoluta, è mutata, ha preso nuove forme. E' un cocktail di idee, di curiosità, di cuore e di cultura che non può che essere benefico, se rimane in questi limiti, per il progresso dell'umanità.
Tutto il resto, poi, va bene per i giornali, per la stampa scandalistica per fare colpo sulle ragazze, per spaventare il vicino di scrivania con un net send che gli apra una finestra sul desktop con un messaggio minaccioso. Ma tali comportamenti con l'hacking, e con l'etica, non hanno nulla a che fare…
Un vero hacker deve sempre essere cosciente della differenza che passa tra l'etica – individuale o di gruppo che sia – e il diritto, tra la realtà e la fantascienza, tra il mondo reale e il mondo delle favole.
L'appellarsi a un etica hacker non deve essere una scusa per giustificare comportamenti gratuiti, inutili o, peggio, palesemente contrari alla legge.
Ci si deve appellare all'etica hacker per portare avanti quella tradizione di libertà, di complicità, di condivisione di conoscenze che ha reso, in cinquant'anni, un servizio pubblico all'umanità, che ci ha dato Internet, che ha fatto arrivare i software crittografici sul nostro pc di casa, che sta facendo crollare monopoli. E' questo il patrimonio che i veri hackers ci hanno lasciato in eredità, e non è affatto poco.
Tutto questo lo dobbiamo anche, e soprattutto, per rispetto a quegli hacker veri che non si sono fermati davanti a leggi ingiuste, e che ora sono davanti a tribunali a combattere per una riforma, dall'interno del sistema stesso, delle leggi che, nel mondo, tutelano interessi personali o commerciali e non l'interesse pubblico. Un paio di nomi? Jon 'DVD' Johansen ed Eric Corley.
Penso che sia questo un momento davvero speciale per ridisegnare un'etica hacker che nasca di nuovo, come una fenice, dalle ceneri delle vecchie tradizioni e che sfrutti al meglio il movimento che si è creato, grazie a Internet, e al software libero, in tutto il mondo.
Come in tutti i momenti di svolta, occorre che gli attori operino con grande attenzione al mondo che li circonda, e, nel caso che ci interessa, anche al diritto. L'importante è di non ricadere nel buio degli anni Ottanta, il periodo che ci ha regalato il sinonimo hacker=criminale.
Un buon punto di partenza è sicuramente quello di diffondere una cultura del rispetto del diritto, e, perché no, se considerato ingiusto, di modifica dello stesso, ma sempre nel rispetto delle leggi, e con gli strumenti che l'ordinamento ci fornisce.
Chi avrebbe mai pensato che un ragazzino norvegese di 16 anni potesse far tremare i muri di Hollywood? Chi avrebbe mai pensato che un hacker solitario uscito dal MIT potesse diffondere il software libero e fare tremare le roccaforti di Redmond?

Sono questi i contributi al progresso, alla scienza, alla ricerca, alla società, che costituiscono l'essenza, e il prodotto, dell'etica hacker. Tutto il resto è noia.