Università degli studi "La Sapienza" di Roma

Corso di laurea in Scienze della Comunicazione
Cattedra di Sociologia della Comunicazione

"Il Web oscuro"

Origine, sviluppo e percezione dell'hacking in Italia

Relatore
Chiar. Prof. Mario Morcellini

Correlatore
Chiar. Prof. Enrico Pozzi

Laureando
Enrico Novari
Matricola n° 12165110
Anno Accademico 1997/1998

Ai miei genitori,
ancora convinti che un cracker
si riconosca per l'essere salato,
ai cereali o integrale.

Indice

Catturato dalla rete

Questa tesi si pone l'obiettivo di analizzare la controversa figura dell'***hacker*** e del suo mondo, dalle lontane origini americane fino ai giorni nostri, attraverso il ruolo svolto nell'immaginario collettivo e nell'evoluzione delle tecnologie informatiche. Non è facile spiegare i complessi passaggi - più o meno logici - che mi hanno portato ad approfondire questa tematica, perché non sono mai stato un grande appassionato di computer, e fino al momento della tesi non mi sono mai posto il problema di acquistarne uno.

La naturale timidezza verso le nuove tecnologie mi ha portato ad un approccio molto critico verso la rete e le sue dinamiche, nella convinzione che fosse un ambiente "strano", di cui poter fare a meno, popolato di soggetti con i quali avevo poco in comune. La tesi stessa, infatti, nasce come approfondimento dei problemi legati al rapporto tra il singolo individuo, con annessa la sfera sociale dove si muove, e le nuove tecnologie, con i conseguenti problemi di privacy e carenze legislative.

Quest'iniziale impostazione è riscontrabile in diversi passaggi del lavoro, tuttavia, una migliore conoscenza del mezzo (prima il computer, poi la rete con i suoi diversi servizi) ed una doverosa messa a fuoco dell'argomento (gli hacker, o meglio "gli smanettoni" e la loro filosofia), hanno contribuito a modificare la mia chiave di lettura ed il mio approccio all'oggetto di studio, fino alla scelta di un'analisi sociale del fenomeno e dei suoi protagonisti.

Oggi devo ringraziare la curiosità di questi individui, il loro essere diversi dagli altri, le loro solitudini davanti alla tastiera, se sono riuscito a superare l'imbarazzo iniziale ed a prendere i primi contatti con un mondo che si è dimostrato assai diverso da come lo immaginavo. Durante le mie navigazioni notturne, sono stati loro a far luce prima sui miei timori e successivamente sul cammino verso l'indagine che questa tesi contiene.

Così, poco alla volta, la mia intransigenza verso questo fenomeno è andata mutando in attenzione, rispetto, curiosità, fino al chiedermi perché questi individui fossero non solo temuti, ma condannati prima ancora di conoscerne veramente comportamenti e motivazioni. Il lettore non si aspetti una categoria omogenea e ben delineata, né caratteristiche in grado di ritrarne un quadro definito.

E' bene anticipare, infatti, che le classificazioni tentate non sono definitive, e difficilmente un hacker vi si rispecchierà pienamente; tuttavia, esse trovano una loro spiegazione nella necessità di approfondire un universo complesso, sconosciuto, oscuro. Un ***Web oscuro***, quindi, che non vuole essere sinonimo di pericolo e malvagità, ma testimonianza di quanta poca chiarezza è stata fatta, fino ad oggi, sulle sue dinamiche sociali.

Enrico Novari

1. Uomini senza ombra e cripto-anarchici

"…Vi sono più cose in cielo e in terra, Orazio,
di quante se ne sognano nella vostra filosofia."
W. Shakespeare, "Amleto", atto I°, scena V.

1.1. Complessità e semplificazione

Il nostro sistema sociale è divenuto incredibilmente complesso, tanto che l'uomo ha smarrito da tempo la capacità di seguirne e comprenderne l'evoluzione. Legato da una forte sensibilità alle condizioni iniziali, il sistema è oggi preda di moltissime variabili, tanto che si è persa la possibilità di effettuare delle previsioni con ragionevole certezza. Le valutazioni che ancora si tentano sulle conseguenze delle azioni sono legate ad un anacronismo proiettivo. Infatti, i valori con i quali ci si appresta ad analizzare tali conseguenze sono ovviamente "figli" del presente, poco adatti quindi a misurarsi con destini e sviluppi che risulteranno coetanei d'altri valori, diversi dagli attuali.

Lo sviluppo della nostra società, ad esempio, sembra porre di fronte ad una scelta dicotomica, di non facile soluzione, tra il benessere e l'efficienza. Se l'obiettivo è un benessere esteso si deve rinunciare ad un certo livello d'efficienza, raggiungibile solo diminuendo la partecipazione al benessere. Questo secolo ha presentato il confronto tra due sistemi, il modello capitalista e quello comunista. Il sistema capitalista si è dimostrato un ottimo produttore di ricchezza, senza riuscire a distribuirla equamente (oggi in U.S.A. vi sono trenta milioni di poveri e quasi due di carcerati) [1], mentre il modello comunista ha palesato evidenti limiti di produzione di ricchezza, pur riuscendo ad essere più equo nella distribuzione.

[1] Dati forniti dal Prof. D.De Masi, docente di Sociologia del lavoro, nella conferenza intitolata "Non dare agli altri quello che vorresti fosse dato a te", avvenuta presso la libreria Forum in data 14/5/'98.

Al mondo sembrano esservi tre fattori strettamente connessi fra loro ed in continuo e vertiginoso aumento: la ricchezza, la sua iniquità distributiva, la globalizzazione. Tutti questi fattori risultano fortemente legati alla tecnologia, più precisamente alla progressiva accelerazione ed alle sue conseguenze.

Una delle definizioni più interessanti della tecnologia è quella di meta-ideologia [2], cioè un'ideologia capace d'essere debole e forte allo stesso momento: debole perché vuota, priva di contenuti propri, forte perché con la possibilità di fungere da contenitore di qualunque contenuto vi si voglia veicolare.

Non potendo che convivere con tale complessità si è tentato di modificare l'ottica del problema, ponendosi nei panni di chi la percepisce e cercando di porre delle semplificazioni. La complessità andrebbe quindi studiata a partire dall'uomo, in quanto è in questi che essa finisce per risiedere, non più negli oggetti o nelle situazioni create dal soggetto. Molte delle tecnologie sviluppate negli ultimi decenni partono da questo presupposto, ovverosia dal semplificare la vita di chi le utilizza o, almeno, dal fornire la sensazione che ciò avvenga. Tuttavia, come spesso accade, nel tentativo di risolvere alcuni problemi si è finiti per crearne altri, non sempre di più semplice soluzione.

Il mondo dell'informazione, sconvolto dal matrimonio tra informatica e telecomunicazioni, ha cercato di porre rimedio alla sua eccessiva vastità con l'introduzione d'Internet: uno strumento continuamente aggiornato con tutte le informazioni circolanti, in continua evoluzione, che si sta dimostrando il gran supporto della società complessa. Il lettore troverà più avanti, nel corso della tesi, approfondimenti sulla storia e lo sviluppo della rete; ciò che ora interessa è rilevare come Internet sia in realtà un mezzo fortemente ridondante, che permette di convivere con questa complessità fornendo la sensazione di dominarla.

I tentativi operati per semplificare la complessità sono spesso sfociati in un aumento della stessa, causato dal proliferare di nuove possibilità che le tecnologie hanno portato con sé, senza parlare del notevole aumento di responsabilità che ciò

[2] Definizione effettuata da G. O. Longo, (autore d'alcuni scritti sulle applicazioni delle nuove tecnologie, nonché della prefazione al testo "Lo sguardo virtuale" di G. B. Artieri, F. Angeli, Milano, 1998), nella conferenza intitolata "Non dare agli altri quello che vorresti fosse dato a te", avvenuta presso la libreria Forum in data 14/5/98.

ha comportato per l'uomo. La rete, ad esempio, permette al giornalista un reperimento più facile d'informazioni, ma lo obbliga a modificare la sua professione, in quanto l'aggiornamento delle notizie in tempo reale su Internet rende l'articolo "vecchio" prima ancora di uscire in edicola. Da qui il trasformarsi della professione del giornalista in un lavoro di commento, d'approfondimento, oppure d'analisi di realtà più piccole, locali, dove la gigantesca ragnatela telematica non è ancora giunta.

Quello appena fornito è solo un esempio della complessa relazione cyberspace/cybertime, causata dalla differente velocità d'espansione dei due soggetti della relazione. Il primo si basa sul progressivo allargamento delle connessioni tra terminali, e si estende a ritmo vertiginoso; il secondo rappresenta il tempo d'elaborazione cosciente da parte dell'organismo umano, e non può che espandersi più lentamente. Di qui uno scarto sempre maggiore tra la massa d'informazione disponibile e quella che l'organismo umano può effettivamente elaborare, con il conseguente affidamento ad operatori "esterni" di un lavoro d'analisi e ricerca, un tempo svolto in prima persona. La fretta e l'ansia che caratterizzano il sapere di quest'alba elettronica sono riconducibili ad una cattiva gestione del cybertime.

D. De Kerckhove, nel suo testo "Brainframes"[3], assegna alla psicologia un'importante e necessaria azione stabilizzatrice: essa governa la nostra vita e ne assorbe, a meno di gravi disturbi, i cambiamenti, conferendo un aspetto di continuità alle vicende quotidiane. Tuttavia, quando gli effetti cumulativi di un cambiamento giungono ad un punto critico, si può verificare un'improvvisa frattura culturale. Ciò può risolversi in nuovo stile nell'abbigliamento o nella musica, in un mutamento di paradigma, persino in una rivoluzione. Internet sembra destinata a rivoluzionare il nostro lavoro, il nostro tempo libero, le nostre abitudini, in breve, la nostra vita. Se ciò non è ancora avvenuto è perché la migliore e più utile tecnologia al mondo non può imporsi ad un pubblico impreparato, perché per essa potrebbe non esserci spazio nella nostra psicologia collettiva, o almeno non ancora.

[3] D. De Kerckhove, ***Brainframes***, Baskerville, Bologna, 1993

Tuttavia vi è chi, come N. Negroponte[4], già si lascia andare ad entusiaste previsioni sul ruolo della rete. Tra le sfere della nostra vita, in relazione alle quali Negroponte ama pronosticare le fortune della tecnologia, vi è la socializzazione. Egli considera il vero valore di Internet (intesa qui nella sua estensione massima del termine, vale a dire come il complesso di tutte le strutture messe in rete) proprio nella sua capacità di socializzazione, e prevede che il suo uso favorirà l'apprendimento della lettura e della scrittura.

I bambini impareranno a comunicare leggendo e scrivendo in rete, ed essa sarà il nuovo mezzo per arrivare alla conoscenza ed al significato delle cose. Gli stessi giochi elettronici insegneranno ai bambini delle strategie e delle abilità, che poi torneranno loro utili nella vita. Negroponte conclude considerando questo processo come irreversibile, in quanto ogni generazione non potrà che essere più digitale della precedente. Le illusioni di un fanatico o le previsioni di un veggente?

La rete ci appare seguendo la metafora del sistema complesso. Essa permette la selezione di possibilità (lo fa ogni ricerca effettuata in un apposito motore), dovrebbe garantire ordine e sicurezza (come vedremo le difficoltà in questo settore non sono poche), connette azioni poste in riferimento tra loro (si pensi alle chatline o all'utilizzo della posta elettronica). La rete rappresenta, tramite la comunicazione, il passaggio dal sistema complesso alla realtà semplificata: quando la pagina situata in qualche imprecisato punto del ciberspazio si materializza, in uscita dalla mia stampante, anche l'ultimo frammento di complessità sembra superato, il sistema figura alla mia mercé.

Berger e Luckmann[5] sono stati tra i primi autori a considerare i caratteri dell'identità moderna in grado di dotarla di maggiore libertà e duttilità, senza però sorvolare sui pericoli anomici introdotti da tale libertà. Secondo il loro pensiero, ognuno di noi ha conoscenza del mondo come costituito da molteplici realtà, fra le quali quella della vita quotidiana è da considerarsi dominante e percepita come ordinata ed oggettiva.

[4] N. Negroponte, ***Essere digitali***, Sperling&Kupfer, Milano, 1995
[5] P. L. Berger e T. Luckmann, ***La realtà come costruzione sociale***, Il Mulino, Bologna, 1969

La realtà della vita quotidiana è legata al “qui” del mio corpo ed all’”adesso" del mio presente; il distacco da fisicità e temporalità di questa situazione è visto possibile solo nel linguaggio simbolico, organizzato in sistemi come la religione e la filosofia. La vita quotidiana è divisa in diversi settori, alcuni di routine ed altri più complessi. Quando ci s’imbatte in una problematica più complessa, la realtà della vita quotidiana cerca d’integrare tale settore con ciò che è già stato reso non problematico.

Oggi che la metafora della rete influenza la nostra società, l’idea di un sistema senza confini sembra annullare il tempo e lo spazio. La realtà della vita quotidiana, legata al “qui” del mio corpo ed all’”adesso” del mio presente, viene stravolta per eccesso di entusiasmo verso le nuove possibilità fornite dalla tecnologia. Tuttavia vi è ancora chi, come Franco Berardi[6], pone la sua attenzione sul rischio posto dal “qui” e “ora” della telematica, l’illusione chimera di una sconfinata banca dati al nostro servizio, che nasconde il paradosso di una memoria fonte della dimenticanza stessa.

Altri esempi di tentate semplificazioni di realtà complesse possono essere individuati nel filosofo tedesco Husserl. Questi si prefigge di cogliere empiricamente le relazioni sociali, definite come delle “idee” dei soggetti. Tali relazioni sociali sono poste alla base del sistema, contribuendo alla sua analisi e semplificazione. Husserl adopera lo strumento della riduzione fenomenologica[7], un processo che mette fra parentesi le nozioni già acquisite sul senso del vivere quotidiano, cercando di modificare l’atteggiamento corrente dell’esperienza.

Inoltre, la riduzione fenomenologica permette di tornare alla vera realtà delle cose, liberando le capacità intuitive della coscienza. Tale coscienza è sempre intenzionale, cioè riferita ad uno specifico oggetto. Husserl divide la realtà mondana in diversi livelli (cose materiali, natura animale, realtà psichica), non ponendola come già data di fronte alla coscienza ma specificando che tale realtà si costruisce grazie alla coscienza stessa.

L’opera di Husserl è ripresa da Schutz, sociologo austriaco, formatosi nello storicismo tedesco. Egli analizza i diversi aspetti che emergono nell’interpretazione

[6] F. Berardi, ***Ciberfilosofia***, Castelvecchi, Roma, 1995
[7] F. Crespi, ***Le vie della sociologia***, Il Mulino, Bologna, 1985

dell'agire e si pone il problema della formazione delle strutture sociali. Il suo obiettivo è osservare come gli uomini fanno esperienza, nel loro atteggiamento naturale, mediante la comunicazione, i segni, i simboli e le istituzioni sociali. Tuttavia un problema appare irrisolto nell'analisi dell'autore austriaco: l'esperienza fatta dal soggetto, nella dimensione riflessiva della coscienza, appare ad ogni individuo come originaria del soggetto stesso; tuttavia, la personalità individuale si forma sempre all'interno di un mondo sociale precostituito. Quale delle due dimensioni debba prevalere non è chiaro, neppure nel rapporto tra la libertà del soggetto ed il carattere deterministico delle strutture oggettive dell'ordine sociale.

Davanti all'introduzione di una nuova tecnologia il dubbio si ripropone: De Kerckhove[8] descrive tale scenario come una guerra non dichiarata alla cultura esistente, nel quale il nuovo inizialmente spaventa ma poi ci si abitua. Come se dopo un periodo di rodaggio, la dimensione della coscienza fungesse da strumento semplificatore assorbendo la novità e, nel passaggio da un'era tecnologica all'altra, fosse il mondo esterno a cambiare e l'individuo a restare sempre lo stesso.

Secondo questa teoria nel nostro cervello si sviluppano cornici in cui noi "inquadriamo" le nuove tecnologie, o meglio, le tecnologie d'elaborazione dell'informazione "incorniciano" il nostro cervello in una struttura, sfidandolo a fornire un modello diverso d'interpretazione, ma ugualmente efficace. Un "brainframe"- termine da cui prende nome il testo di De Kerckhove - non è solo un atteggiamento o una mentalità, ma è tutto questo e molto di più: esso è localizzato nella struttura profonda della nostra coscienza.

Il concetto di semplificazione è da sempre collegato a quello di fragilità, poiché in ogni processo semplificativo si perde qualche elemento: una connessione, uno sguardo d'insieme, una capacità di resistenza, la cui mancanza fa apparire fragile l'oggetto semplificato se rapportato alle insidie, siano esse interne od esterne. Tali insidie sono rappresentate da una serie di problemi, alcuni sorti con la nascita della rete, altri precedenti ad essa ma capaci di nuove espressioni grazie alla rete stessa. Una delle insidie che devono una nuova modalità d'espressione allo sviluppo della rete, e delle nuove tecnologie dell'informazione, è la criminalità informatica.

[8] D. De Kerckhove, ***Brainframes***, op. cit.

Questo particolare tipo di criminalità richiede una conoscenza tecnico-informatica nettamente superiore alla media e viene fatto rientrare, all'interno della dicotomia tra crimini che sfruttano l'uso del computer e crimini contro il computer, nella prima famiglia. Ingrassia e Paterna[9] parlano di "computer crime" nel caso di un'appropriazione indebita, effettuata da una banca riempiendo i moduli prestampati che servono a trasferire somme di denaro da un conto all'altro, solo se la conoscenza dei controlli specifici del sistema computerizzato è indispensabile al truffatore per evitare che il reato venga scoperto.

In realtà, l'introduzione del computer, in tutti i settori della vita moderna, comporta tali e tante occasioni per fatti illeciti e delittuosi di nuova specie che tale specificazione appare oggi solo uno dei numerosi casi di "computer crime", neppure il più frequente.

1.2. Dall'azione sociale al clipper chip.

Fortemente discriminante, nell'approccio al tema della complessità e della tentata semplificazione della stessa, risulta essere il concetto d'azione sociale. Si può considerare l'azione sociale come conseguenza di una più o meno riuscita organizzazione unitaria del sistema, all'interno del quale l'azione si svolge, come l'interiorizzazione di talune norme e valori che indirizzano verso certi tipi d'azione e di comportamento.

Parsons, ad esempio, scompone l'azione sociale in tre distinti fattori: soggetto o attore sociale, la situazione in cui avviene l'azione o condizione oggettiva, un ordine simbolico formato dall'insieme dei riferimenti culturali che orientano l'agire.

La stessa azione può essere studiata a partire dal singolo individuo e dalla sua intenzionalità, giungendo alla possibile unità ed organizzazione di un sistema sociale solo come conseguenza di tale azione. In questo modo è il soggetto a costruire e vivere le diverse situazioni sociali. Il suo agire, se dotato di senso, si

[9] Ingrassia e Paterna, ***Comunicazione sociale: crimini e devianze nel postmoderno informatico***, Giappichelli G., Torino, 1989

differenzia dal semplice comportamento a causa dell'azione progettata che lo precede. Tuttavia, il significato di un'azione compiuta non è quasi mai lo stesso di un'azione progettata, anche quando l'agire si è svolto secondo il piano prestabilito.

L'azione del soggetto, se collegata a quella di un altro, da' luogo ad una relazione sociale (o intersoggettività), posta alla base della vita associata. Inoltre, l'introduzione del concetto di "altro" come individuo diverso da me[10], da' vita ad una tematica d'interazione fortemente sensibile agli sviluppi della società stessa (es. le tecnologie). Schutz[11], ad esempio, attua delle distinzioni sul significato dell'agire tra chi lo compie, il soggetto cui l'azione è rivolta, ed un osservatore esterno.

Se il soggetto cui l'agire è rivolto può arrivare a condividere lo stesso mondo del soggetto agente, ponendosi sullo stesso piano di quest'ultimo, uno scienziato sociale, che svolge il ruolo d'osservatore esterno di tale azione, appartiene ad un mondo diverso da quello di entrambi i soggetti precedenti, e ciò gli permette di fornire un significato differente all'agire osservato.

Com'è facile intuire, siamo di fronte a due prospettive antitetiche[12], entrambe interessate ad intervenire sulla complessità del sistema ed a studiare il perché di un certo sviluppo della società: una fedele al percorso dal sistema sociale all'azione, l'altra più incline ad uno sviluppo inverso.

Concetti come società, sistema, ambiente, mondo, rappresentano la base della teoria funzionalista, le fondamenta sulle quali si costruisce l'intera struttura teorica, attraverso il diritto, fino alla sua devianza. Durkheim vede la società come un complesso di relazioni sociali osservabili tra i membri di una collettività, non corrispondente a tutta la realtà sociale ma solamente ad un piano o livello specifico di essa.

[10] Tale concetto viene introdotto agli inizi del secolo da C. H. Cooley in "Human Nature & the Social Order" (1902) e successivamente ampliato da G. H. Mead in "Mind, self, society" (1934).
[11] F. Crespi, ***Le vie della sociologia***, op. cit.
[12] La prima prospettiva ha origine con la teoria funzionalista di Durkheim, si sviluppa in quella struttural-funzionalista di Parsons e nella teoria dei sistemi di Luhmann. La seconda prospettiva fa riferimento ad una sociologia fenomenologico-costruzionista, che vede il suo sviluppo cronologico dall'analisi di Husserl e Schutz alla costruzione sociale di Berger e Luckmann.

L'insieme delle credenze e dei sentimenti, comune alla media dei membri di una società e definito come "coscienza collettiva"[13], è posto all'origine di un ampio corpo di norme consuetudinarie, convenzioni sociali e commerciali, vincolanti come norme giuridiche. Ogni attività avviene quindi in uno schema d'ordine, caratterizzato da un sistema di norme organizzatrici.

La necessità d'ordine e d'integrazione sociale guida anche l'approccio di Luhmann ai sistemi sociali, basato su un'ipotesi antropologica: la rilevanza del bisogno di sicurezza nei rapporti interumani tra i soggetti, in altre parole, il desiderio di vincere la paura che nasce dalla complessità del mondo. Tale complessità è indeterminabile, una sorta d'illimitate possibilità che non possono mai essere circoscritte, delle quali l'ambiente rappresenta quelle che potrebbero verificarsi in una situazione concreta.

Tuttavia, l'ambiente è ancora intuitivamente legato ad insicurezza e disordine, in quanto non basta l'aver individuato la situazione ma occorre selezionare alcune possibilità e negare le altre. A ciò è predisposto il sistema, la cui funzione è garantire sicurezza ed ordine connettendo tra loro azioni dotate di senso e riferite le une alle altre. Il sistema sociale è quindi formato non da uomini ma da azioni, da atti comportamentali dello stesso individuo che possono rientrare in sistemi diversi.

Il concetto di sistema, descritto come l'insieme delle relazioni d'interdipendenza tra più elementi, è basato sui principi d'autoconservazione e mantenimento del proprio equilibrio; da questo deriva una continua tensione verso la stabilità nei rapporti tra diversi attori e tra il singolo attore e l'ambiente.

Tale tensione, da mantenersi tramite il consenso collettivo, focalizza dunque l'intero lavoro di questi autori sul valore positivo delle forme normativo-istituzionali, ed in generale di tutto ciò che può indirizzare il comportamento individuale. Essi risultano incapaci di cogliere la riduttività ed il rischio causati dalla cristallizzazione di tali forme, fino ad una totale sovrapposizione tra l'ordinamento sociale e quello giuridico.

[13] R. Collins, ***Teorie sociologiche***, Il Mulino, Bologna, 1992

Un esempio di tale focalizzazione è fornito dal concetto di "aspettativa di comportamento"[14], che permette a Luhmann di contrastare l'insicurezza che attanaglia i soggetti quando essi devono rapportarsi al sistema. Tali aspettative si formano mediante la selezione di un repertorio di possibilità d'azione, grazie al quale è possibile orientarsi più rapidamente. L'assorbimento d'insicurezza nel sistema avviene così attraverso la stabilizzazione d'aspettative, non già attraverso quella del comportamento stesso.

Il passaggio successivo prevede la trasformazione di tali aspettative, attraverso la loro stabilizzazione, in norme giuridiche tali da rappresentare una guida al comportamento. Un esempio di tale passaggio è fornito dal convegno "Internet e privacy", svoltosi a Roma[15] nel maggio'98, che ha sancito l'abbandono della posizione americana dell'autoregolamentazione, finora considerata "anarchica".

Regole giuridiche, strategie istituzionali, norme sovranazionali, tecnologie di difesa della privacy: questi i termini e i progetti che la cultura di rete europea vuole attuare, destinati a far discutere soprattutto i vecchi ma indomiti "anarchici" di Internet. Essendo la rete nata e cresciuta in un ristretto ambito scientifico, riservato a pochi iniziati, la necessità di munirsi di regole ben precise ha tardato a prendere piede; tuttavia, la veloce ed incontrollata espansione, seguita al contatto con il mondo economico, impedisce ormai di procrastinare il passaggio dalle aspettative ad una precisa guida al comportamento.

Tale necessità non va confusa con la visione negativa dell'uomo, e delle sue capacità d'autoregolamentazione, insita in Durkheim. Secondo tale autore, la società deve stabilire dei limiti al benessere economico e sociale del singolo individuo, il quale si pone delle mete sempre più alte e tende, per sua natura, ad imbattersi in inevitabili crisi. Sorge però il sospetto che, in Durkheim, sia forte il timore che i membri delle classi economicamente sottoprivilegiate non accettino la loro condizione, nonostante l'autore li inviti poco velatamente ad accontentarsi di quello

[14] Le aspettative di comportamento sono divise in aspettative normative e cognitive. Le aspettative cognitive sono capaci d'imparare dal mancato avverarsi di un comportamento atteso, e modificano se stesse come reazione a tale delusione. Le aspettative normative sono incapaci d'imparare e di modificarsi in base ad una delusione, prevedendo la sanzione come unica reazione a tale delusione.

[15] "Tra privacy e libertà Internet in cerca di regole", articolo curato da A. Usai, pubblicato sul sito Internet www.repubblica.it di "La Repubblica", in data 8/5/1998.

che hanno[16]. Si motivano così le critiche al funzionalismo di essere una teoria che bada al mantenimento dello status quo, e lo giustifica a partire dalla sua stessa presenza correndo il rischio di cadere nella tautologia.

Questa sfiducia verso le capacità d'autoregolazione del singolo contrasta nettamente con quanto affermato nell'introduzione di questo lavoro, in relazione all'ampliamento della singola libertà d'azione seguito all'introduzione di Internet. Ci preme ribadire che al progressivo aumento del binomio libertà-responsabilità si devono il progresso e l'evoluzione della nostra società, e che le autorità morali imposte da un bene comune rischiano spesso di seguire interessi che di comune hanno assai poco.

Le aspettative di comportamento, una volta stabilizzate, danno origine ad una serie di norme; queste, calate nella realtà sociale di chi le deve rispettare, convergono sugli individui originando degli insiemi di comportamenti definiti ruoli. Il termine ruolo proviene dal francese ***role***, contrazione del latino ***rotulus,*** che designava il rotolo sul quale l'attore leggeva in scena la propria parte[17]. Durkheim non usa il termine "ruolo", ma teorizza lo studio delle norme sociali, con il loro carattere di imposizione precostituita del modo più appropriato di agire, come l'oggetto tipico su cui deve fondarsi la sociologia.

Singolare è il tentativo di Parsons di classificare i principali ruoli di una società secondo il tipo di norme che li compongono; ogni norma è distinta dal prevalere di una delle due scelte che le cinque originarie variabili strutturali dicotomizzate lasciano all'attore sociale. Il tentativo si dimostra tuttavia sterile perché in tutte le società, più o meno sviluppate, non è possibile effettuare tale dicotomizzazione; infatti, le due possibilità poste da ogni variabile strutturale (ad esempio affettività e neutralità affettiva, universalismo e particolarismo) si combinano inestricabilmente nei ruoli più diversi.

Il concetto di ruolo, nella teoria dei sistemi, inquadra un insieme eterogeneo, rappresentato da un fascio di aspettative non collegato stabilmente a determinati

[16] Sotto quest'aspetto, Durkheim sembra quasi un precursore della teoria del "Knowledge-gap" (Tichenor, Donohue, Olien, 1970) secondo la quale, man mano che aumenta l'introduzione d'elementi innovativi nella società, aumenta anche lo scarto di conoscenza all'interno di segmenti diversi della popolazione stessa.
[17] M. I. Macioti, ***Il concetto di ruolo nel quadro della teoria sociologica generale***, Laterza, Bari, 1993

uomini, ma possibile di assunzione da parte di diversi soggetti. La sua estensione va dal frammento del comportamento individuale all'unità, rappresentata da molti individui tra loro intercambiabili.

Ci preme chiudere questa parentesi sul ruolo ricordando[18] che non esiste una definizione del concetto di ruolo che sia uniformemente accettata, da cui poter prendere le mosse per una sua analisi; non si devono sopravvalutare gli aspetti strutturali né la spontaneità individuale, ma cercare di fonderli assieme.

Su tale complessità di significato del concetto di ruolo, i costruzionisti sviluppano la loro analisi dei processi di socializzazione, nei quali il singolo tende a divenire partecipe dell'universo simbolico proprio della sua società.

La socializzazione, divisa in primaria e secondaria, vive una fase decisiva nella formazione, nella coscienza dell'individuo, della figura di un "altro generalizzato"[19]. Perché l'"altro generalizzato" possa formarsi nella coscienza di un qualunque individuo, questi deve potersi rapportare ad altri soggetti, deve interagire con loro. L'interazione sociale può avvenire sotto varie forme, tuttavia il modello "faccia a faccia" rappresenta comunemente il prototipo di base. Sotto la spinta del progresso tecnologico tale modello si è evoluto, fino a divenire "virtuale" in seguito all'introduzione della rete come strumento di comunicazione.

Dal prototipo originale di comunicazione, fino alla tastiera di Internet, il partner comunicativo è andato via via scomparendo, la mediatizzazione della relazione umana ha causato la progressiva perdita delle componenti corporeo-referenziali dell'interazione; divenendo queste sempre meno visibili al proprio interlocutore, si è passati a scaricare la dimensione somatico-passionale prima sulla voce ed ora, con il Web, sui messaggi scritti.

[18] M. I. Macioti, ***Il concetto di ruolo nel quadro della teoria sociologica generale***, op. cit.
[19] Tale figura rappresenta un'astrazione dai ruoli e dagli atteggiamenti delle persone concrete, un'identificazione con una generalità di altri, con una società. Quando l'altro generalizzato si è ormai cristallizzato nella coscienza, s'instaura un rapporto simmetrico tra la realtà soggettiva e quella oggettiva e termina la socializzazione primaria. Quella secondaria è rappresentata invece dall'interiorizzazione di "sottomondi istituzionali", e si esplicita nell'acquisizione della conoscenza legata al ruolo. Se il momento soggettivo è analizzato nei termini di socializzazione (ruoli, significati, valori), quello oggettivo è rappresentato dalle forme culturali codificate e dalle istituzioni normative.

Sull'evoluzione di questo tipo d'interazione, riassumiamo brevemente un esperimento di "face to face", citato da De Kerckhove all'interno del suo testo "Brainframes"[20]. Due persone sedevano dandosi vicendevolmente la schiena, e conversavano in tempo reale, ciascuno con di fronte a se l'immagine dell'altro su una TV a circuito chiuso. Indipendentemente dal fatto che le persone si conoscessero o meno, si sentivano come se non esistesse nessuna delle solite barriere causate dall'immediatezza del guardarsi negli occhi. Nel contesto di questa nuova intimità elettronica, termina De Kerckhove, "avreste addirittura potuto mettervi le dita nel naso".

La perdita delle componenti corporeo-referenziali del partner comunicativo ha introdotto non pochi problemi sul riconoscimento dell'identità dello stesso. Con il termine "pseudospoofing"[21], ad esempio, s'intende l'uso di un nome (o d'altri elementi d'identificazione della persona) di fantasia, ma assolutamente credibile e presentato come veritiero. Il problema dell'uso di una falsa identità acquisisce particolare rilevanza sotto vari aspetti: se a livello generale richiama valori etici prima ancora che giuridici, nello specifico può assumere rilievo in relazione alle ipotesi di conclusione di contratti, o di commissione di crimini, attraverso le reti telematiche. La digitalizzazione dell'identità crea distonia, non si sa più bene con chi si ha a che fare, non si è più certi di nulla che non riguardi se stessi.

Nascono così quelli che Franco Berardi[22] definisce come "uomini senza ombra", tra i quali rapportarsi diventa problematico. Infatti, qualunque cyber-etichetta si usi, non si riescono ad evitare crisi di "verità". Le manifestazioni comunicative risultano così tutte ad altissimo contenuto simulato, l'interazione diviene possibile solo accettando in partenza questo dubbio sull'identità. Dai dubbi relativi all'identità delle persone, a quelli sui contenuti trasmessi, il passo è breve.

Negli ultimi anni, ad esempio, le agenzie investigative americane (CIA, FBI) sono state partigiane di un'interdizione radicale d'ogni diffusione pubblica di metodi di criptazione insuperabile. Si tratta di quei programmi in grado di trasmettere le informazioni mediante un codice talmente complesso da risultare quasi

[20] De Kerckhove, ***Brainframes***, op. cit.
[21] C. Serra e M. Strano, ***Nuove frontiere della criminalità***, Giuffrè, Milano, 1997
[22] F. Berardi, ***Ciberfilosofia***, op. cit.

incomprensibile. In nome della ragione di stato, il governo americano vuole mantenere la possibilità di decifrare ogni comunicazione elettronica, quando necessario (es. droga, denaro sporco, terrorismo), per assicurare l'ordine pubblico.

Una discussa proposta di legge americana[23] vorrebbe obbligare i fabbricanti di materiale di comunicazione ad includere, nei loro prodotti, un componente elettronico noto come "clipper chip", in grado di aiutare la polizia a spiare qualsiasi collegamento sospetto.

In USA è vietato commercializzare ed esportare all'estero programmi di criptazione troppo potenti, impossibili da decifrare in caso di bisogno; tuttavia tali programmi sono ormai discretamente accessibili mediante la rete, essendo disseminanti in diversi server grazie al militantismo dei cripto-anarchici. Essi sostengono che per liberarsi definitivamente dalla tutela del governo occorra la criptazione, applicata soprattutto al settore economico: creare imprese off-reality e contabilità virtuali, sfuggire al fisco e sparire nelle profondità del cyberspace, il regno di chi si sarebbe liberato per sempre dall'obbligo statale.

1.3. Il diritto e la sua assenza.

Nella dimensione temporale la funzione del diritto deve unificare il riferimento al passato, proprio delle aspettative, al riferimento al futuro, inteso come guida al comportamento: la combinazione di tali riferimenti deve essere sintetizzata dalla norma giuridica. Le norme permettono di etichettare il comportamento come diritto o come illecito. In ogni caso, senza norme giuridiche non può esistere alcun diritto (e nemmeno alcun illecito).

Tutte le comunicazioni sociali relative al diritto formano il sistema giuridico, che rappresenta il sistema immunitario della società; tale sistema viene messo in allarme da contraddizioni e deviazioni, e deve non solo ripristinare lo status quo ma anche saper reagire con l'eventuale accettazione di certi mutamenti. Infatti, il sistema del diritto abbraccia sia il comportamento conforme sia quello difforme.

[23] Vedi G. Alessio, ***L'Internet***, SEAM, Roma, 1997.

Essendo il risultato di una prestazione selettiva, il diritto trae la propria validità dall'efficacia dei meccanismi di tale selezione, i quali raggiungono la piena maturità quando si dimostrano indipendenti dalla momentanea distribuzione delle forze. L'evoluzione del diritto muove verso una forma positiva, consapevole della sua contingenza. Tale contingenza permette al diritto positivo di essere trasformato in base ad altre decisioni, la cui produzione è regolata da procedure di natura giuridica. Luhmann[24] identifica l'ordinamento giuridico con l'ordinamento sociale, in quanto schema normativo che agisce in tutti i sistemi sociali, compiendo una riduzione di complessità e costituendo una garanzia d'ordine facilmente realizzabile.

E' dunque la società, come sostiene Durkheim, la fonte di quelle regole che presiedono alla costituzione di accordi. Le leggi morali e giuridiche sono quindi prive di un fondamento assoluto e variano col mutare del tipo di società. All'interno della teoria funzionalista, la legittimazione è una delle quattro sotto-funzioni della funzione d'integrazione: il più importante dei quattro imperativi funzionali[25]. Tale sotto-funzione deve essere analizzata in profondità dal sistema giuridico, ma non dall'uomo di legge tout-court, il quale deve interessarsi dell'applicazione delle norme e non della loro giustificazione politica e morale.

Luhmann sottende alla legittimazione del diritto una formazione di norme giuridiche, avvenuta attraverso l'ipostatizzazione dei procedimenti di produzione; tale fissazione di procedimenti è intesa quale serie di successioni regolate d'atti, rivolti alla produzione di una decisione giuridicamente rilevante. La convinzione dell'autore tedesco, secondo il quale il processo formativo di una norma è sufficiente a giustificarne l'accettazione, è fortemente criticata da Habermas[26]. Questi sottolinea che la genesi di un procedimento si può giustificare solo indirettamente mediante un rinvio ad istanze formative, e queste devono essere legittimate a loro volta da un fattore esterno al procedimento stesso.

Può accadere che in una società siano prodotte troppe norme, rispetto alla capacità di quella società d'istituzionalizzare il consenso: ecco che il diritto assume la

[24] N. Luhmann, ***Sociologia del diritto***, Laterza, Modena, 1977
[25] I quattro imperativi funzionali del sistema di Parsons sono: l'adattamento all'ambiente naturale e agli altri sistemi sociali, la formulazione ed il perseguimento di scopi collettivi, l'integrazione, la conservazione e la riproduzione delle strutture motivazionali di base (L.Gallino, ***Dizionario di Sociologia***, UTET, Torino, 1993).
[26] N. Luhmann, ***Sociologia del diritto***, op. cit.

funzione di assicurare l'armonico funzionamento dei meccanismi di generalizzazione delle aspettative. Luhmann ritiene di conseguenza che i valori guida del giudice siano l'adattabilità e la variabilità delle stesse aspettative.

Il giudice, infatti, deve essere vincolato alla norma mentre il legislatore è estraneo a tale vincolo, da qui deriva la struttura mutabile del diritto stesso. Tale visione è strettamente collegata a quella[27] secondo cui il giudice dovrebbe concentrarsi più sulle cause delle proprie decisioni, e meno sulle conseguenze, evitando di farsi influenzare dai valori sociali ed applicando la norma come essa viene fornita.

Numerose critiche hanno raggiunto Luhmann in seguito a quest'affermazione, tutte concordanti sul dovere di un esplicito orientamento ai valori sociali da parte del giudice; il suo compito, infatti, sarebbe quello di armonizzare le prescrizioni legislative attraverso le idee di giustizia, dominanti in un certo contesto sociale. Luhmann ribatte avversando l'orientamento alle conseguenze, il quale renderebbe frammentari gli ordinamenti classificatori e imporrebbe al giudice una sorta di "paraocchi", in quanto non sarebbe possibile conoscere tutte le conseguenze collaterali di una certa decisione.

Nonostante il diritto sembri nascere con gli individui, in quanto legato alle loro aspettative, possono esservi delle situazioni in cui fattori esterni creano delle zone d'ombra, rese tali dalla carenza normativa. La progressiva accelerazione tecnologica, ad esempio, comporta la difficoltà di un adeguamento socio-legislativo, con il rischio di discrepanze cognitive che rendono il sistema più debole di fronte alle aumentate possibilità d'azione dei singoli individui, proprio perché soggetto ad una situazione anomica, almeno nella maggior parte dei contesti sociali.

L'assenza di norme è spesso frutto di una scelta ponderata, data dall'eccessiva rapidità dei mutamenti socio-scientifici, come avviene nel caso attuale dello sviluppo delle nuove tecnologie. Tale rapidità dovrebbe trovare un freno spontaneamente con il passare del tempo, in quanto la società, secondo Durkheim, possiede in sé sia le cause dell'anomia sia i rimedi alla stessa.

[27] N. Luhmann, ***Sociologia del diritto***, op. cit.

Ciò non toglie che l'autore evidenzi i potenziali effetti distruttivi originati da un vuoto di norme e valori. Tali effetti vengono individuati nelle tensioni conflittuali interne all'organizzazione del lavoro e nel cronico moltiplicarsi della devianza, che caratterizzano la società industriale.

Il sorgere delle leggi, in grado di regolare le accelerazioni socio-tecnologiche improvvise, è visto inizialmente come spontaneo, legato allo scorrere del tempo ed all'intrecciarsi di rapporti tra gli organi di una società. Più tardi il pensiero dell'autore viene a specificarsi sull'identità di tali organi, individuati in corporazioni o gruppi professionali, costituiti sia dai datori di lavoro sia dai lavoratori d'ogni specifico settore. A queste parti sociali in continuo rapporto è dato di risolvere le controversie e creare solidarietà.

Parsons invece identifica il concetto d'anomia com'estremo di una scala d'integrazione, compresa tra l'assenza totale di questa e la completa istituzionalizzazione. Tale scala di valori è posta all'interno di uno dei quattro imperativi funzionali del sistema, distinguibili in adattamento, conseguimento degli scopi, mantenimento delle strutture latenti ed integrazione[28]. Facile immaginare, all'interno di tale organizzazione teorica, come l'autore identifichi l'anomia con il crollo completo di un ordine normativo e non la giudichi assolutamente implicita alla natura del sistema.

La situazione attuale in cui verte la rete figura come tipico esempio d'anomia, originata da un'eccessiva rapidità tecnologica. Al riguardo è recente un intervento, apparso sui maggiori media d'informazione, da parte di Berners-Lee[29], inventore del sistema Web che permette di trasmettere on-line non soltanto testi, ma anche immagini e suoni. In sostanza Berners-Lee punta il dito su uno strumento di comunicazione ed informazione, Internet, divenuto a suo avviso troppo potente perché sfuggito alle possibilità di regolazione da parte dei suoi utenti.

---

[28] L'integrazione è la più importante delle quattro funzioni descritte, a sua volta scomponibile in quattro sotto-funzioni: la legittimazione (il fornire una base per l'ottemperanza di una norma), l'interpretazione (il determinare il significato vero e proprio di una norma e la sua applicabilità ai casi singoli), la sanzione (la conseguenza che scaturisce dal non aver adeguato la propria condotta ad una norma), e la giurisdizione (la concreta applicazione e la specificazione delle categorie d'unità su cui una norma è applicata). P. De Nardis, ***L'equivoco sistema***, F. Angeli, Milano, 1991.

[29] Dall'articolo intitolato "Internet devasta la privacy", pubblicato senza il nome dell'autore sul sito www.repubblica.it di "La Repubblica", in data 16/4/1998.

L'intervento rileva la necessità di mantenere la massima vigilanza e prudenza sui modi d'utilizzazione di questo strumento. Tuttavia, esso si conclude con un ambiguo richiamo all'indipendenza della tecnologia, rispetto alle norme stabilite dai sistemi sociali: la necessità di porre delle regole non deve ritardare il progresso tecnologico.

In realtà la rete ha già fornito esempi d'autoregolazione, anche se pallidi e non sempre rispettati: tali esempi sono riassumibili sotto il nome di "netiquette", acronimo composto dai termini ***net*** ed ***etiquette.*** Con la netiquette s'intende un codice, non scritto, per un contegno decoroso in rete. La maggior parte di queste regole è dettata dal buon senso e dalle buone maniere, tuttavia ci sono dei casi in cui la vita di rete non ha analogie con la vita reale (ad esempio sull'opportunità o meno di svelare il proprio sesso).

Tra i suggerimenti forniti dalla netiquette ricordiamo: la brevità dei messaggi, non dedicare ogni singola comunicazione a più di un argomento, citare brevi brani del messaggio al quale si risponde, non scrivere in lettere maiuscole (dà l'impressione di urlare), leggere le dovute FAQ (le domande poste più spesso con le relative risposte) prima di entrare in un gruppo di discussione, non sprecare energie per filoni tematici ormai morti, non molestare le donne[30].

Complementari al diritto, nella sua funzione d'integrazione e controllo, si pongono altri strumenti sociali, capaci d'intervenire dove le norme non sortiscono gli effetti previsti. Tali strumenti sono: la forza fisica, la terapia e l'annichilazione. La forza fisica vede la sua incidenza poggiare non tanto sugli effetti fisici diretti, quanto sulla sua generalizzazione come simbolo; tale generalizzazione consente eventualmente di tralasciare la sua applicazione. La forza fisica è complementare alla rappresentazione ed alla presenza del diritto nella società, in quanto l'evoluzione del diritto è da sempre legata alla storia dell'ingabbiamento della forza fisica stessa.

La terapia, in ogni sua forma, è un fenomeno con particolari ordinamenti istituzionali legati alla categoria del controllo sociale. Ogni terapia deve possedere un corpo di conoscenza che includa una teoria sulla deviazione, un apparato

[30] McGraw-Hill, ***Professione Internet***, supplemento al quotidiano "La Repubblica", inserto n.5 (pag. 94-5), Gruppo Editoriale l'Espresso SPA, Roma, 1998

diagnostico ed un sistema concettuale per la cura delle anime. Una terapia che ha successo risocializza il deviante nella realtà soggettiva dell'universo simbolico della società.

L'annichilazione nega la realtà di qualunque fenomeno, o interpretazione di fenomeno, che non rientri in quell'universo. Ciò può essere fatto assegnando ai fenomeni devianti uno stato ontologico inferiore, oppure provando a spiegare tutte le definizioni devianti della realtà in termini di concetti appartenenti al proprio universo, cioè trasformando la negazione del proprio mondo in un'affermazione di esso.

Terapia ed annichilazione hanno come obiettivo principe l'integrazione, riferita a due livelli: un livello orizzontale, nel quale si cerca di legare l'ordine istituzionale complessivo ai vari individui che vi partecipano rivestendo diversi ruoli, e un livello verticale interno alla vita del singolo individuo, la totalità della quale deve essere resa significativa per il soggetto in sé.

Simile ai meccanismi d'integrazione citati, con cui condivide l'intervento sulle azioni sociali degli individui, è lo strumento della sanzione, la cui analisi rivela finalità secondarie. Nel pensiero di Durkheim e di Parsons le sanzioni colpiscono le azioni sociali quando queste violano le norme in vigore, ma sembrano più dirette verso il resto della società - che abbia o meno in potenza la tendenza a violare tali norme - che verso il deviante stesso. Divergono però le motivazioni che tali autori adducono per spiegare il valore della sanzione[31].

Durkheim v'intravede un rafforzamento del legame di solidarietà tra chi non la subisce, ed arriva ad affermare che una società sana ha tanto bisogno del crimine quanto delle pene. Parsons considera la sanzione un'espressione dei sentimenti posti a difesa dei valori istituzionali violati dal crimine. L'autore americano vi attribuisce un valore di ripristino della normalità, fedele alla convinzione secondo la quale la conformità ed il controllo sociale vincono sempre, e la pone molto in basso nella sua lista degli elementi del controllo sociale.

[31] F. Crespi, ***Le vie della sociologia***, op. cit.

Nella nostra società risulta assai difficile comminare una sanzione adeguata in seguito all'accadere di crimini informatici; tale difficoltà si deve ad un altissimo "numero oscuro", una gran quantità di azioni illegali non denunciate di cui, a volte, le vittime non si accorgono neppure. In questa situazione è possibile rintracciare un'interessante pratica attuata, soprattutto all'estero, dalle multinazionali, pratica simile ad un processo d'annichilazione.

Se varie indagini sembrano confermare la riluttanza, da parte delle vittime dei crimini informatici, a denunciare i fatti alle autorità[32], non vi sono ancora dati precisi al riguardo di un'altra conseguenza anomala di tali crimini. Tale conseguenza è da riscontrarsi in una promozione a più alti incarichi, con cui varie multinazionali "premiano" i loro dipendenti, colti ad aver aggirato le difese tecnologiche delle proprie banche dati. Mediante tale sistema le multinazionali raggiungerebbero un duplice scopo: comprare il silenzio del dipendente che potrebbe fare cattiva pubblicità ai loro sistemi di difesa e utilizzare le stesse capacità tecniche del soggetto per migliorare i sistemi stessi.

Tale pratica può considerarsi simile ad un processo d'annichilazione. Infatti, le stesse capacità che permettevano di aggirare le difese delle maggiori banche-dati, magari solo per vincere i pochi dollari di una scommessa tra amici, vengono così retribuite con stipendi da favola proprio dalle vittime iniziali. Tali vittime risultano così essere fedeli al luogo comune "se qualcuno penetra nel tuo sistema è colpa tua"[33]. Il massimo grado di questo processo si raggiunge quando un ex-hacker diviene cacciatore di criminali informatici, mettendo le sue capacità al servizio di quel "sistema" avversato in precedenza.

1.4. Omologazione e devianza.

L'influenza che ruoli e modelli, attraverso aspettative di comportamento più o meno stabilizzate, possono avere sulle azioni dei soggetti, sembra permettere alla costruzione funzionalista di riuscire nel suo intento. Ordine ed integrazione sociale

[32] C. Serra e M. Strano, ***Nuove frontiere della criminalità***, op. cit.
[33] Vedi nota precedente.

appaiono così raggiungibili, con l'unico rischio che la società vada verso un'eccessiva omologazione, epilogo che non sembra preoccupare eccessivamente gli autori funzionalisti.

Tuttavia, le azioni degli individui hanno più volte dimostrato di poter deviare da ruoli prestabiliti, rifacendosi a valori diversi da quelli posti alla base del sistema. La società continua ad imbattersi in forme di devianza più o meno organizzate, per difendersi dalle quali si è analizzato l'utilizzo di strumenti complementari al "semplice" diritto.

I concetti d'omologazione e devianza sono entrambi contenuti in quello di globalizzazione; tale condizione è possibile perché il comportamento che esula dalle aspettative nasce con le aspettative stesse e non c'è verso di evitarlo. Un esempio di tale sviluppo è dato dalla sensazione, fornita dalla globalizzazione stessa, di essere contemporaneamente più vicini e più lontani, più simili e più diversi: vicini e simili perché ormai ogni genere di oggetto proviene da tutto il mondo (profumi francesi, cibi cinesi, notiziari americani), lontani e diversi perché la sensazione di mondialità che ne deriva è solo un'illusione (si pensi al terreno fertile trovato, in questo fine secolo, da tutti i movimenti indipendentisti, dalle regioni dell'ex-Jugoslavia alla "Padania" italiana).

La globalizzazione può essere considerata come un fattore legato all'istinto[34]: ogni essere umano ha sempre cercato di conoscere, possedere, viaggiare, avere contatti con aree sempre più grandi del pianeta. Tale necessità è dentro di noi, gli esempi al riguardo sono numerosi: si pensi al bisogno di dire "io ci sono stato", alla progressiva cartografizzazione del pianeta, alle svariate forme di globalizzazione che hanno accompagnato l'uomo nella sua storia (lo scambio di merci, la colonizzazione, l'imposizione della propria moneta e della propria cultura). Tale tematica entra in gioco ogniqualvolta un autore tenta di proiettare il proprio pensiero in qualche previsione. Luhmann, ad esempio, vuol mettere in guardia sul rischio che, in futuro, le questioni risolvibili a livello della società mondiale non vengano più problematizzate nei sistemi politici di tale società; oppure che vengano prese in considerazione solo sotto un'angolazione locale, quindi non possano più essere

[34] Concetto espresso dal Prof. D. De Masi (vedi nota n° 1).

risolte nella forma del diritto, essendo quest'ultimo sempre meno locale e sempre più internazionale.

Nelle società moderne, il conflitto tra ideologie sembra sostituito da diversi gradi di tolleranza, e la necessità funzionalista di un'integrazione forzata non sembra più così urgente. Se è vero che la complessità della società ha aumentato il tetto di tolleranza, è anche vero che il rischio sociale si è globalizzato, come evidenziato dall'ultimo assalto d'alcuni criminali informatici ai satelliti del Pentagono. E' notizia recente, infatti, che il sistema informatico posto a controllo dei satelliti della difesa statunitense è stato violato da un gruppo di pirati del computer[35]. Tale intrusione segna un nuovo salto di qualità nella cyber-guerra che oppone ormai da anni il Pentagono agli hackers[36].

Posta la globalizzazione come momento d'espansione, di "conquista" nel significato culturale del termine, la prima conseguenza palpabile risiede nella fase dell'omologazione. Il processo d'omologazione avviene di continuo a diversi livelli: si omologano le necessità, arrivando a farle sorgere dove esse non sono presenti, si omologano i gusti e le scelte culturali, si omologa la vasta area del privato e dell'inconscio; ormai tutti abbiamo le stesse paure (ad esempio l'A.I.D.S.) e le stesse gioie (pare che due miliardi di persone abbiano seguito il concerto di Capodanno).

Infine abbiamo l'omologazione di tipo tecnologico, un potente catalizzatore basato sul fenomeno della delega. Tra i vari tipi di delega, quella tecnologica porta ad affidare sempre più compiti e responsabilità alle macchine ed ai programmatori. Un tempo, infatti, i programmi erano fatti "in casa", su misura per le necessità dell'utente; oggi, se un programma funziona, diviene lo stesso in tutto il mondo e "costringe" i vari utenti ad utilizzarlo, pena uno scarto di competenza sempre più difficile da colmare. La nuova frontiera sembra dunque non essere più tra ricchi e poveri di denaro, ma di competenza tecnologica.

[35] Articolo intitolato "Gli hackers assalgono il Pentagono" pubblicato, senza il nome dell'autore, sul sito www.repubblica.it di "La Repubblica", alla fine del mese d'aprile del 1998.
[36] Nel corretto utilizzo del termine inglese, tale parola meriterebbe la "s" finale ogniqualvolta si riferisce a più di un elemento. Ma all'interno di una tesi in italiano, i puristi mi perdoneranno, manterrò invariato il termine sia di fronte ad una definizione singolare che di fronte ad una plurale.

Un monito all'omologazione viene posto già da Husserl[37]. La sua critica all'oggettivismo, introdotto dalla scienza positiva, incoraggia l'individuo a ritrovare quel senso intersoggettivo in grado di orientare la società e l'umanità, riattingendo alla semplice esperienza pre-scientifica dei soggetti.

Il rischio che l'oggettivismo scientifico sia applicato alla conoscenza, mediante l'immagazzinamento e l'elaborazione d'informazioni, si conferma quanto mai attuale. Si pensi alla dipendenza da possibilità esterne d'elaborazione, che comincia a minare la capacità umana d'esternazione; così facendo si finisce per portare fuori dal soggetto, per estroflettere, una capacità che invece proviene dal suo interno, rendendo tali esternazioni sempre più omologate fra loro.

Il concetto d'omologazione è parzialmente sovrapponibile a quello di conformità sociale, sul quale può risultare utile aprire una breve parentesi. Alcuni autori, come Boudon e Bourricaud[38], ispirandosi ai noti concetti di Durkheim di solidarietà meccanica e solidarietà organica, hanno proposto la distinzione tra una conformità sociale per somiglianza, ispirata alla solidarietà meccanica, ed una conformità sociale per convergenza, ispirata alla solidarietà organica. Nel primo caso ogni individuo, che si distingue troppo dal gruppo, minaccia di far ricadere la propria diversità sull'unità del gruppo stesso e sulla solidarietà tra i suoi membri. Nel secondo caso si riconosce come legittima l'autonomia d'ogni individuo di poter perseguire i propri interessi, purché nell'ambito di comportamenti consentiti.

In contrapposizione all'omologazione e parimenti rischioso, nel caso in cui il comportamento del soggetto esuli dalle norme prestabilite e dai relativi ruoli, si profila il fenomeno della devianza. Le interpretazioni di tale fenomeno sono state molto divergenti tra loro, anche prendendo in considerazione autori appartenenti alla stessa scuola di pensiero. All'interno della corrente funzionalista la devianza è stata considerata come incompletezza o deficienza morale, produzione strutturale da parte della società, fenomeno originato da fattori sociali, di cui non si è mai tentata una lettura legata alle intenzioni del singolo.

[37] E. Husserl, ***La crisi delle scienze e la fenomenologia trascendentale*** (1936), opera in bibliografia del 1954.
[38] F. Crespi, ***Le vie della sociologia***, op. cit.

E' possibile parlare di comportamento deviante solo concependo l'atto sociale come regolato da norme fondate su determinate idee di valore.

Per Durkheim non è la presenza del crimine e della devianza ad essere un'anomalia, ma l'aumento improvviso dell'indice medio di criminalità all'interno della società. Il criminale non è un essere radicalmente asociale e parassitario, un corpo estraneo che la società non può assimilare, piuttosto un elemento costitutivo della vita sociale regolarmente operante[39].

Parsons individua due cause principali di devianza: un difetto di socializzazione, vale a dire una scarsa interiorizzazione di valori e norme, e tensioni psicologiche legate all'infanzia, in base alle quali viene meno l'adesione al sistema normativo[40]. La connotazione totalmente negativa di questo concetto impedisce al sociologo americano di vederlo come un momento di positiva apertura, di scelta di nuovi percorsi all'interno del sistema sociale, e ne fa un rischio da evitare e correggere. Tale rischio è una mancanza da ascrivere alla funzione d'integrazione del sistema, che rimanda ad un inefficace controllo delle naturali spinte centrifughe del soggetto, che lo porterebbero a perseguire le proprie gratificazioni e la propria utilità qualora non adeguatamente "socializzato".

Secondo Berger e Luckmann è più probabile deviare da programmi stabiliti per noi da altri, che non da programmi che noi stessi abbiamo concorso a stabilire. Ogni deviazione appare come un distacco da un ordine istituzionale, e può essere designata in vari modi: depravazione morale, malattia mentale, ignoranza, … Tali sottili distinzioni avranno ovvie conseguenze per il trattamento del deviante, ed ognuna di queste riceverà uno stato conoscitivo inferiore all'interno di quel particolare mondo sociale, che diventa il mondo ufficiale.

Il comparire di versioni divergenti all'interno di un universo simbolico comune mette a repentaglio la struttura della società. Quando tali versioni vengono ad essere condivise da alcuni gruppi interni al sistema, la versione divergente può cristallizzarsi in una realtà autonoma e costituire una sfida allo stato di realtà dell'universo simbolico. Il rischio per il sistema è che tale momento possa essere l'inizio di un

[39] L. Berzano e F. Prina, ***Sociologia della devianza***, La Nuova Italia Scientifica, Roma, 1995.
[40] Ibidem

cambiamento di tipo rivoluzionario, per la formazione del quale occorre la presenza nella popolazione di “elementi motivanti alienazione” diffusi e distribuiti.

Il fattore determinante, in quest’ottica, è costituito dall’elemento “comunicazione”, che costruisce valori ed identità di un aggregato sociale intorno a significati condivisi.

Il gruppo che ha oggettivato la realtà divergente diviene così consapevole d’essere portatore di una definizione alternativa di realtà. Lo scontento diffuso arriva ad organizzarsi, e i soggetti si motivano a vicenda un comportamento non concordante con le interpretazioni ufficiali dei valori. A questo punto il deviante viene visto come un disadattato, come colui che ha strutturato, in seguito ai motivi analizzati precedentemente, una personalità sulla base di bisogni e disposizioni con tendenze negative verso il sistema d’aspettative condivise.

Nella sua posizione di criminale il deviante è spinto anche dalla società stessa, in quanto sia le aspettative di ruolo applicate all’esecutore dell’atto criminale da quel momento in poi, sia il sistema di sanzioni, risultano strutturati in maniera specifica per “sospingere” il deviante in una certa posizione. Infatti, le dinamiche sociali interne alle diverse realtà (es. la politica, l’economia) sono le maggiori indiziate per quanto riguarda la definizione di canoni di devianza, giudicati validi in uno specifico momento.

Il comportamento deviante deve essere dunque inteso come la conseguenza di una complessa rete d’interazioni sociali, che producono significati intorno all’azione e al suo autore, denotando così il tentativo di avvicinarsi ad un nuovo approccio epistemologico. Tale approccio deve evitare i nessi deterministici causa-effetto e le forme di generalizzazione che si estendevano, nei vecchi paradigmi, ad ogni crimine e ad ogni criminale. L’azione criminale comprende diverse funzioni interagenti tra loro: alcune strumentali (es. rubo con il computer perché mi servono i soldi) e altre più espressive, che appartengono a piani della coscienza più profondi (es. rubo con il computer per dimostrarmi quanto sono bravo).

Dietro ad un abuso informatico, rappresentato per esempio dall’intrusione clandestina in una rete telematica, possono celarsi intenti ascrivibili a categorie molto

diverse di criminali: semplici curiosi in cerca di emozioni, “ladri” d’informazioni che usano il computer come grimaldello, spie industriali, concorrenti commerciali ed industriali sleali, terroristi, pedofili e trafficanti di droga. Per la comprensione dell’approccio alla devianza criminale, più di tratti particolari della personalità dei delinquenti, sembra essere determinante l’insorgenza o meno di razionalizzazioni che precedono il crimine.

Tali razionalizzazioni rappresentano delle tecniche di neutralizzazione finalizzate alla negazione della propria responsabilità, e permettono l’inizio di un processo psicologico che conduce alla commissione del reato. Lo scarico o la diminuzione di responsabilità, la sottostima dei danni provocati, la concezione dell’atto illegale come una punizione meritata nei confronti della vittima, possono essere quindi intesi come un’attività tendente all’annullamento dei sensi di colpa, delle inibizioni e dei rimorsi.

Generalmente viene definita come “sindrome da Robin Hood”[41] una situazione vittimologica del criminale, dovuta al fatto che a subire il crimine informatico sia quasi sempre un’organizzazione e non una persona.

Ciò contribuisce a semplificare l’applicazione e l’efficacia delle tecniche di neutralizzazione. La stessa dimensione spaziale dove talvolta si consuma il reato, rappresentata dal ciberspazio e quindi caratterizzata da una complessa definizione e da scarsa tangibilità, può essere un elemento rilevante sui livelli di “percezione” del crimine. Come si vedrà meglio in seguito, i meccanismi che possono condurre un criminale informatico, che ha avuto un’esperienza casuale o sperimentale d’attività deviante, a raggiungere un modello più consolidato di tale attività intraprendendo una carriera criminale, sono molteplici e sono stati oggetto di numerosi studi criminologici.

Sulla presenza di una sorta di codice subculturale, nel mondo sotterraneo degli hackers, sembra non esserci alcun dubbio. Molti autori hanno testimoniato l’esistenza di numerose regole non scritte, d’alcuni aspetti d’autodefinizione nell’ambito dei navigatori clandestini del cyberspace. Secondo Bruce Sterling[42]- autore del testo “Giro di vite contro gli hackers” - quando si è un hacker, è l’intima

[41] C. Serra e M. Strano, ***Nuove frontiere della criminalità***, op. cit.
[42] B. Sterling, ***Giro di vite contro gli hackers***, Shake ed., Milano, 1993

convinzione di appartenere ad un'élite che autorizza a violare le regole o piuttosto a trascenderle. In effetti, non sembra trattarsi di una situazione d'assoluta assenza di norme, ma si configura un'etica a se stante, responsabile di numerose dispute intraculturali.

Tra i principi più noti dell'etica hacker[43] possiamo citare: la più assoluta libertà d'informazione, il dubitare continuamente di qualunque forma d'autorità, il promuovere situazioni di decentramento, la richiesta di essere giudicati per il proprio operato e non sulla base di criteri differenti (es. il ceto, l'età, la razza o la posizione sociale), infine la convinzione che con il computer si possa creare arte e che il p.c. possa cambiare la vita in meglio.

[43] S. Levy, ***Hackers, gli eroi della rivoluzione informatica***, Shake ed., Milano, 1996.

2. Hacker: origine e sviluppo di una leggenda

"…stat rosa pristina nomine,
nomina nuda tenemus."
U. Eco, "Il nome della rosa".

Il termine "hacker" si avvia a divenire un termine "ombrello", sotto il quale vanno radunandosi diversi valori e significati legati alla poliedricità della figura. Vi sono variabili temporali, logistiche e strutturali che favoriscono tale complessità, di norma volutamente ridotta dalla stampa in un generico significato di "criminale informatico".

La variabile temporale si spiega con l'evoluzione del fenomeno, sorto negli USA alla fine degli anni '50 e, tuttora, in frenetico movimento verso un futuro dove realtà e immaginazione si avvolgono vicendevolmente. La variabile logistica deriva da una certa eterogeneità del fenomeno "hacker", secondo la quale vivere questa realtà in Germania, ad esempio, non presuppone solo un contesto ed un background culturale diverso, ma come logica conseguenza anche un'etica ed un comportamento propri di quella diversità. La variabile strutturale, infine, è intrinsecamente legata al substrato "tecnico" del termine, ed incide diversamente secondo il mezzo adoperato e le funzioni ad esso collegate.

Alcune caratteristiche, tuttavia, sono proprie del soggetto "hacker", e come tali mi auguro che emergano nelle pagine successive: la curiosità, la volontà di capire il "perché" delle cose senza fermarsi al "come", una filosofia di socializzazione, apertura, decentralizzazione, unita al voler mettere le mani sulle macchine a qualunque costo, per migliorarle e per divertirsi. Tali caratteristiche legano, mediante un filo invisibile, studenti americani del '58 e "smanettoni" italiani del'98, attraverso quarant'anni vissuti nuotando controcorrente.

2.1. Trenini elettrici, telefoni e computer: la nuova frontiera americana.

Nell'anno accademico 1958-59, il Massachussets Institute of Technology di Boston (d'ora in poi MIT) ospitava al suo interno una serie di gruppi, di piccoli club che univano studenti dagli interessi comuni fuori delle ore di studio. Uno di questi gruppi era il ***Tech model railroad club*** (Tmrc), la cui stanza era occupata da un enorme plastico ferroviario molto dettagliato, perfettamente funzionante grazie ad un immenso intreccio di cavi, relè ed interruttori situati sotto il modello. Tale club assegnava ai suoi soci una chiave d'accesso ai locali, prima di ricevere la quale uno studente doveva dedicare almeno quaranta ore di lavoro al plastico.

All'interno del Tmrc esistevano due sottogruppi: alcuni soci amavano passare il loro tempo a costruire e dipingere modellini di determinati treni, di valore storico o affettivo, oppure a creare realistiche scenografie per il loro passaggio. Gli altri iscritti frequentavano il "Signal&Power subcommittee" (S&P), la sottocommissione del club per lo studio dei segnali e dell'energia, indirizzando la loro attenzione a tutto ciò che accadeva sotto il modellino ferroviario.

Il gigantesco sistema, che faceva muovere i trenini e funzionare tutti i singoli scambi, era continuamente testato, danneggiato, riparato e perfezionato, ossessionando i membri del S&P riguardo al suo funzionamento, alla reazione delle sue parti ai vari cambiamenti, alla creazione di nuove connessioni in grado di renderlo sempre più complesso. Molti pezzi del sistema provenivano dalla compagnia dei telefoni Western Electric, sponsor dell'istituto, che incaricava il rappresentante dei club d'occuparsi del sistema telefonico universitario. Il materiale della compagnia veniva riadattato a nuovi scopi sul modellino, ma presto non bastò più a saziare la sete di curiosità ed ingegno degli studenti.

Fu così che i membri del S&P si misero alla ricerca della leggendaria stanza Eam, l'***Electronic account machinery***, la quale ospitava dei macchinari che funzionavano come computer. In quel periodo non erano molte le persone ad aver visto un computer, sul quale lavoravano pochi fortunati tecnici, in camice bianco, intenti ad inserire schede perforate grandi come schedari metallici, davanti ad un selezionato gruppo di laureandi. Tutta questa gente era indaffarata a perforare

schede, infilarle nei lettori, premere una sequenza di pulsanti e girare degli interruttori sulla macchina, e vietava rigorosamente di avvicinarsi a qualunque estraneo. Così, inizialmente senza nessun'autorizzazione, alcuni membri[1] del Tmrc iniziarono a frequentare l'Eam, realizzando le prime intrusioni notturne dedicate ad un imperativo molto caro all'etica hacker, quello dell "hands-on" (letteralmente, "metterci le mani sopra").

All'interno del vecchio gergo del MIT, il termine "hack"[2] era usato per designare gli scherzi elaborati dagli studenti (es. rivestire d'alluminio la cupola che domina l'università), tuttavia all'interno del Tmrc era un termine degno di rispetto. Tale termine indicava un progetto intrapreso, o un prodotto costruito, che trasmettesse, oltre lo scopo specifico, il piacere della pura partecipazione. Un semplice collegamento di relè era definito un "hack semplice", tuttavia per essere tale doveva dimostrare stile, virtuosismo tecnico, innovazione. I più produttivi, all'interno del S&P, amavano autodefinirsi degli hacker.

Numerosi furono i tentativi notturni per tentare di collegare il funzionamento del plastico all'Eam, finché i tecnici della sala non acconsentirono a rendere meno private le sedute per l'uso del computer. I giovani hacker furono gradualmente ammessi al funzionamento dell'Eam e delle macchine che ne rappresentarono gli sviluppi, fino ad una collaborazione attiva con i professori. Questo può considerarsi il primo vero approccio di un gruppo di giovani hacker alle tecnologie di quel tempo, ma la rapidità di sviluppo dimostrata da tali tecnologie, unita alle citate caratteristiche di quei soggetti, avrebbe scritto altre pagine importanti nella storia della comunità scientifica americana.

Intorno ai nuovi computer del MIT, grazie ad un ristretto gruppo di studenti, andava lentamente nascendo un corpo organico di concetti, convinzioni, costumi, che tali individui avrebbero contribuito a diffondere una volta usciti dal college. Inoltre, il continuo ricambio di studenti unito al contatto tra le matricole e gli "anziani", avrebbe permesso alla cultura hacker di fare nuovi adepti, fondendo alcuni principi basilari con i diversi momenti storici.

[1] Non parliamo di studenti qualunque, ma di figure appartenenti alla storia dello sviluppo dell'etica hacker in America: nomi come P. Samson, B. Saunders, A. Kotok, B. Wagner, cui si aggiunsero P. Deutsch e R. Greenblatt.
[2] S. Levy, ***Hackers,*** Shake, Milano, 1996.

Tali principi basilari di hackeraggio, affinati con la convinzione sorta in seguito al passare degli anni, furono: il diritto alla libertà d'accesso ai computer ed a tutto ciò che insegna qualcosa su come funziona il mondo, il famoso slogan "l'informazione vuole essere libera", la promozione d'ogni tipo di decentramento culturale ed amministrativo (la massima rappresentazione dell'odio verso l'universo burocratico accentratore si materializzava, in quegli anni, nell'IBM), la convinzione che con i computer fosse possibile fare arte e cambiare la vita in meglio.

Tali convinzioni erano destinate a portare verso degli scontri ideologici con l'ordine istituzionale di allora, rigido e accentratore, ed i primi segnali destabilizzatori cominciavano già a manifestarsi all'interno del MIT. Nell'inverno del '60, gli hacker del Tmrc s'impegnavano nella schedatura della rete telefonica locale, registrando inizialmente i luoghi raggiungibili dalle linee del MIT, ed in seguito quelli connettibili ai collegamenti registrati. Mediante tentativi e catalogazioni successive, tentavano vari codici d'accesso, segnavano fin dove erano arrivati, e aggiungevano altri numeri per collegarsi oltre.

Alcuni studenti riuscirono, tramite tale sistema, a collegarsi con linee urbane, alla ricerca di difetti di progettazione e di debolezze del sistema telefonico in grado di far chiamare illegalmente, senza pagare. Nonostante la motivazione principale restasse la ricerca, queste piccole frodi evidenziarono il rischio di una facile deviazione da tale scopo, come se già allora gli hacker manifestassero una certa debolezza verso piccole forme d'illegalità.

Un'interessante caratteristica di quegli anni è rappresentata dal fatto che la cultura hacker poteva essere definita prettamente maschile. In realtà, vi erano donne che lavoravano come programmatrici, alcune molto brave, ma rimanevano sempre ai margini dell'universo hacker senza prenderne la "vocazione". Altri rilievi interessanti, riportati da Levy, riguardano la scarsa attenzione dei giovani hacker verso il proprio "look" e la propria pulizia, lo svolgimento di una vita spesso asessuata, segnata da un'estrema adattabilità verso qualunque tipo d'orari e sistemazioni[3].

[3] S. Levy, ***Hackers***, op. cit.

Il rapporto “conflittuale” con la rete telefonica divenne una costante di quegli anni. Nel 1964 un brillante hacker del MIT, Stewart Nelson, programmando con il Pdp-1 (l’Eam poteva considerarsi un ricordo), generò delle particolari frequenze sonore identiche a quelle utilizzate dalle compagnie dei telefoni, cosa che gli avrebbe permesso di telefonare ovunque, negli USA, scaricando il costo sulle compagnie stesse.

Tuttavia Nelson, assieme ad altri hacker dediti a simili pratiche, era convinto di rendere un servizio a tali compagnie, in quanto “collaudatore” delle dorsali installate da queste ultime (che a volte ricevevano, a proprie spese, strane segnalazioni da parte di studenti che rivelavano errori e difetti all’interno della rete, puntualmente riscontrati in seguito).

In realtà, nell’America degli anni ’60 e ’70, un uso “alternativo” delle linee telefoniche era divenuto molto frequente, tanto che nel 1971 un leader Yippie[4], A. Hoffman, promosse un bollettino chiamato “Youth International Party Line”. In tale bollettino egli raccolse e pubblicò tutta una serie di famose tecniche di pirateria telefonica[5] (e non solo), con l’intento dichiarato di creare controstrategie verso i computer che iniziavano a porre l’uomo sotto controllo.

Il “Party Line”, pubblicato nel Greenwich Village per un paio d’anni, divenne in seguito il mitico TAP (Technical Assistance Programme), un foglio mensile curato da una rete di “pirati telefonici” (in americano ***phone phreakers***), che fu un punto di riferimento per molta gioventù d’allora, e continuò le pubblicazioni fino al 1983 quando fu incendiata la casa del suo editore[6]. Rimasero famose le dispute legali che videro tale testata protagonista, accusata spesso di sfruttare l’estremo bisogno di comunicazione vissuto dalla giovane generazione USA degli anni ’70.

[4] Una delle radici dell’underground hacker moderno può essere ricondotta agli Yippie, un movimento anarchico oggi quasi dimenticato, i quali avevano preso il nome da un quasi del tutto fittizio “Partito Internazionale dei Giovani (Youth International Party). Gli Yippie portarono avanti una rumorosa e vivace politica di sovversione surrealista e d’oltraggiose offese politiche. I due leader più in vista furono A. Hoffman e J. Rubin.

[5] Come lo “scanning senza centralino”, le famose boxes (black, blue and red) e svariati altri metodi per truffare le compagnie telefoniche.

[6] Un’altra rivista specializzata in hackeraggio telefonico fu quella del movimento “Ramparts”, che nel 1972 fu coinvolta nello scandalo delle “blue-box”.

Tal esigenza comunicativa, presente sia come motivazione individuale sia come linfa di numerosi movimenti libertari, si fuse ovunque ad una forte opposizione verso l'uso militare delle innovazioni informatiche, incentivando una "via tecnologica alla comunicazione" di stampo molto personale[7].

Sull'hackeraggio, secondo R. V. Scelsi[8], venne a quel punto a determinarsi una sorta di mito, che tese a miscelare tra loro aspetti ideologici tipicamente americani. Da un lato una sorta di "corsa all'oro" collettiva, dall'altra la visione del "self made man", in grado d'imporsi grazie alla propria genialità. Tale visione, univoca ed omogenea, rischia tuttavia di soffocare la variabile temporale, che differenzia gli hacker dei primi anni '70 da quelli della generazione precedente. Infatti, se i primi studenti del S&P studiavano le mistiche applicazioni dell'intelligenza artificiale sui primi mainframe del MIT, la generazione successiva tentò di diffondere la cultura hacker fuori dai college, sospinta dal sogno di avvicinare la gente ai computer.

Il nuovo decennio vide la volontà di portare i computer fuori dalle stanze protette delle università, lontano dai dipartimenti di contabilità delle grandi aziende, permettendo alla gente di esplorarli da sola, di "metterci su" le mani[9]. Per la prima volta si pensò a dei ***computer center*** di quartiere, dove la gente andasse a divertirsi come allora avveniva al bowling. Fu il periodo in cui un ex-scrittore di musical rock, Ted Nelson, scrisse la "bibbia" degli hacker, un testo intitolato ***Computer Lib/Dream Machine***, che dopo un difficile inizio fu più volte ristampato[10].

Nel 1975 l'idea che ogni persona dovesse possedere in casa propria un computer era considerata da quasi tutti un'assurdità, tuttavia nella primavera di

[7] Tale opposizione, alle origini, non era in grado di distinguere tra le nuove tecnologie e l'uso che ne veniva fatto, e ciò coinvolse anche gli hacker del MIT. Nel '68 e nel '69, due marce di protesta ebbero il loro culmine davanti al college, ed obbligarono i giovani studenti a porsi le prime domande sull'immagine che la gente si era creata di loro (era noto a tutti che le attività di ricerca svolte all'interno del MIT fossero finanziate dal Ministero della Difesa). Gli hacker si difesero sottolineando che nessuno aveva mai chiesto loro di concepire delle applicazioni militari specifiche, ma non poterono negare che il Ministero avesse molte speranze in proposito.

[8] R. V. Scelsi, ***Cyberpunk***, Shake, Milano, 1992.

[9] Un esempio di questi tentativi era rappresentato dalla "People's computer company", un'organizzazione politicizzata all'interno del movimento pacifista, che tentava di far convivere questa caratteristica con il suo intenso feeling per l'informatica. Essa pubblicava un periodico con il proprio nome, nel quale si discuteva la tesi di non "educare" i bambini all'uso del computer, lasciando che essi sviluppassero da soli tale approccio.

[10] L'opera, autoprodotta nel 1974, era composta di due parti: la prima sull'epopea della "computer revolution" e la seconda sulle previsioni in relazione al futuro dei computer.

quell'anno nacque ***l'Homebrew computer club***, uno dei gruppi che ebbe maggiore importanza nello sviluppo di quest'idea. Tramite riunioni quindicinali, alla quarta delle quali si erano superati i cento partecipanti, la piccola confraternita hacker propose dibattiti, diede lezioni di programmazione e costruzione, approfondì lo studio di nuovi sistemi e ne insegnò l'utilizzo, reperì e distribuì le prime fanzine che tale tematica cominciava a proporre, in altre parole, contribuì allo sviluppo di una cultura che "addestrava" una generazione di hacker verso una nuova industria: i computer da tavolo.

Tale mercato, allora trascurato dalle grandi industrie, vide questo gruppo d'individui condividere esperienze e consigli, far progredire una piccola "arte", coltivare l'obiettivo che i computer arrivassero a costare di meno. Tutto ciò non deve illudere sul fatto che gli hacker perseguissero il sogno di una gran trasformazione sociale; in realtà, come sottolinea Levy, gli hacker "fecero gli hacker", in pratica seguirono il loro interesse, la loro passione, ma per fondare un sistema sociale basato su valori diversi, ammesso che ciò fosse possibile, ci sarebbe voluto ben altro programma.

L'IBM e gli altri "giganti" tecnologici di quel periodo non si accorsero di questi casuali assembramenti di hacker sotto forma di computer clubs (dei quali l'Homebrew era il più famoso, ma non certo l'unico), continuando a coltivare la loro idea di essere i padroni assoluti dei calcolatori.

L'armonia che sembrava raggiunta dagli hacker dell'Homebrew svanì di fronte ad uno dei temi più scottanti ed attuali (allora come oggi) del mondo informatico: la proprietà del software. Come accennato, nel club vi era l'abitudine di creare insieme i programmi ed il loro sviluppo, ed a chiunque riusciva ad apportare dei miglioramenti a linguaggi e programmi sembrava logico condividerli con gli altri soci. Una giovane casa di produzione software, la Mits, stava lavorando ad un programma in Basic per l'Altair, uno dei primi computer ad avere una diffusione rilevante.

Tale programma fu ultimato per primi da due giovani hacker di Seattle, B. Gates e P. Allen, i quali lo vendettero alla Mits in cambio di una percentuale su ogni copia venduta. Quello appena descritto rimase il primo caso in cui sorsero dei problemi sulla proprietà di un programma software, fino ad allora condivisa dai soci

dei vari club come del materiale comune. Alcune copie del software di Gates e Allen cominciarono, infatti, a girare prima dell'uscita ufficiale del programma, e la giovane comunità informatica si divise sulla dura lettera pubblica di sfogo con cui B. Gates, allora studente diciannovenne, accusava l'Homebrew di furto.

Nessuno sembrava vietare ad un giovane autore di software di essere pagato per il suo lavoro, ma forse era troppo chiedere agli hacker di abbandonare per sempre l'idea che i programmi appartenessero a tutti. Tale idea rappresentava, allora come oggi, una parte troppo grande del sogno hacker per essere messa da parte, ed è curioso notare come dopo vent'anni i ruoli non siano cambiati e B. Gates, oggi l'uomo più ricco del mondo, debba ancora fronteggiare quotidianamente quest'ideale di condivisione delle informazioni.

In realtà, ed oggi lo stesso Gates n'è consapevole, il fatto che tutti abbiano un software e siano capaci di usarlo finisce per favorire il suo proprietario, che ne vede comunque aumentata la pubblicità e le vendite, soprattutto quando quel programma diviene uno "standard" ed obbliga molte aziende ad acquistarlo. Inoltre, la circolazione di diverse versioni di un software migliora il programma stesso, ne elimina eventuali errori e disfunzioni, permette alla stessa casa produttrice di mettere sul mercato degli sviluppi dell'originale dei quali resta la legittima proprietaria.

Alle sedute dell'Homebrew partecipavano anche altri due giovani hacker, S. Jobs e S. Wozniak, i quali erano destinati senza saperlo a scrivere una pagina importante nella storia dell'informatica americana. Un loro progetto, finanziato tramite la vendita di blue boxes agli studenti dei colleges californiani, era in procinto di concludersi con la produzione, nel loro garage, del primo vero ***home computer*** della storia: l'Apple.

Questi due giovani studenti, in seguito fondatori di una delle più famose case informatiche, ***l'Apple computer Inc.***, incarnarono la necessità di quella "democratizzazione" dell'informatica, nata nei corridoi del MIT, e conseguenza della

volontà di minare un monopolio di sapere e di calcolo rappresentato dai mainframe IBM[11].

Quella intrapresa da Wozniak e Jobs fu una decisione storica: ora che anche altre persone stavano costruendo macchine con terminali e tastiere, che sarebbero state utili non solo agli appassionati ma anche alla gente comune, la direzione di quell'industria nascente stava per sfuggire dalle mani degli hacker. Erano passati quasi vent'anni da quando gli studenti del Tmrc avevano cominciato a lavorare all'Eam.

Oggi può essere visto come duplice il ruolo giocato dalle figure di Jobs e Wozniak nel processo di modernizzazione del capitale: se da una parte tali soggetti figurarono come sabotatori della privatizzazione dell'informazione, dall'altra con la loro invenzione divennero degli innovatori nello sviluppo di tale merce immateriale, il futuro nuovo campo di dominio del capitale.

Dalla metà degli anni '70 molti giovani, in parte ancora provenienti dal MIT[12], diventarono linfa attiva del fenomeno ***Silicon Valley***, la regione dove si andarono a concentrare le migliori menti tecnologiche, il traino della scalata americana al successo mondiale nei settori della componentistica e della programmazione informatica. Questi giovani hacker videro le loro pratiche d'intrusione e di sperimentazione agevolmente sopportate dalle multinazionali del settore, che intuirono la presenza della genialità dietro quell'esuberanza giovanile, incapace di seguire un orario di lavoro o d'inserirsi in gruppi guidati di ricerca.

Nell'aprile del 1977 si organizzò in California la prima fiera dedicata all'informatica, all'interno della quale andò sviluppandosi il contatto tra gli hacker ed il mondo reale, venuto alla luce mediante la nascita dell'Apple computer Inc. Durante il week-end di durata si registrarono c.ca 13mila presenze, e tale esperienza

[11] I primi computer dell'Apple Inc. erano venduti a 666dollari e 66, e gli annunci della giovane casa informatica dicevano: "La nostra filosofia è fornire software per le nostre macchine, gratuitamente o ad un costo minimo". S. Levy, ***Hackers***, pag. 257, op. cit.

[12] S. Levy, nel citato ***Hackers*** (pag. 143), racconta come avveniva il distacco degli hacker maturi dal MIT: "…talora i planner scoprivano che un hacker si trovava intrappolato in qualche problema sui sistemi, oppure si fissava così tanto su attività extracurricolari… che i planner ritenevano che il suo lavoro non sarebbe stato a lungo interessante… Il tempo era terminato, in un certo senso. Avevano bisogno di lasciare il laboratorio… così, casualmente, capitava che ricevessero offerte di lavoro sorprendenti, oppure che si organizzasse qualche missione esterna… e se ne partivano in silenzio verso nuove aziende o altri laboratori".

rappresentò una sorta di “Woodstock dei computers”: una rivendicazione culturale, un segnale che il movimento si era diffuso così ampiamente da non appartenere più ai suoi progenitori.

I due anni successivi furono caratterizzati da una crescita senza precedenti per tale industria[13], iniziata inconsapevolmente dagli hacker della seconda generazione. Molti dei soci dell’Homebrew si trovarono di fronte al bivio di Jobs e Wozniak: entrare nel mondo degli affari o continuare ad “hackerare” come avevano sempre fatto. Tutto ciò portò al venir meno di quella pratica, a lungo sacra per il club, della condivisione delle tecniche, del rifiuto di mantenere segreti e proprietà sul flusso dell’informazione. La conseguenza fu un calo di partecipazione diretta non solo all’Homebrew, ma anche in tutti quei club minori che avevano costituito la spina dorsale del movimento informatico degli anni ’70.

L’industria dell’informatica produsse, prima della fine del decennio, milioni di computer, ognuno dei quali figurava come un invito, una sfida a programmare, ad esplorare, a creare nuovi linguaggi-macchina e nuovi mondi. I computer uscivano dalla catena di montaggio come materia prima, come fogli bianchi: una nuova generazione di hacker, quella degli anni ’80, si sarebbe occupata di plasmare quella materia, di riempire quei fogli, di creare un mondo che avrebbe guardato ai computer in maniera molto diversa dal decennio precedente.

La terza generazione di hacker fu composta da una cerchia di persone definite ***Software Superstar***[14], individui molto bravi a programmare sui p.c., ma lontani anni luce dai principi dei loro progenitori. La denominazione di hacker può essere mantenuta in virtù della curiosità, del voler “mettere le mani” sulla macchina, dell’amore per il computer, fermo restando un indirizzo di comportamento ben preciso: gli assegni delle royalties. S. Levy, nel più volte citato ***Hackers***, tratta questo momento storico come una continuazione dei precedenti, continua a riferirsi ad un’etica hacker che, a suo avviso, aveva solo incontrato il mercato.

In realtà, appare difficile immaginare un continuum tra il ventennio precedente e gli anni ’80, se non nel fatto che molti dei dirigenti delle case informatiche più

[13] Nel 1978 W. Christensen e R. Seuss crearono la prima BBS (bullettin board system).
[14] S. Levy, ***Hackers***, op. cit.

famose avevano un passato da hacker, e probabilmente avrebbero sempre mantenuto alcuni valori legati, però, ad un mondo passato. Si era realizzato, questo è vero, il sogno hacker di un computer per la gente comune, ma non si può non rimanere scettici di fronte ad affermazioni come "… perfino l'iter di comprare software già pronto da lanciare era tutto racchiuso in una certa atmosfera hacker, …c'era un'aria d'illegalità intorno al prodotto, era poco più rispettabile dei libri pornografici"[15].

I prodotti per eccellenza del terzo decennio furono i giochi, intorno ai quali si scatenò un mercato inimmaginabile fino a pochi anni prima. L'utente si sentiva in grado di domare il computer solo perché vi faceva girare l'ultimo software acquistato, e diveniva sempre più bravo nel giocarci fino a doverne acquistare un altro. Se qualcuno avesse voluto scrivere da sé il proprio kit di software, era finito il tempo della collaborazione in grande scala e dei lavori di gruppo. I pochi veri hacker dovevano scrivere da soli i propri programmi, migliorandoli solo con aggiunte casuali da parte di gruppi d'amici.

All'interno delle case produttrici dei giochi l'aria non era molto diversa: spesso burocrazie interne soffocavano le rare istanze hacker, i programmatori non erano assolutamente pagati per quanto riuscivano a far guadagnare le loro aziende, e convincere gli esperti di marketing a produrre un gioco innovativo era difficilissimo. Inoltre alcune case, come l'Atari, non segnalavano mai sulla confezione il nome del programmatore del gioco, rifiutandosi spesso di rendere pubblico il nome dell'artista quando la stampa lo richiedeva[16].

Il mercato non aveva aspettative e le sue caratteristiche finivano per coincidere con le finalità artistiche dei creatori di giochi, i "nuovi" hacker. Essi potevano tranquillamente creare i giochi con cui volevano giocare, ornando i programmi commerciali con raffinatezze che evidenziavano le loro capacità artistiche, e cercando di migliorare continuamente le possibilità dell'utenza. La pratica di esaltare il creatore del gioco di maggior successo divenne la norma, e cancellò per sempre il periodo in cui un hacker si sarebbe ritenuto più che soddisfatto nel vedere qualcuno che apprezzava l'artisticità del suo software.

[15] S. Levy, ***Hackers***, pag. 310, op. cit.
[16] A seguito di tali comportamenti cominciarono i primi abbandoni dell'azienda, che culminarono con la distruzione della quota di mercato dell'Atari nel settore dei giochi.

Ma il mercato di massa, nel momento della sua maggiore espansione, finì per trovare controproducenti dei giochi che fossero sempre migliori dei precedenti, l'importante divenne solo il profitto che avrebbero saputo dare alle case produttrici.

Se il mondo reale aveva cambiato l'hackeraggio, non era facile stabilire quanto ciò fosse una conseguenza ineluttabile della vasta produzione dei computer o se i fatti avrebbero potuto prendere una piega diversa. Si può affermare con certezza, però, che le profezie di chiunque avesse pronosticato la crisi dell'IBM erano andate in fumo. Il gigante dell'informatica aveva cambiato la propria strategia e si era adattato ai tempi: aveva aperto la sua macchina ed invitato società esterne a scrivere del software per il proprio prodotto, secondo una perfetta applicazione… dell'etica hacker[17].

L'azienda che riuscì a sfruttare nel modo più favorevole tale possibilità fu la MicroSoft di B. Gates, che la storia considera come una sorta di "traditore" dell'etica hacker. Egli scrisse un nuovo sistema operativo per l'IBM che divenne immediatamente uno standard industriale, ma è certo che l'etica hacker, a causa del denaro, aveva finito col tradirsi da sola prima che lo facesse Gates. Tuttavia, vi fu un momento in cui essa parve tornare agli antichi splendori, tentando una resistenza alla "copy protection".

La copy protection fu una reazione da parte delle case informatiche al mercato delle copie pirata. Il termine indica un procedimento con il quale si manometteva intenzionalmente parte del programma al fine di impedirne la duplicazione. Il blocco alle copie digitali non incrementava il valore del programma per l'utente, ma avvantaggiava il venditore del software. Taluni, con gran disappunto degli editori, si prodigarono per riuscire a copiare ugualmente i dischetti, ed alla fine vi riuscirono.

Queste persone erano degli hacker, fedeli al fatto che invalidare la protezione di una copia fosse naturale, convinti che ogni programma fosse migliorabile e che, quindi, era giusto penetrarvi e "collaborare" a tal fine. La reazione delle grandi aziende fu una trovata d'ingegno: cominciarono ad assumere la stessa categoria di

[17] Un'applicazione, a dire la verità, molto parziale, in quanto la segretezza sulle caratteristiche del software inserito rimase ferrea.

giovani hacker che rappresentava una minaccia, per escogitare contromisure tecniche di protezione. In altre parole c'erano ex-hacker, fortunati dirigenti d'azienda, che assumevano giovani hacker per difendersi da altri hacker, i quali reclamavano la stessa libertà che un tempo aveva ispirato gli attuali dirigenti.

Il termine "hacker" si trovava così a rappresentare diverse realtà. La generazione del Tmrc lo aveva considerato un termine da usare con parsimonia, uno status accessibile a pochi eletti capaci di fare arte con il computer. Il concetto aveva rappresentato delle abilità di comportamento ed i risultati da esse generati, e solo per traslato si era applicato ai soggetti che le possedevano. La generazione successiva era riuscita a portare il computer tra la gente, ed aveva cercato di far conoscere la cultura hacker alle persone interessate ad usarlo. Ciò non vuol dire che diventavano tutti degli hacker, ma fare delle nette distinzioni era più difficile perché la cultura dell'informatica si sovrapponeva in più punti a quella hacker, in quanto erano stati loro a far conoscere entrambe.

Il progressivo sbiadimento del termine prosegue nel decennio successivo, quando arriva a denotare i giovani autori di software di successo solo in virtù della loro abilità nello scrivere i programmi. Si era perso il contenuto etico del concetto, quei valori che erano stati di pochi ma che, una volta diffusi, venivano plasmati a concezioni e necessità diverse. Neppure giovò, ai primi hacker, il divenire popolare del termine, che col tempo andò assumendo una connotazione specifica negativa.

La parola, una volta in possesso dei media, divenne sinonimo di "trasgressore digitale", accoppiata allo stereotipo di un secchione poco sociale con l'abilità di evocare dal computer una strana magia criminale. A riprova di ciò si pensi che, prima di uscire nelle sale cinematografiche, il film culto "Wargames" venne sottoposto alla visione di un comitato del Congresso americano, per assicurarsi che non contenesse un incitamento alla pratica dell'hackeraggio. A poco valsero le varie "conferenze hacker" che, sul finire degli anni '80, tentarono di riportare il termine agli antichi splendori.

A riprova del definitivo cambiamento di clima si possono citare le numerose operazioni delle forze dell'ordine, iniziate nel 1987, che portarono i Servizi Segreti

americani a raccogliere, in pochi anni, un dossier d'indagine su tutti i soggetti che sembravano contare veramente nell'underground digitale statunitense.

2.2. Il Chaos Computer Club e l'Icata'89: il fenomeno hacker sbarca in Europa.

La prima realtà hacker nella situazione europea è rappresentata dal Chaos Computer Club d'Amburgo, fondato nel 1984[18], che ha mostrato fin dagli inizi una gran consapevolezza delle proprie origini culturali e politiche. Il CCC, richiamandosi esplicitamente all'esperienza del TAP (il Party Line di Hoffman), è diventato un punto di riferimento per tutto il movimento underground europeo, che muoveva i primi passi verso la frontiera digitale.

Ricalcando le gesta dei loro progenitori americani, i membri del CCC ne hanno mutuato la filosofia della socializzazione del sapere tecnologico, realizzabile mediante banche-dati accessibili via telefono, sistemi aperti al pubblico, raccolta e distribuzione gratuita di password d'ogni tipo. Per non incorrere in persecuzioni penali, il club ha aperto da subito una sede registrata e si è fatto classificare giuridicamente; ciò lo ha costretto a tenere una dettagliata regolamentazione degli iscritti.

Il primo bersaglio del gruppo è stato il progetto BTX delle Poste tedesche, un servizio computerizzato in grado di offrire scambi di comunicazioni personali, prenotazioni di merci ed altri servizi in rete. In quegli anni, il governo tedesco stava lanciando l'idea di un censimento informatizzato di tutta la popolazione, ed il CCC ne ricevette preoccupazioni molto fosche riguardanti le future libertà dei singoli cittadini.

Tramite una password, che in seguito il club dichiarò di aver ricevuto, a causa di un errore del BTX, dall'Haspa, la Cassa di Risparmio d'Amburgo, il CCC inventò una beffa alla stessa banca. Collegati al computer dell'Haspa tramite il BTX, i membri del club gli lasciarono in memoria di richiedere in continuazione un certo servizio che

[18] Ma le prime riunioni, allora spontanee e prive di una sede stabilita, si svolgevano già dal 1981, tra persone che volevano lavorare con i computer e realizzare una propria rete. (***Cyberpunk***, di R. V. Scelsi, op. cit.)

essi offrivano in rete, ricavandone in una sola notte c.ca 135mila marchi. Invece di ritirare il denaro il CCC denunciò la poca affidabilità del sistema, e lo scandalo che ne seguì fece naufragare il progetto delle poste tedesche.

Le gesta del CCC lo hanno portato a divenire uno spauracchio, nel mondo della security degli ultimi anni '80, ad attirarsi le accuse di lavorare per i servizi segreti dell'est[19], di mantenere i piedi in due staffe: da una parte predoni dello spazio virtuale, dall'altra i principali artefici del successo dell'industria elettronica. In realtà essi hanno svolto un ruolo chiave nella diffusione della cultura tecnologica alternativa, della quale hanno sempre cercato di socializzare gli strumenti ed i saperi per arrivare a creare da sé l'informazione.

Essere un hacker del CCC, nelle parole di uno dei leader, Wau Holland, vuol dire "essere dentro una situazione appena questa accade e poter da questa creare nuovi significati; … la nostra filosofia è una sola, libertà, ed in questa prospettiva cerchiamo di lavorare attraverso lo scambio d'idee ed invenzioni sociali con altre persone"[20].

Un altro dei leader storici, S. Wernèry, ci tiene a sottolineare che: "Gli hacker sono persone che non distruggono, essi si considerano ospiti quando sono in altro sistema e quindi godono dell'ospitalità e sono cordiali con il loro ospite… La più grande catastrofe, per un hacker, è la sempre maggiore dipendenza dell'uomo dalla tecnologia, una società civile sempre più dipendente dalla tecnica… Gli hacker non devono essere criminalizzati, ma inseriti socialmente, in modo che le loro forze si possano sviluppare verso una direzione costruttiva. Questo è realizzabile con una legge che disciplini le loro azioni, così come accade per i radioamatori"[21].

Purtroppo i fatti successivi sembrano aver preso una piega diversa: lo scorso dicembre, nel parco di Neukoelin (Berlino), è stato trovato il corpo senza vita di Boris Floricic, uno dei fondatori del CCC, famoso per le sue denunce contro i pericoli della società cibernetica. Floricic era stato il primo a sottolineare la vulnerabilità d'alcuni

[19] Vedi C. Stoll, ***Il nido del cuculo,*** Sperling&Kupfer, Milano, 1990 e B. Sterling, ***Giro di vite contro gli hackers***, Shake, Milano, 1993.
[20] R. V. Scelsi, ***Cyberpunk***, pag. 134-137, op. cit.
[21] Da "Intervista con Steffen Wernèry, realizzata in Germania nel gennaio 1989", ad opera di F. Berghella e R. Cena, capitolo di "***Computer Crime, Virus, Hackers"***, rapporto dell'IPACRI edito dalla Buffetti, Roma, 1989.

sistemi elettronici, ed a battersi contro il dominio digitale dei servizi segreti internazionali: il fatto che il suo corpo sia stato ritrovato penzolante da un albero, con una corda intorno al collo ed i piedi appoggiati al terreno, pone molte ombre sulla tesi di suicidio perorata dalla polizia tedesca[22].

Seguendo il modello del CCC d'Amburgo, in breve tempo sorsero dei gruppi simili: gli ***Hack Tic*** in Olanda, i ***Bayerische HackerPost*** ed i ***Links*** a Monaco, club minori a Stoccarda. Quasi tutti mantennero come caratteristica basilare la visibilità. Strumenti essenziali per questa contaminazione in tutta l'area nordeuropea sono stati gli incontri annuali, i Chaos Communication Congress, organizzati tra Natale e Capodanno; in tali incontri, tutto il movimento (c.ca 400 persone) ha colto l'occasione per scambi di dati, discussioni, workshop, ma anche per assistere da vicino ad operazioni di hackeraggio ai danni di grosse reti pubbliche.

Ma l'incontro progettuale dall'esito più felice è stato sicuramente quello con la parte più politicizzata del movimento americano, avvenuto ad Amsterdam nel 1989 in un vero e proprio congresso, dove l'underground europeo e quello americano, pur tra mille diverse sfaccettature, si sono riconosciuti nell'immaginario collettivo del Cyberpunk[23].

Il discorso d'apertura dell'ICATA'89 di Amsterdam è stato effettuato da un vecchio membro dell'Homebrew computer club, Lee Felseistein, secondo il quale le scelte operate dai tecnologisti avevano posto dei limiti alle azioni politiche perché si erano basate sul concetto di gerarchia e di minaccia fisica; vi si doveva opporre una comunicazione diffusa nei due sensi, non gerarchizzata, agendo per occupare gli spazi pubblici. L'obbligo era d'allargare il più possibile la comunicazione, creando degli strumenti per la formazione e la rinascita di comunità tra loro comunicanti.

Il 4 agosto, al termine dei tre giorni del congresso, veniva adottata una dichiarazione programmatica finale, basata su alcuni principi di base; tra questi la pratica dell'hackeraggio era letta come necessaria per infrangere il monopolio statale

[22] Vedi ***Hacker, il nuovo cattivo di Hollywood*** di P. Casella, pubblicato il 29/1/'99 nella sezione "attualità" del sito www.caffeeuropa.it.
[23] Parlando di Cyberpunk, si fa riferimento ad un complesso d'idee, ad un insieme di figure narrative e retoriche, ad alcuni autori e gruppi che sembrano dare espressione politica alle utopie ed alle paure collegate, in quegli anni, allo sviluppo tecnologico. La narrativa che da voce a questo fenomeno culturale nasce negli USA, e viene principalmente identificata con i romanzi di W. Gibson e B. Sterling.

delle multinazionali dell'informazione. Profondamente turbati dalla prospettiva di una tecnologia dell'informazione senza controllo democratico, né partecipazione popolare efficace, gli hacker dichiaravano che - lo scambio libero e privo d'ostacoli dell'informazione è un elemento essenziale delle libertà fondamentali, da riconoscersi in ogni circostanza, e nulla deve impedire l'esercizio di questo diritto. L'intera popolazione deve controllare, in ogni momento, i poteri del governo perché l'informazione possa allargare e non ridurre l'estensione di tale diritto.

L'informazione – proseguivano gli hacker – appartiene a tutto il mondo, ed informatici, tecnici e scienziati sono al servizio di tutti. Al diritto all'informazione va unito quello di scegliere il vettore di quest'informazione, evitando che sia imposto un unico modello d'informatizzazione. Nessun'informazione di natura privata deve essere immagazzinata, o ricercata, tramite mezzi elettronici senza esplicito accordo della persona interessata[24]: i dati pubblici devono essere resi liberamente accessibili, quelli privati vanno protetti senza incertezze. Tutte le legislazioni contro pirati informatici, che non perseguono scopi criminali o commerciali, devono essere ritirate immediatamente. L'informatica deve essere usata come puro strumento d'emancipazione, di progresso, di formazione e di piacere.

Ogni informazione – concludevano gli hacker dell'ICATA'89 – è al contempo deformazione. Il diritto all'informazione è anche diritto alla deformazione, in quanto più si produce informazione più si crea un caos sfociante in sempre maggiore rumore. La distruzione dell'informazione, come la sua produzione, è nel diritto inalienabile di ognuno. I canali regolamentari e convenzionali d'informazione devono essere sovvertiti, mentre la libertà di stampa deve applicarsi anche alle pubblicazioni tecno-anarchiche che reclamano la liberazione dei popoli[25].

[24] Notare le somiglianze con alcuni passaggi della recente legge n.675/96 sulla privacy.
[25] I principi enunciati sono rintracciabili nel testo ***"Cyberpunk"***, di R. V. Scelsi, pag. 107-109, op. cit.

2.3. La nascita della cultura hacker in Italia: dagli smanettoni ad Internet (‘82-‘94).

Nell’Italia dei primi anni ’80 non si parlava ancora di hacker, né dei diversi significati legati in seguito a tale termine. In quegli anni stavano nascendo i primi circoli, a volte veri e propri sgabuzzini, dove si vendevano computer e programmi, messi assieme da appassionati un po’ incoscienti che avevano deciso d’investire in questo settore. I rapporti tra il negoziante ed i ragazzi acquirenti non erano ancora ben definiti: egli barattava con loro alcuni giochi, a volte ne acquistava alcuni dai suoi clienti se gli sembravano ben fatti, ed era sempre ben fornito di copie non proprio legali dei software più richiesti.

Ai primi tentativi delle case straniere di proteggere i propri prodotti, facevano sempre seguito nuove tecniche d’intrusione[26]. I primi hacker (nel significato letterale inglese del termine “to hack”) furono degli utenti presto stanchi di giocare, che cercarono nei videogames degli stimoli diversi, ed iniziarono la sfida al funzionamento finendo per modificarne il linguaggio. La conoscenza del linguaggio macchina permise di rimuovere le protezioni e di creare la prima divisione interna al mondo degli appassionati: quelli che volevano soltanto giocare, e quelli per i quali la cosa più importante era capire il gioco in sé[27]. Spesso questi patiti dell”hands on” italiano erano raggirati dal mercato, che ne sfruttava la passione ottenendo manodopera qualificata a costi praticamente nulli.

In assenza di corsi sull’Assembler, il linguaggio più usato dai computer di quegli anni (Commodore 64, ZX Spectrum, …), gli smanettoni erano costretti a fare da soli, scambiandosi informazioni per vie più o meno ufficiali. Questo li portava ad essere spesso molto più avanti della media italiana, ma ne rallentava lo sviluppo, che in un contesto diverso sarebbe potuto essere meno faticoso e approssimato. Forse perché ignorati dalle università e dai centri organizzati del sapere, i giovani hacker italiani andavano nel frattempo sviluppando un’altra caratteristica simile ai colleghi

[26] In Italia vi erano diversi gruppi, alcuni molto bravi e specializzati nel penetrare nelle protezioni. I più famosi erano Paradox, Paranoimia, RobocopBBS, Italian Bad Boys e Comax. (***Spaghetti hacker***, di S. Chiccarelli e A. Monti, Apogeo, Milano, 1997).

[27] S. Chiccarelli e A. Monti, nel loro “Spaghetti hacker” (vedi nota precedente) attribuiscono a questa seconda categoria la definizione di “smanettoni”, e la descrivono come la via italiana al complesso tema del rapporto con la tecnologia ed il futuro, fatta di gioco, intelligenza e passione per le macchine. Caratteristiche autonome, soprattutto non criminali, sembrano differenziare questa categoria dai “cugini” americani.

statunitensi, vale a dire l'intolleranza e la poca fiducia verso il mondo accademico-istituzionale, il che li faceva sentire "fuori dagli schemi".

In seguito all'arrivo in Italia dei primi accoppiatori telefonici per Apple II, messi insieme a modem a 300 baud autocostruiti, gli smanettoni cominciarono a "muoversi" tramite il computer, usando la rete ITAPAC della SIP. Le mete preferite di quei "viaggi" erano il QSD, una messaggeria francese su Minitel, ed Altos e Altger, dei computer tedeschi sui quali erano istallati sistemi UNIX capaci di far comunicare gli utenti in tempo reale. Tali macchine finirono per essere un punto d'incontro per molti hacker europei, che si scambiavano informazioni tecniche, password, ma soprattutto parlavano e rivelavano una passione comune.

In Italia, nel 1986, vi erano già tre BBS, fra le quali il primo storico nodo della rete FidoNet. Legati alle BBS sorsero anche i primi club di hacker, il più famoso dei quali era il DTE222 di Milano, i cui maggiori esponenti avevano nomi celebri come ***Virus*** o ***Blue Boy***. Nello stesso anno nasceva il servizio Videotel, che nel 1989 migliorò le sue qualità interattive consentendo la nascita di messaggerie per gli utenti.

Intorno al Videotel nacquero le prime "comunità virtuali", tanto che questo raggiunse nel 1991 i 177mila utenti. Nonostante la quasi totale mancanza di contatti con i colleghi statunitensi, presero piede una serie di concetti che ricalcavano le stesse richieste che il movimento americano aveva effettuato negli anni '70: la libertà d'informazione, la lotta alle corporazioni e la volontà di esplorare nascevano dal comune denominatore del ciberspazio.

Naturalmente, i giovani hacker degli anni '80 cercarono subito un sistema per non pagare il Videotel, per usarlo come collegamento con i computer della SIP, per raggiungere altre reti. Pare che la SIP, per lanciare il servizio, regalasse password e fingesse di non vedere lo scambio che ne veniva fatto, così molte di queste divennero di dominio pubblico. Inoltre, l'algoritmo per la creazione del PIN (il numero segreto d'accesso) era molto semplice da individuare, tanto che in poco tempo si crearono dei veri e propri programmi in grado di generare quei codici.

Il “mercato” delle password era in continuo fermento, in quanto ognuna di esse, con l’aggiunta del rispettivo PIN, consentiva di collegarsi in rete gratuitamente, scaricando i costi sullo sfortunato effettivo possessore di quell’accesso[28]. Accortasi tardi di ciò che stava accadendo, la SIP tentò di cambiare nuovamente il sistema delle password, rendendo più ardua la loro scoperta. Tale cambiamento, unito ad altri fattori come l’aumento delle pagine dedicate ai servizi ed alla pornografia, l’arrivo di molti avventurieri che volevano guadagnare facilmente col Videotel, un contenzioso in corso tra gestori e FIS[29], contribuì ad un brusco calo d’utenti, concluso con l’interruzione del servizio Videotel nel 1992.

Gli hacker utenti di Videotel si trasferirono in massa sulle BBS amatoriali, alcune delle quali stavano diventando dei veri e propri negozi on-line di software di contrabbando (***warez***, da una storpiatura dello stesso termine software): per ogni programma inviato c’era un corrispettivo variabile di warez che si poteva prelevare. In Italia, a differenza degli USA, il software fu spesso concepito come un semplice oggetto commerciale, e la programmazione non fu mai un’arte fine a se stessa. Tale carenza ideologica ha contribuito all’identificazione, tutta italiana, dell’hacker come delinquente[30], anche se in tale pratica sembra nascere prima il delinquente ed in seguito l’hacker.

Le prime BBS erano isolate e di non facile accesso. Dopo aver ottenuto, spesso con molta pazienza, il permesso del sysop[31], si accedeva ad un livello iniziale, più basso, che non consentiva il collegamento a tutte le aree della BBS. Le BBS pirata erano divise gerarchicamente secondo il ruolo svolto all’interno del sistema, e tale divisione permetteva al software appena realizzato di girare velocemente. All’inizio degli anni ’90 circolò la voce che delle case di software

[28] In relazione all’etica hacker, Chiccarelli e Monti (***Spaghetti Hacker***, pag. 41, op. cit.) rivelano che “si faceva molta attenzione a non caricare un utente privato di costi aggiuntivi, prediligendo l’uso di PIN e password di grosse realtà commerciali o pubbliche, confortati dalla consapevolezza che tanto anche i loro dipendenti facevano altrettanto”.
[29] Fornitori dei servizi d’informazione.
[30] La nostra società, a base culturale umanistica, deve aver deciso in partenza che in tale figura vi fosse qualcosa di pericoloso, affibbiandole una connotazione negativa assente, come visto, nel termine inglese.
[31] Acronimo di System Operator (noto anche come Sysadmin, System Amministrator), cioè il gestore della BBS, che si riservava di accettare o meno le richieste d’accesso.

usassero le BBS pirata per fare pubblicità ai loro prodotti, ma restarono solo delle supposizioni prive d'effettivi riscontri[32].

Le comunità più numerose si formarono attorno a due BBS romane, MC-Link e Agorà, ed una milanese, Galactica (che in seguito sarà la prima ad offrire un accesso completo ad Internet per 200mila lire). Il sistema ***matrix***, di tecnologia FidoNet, consentì lo scambio di posta elettronica tra diverse BBS, mediante chiamate telefoniche automatizzate. Le caratteristiche FidoNet (una semplice struttura gerarchica, costi ottimizzati, tempi ragionevolmente brevi, una richiesta di risorse tecniche non eccessive) permisero al sistema di soddisfare a lungo la smania telematica degli smanettoni, molti dei quali riuscirono a divenire gestori di un nodo, mettendo così in pratica un sogno.

Essere un nodo FidoNet permetteva, al giovane hacker italiano, di amministrare una piccola parte del ciberspazio nostrano, avere nuovi contatti, superare ostacoli tecnici sempre diversi, imparare a realizzare ed a configurare nuovi programmi. Le esperienze quotidiane su quella nuova rete erano raggruppate in un vero e proprio codice di comportamento, la Policy. Questa era un documento molto complesso, che regolava sia gli aspetti tecnici sia i comportamenti degli utenti[33]. Se certe norme potevano apparire ragionevoli, il contenuto di altre poteva suscitare reazioni fra gli utenti più sensibili alla tutela dei diritti civili.

Ad esempio, il sysop era considerato responsabile per il traffico generato nel suo nodo, anche se immesso in rete da altri utenti, e persino per quello che transitava il suo nodo come semplice passaggio verso altre destinazioni. I messaggi non potevano avere alcun tipo di crittografia, e FidoNet non si sentiva in grado di garantire alcuna privacy sui messaggi in questione[34]. Risultano così comprensibili i motivi per cui, in quel periodo, gli smanettoni più estremisti, sostenitori di una vera

[32] Tuttavia, se si presta fede alla teoria già discussa in merito al caso di B. Gates, vale a dire la possibilità che un programma acquisti fama e venga migliorato in seguito al suo percorrere vie non ufficiali, tali supposizioni appaiono meno inventate.
[33] S. Chiccarelli e A. Monti, nel loro ***Spaghetti hacker*** (op. cit.) commentano (pag. 113): "Per inciso è singolare che tutti quelli che al momento si stanno scervellando sul modo di regolamentare la Rete – Unione Europea in testa – non abbiano preso in considerazione il frutto dell'esperienza dei migliori consulenti che avrebbero potuto sperare di trovare: quelli che una Rete mondiale la avevano "creata".
[34] Tali affermazioni non avevano nessun valore rispetto alla legge italiana, per la quale si è responsabili in ambito penale solo ed esclusivamente per ciò che si fa.

contro-cultura hacker, abbandonarono la madre FidoNet per creare una rete alternativa di nome Cybernet, che fece del Cyberpunk uno stile di vita.

La cultura Cyberpunk permise agli hacker italiani di confrontarsi con esperienze europee ed americane, di scoprire alcune origini comuni, di dare sfogo alla loro insofferenza verso il sistema, ma non fu mai un riferimento univoco per tutti gli smanettoni italiani. Possiamo considerarla una delle matrici della cultura hacker italiana, sicuramente quella che maggiormente l'avvicina ai cugini statunitensi.

Una delle tematiche Cyberpunk che ebbe maggior fortuna in Italia fu "INFORMATION WANTS TO BE FREE", l'informazione vuole essere libera. Seguendo questo slogan, Cybernet divenne il primo luogo pubblico italiano nel quale si discusse liberamente di hacking, phreaking, etica hacker, cyberpunk. In quest'oasi tecnologica gli hacker italiani trovarono il luogo ideale per vivere una nuova visione del mondo, che passava attraverso l'analisi del rapporto uomo-macchina per giungere a concezioni molto ardite a quei tempi.

In Italia, già dal 1987 l'ampio dibattito interno all'area underground, relativo ai mutamenti sociali in atto nelle metropoli, aveva prodotto la nascita di una rivista storica, ***Decoder***, il cui titolo faceva chiaramente riferimento all'omonimo film di K. Maeck. Questi, intervistato in merito al suo film, spiegava: "La decodifica dell'informazione nascosta, sperimentata con questi nuovi bit e chips, è il tema principale del film.(…) La guerra totale vera è diventata guerra d'informazione; viene combattuta ora distribuendo informazione"[35].

In seguito alla diffusione in Italia d'alcuni testi base della cultura Cyberpunk, come ***Neuromancer*** e la ***Trilogia dello Sprowl*** di W. Gibson, molti smanettoni trovarono codificati modi di vita, comportamenti e valori, l'esistenza di una vera e propria ideologia che essi condividevano senza saperlo. Gibson, insieme con Sterling, Cadigan, Rucker e molti altri, svolse un ruolo fondamentale nella formazione del background culturale degli hacker italiani. Infatti, se in America la tecnologia aveva da sempre accompagnato la vita quotidiana di molte persone arrivando ad

[35] FTI (Forum per la Tecnologia dell'Informazione), ***Osservatorio sulla criminalità informatica. Rapporto 1997***, (pag. 40), Franco Angeli, Milano, 1997.

influenzare pesantemente la società, in Italia non si era mai sviluppato un diffuso movimento culturale che avesse una base simile.

Nel marzo del 1988, il Ministero dell'Università e della Ricerca Scientifica e Tecnologica (MURST) aveva istituito il GARR[36], una commissione apposita con l'obiettivo di far convergere tra loro alcune reti, di proprietà delle facoltà universitarie più tecniche (Fisica ed Ingegneria). Con il passare del tempo, la rete universitaria (ormai definita rete GARR) continuava a crescere ed espandersi, e ciò portò alla riorganizzazione della commissione che modificò il proprio nominativo in OTS-GARR[37] (1994).

Molteplici i ruoli svolti dal GARR nel passaggio tra i due decenni, ma il più importante nella storia dell'hackeraggio in Italia rimane l'avervi "portato" Internet. Tramite la Rete, generazioni di smanettoni hanno potuto conoscere un nuovo mondo, migliorare la propria preparazione acquisendo notevoli abilità tecniche, prendere coscienza della propria funzione in un sistema. Vista la necessità dell'autorizzazione di un docente per accedere alle macchine, molti giovani hacker cominciarono a frequentare di più l'università per entrare nelle grazie di qualche professore, per convincerlo dell'assoluta necessità di aprir loro un account per motivi di "ricerca scientifica".

In realtà il mondo universitario, che avrebbe potuto costituire il fulcro dello sviluppo di Internet a livello italiano, non dimostrò mai una particolare attenzione per il nuovo medium, forse considerato un nuovo giocattolo troppo costoso per chi doveva occuparsi di ben altri argomenti. In ogni modo le università furono, senza dubbio, una delle prime palestre dove gli smanettoni appresero i rudimenti della navigazione in rete, lasciando le LAN accademiche quando si sentirono in grado di camminare (anzi, navigare) da soli.

La razza dello smanettone italiano non prosperava soltanto fra fisici ed ingegneri, ma anche in facoltà non tecniche; infatti, la vera ambizione degli hacker nostrani era l"hands on" sulle macchine, di qualsiasi facoltà fossero, e spesso tale ambizione si fondeva ad interessi umanistici e letterari. Inoltre gli smanettoni non

[36] Gruppo per l'Armonizzazione delle Reti di Ricerca.
[37] Organismo Tecnico Scientifico relativo al Gruppo per l'Armonizzazione delle Reti di Ricerca.

Figura 1 **Principali differenze fra un hacker ed uno smanettone**

	Hacker Made in USA	Smanettone Made in Italy
Ambiente	Le tecnologie accompagnano la vita quotidiana, ed influenzano la società	Le tecnologie hanno scarsa influenza sulla vita quotidiana e sulla società
Origine	College, fine anni'50.	Primi piccoli negozi di p.c., inizio anni'80
Rapporto con gestori conoscenza	Rapporto definito con i gestori della conoscenza tecnologica (professori)	Rapporto indefinito con i gestori della conoscenza tecnolog. (primi negozianti)
Primi strumenti	Plastici elettrici, linee telefoniche	Videogiochi
Corpo organico di concetti e costumi	Costituzione lenta ma continua, volontà di diffusione fuori dai college	Assenza di tale corpo organico di concetti e costumi
Commistioni politico-ideologiche	Presenti, con movimenti anarchici e pacifisti	Assenti
Conseguenze della propria passione	Passione come punto di contatto con colleghi di studio ed insegnanti	Passione come fonte d'isolamento all'interno dell'università
Storia e scontri generazionali	40 anni di storia hacker, diverse generazioni, forti scontri generazionali	15 anni di storia hacker, meno differenza tra generazioni, ridotti scontri generaz.
Rapporti con il mercato	Confusi, spesso il mercato riesce a piegare i giovani alle proprie regole	Il mercato ed i soldi non fanno scendere i giovani a compromessi
Rapporti con la stampa	Buoni nei momenti di maggiore tensione con le forze dell'ordine	Cattivi nei momenti di maggiore tensione con le forze dell'ordine

Fonte: Nostra elaborazione sulla base delle informazioni bibliografiche.

Figura 2 **Punti di contatto fra un hacker ed uno smanettone**

- Caratteristiche: curiosità, filosofia di socializzazione, apertura e decentramento, la sfida, l'imperativo dell'hands on, la libertà di comunicazione, l'elevato know-how tecnologico.
- Sviluppo della cultura come prettamente maschile, almeno nei primi decenni.
- Tendenza a sfociare nell'illegalità, scontri con le forze dell'ordine.
- Intolleranza verso il mondo accademico-istituzionale.
- L'affiliarsi dei soggetti in club ed associazioni.
- La presenza del movimento Cyberpunk nel sostrato culturale di riferimento.
- La difficoltà, da parte delle forze dell'ordine, di additare alla popolazione il crimine informatico come attentato alla sicurezza, risultato raggiunto solo negli ultimi anni.

Fonte: Nostra elaborazione sulla base delle informazioni bibliografiche

erano solo studenti, ma annoveravano nelle loro fila diversi assistenti di varie cattedre che, fatto firmare all'ignaro docente il modulo di richiesta, utilizzavano successivamente in proprio tale opportunità.

Un dato preoccupante, però, riguardava l'isolamento dei giovani hacker rispetto agli altri studenti, per non parlare del corpo docente, che sembrava non rendersi conto delle sconfinate possibilità proposte dalla rete. Tale situazione fu una delle cause della ricerca, da parte del giovane studente isolato, di connettersi ad Internet da casa, perché collegarsi dall'università dava soltanto dei problemi in più e non sembrava offrire niente in cambio. Tra l'altro, come precedentemente citato, in quel periodo la BBS Galactica fu la prima ad offrire collegamenti completi a 200mila lire l'anno, ed agli smanettoni non parve vero.

2.4. USA'90 e Italia'94: le grandi operazioni di repressione.

La nascita e lo sviluppo della cultura hacker in USA ed in Italia, fin qui tracciate, hanno evidenziato uno svolgimento simile in alcuni punti e molto diverso in altri, tanto da delineare una sorta di ***via italiana*** al rapporto con le nuove tecnologie; queste ultime, peraltro, inevitabilmente d'origine statunitense. Tuttavia vi è un momento critico simile, attraversato ovviamente in tempi diversi, che induce quasi a ritenere che vi siano dei passaggi obbligati, degli interventi urgenti, delle prese di consapevolezza necessarie sulla via della "maturità informatica".

Il riferimento è a due famosi interventi delle forze dell'ordine, il primo avvenuto negli USA nel 1990-91, il secondo in Italia nel 1994, entrambi aventi come obiettivo il sottobosco della criminalità informatica, o almeno coloro che si ritenevano esserne i rappresentanti. Punti di somiglianza sono rintracciabili nelle modalità con le quali sono state condotte le operazioni, nello scopo più generale delle medesime, nella scarsità dei risultati ottenuti, nonché in una certa presa di coscienza interna al mondo degli hacker, originata dall'aver subito un trattamento lesivo verso le proprie libertà.

La vasta operazione di polizia, cominciata negli Stati Uniti nel 1990 in seguito ad un guasto all'interno di un sistema di comunicazione dell'AT&T, una nota

compagnia elettrica, è ufficialmente conosciuta come Hacker Crackdown, anche se il suo vero nome era "Operazione Sundevil". Tale operazione deve la sua fama all'omonimo libro di B. Sterling[38], il quale l'esamina nei minimi particolari svelandone i più curiosi retroscena. L'autore rivela come già da tempo i servizi segreti americani avessero nel mirino una serie di personaggi e di BBS, che svolgevano dei traffici ritenuti poco legali, e che si aspettasse soltanto l'occasione propizia per dare il via ufficiale.

Il lento avvicinamento era cominciato nel 1984 con il ***Comprehensive Crime Control Act*** [39], cui era seguita, l'anno successivo, la messa a punto della prima BBS trappola, dove il sysop ed alcuni utenti erano degli agenti alla ricerca di cyber-criminali. Nel 1986 erano stati approvati il ***Computer Fraud and Abuse Act*** e l'***Electronic Communication and Privacy Act***, ma questi tentativi per tenere aggiornato il sistema legale evidenziarono presto i loro difetti nel regolare una materia, i reati informatici, in rapido sviluppo[40].

Nel 1987 i giudici di Chicago avevano formato la Computer Fraud and Abuse Task Force, la più aggressiva unità contro i criminali informatici, uno degli obiettivi della quale era operare per convincere l'opinione pubblica che tale minaccia fosse davvero importante e pericolosa per la pubblica sicurezza[41]. I vari dossier, raccolti su quelli che si ritenevano essere gli esponenti di spicco della criminalità informatica americana, non aspettavano altro che essere aperti.

Il 15 gennaio 1990, Martin Luther King Day, quando il servizio telefonico dell'AT&T andò in tilt a causa di un piccolo difetto di programmazione in un software nuovo di zecca, e c.ca 70milioni di chiamate rimasero interrotte per quasi nove ore, a qualcuno non parve vero di far pagare agli hacker con gli interessi anni d'abusi sul sistema telefonico, anche se nell'incidente in questione essi non avevano alcuna responsabilità.

---

[38] Il titolo originario dell'opera è ***Hacker Crackdown***, che in italiano è stato tradotto come ***Giro di vite contro gli Hacker*** (Shake, Milano, 1993).
[39] La legge americana sulle truffe mediante computer e carte di credito.
[40] Prova ne fu la scarsità di processi prodotti da tali leggi negli anni '86-'90.
[41] E' importante sottolineare che in USA, come in Italia, la polizia dovette faticare molto per additare alla popolazione il crimine informatico come un attentato alla sicurezza, e che entrambe le operazioni non ebbero un gran successo sotto quest'aspetto.

L’operazione che ne seguì agì su scala nazionale, provocò arresti, accuse legali, un processo drammatico e spettacolare, numerose dichiarazioni di colpevolezza e sequestri di macchine e dati in tutti gli USA. Il Servizio Segreto degli Stati Uniti, le organizzazioni private di sicurezza delle compagnie telefoniche, le polizie locali e nazionali di tutto il paese misero insieme le forze in un deciso tentativo di annientare l’underground elettronico americano, anche se i risultati furono sicuramente inferiori alle attese.

Fin dall’inizio la segretezza fu un grosso problema: gli hacker erano sempre stati molto sfuggenti, i crimini erano molto tecnici e difficili da descrivere (sia per la polizia sia per il cittadino medio) e, quando in altre occasioni si era tentato di farlo, l’effetto era stato quello di aumentarne enormemente il numero. I capi delle telco, le organizzazioni private di sicurezza delle compagnie telefoniche, non avevano nessun interesse a pubblicizzare la debolezza dei loro sistemi, e si temeva che una campagna aperta contro gli hacker avrebbe lasciato tali sistemi inermi di fronte ad un contrattacco dei pirati informatici. Tuttavia, si cercò ugualmente d’avere la pubblicità necessaria contemporaneamente alla segretezza richiesta: si diede gran risalto agli arresti dei singoli hacker, e si lasciarono nel vago le azioni da loro commesse.

Le eventualità che gli hacker accusati potessero richiedere un processo, che i giornalisti arrivassero a considerarli dei “bravi ragazzi” trattandoli con indulgenza, che ricchi imprenditori dell’alta tecnologia offrissero loro aiuti economici e morali, non furono mai prese in considerazione dagli autori dell’operazione Sundevil, tanto che l’accadere di ognuno di questi eventi finì per minare le basi dell’operazione stessa.

Il gruppo underground più rumoroso ed indisponente, con il quale le autorità americane si erano più volte scontrate, era la “Legion of Doom”, e si tentò subito di colpevolizzare loro per il collasso del sistema telefonico. Non erano tanto i reati effettivamente commessi, quanto la potenzialità di questo gruppo (che la polizia ritenne a lungo molto numeroso ma che, in realtà, non lo fu mai) a spaventare gli agenti, e l’obiettivo d’incastrarli fu affidato alla citata Computer Fraud and Abuse Task Force.

Si arrivò a dimostrare che gli hacker della “Legion of Doom” (la polizia n’arrestò solo tre, ma rimase convinta che fossero in numero maggiore) avrebbero

avuto le capacità per far collassare la rete telefonica, ma non si raccolsero mai prove inconfutabili della loro colpevolezza. La Task Force tentò d'incastrarli con una faccenda di software sottratto illegalmente all'AT&T, ma l'accusa restò sullo sfondo perché non fece nessuna presa sull'opinione pubblica.

Vari soprusi furono commessi dagli agenti implicati nell'Hacker Crackdown[42], ma taluni di essi sfiorarono il ridicolo, e finirono per arrecare del danno alla polizia stessa che fu accusata d'ignoranza e superficialità nella condotta delle operazioni. Quaranta computer furono sequestrati senza motivo, assieme a stampanti, dischetti[43], mouse ed ogni genere d'accessorio che la polizia ritenne pericoloso. Anni dopo il termine dell'operazione, tale materiale doveva ancora essere restituito ai proprietari.

Un editore di fantascienza, Steve Jackson, vide un suo manuale di giochi di ruolo sequestrato, con l'accusa di essere un "manuale per il crimine informatico", assieme a tutti i computer ed al materiale già pronto per la stampa. Si può immaginare il risalto che diedero i media al sequestro di un computer, da parte del Servizio Segreto, per evitare la pubblicazione di un libro di fantascienza cyberpunk.

L'operazione Sundevil non si concentrò solo contro la "Legion of Doom", ma colpì anche diverse BBS[44], che agli occhi della polizia rappresentavano solamente dei gruppi di persone intente a cospirare contro la legge.

In realtà tale visione non era totalmente errata, in quanto le BBS underground offrivano anche programmi per lo "scanning" dei codici telefonici, software per depredare le compagnie che gestivano carte di credito, password violate, schemi per blue box, manuali d'intrusione, file sull'anarchia e materiale pornografico. Tuttavia, ciò non giustificava il contenuto dei manuali d'addestramento federale d'allora, che descrivevano i bollettini solo come focolai del crimine infestati da pervertiti e pedofili.

La conseguenza di maggior rilievo di tutta l'operazione Hacker Crackdown fu la nascita dell'***Electronic Frontier Foundation***, un nuovo ed insolito gruppo d'interesse

[42] Tuttavia si può affermare che non vi furono feriti, né accuse di maltrattamenti fisici d'alcun tipo.(***Giro di vite contro gli hacker***, B. Sterling, op. cit.)
[43] C.ca 23mila floppy disk.
[44] C.ca una ventina, tra le quali "Illuminati", "Clli Code", "Phoenix Project", "Dr. Ripco".

fieramente impegnato a stabilire e difendere le libertà civili elettroniche, finite sulla cresta dell'onda durante la repressione degli hacker. Il "giro di vite" - per usare la terminologia di B. Sterling - fu notevole di per sé, e provocò negli anni a seguire un fitto dibattito sulla criminalità informatica, sulle punizioni da infliggere, sulla libertà di stampa e sulla legittimità dei mandati di perquisizione e sequestro.

Tale dibattito deve aver avuto una scarsa risonanza in Italia, almeno con riferimento alla salvaguardia delle libertà civili elettroniche, se consideriamo le modalità d'intervento e la condotta dell'operazione ***Hardware 1***, avvenuta nel 1994, che ricalca in alcuni sviluppi quella statunitense. Tale operazione, ribattezzata "Italian Crackdown", fu la più vasta azione di polizia mai condotta nei confronti della telematica amatoriale, con base in due diverse procure (Pesaro e Torino) e la volontà esplicita di applicare un Decreto Legge, il n.518/92, che rappresentava allora la più recente normativa in materia di software.

Le ipotesi di reato attinenti alla criminalità informatica e telematica furono "associazione a delinquere, ricettazione e contrabbando finalizzati alla diffusione di programmi per computer illegalmente copiati, e utilizzo fraudolento di chiavi d'accesso per entrare in elaboratori di pubblica utilità".

L'inchiesta iniziò con l'individuazione di una piccola banca-dati di provincia, sospettata di duplicare e distribuire clandestinamente del software[45], per allargarsi a macchia d'olio ad altre banche dati ed utenti, sospettati di aver avuto collegamenti con la prima. Nel corso dell'operazione la Guardia di Finanza effettuò più di cento perquisizioni tra uffici e domicili, pose sotto sequestro 120 sistemi informatici[46] e c.ca 60mila dischetti, dimostrando uno sfrenato protagonismo ed una conoscenza informatica inadeguata a tale compito[47].

S. Chiccarelli e A. Monti, nel citato "Spaghetti hacker", si chiedono perché molti innocenti furono travolti da una bufera giudiziaria per essere semplicemente

[45] Il Computer club PS-Flash Group di Pesaro.
[46] Con relativi modem, stampanti, mouse (?), tappetini per mouse (?), nonché tutta l'attrezzatura tecnologica al cui interno si riteneva potessero trovarsi software non in regola con le leggi sul copyright.
[47] Diversi testi (vedi ***Spaghetti hacker*** di Chiccarelli e Monti, op. cit., e ***Nubi all'orizzonte*** di Strano Network, Castelvecchi, Roma, 1996) riportano particolari d'ignoranza tecnica da parte di chi eseguì le operazioni poliziesche, come l'incapacità di riconoscere la differenza tra un programma commerciale, uno ***shareware*** o un ***public domain***.

parte di una ***nodelist***, come si arrivò a confondere l'attività di duplicazione criminale di software con quella relativa alla telematica amatoriale, e perché si diede inizio ad una demonizzazione sistematica di quest'ultima.

L'intero "castello investigativo", in tale operazione, si basò sull'attribuzione di una diretta responsabilità ai sysop che gestivano le BBS. Ogni gestore fu chiamato in causa per il contenuto dell'intero flusso di programmi e di dati che passavano, o risiedevano temporaneamente, nella memoria delle BBS amministrate. I sysop furono considerati alla stregua di censori del sistema, obbligati a verificare in tempo reale l'intero flusso comunicativo proveniente dagli utenti, e responsabili di qualsiasi minimo contenuto illegale si muovesse col flusso stesso.

Seguendo questo principio, caddero nella "rete" numerose attività telematiche amatoriali d'impostazione solidaristica, le più famose delle quali furono due BBS internazionali note per il loro impegno sociale, Peacelink e FidoNet. Queste ultime erano in contatto telematico con i territori dell'ex-Jugoslavia, dove veicolavano aiuti umanitari attingendo, di contro, preziose informazioni sull'andamento reale del conflitto. L'attacco giudiziario al nodo centrale di Peacelink[48], situato a Taranto, provocò un'interrogazione parlamentare e l'insorgere di numerose personalità ed organizzazioni di tutto il mondo, che espressero solidarietà alla BBS e sdegno verso le modalità di condotta dell'operazione[49].

Forse a seguito di tali proteste, i magistrati dell'operazione "Hardware 1" sostennero, tra le righe dell'inchiesta, che i sysop avrebbero potuto affidarsi ad un rapporto fiduciario con gli utenti, mantenendo nello stesso tempo una generica prudenza nell'accettare nuovi accessi alle BBS, per diminuire la possibilità di violazioni alla legge sul software. La natura e il merito delle discussioni seguite a tali affermazioni sono facilmente intuibili.

La parte d'operazione svolta dalla Procura di Torino merita di essere citata com'esempio d'intervento contro la criminalità informatica, per l'intelligenza della

[48] La BBS tarantina fu sequestrata con l'accusa d'aver detenuto programmi per computer duplicati abusivamente a fini di lucro.
[49] Alla fine delle indagini sulla BBS tarantina, non si rivelò alcun'attività commerciale, nessuna presenza di software di contrabbando né d'effettive realizzazioni di lucro.

condotta e per i risultati ottenuti. Sotto il nickname[50] di ***Spetnaz***, un investigatore della Guardia di Finanza cominciò a collegarsi con alcune BBS, cercando di registrarsi come utente e di acquisire un minimo di "notorietà" nel settore, guadagnandosi la fiducia del sysop.

Ogni sessione di collegamento ed ogni ***chattata*** con i sysop[51] venne scrupolosamente filmata, e si stamparono le relative schermate, con lo scopo di verificare l'esistenza d'eventuali collegamenti fra le 12 differenti BBS pirata finite nel mirino degli agenti, ed i percorsi seguiti dai vari software per arrivare in Italia. In tali BBS, oltre al software, era frequente trovare indicazioni tecniche, programmi per creare le "famose" box e numeri di calling card con le relative password.

Acquisiti tutti i dati sugli intestatari delle utenze telefoniche, si commise un errore costante in operazioni del genere, e per paura di tralasciare qualcosa si sequestrò tutto ciò che era possibile sequestrare. Fortunatamente, qualche pubblico ministero accortosi dell'errore fece restituire il materiale che non era strettamente pertinente all'inchiesta, e ciò non modificò i termini della questione. Infatti, il risultato delle indagini fu talmente chiaro che molti indagati preferirono patteggiare e non affrontare il processo.

Dagli atti dell'intera operazione trasparì, tuttavia, l'impressione che in molti inquirenti permanesse confusione sul concetto di sistema telematico e sulla figura fondamentale dell'hacker, equiparato ad un vandalo la cui unica attività era procurarsi accessi per inoculare virus o distruggere dati[52].

Al termine dell'esame dell'azione investigativa vanno effettuate alcune considerazioni. Se alcuni frangenti dell'operazione, come l'indagine di Torino, risultarono effettivamente necessari e portarono a risultati interessanti, altri rimasero avvolti nel mistero o si sciolsero come bolle di sapone. L'effetto intimidatorio, in perfetto stile americano, diede un discreto risultato negli anni successivi, quando i pirati del copyright videro ristagnare il loro mercato, anche a causa di un aumento

[50] Soprannome che l'utente può scegliere al momento di fare il suo ingresso in una BBS.
[51] A differenza di quanto accade con Internet, la presenza di una sola linea telefonica permette solo ad un utente per volta di comunicare con il sysop.
[52] Anche Internet non fu da tutti compresa nella sua integrità, ed in alcuni atti venne descritta come "un'organizzazione" alla quale aderivano le BBS. (S. Chiccarelli e A. Monti, ***Spaghetti hacker***, pag. 144, op. cit.).

della percezione del crimine di copyright come tale. Si deve sottolineare, però, che tale effetto fu causato anche dai metodi usati dalla polizia giudiziaria, che spesso usò il sequestro per “verificare” il rispetto della normativa penale sul software, e non sulla base di una notizia di reato attuale e flagrante.

S’ignora tuttora se vi fossero scopi di tipo politico ed economico, oltre alla riduzione del mercato clandestino di software, o se l’intenzione fosse quella di un giro di vite in stile Hacker Crackdown. Certo è che le due operazioni provocarono una presa di coscienza importante all’interno della cultura hacker, un periodo magico per le due comunità on-line, forse irripetibile per intensità e fervore d’iniziative. In Italia, in particolare, la prima decisa azione giudiziaria in questa direzione stimolò enormemente un progetto collettivo per la difesa della frontiera elettronica, intesa come insieme di diritti civili.

Da quel momento, nessuno smanettone è rimasto più lo stesso, avvolto com’era nel suo mondo spesso fuori dalla realtà e convinto d’essere irraggiungibile dagli altri. La telematica ha cominciato ad annegare nel mare dei mass-media, i quali spesso l’hanno utilizzata come “fabbrica di mostri”. Da allora il rapporto con la rete, o meglio con i fatti ad essa legati, ha visto i media sempre molto critici, pronti a leggere ogni evento in modo tale da mettere Internet ed il suo mondo in cattiva luce.

2.5. Dal Crackdown ai giorni nostri: il business, Luther Blisset e Firenze’98.

Con l’arrivo di Internet nelle case nacque la terza generazione degli hacker italiani, la più fortunata come mezzi a disposizione ma anche quella più studiata, seguita, controllata. IRC, il canale di chat on-line, fu subito eletto punto d’incontro per i nuovi smanettoni, che la notte invasero le aree #cybernet e #italia lasciate libere dai fortunati universitari che le utilizzavano di giorno.

Il sistema operativo più usato divenne LINUX, scritto inizialmente come kernel[53] per UNIX da uno studente universitario finlandese, che ebbe l'idea di lasciarlo circolare in rete liberamente. Molti programmatori ne rimasero entusiasti e lo completarono aggiungendo varie utility al nucleo originario, creando una delle più belle storie raccontate dalla rete: quella di un progetto in grado di abbattere i confini fra le nazioni e le barriere tra le persone, di un sistema operativo che tutti contribuirono nei modi più diversi a sviluppare, che circola tuttora in rete dalla quale è scaricabile gratuitamente.

Il mercato del post-crackdown era in continua evoluzione: i prezzi cominciavano a scendere e vari soggetti, tra i quali una torma di Internet Provider più o meno improvvisati, si lanciavano in affari spesso senza la minima cognizione di cosa stesse avvenendo. Gli smanettoni ricevettero una corte serrata da parte di sedicenti provider che, per risparmiare e per non sapere chi altri contattare, cercarono di assumerli per le loro conoscenze nel settore.

Per la prima, volta in Italia, s'impiegarono dei ragazzi per amministrare delle macchine, e ci si accorse del valore delle reali capacità opposte ai titoli accademici. La stessa Telecom si trovò con dei problemi nella formazione del personale tecnico, che aveva "scoperto" il router TCP-IP collegato ad una linea dedicata ma aveva scarsa conoscenza del suo funzionamento.

Come si può immaginare, il rapporto tra i giovani hacker ed i loro datori di lavoro non fu mai facile, in quanto le distanze fra i due mondi restarono sempre abissali. Tuttavia, a differenza di quanto era successo negli USA, dove la terza ondata era scesa a compromessi con le regole del mercato, i nostri smanettoni continuarono ad essere loro stessi, e gli unici accordi furono sulle ore di lavoro (anche il più elastico degli imprenditori difficilmente accettò turni tipo 19.00-5.00).

A questi giovani hacker non parve vero di essere pagati per fare quello che avevano sempre fatto a spese loro, e con l'abilità acquisita dall'esperienza impararono ad entrare in ogni sistema, in ogni nuovo host appena installato, in tutti i siti più interessanti, dove modificavano intere pagine Web nella disperazione dei

[53] Il nucleo che si occupa della gestione a basso livello dell'hardware e delle risorse del sistema (S. Chiccarelli ed A. Monti, ***Spaghetti hacker***, op. cit.).

legittimi autori. Delle backdoor[54] erano installate quasi ovunque, nella certezza che se un'azienda avesse subito un'intrusione, avrebbe volutamente evitato di fare pubblicità al fatto.

Gli hacker non erano in cerca di notorietà o guadagno, erano solo curiosi, tanto è vero che numerosi sysop furono avvisati della facilità con cui si penetrava nei loro sistemi e del pericolo che stavano correndo. Alla lunga ciò risultò utile al sistema, perché anche i sysop meno intraprendenti presero delle misure per elevare la sicurezza delle loro macchine.

Altro fenomeno interessante, quanto di breve durata, fu quello delle riviste elettroniche di hacking. Se la prima era stata ***Il DTE222 Hacking Journal*** nel 1987, la più famosa della nuova ondata fu ***The Black Page***, dove si potevano trovare rivelazioni sull'Italian Crackdown, vari programmi più o meno legali, suggerimenti sul trashing, articoli di vario genere su droghe, centri sociali, crittazione e privacy.

Un'altra rivista degna di nota fu opera di Luther Blisset, una delle figure più anomale e sfuggenti nel panorama dell'underground digitale anni'90. Luther Blisset è un progetto di nome collettivo che nasce dal body-artist e performer Harry Klipper, seguace della corrente neoista inglese. Egli si è appropriato del nome di un calciatore d'origine giamaicana – Luther Blisset – per firmare le proprie azioni negli anni '80. L'uso delle reti telematiche ha permesso la diffusione delle sue performance ed il suo invito a aderirvi in tutto il mondo.

Anonimi hanno costruito al computer il volto di Blisset e lo hanno immesso nel ciberspazio, trasformandolo in un personaggio immaginario che, grazie al concorso di numerose persone, ha oggi una sua personalità, pubblica degli scritti[55], interviste, dichiarazioni inventate da anonimi partecipanti al progetto. Una delle caratteristiche del suo pensiero è l'estrema libertà telematica, la de-regulation totale, che a volte rischia di divenire una sorta di "guida alla libertà" per gli altri.

La Rete ha inevitabilmente assunto, negli ultimi anni, il ruolo di protagonista.

[54] Passaggi creati e nascosti dagli hacker, che permettono di entrare in un programma senza dover utilizzare l'ingresso principale.
[55] Tra i vari ricordiamo il recente ***Net Gener@tion, manifesto delle nuove libertà***, Mondadori, Milano, 1996.

Appare inimmaginabile, al giorno d'oggi, un'operazione di hackeraggio che non la riguardi, una ricerca sugli hacker che non l'analizzi, una previsione in cui non sia, in qualche modo, inserita. L'estensione del suo bacino d'utenza, una delle ultime ricerche riporta c.ca 2 milioni e 620mila utenti italiani[56], ha reso ancora più difficile l'analisi delle caratteristiche degli hacker nostrani, confusi in una moltitudine d'utenti che vorrebbero aspirare a tale nomea senza averne le capacità.

Gli ultimi anni hanno visto l'entrata in vigore di una serie di leggi destinate a regolare il cyberspace, e dove non sono arrivate le leggi esistono una serie di software e programmi che tentano di frenare le scorribande degli smanettoni. Tali prodotti sono la conseguenza di un vero e proprio business, legato alla sicurezza informatica, sorto negli ultimi anni ma già capace di costituire un importante mercato. L'IBM, ad esempio, ha proposto un servizio che s'impegna ad "entrare" nei sistemi di cui si vuole testare il grado di sicurezza, ed a chiuderne le eventuali falle o backdoor; inoltre, lo stesso servizio è a disposizione 24 ore al giorno se si teme che sia in corso una qualche forma di hackeraggio e si desidera l'intervento d'esperti.

Un servizio simile è proposto anche dal CERT-IT, il Computer Emergency Response Team Italiano, fondato presso il Dipartimento di Scienze dell'Informazione dell'Università degli Studi di Milano. La sensazione è che gli smanettoni, senza volerlo, abbiano creato un mercato dove sono tra coloro che si arricchiscono di meno, e sul quale conviene un po' a tutti creare dibattiti, incontri, testi e fanzine di vario tipo, ingigantendo il problema-hacker in Italia oltre la sua effettiva pericolosità.

La maggior parte di tali incontri, secondo le osservazioni di S. Chiccarelli e A. Monti nel più volte citato ***Spaghetti hacker***, sono stati un insuccesso sotto il profilo dei risultati. Il Convegno di Prato del 1995, ad esempio, dedicato al "Diritto alla comunicazione nello scenario di fine millennio", ha prodotto una mozione che denota gran preoccupazione verso i temi legati alla comunicazione elettronica, ma non è riuscito a gettare le basi per un coordinamento nazionale che collaborasse in una fase successiva.

[56] Vedi l'articolo "Gli Italiani scoprono il Web", firmato F.D.S e pubblicato sul settimanale ***Computer Valley***, edito dalla McGraw-Hill e supplemento di "La Repubblica", n.41, luglio '98, pag. 15.

L'obiettivo di creare un soggetto "politico", che rappresenti le istanze del movimento e collabori fattivamente ai processi decisionali relativi alla telematica, non è stato raggiunto, ed allora gli smanettoni hanno provato ad organizzarsi per conto loro. Dal 1996, infatti, gli hacker nostrani hanno il loro evento annuale e ufficialmente riconosciuto: il Gathering. Si tratta di un incontro le cui atmosfere ricordano l'Homebrew club americano, dove si ritrovano singoli o gruppi di hacker accomunati dalla passione per lo sviluppo d'animazioni e grafica computerizzata di livello professionale, le cosiddette ***demo***.

La prima edizione si è svolta contestualmente al meeting delle associazioni telematiche, per vedere quale dei due eventi potesse avere un futuro. Contro ogni pronostico il meeting è nato e morto nel 1996, mentre il Gathering ha celebrato nel '97 la sua seconda edizione[57], consacrandosi come l'equivalente italiano dell'***Assembly***, una manifestazione di demo organizzata a Helsinki e sponsorizzata da grandi industrie d'informatica e telecomunicazioni.

Forse è presto per dirlo, ma il momento attuale sta vedendo nascere una quarta generazione di hacker italiani, la cui fisionomia non appare però ancora ben definita. Sono coloro che, cominciando per curiosità, si sono trovati subito tra le mani macchine mostruosamente potenti e modem a 33600 bps, con collegamenti ad Internet che regalano pagine Web ed abbonamenti ad e-zine. Il loro numero non ha ancora evidenziato l'esplosione attesa, tuttavia ciò che li circonda, e l'estrema facilità per arrivarci, stanno creando una generazione di pseudo-hacker sfacciati ed irrispettosi di qualsiasi etica.

Il limite di questa generazione sta nell'aver avuto tutto subito e con troppa facilità, ed in un approccio quasi totalmente Web e "search engine". A molti, infatti, è bastato fare una search su Altavista, chiedendo informazioni sul termine ***hacker***, per avere accesso ad una quantità d'informazioni impressionante e di grand'interesse per un neofita (anche se spesso datata ed obsoleta). Fioriscono canali IRC dove giovani smanettoni si fingono hacker nella speranza d'incontrarne qualcuno vero, alimentando leggende ed iniziando attività che non hanno nulla a che fare con l'hacking citato in queste pagine.

[57] Dove sono state registrate oltre 400 persone fra curiosi e visitatori, oltre a più di 100 partecipanti alle gare di ***demo***.

Sembra che la nuova moda sia lo scimmiottare gli hacker made in USA, forse a causa della mancanza di un'etica propria che i più giovani non hanno ancora formato, o forse per il Crackdown così lontano, che non ha insegnato loro nulla e che fa sembrare loro tutto dovuto. Alcuni dei più anziani, con molta pazienza, cominciano ad insegnare "come ci si muove " ai neofiti, nella speranza che riesca a svilupparsi un movimento hacker simile a quello degli altri paesi, o forse per evitare che, ancora una volta, l'etica hacker sia soffocata nel nostro paese dalle gesta insane di un gruppo d'adolescenti.

In questo fiorire di neo-smanettoni, la scena hacker sembra vivere un momento abbastanza tranquillo. Dal 1996 non ci sono stati arresti o indagini, e questa tranquillità sembra non far percepire alcun pericolo ai più giovani, mentre gli "anziani" si chiedono se non sia la quiete che precede la tempesta. Anche per interrogarsi su questioni del genere, agli inizi di giugno si sono riuniti a Firenze centinaia di giovani, per partecipare all"Hack-it98".

Organizzata nei locali di una fabbrica dismessa, la manifestazione ha visto tre giorni di seminari, lezioni, eventi e svariate navigazioni, con tematiche quali la crittografia, la privacy e l'alfabetizzazione informatica. Una disamina dell'utenza ha denotato dei soggetti giovani ma non giovanissimi, di prevalenza maschi, interessati soprattutto a rivendicare il diritto alla libera espressione ed all'autogestione delle risorse in rete, provenienti da riferimenti culturali e politici molteplici e contraddittori, dal Cyberpunk, a Che Guevara, al Subcomandante Marcos.

L'iniziativa ha rifiutato qualsiasi sponsorizzazione o finanziamento, basandosi su un'organizzazione collettiva e su un programma pre-elaborato mediante mesi di discussioni in rete. Il desiderio comune, emerso in questi tre giorni, è stato quello di creare spazi di comunicazione assolutamente indipendenti.

3. Tra hacking e criminalità: un confine discusso.

"Ma da quando aveva cominciato la sua carriera da cow-boy dilettante, si era fatto un'idea su quanto poco sapeva su come funzionavano le cose, e non solo nella matrice. E così aveva cominciato a porsi delle domande, e a pensare".
W. Gibson, "Giù nel Cyberspazio".

3.1. Hacker italiani: criminali o smanettoni?

La figura del pirata informatico ha sempre risentito, anche in realtà diverse, di forti influssi statunitensi, che hanno reso più difficile un'identificazione adeguata del soggetto. Nonostante tali difficoltà, lontano dagli stereotipi del Robin Hood telematico e del genio maligno della tastiera, negli ultimi anni si è da più parti tentato un ritratto attendibile dell'hacker italiano.

Nel 1996 la sezione ***Criminalità informatica***[1] dello SCO (Servizio Centrale Operativo della polizia di Stato) ha tracciato un identikit dell'"hacker tipo", in parte ancora valido, con queste caratteristiche: maschio, giovane d'età (il 59% tra i 19 ed i 25 anni, il 29% tra i 25 e i 35), in prevalenza studente (47%) o impiegato (38%, la quasi metà di questi nel campo informatico), agirebbe di prevalenza tra le 20.00 e le 3.00, colpendo soprattutto aziende private (78%).

Il profilo psicologico di tale individuo sembra completato dalle seguenti caratteristiche[2]: sveglio, impaziente, molto motivato, audace e avventuroso, disposto ad accettare la sfida tecnologica. Meno attendibili sembrano essere altri tratti di tale identikit, spesso conseguenza di un fervido immaginario collettivo alimentato dai

[1] Le esperienze operative maturate nel corso degli anni da tale sezione sono confluite, dal luglio del 1996, in un nuovo organismo denominato ***Nopt***, Nucleo Operativo di Polizia delle Telecomunicazioni, collocato nella struttura dell'ispettorato generale di Pubblica Sicurezza presso il Ministero delle Comunicazioni.
[2] Vedi "Nubi all'orizzonte" di S. Network, op. cit., al capitolo "Computer Crime", secondo la descrizione del criminale informatico compiuta da Parker.

media, che descrivono il giovane hacker come solitario, di razza bianca, con un'intelligenza spesso superiore alla media, dedito a passare le notti davanti alla tastiera dormendo durante il giorno, ed all'uso di stupefacenti di vario genere. In queste descrizioni vengono fuse, arbitrariamente, le figure di hacker, smanettone e criminale informatico.

Tentare, fuori dai luoghi comuni, di capire e definire cosa sia un hacker, quali valori segua, il perché del suo comportamento, è un compito non facile, che ci porta a riflettere sull'influenza della tecnologia sul nostro modo di intendere la cultura, l'etica e la vita stessa. Nato come una sfida all'intelligenza, come un modo per affrontare e risolvere con efficacia il rapporto col mezzo informatico, l'***hacking*** ha dovuto subire in seguito una connotazione più negativa, solo in parte sfumata da una visione più romantica.

Tale visione, quella dell'anarchico corsaro telematico che non tollera restrizioni alla propria libertà di navigazione, che sottrae tesori di valore alle grandi multinazionali del software e rende disponibili a tutti, in rete, le sue conoscenze e le sue scoperte, si scontra quotidianamente con vicende di frodi economiche, di pornografia infantile via Internet, di duplicazione illegale di software e di spionaggio industriale, tutte molto poco romantiche.

Appare difficile definire, con certezza, fino a dove un comportamento possa essere definito da hacker e da quale punto in poi da criminale informatico, anche a causa di una diffusa sovrapposizione dei termini che ha provocato le ire del "popolo della rete". Diametralmente opposto, infatti, sembra essere il significato del termine "hacker" per gli abituali utenti del Web, rispetto a quello assunto dai media (stampa e televisione in primis) e dalle forze dell'ordine, con un relativo diverso carico di valori e d'atteggiamenti.

Conseguenza di tale distonia appare la diversa attenzione di cui è oggetto il fenomeno della criminalità informatica in Italia, la sua pericolosità, la sua repressione e le difese che vanno attuate nei suoi confronti, secondo gli interlocutori di tale tematica. I media, l'apparato giuridico e le squadre di polizia telematica, oltre naturalmente a chi lavora nel settore della sicurezza informatica, non smettono mai di porre l'accento sui rischi per le banche dati mal protette, per la privacy, per la

vulnerabilità del sistema di fronte al pericolo di tale criminalità, verso la quale si chiedono pene più severe e misure di sicurezza più all'avanguardia.

Di contro, esiste una corrente di pensiero che tende a sdrammatizzare questo pericolo, a chiedere delle pene meno severe per i giovani hacker nostrani, a denunciare un allarmismo eccessivo che porterebbe benefici esclusivamente ai programmatori di nuovi sistemi di difesa, che trova voce in numerosi newsgroup telematici, pubblicazioni[3], forum di discussione e convegni[4]. A questa corrente appartengono coloro che non credono ad un'identificazione ***tout court*** degli hacker nostrani con la criminalità informatica, che temono per i diritti relativi alla libertà di comunicazione telematica, e per l'identificazione come possibile criminale di chiunque abbia un modem, un po' di curiosità, ed ami navigare in rete[5].

Come spesso accade, la realtà non rispecchia perfettamente nessuna delle due tesi, o forse le comprende entrambe, in quanto la figura dell'hacker, estremamente polivalente nelle sue implicazioni etiche, non circoscrive un unico comportamento ma comprende un possibile campo d'applicazioni molto eterogeneo. Rientrano così sotto tale etichetta le "crociate" contro le tariffe urbane a tempo, ree di incidere sui costi di comunicazione senza offrire vantaggi reali agli utenti, e quelle contro la limitazione di qualunque libertà d'espressione o di privacy (es. i cookies) dell'utente telematico.

Fedele ad un ideale un po' anarchico, imbevuto di passione antiburocratica, nemico giurato delle multinazionali che ama colpire nei modi più disparati, viene considerato un hacker, ad esempio, chi decompila un nuovo sistema molto costoso, ne trova le chiavi, crea un piccolo software in grado di "sproteggere" tale programma, e trasforma il tutto in una pubblicazione shareware disponibile in rete.

Contemporaneamente, però, viene definito hacker anche chi progetta un nuovo virus, v'infetta una serie di dischetti venduti ad un prezzo minore ed in seguito scarica la responsabilità sugli acquirenti che, per risparmiare, non hanno comprato programmi originali ma floppy disk più a buon mercato (oppure ricatta gli acquirenti

[3] Per tutte valga il recente ***Spaghetti Hacker***, ad opera di S. Chiccarelli ed A. Monti, op. cit.
[4] Quello di Prato del 1995 è stato più volte citato in questo lavoro.
[5] Identificazione errata, tuttavia avvenuta spesso in alcune operazioni di polizia telematica, come nel più volte citato Italian Crackdown.

per fornire loro il necessario antivirus). Numerosi sono gli hacker "pentiti" che, affinate le loro capacità di programmatori, si sono poi offerti con referenze d'alto livello alle grandi multinazionali del software[6], proprio le loro nemiche di un tempo.

Oggi essere un hacker, nel senso più pratico ed operativo del termine, non richiede grandi mezzi o conoscenze: basta il normale p.c. collegato ad un modem, una certa dose di curiosità, le domande giuste a qualunque motore di ricerca su Internet, ed ecco che si viene "invasi" dalle più svariate informazioni su come inserirsi in tale banca dati o come impadronirsi di un sistema da usare per altri collegamenti, senza pagare nulla.

Veri e propri kit di software possono così essere scaricati da Internet ed insegnare, in poco tempo, a rubare password (il programma si chiama "Crack"), a scansionare migliaia di numeri telefonici individuando quelli connessi ad un modem ("War Dialing"), ad accedere direttamente nelle directory principali dei sistemi ("Rootkit") [7].

Tuttavia, più difficile sembra sposare la "vera" filosofia hacker, ed è tramite questa che il popolo della rete tiene a distinguersi dalla "volgare" criminalità informatica. Il problema è che ci si appella ad un'etica non scritta, molto variabile, tratteggiata solo in parte e largamente lasciata alla libertà d'esperienza del singolo. Essere un hacker diviene così una specie di mito, reso tale dalla vaghezza dei termini con cui esprimere tale appartenenza, e migliaia di giovani si cimentano con le più stravaganti "imprese telematiche", desiderosi solo di mettersi in mostra. Dietro alcuni valori guida come la libertà d'espressione, l'individualità, la curiosità dell'***hack on*** (letteralmente "metterci le mani sopra", dall'inglese ***to hack***) e lo spirito

[6] Tale fenomeno è per ora molto in voga all'estero, meno in Italia. Nel 1992 l'FBI trova 176 numeri di carte di credito, tutti naturalmente rubati, nella casa di Marty Rosenfeld, un venticinquenne di Brooklyn e lo arresta. Dopo quattro anni di carcere, Marty viene assunto dalla McDonald di Manhattan per supervisionare la sicurezza della sua rete interna. Un pool di ex-hacker, i texani del Whell Group Corp, dopo essersi fatti conoscere dal gran pubblico con incursioni nei più impenetrabili sistemi, si sono messi a vendere pacchetti di sicurezza alle aziende americane (tra i loro clienti risulta esservi perfino il Pentagono). Fonte: "Pirati o Robin Hood", di D. Vulpi, archivio dossier del sito www.galileo.it.

[7] Quattro pirati informatici spagnoli, nel gennaio del 1998, sono riusciti a violare i segreti più riservati della NASA, l'ente spaziale americano. Non contenti, hanno messo su una pagina Web dal titolo ***Mentes inquietas*** dove spiegavano i trucchi per violare le reti più protette. Dopo mesi d'indagine le "Menti inquiete" sono finiti in manette, e si sono giustificati affermando che "il nostro era furto per solo piacere, senza motivo economico". Fonte: vedi nota precedente.

d'avventura, diventa facile scorgere altri scopi, non sempre accettabili in sé o nei mezzi con cui si tenta di perseguirli.

Alla volontà degli hacker di fungere da stimolo nei confronti delle multinazionali dell'informatica, ad esempio, che si vorrebbero meno prese dalle proprie mire egemoniche e più sensibili alla qualità dei programmi messi sul mercato, non corrisponde sempre un comportamento del tutto condivisibile.

I "pirati telematici", infatti, si divertono a dimostrare la vulnerabilità dei programmi delle maggiori case[8] attaccandoli dall'esterno, ridicolizzando le loro difese, assumendo il comando di quei sistemi fra lo sgomento e l'indignazione di chi ha regolarmente acquistato quel programma e lo usa quotidianamente per lavorare. Come spiegare a tali vittime che tutto ciò avviene per spingere le multinazionali a migliorarsi?

A volte è solo il gusto della beffa, privo di motivazioni ideologiche, a muovere un giovane hacker. Più spesso, però, la molla è un rifiuto di omologarsi al sistema, ed in questo l'essere un "pirata informatico" aiuta a sentirsi diversi, fuori dagli schemi, più ribelli. Crescendo, tale atteggiamento può sfociare nella denuncia di un serio professionista del rischio d'un sistema eccessivamente controllato, ma può anche divenire un metodo per fare soldi "facili" ed in maniera non sempre pulita, tramite furti di password, calling card, numeri di carte di credito, intrusioni in sistemi di home banking[9], clonazione di telefoni.

---

[8] L'articolo "Hacker, assalto alla Microsoft", pubblicato sul sito www.repubblica.it in data 4/8/'98 e privo d'autore, rivela proprio un tentativo simile perpetrato ai danni di tale casa informatica da un gruppo di hacker americani denominati "Cult of the Dead Cow" (vedi www.cultdeadcow.com). Mediante un programma chiamato "Back Orifice", evidente parodia del celebre "Back Office" della Microsoft, essi hanno annunciato di essere in grado di forzare il sistema operativo del colosso di B. Gates. Il ruolo di "benefattori dell'umanità informatica", che tale gruppo di hacker aspira ad ottenere in quanto capace di costringere una grande casa informatica a migliorare le difese di un proprio prodotto, viene però contestato dal presidente dell'Information Security Advisors Group, che li ha accusati di torturare vittime innocenti. Oggi Back Orifice è uno dei programmi più usati per introdursi all'interno del sistema e prenderne il controllo completo. Per ulteriori notizie vedi "Il Back Orifice, porta aperta nel Pc" d'E. M. Ferrari, pubblicato su ***Computer, Internet ed altro*** n.7, pag.7, del 19/11/'98.

[9] Vladimir Leonidovich, un hacker russo di c.ca trent'anni, ha ammesso di aver sottratto più di 6miliardi dai conti correnti della clientela dell'istituto bancario Citibank, tra il '94 ed il '95. Tramite una ventina d'intrusioni, l'hacker sovietico è riuscito a trasferire l'ingente somma di denaro in cinque differenti banche, dislocate in Finlandia, Olanda, Israele e Usa. Leonidovich rischia una pena di cinque anni di reclusione ed una multa di c.ca 450 milioni. (Vedi l'articolo ***Hacker reo confesso***, ad opera d'A. Maselli, pubblicato sul settimanale "Computer Valley" n.27, pag.29, del 16/4/'98, allegato al quotidiano "La Repubblica").

Sembrano allora entrare in gioco altre motivazioni, apparentemente estranee alla figura romantica del pirata del cyberspazio: vendetta, affermazione personale, lucro, che evidenziano nuovamente la citata difficoltà di tratteggiare vere e proprie differenze tra l'hackeraggio e la criminalità informatica.

Anche in seguito a tale difficoltà, per provare a fare luce nel sottobosco degli "amanti della tastiera", si è da più parti provveduto al tentativo di classificare questo insieme d'individui: hacker, cracker, phreaker, insider, courier, supplier e lamer sembrano essere il risultato di questo tentativo.

- Gli ***hacker***, che qui assumono il senso originario del termine, vengono descritti come abili programmatori, ricercatori puri, mossi dalla voglia di sapere e dal desiderio di poter esercitare pienamente la propria libertà informatica, esplorando senza limiti il mondo cibernetico. Curiosi e burloni, sono animati dal gusto della sfida e dalla dimostrazione di destrezza, ed hanno il bisogno di comunicare continuamente agli altri le proprie imprese[10].

- I ***cracker***, più aggressivi e distruttivi, sono portati a produrre lesioni ai sistemi che subiscono le loro intrusioni. Abili scassinatori, animati dalla pulsione di rubare, sarebbero stati i primi ad attuare la sprotezione dei programmi in commercio per studiarne formazione e punti deboli, e ad introdurre il fine di lucro legato al warez, il "mercato nero" del software[11].

- Il termine ***phreaker*** ha origine negli USA di fine anni '50, e rappresenta forse la prima differenziazione interna al giovanissimo fenomeno hacker. In quel periodo, una parte di giovani hacker si specializzò in incursioni in

[10] Il famoso ***Jargon File***, un glossario globale della cibercultura nato nel 1975 ed aggiornato continuamente in rete (dove è disponibile all'indirizzo http://beast.cc.emory.edu/jargon30/jargon.html), propone ben otto definizioni del termine "hacker", la prima e la più estesa delle quali riporta "A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary". Due accurate definizioni sono date anche dell'etica hacker, la prima delle quali riporta: "The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing free software and facilitating access to information and to computing resources wherever possible".

[11] Sempre dallo Jargon File è possibile riportare un'interessante definizione di cracker: "One who breaks security on a system. Coined by hackers in defense against journalistic misuse of hacker. Use of this neologism reflects a strong revulsion against the theft and vandalism perpetrated by cracking rings. Thus, there is a far less overlap between hackerdom and crackerdom than the reader misled by sensationalistic journalism might expect…".

linee telefoniche mediante le varie “box” ed il furto dei codici d’accesso, riuscendo a chiamare luoghi molto lontani accreditando le telefonate sul conto d’ignare compagnie telefoniche, o di qualche sfortunata azienda di gran nome[12]. Bruce Sterling, nel suo più volte citato “Giro di vite contro gli hacker”, rivela che tale sistema sarebbe oggi molto diffuso presso gli immigrati provenienti dal terzo mondo, che accumulerebbero così enormi bollette non pagate per chiamate ai Caraibi, nel Sud America o nel Pakistan[13].

- Gli ***insider*** sono un pericolo vero per le aziende, ed appartengono spesso ad una criminalità più organizzata rispetto ai “semplici” cracker. Essi agiscono all’interno delle industrie e delle banche, comunicando all’esterno le informazioni che occorrono per violare i sistemi od organizzare truffe ai conti dei correntisti. Com’è facilmente immaginabile non occorre essere dei maghi del computer per venire classificati come insider, tuttavia tale categoria è considerata tra le maggiormente responsabili nella commissione dei reati informatici[14].

- I ***courier***, o corrieri, collaborano attivamente con i cracker, per i quali provvedono a spostare i programmi ormai privi di protezione da un sito all’altro, in modo che tutti i diversi gruppi che navigano in rete a caccia di tali shareware possano aggiornarsi con le ultime novità.

- I ***supplier***, al contrario, sono coloro che forniscono i programmi originali ai cracker, in maniera che questi li prendano ed eliminino le protezioni. Rappresentano una delle categorie più oscure del panorama telematico, in quanto resta un mistero come riescano a procurarsi tali programmi prima della loro uscita ufficiale sul mercato.

[12] Vedi cap. 2.
[13] Il sistema utilizzato sarebbe quello del “shoulder-surfing”, che consiste nello sbirciare sopra la spalla di una vittima mentre sta digitando il proprio numero su un telefono pubblico (Vedi B. Sterling, “Giro di vite contro gli hacker”, pag.51, op. cit.).
[14] Sembra che la delinquenza tecnologica sul posto di lavoro abbia già procurato, in Francia, danni per 12,7 miliardi di Franchi, dalle truffe vere e proprie alla vendetta del dipendente che dopo il licenziamento cancella tutti i dossier dell’azienda. Pare che nel mondo siano vittime dei propri dipendenti il 50% delle imprese (da “I tecnodelinquenti fanno danni per miliardi” di A. Di Nicola, pubblicato a pag.11 del n°14 di "Computer, Internet ed altro”, inserto di “La Repubblica”, in data 21/1/’99).

- Il ***lamer*** è colui che vorrebbe imitare l'hacker, ma non vi riesce perché privo della curiosità e dell'imperativo dell"hands on" propri di quest'ultimo. Chiccarelli e Monti, nel loro ***Spaghetti hacker***, scrivono"…l'hacker non vi chiederà mai di spiegargli qualcosa, ma vi chiederà solo dove può reperire le informazioni per capirle da sé; un lamer, viceversa, vi tedierà finché non gli spiegherete il mero funzionamento superficiale e non gli importerà invece di capire il perché"[15].

Tuttavia, tralasciando queste categorizzazioni, alcune delle quali finiscono col sovrapporsi se eccessivamente specificate, il crimine informatico, inteso come violazione di una norma giuridica, rappresenta un problema concreto e di non facile soluzione, a prescindere dal come si vogliono definire gli autori di tale azione.

3.2. Il crimine informatico: statistiche, operazioni, rapporto con la stampa.

La criminalità informatica è un fenomeno complesso e variegato, di dimensioni internazionali[16], che include una vastissima casistica d'illeciti, raggruppabili in due diverse categorie:

- Atti commessi per mezzo di sistemi informatici, che in questo caso assumono il ruolo di strumenti per l'attuazione dell'illecito;

- Atti commessi in danno di sistemi informatici, che in questo caso sono considerati oggetto dell'attacco illecito.

[15] S. Chiccarelli e A. Monti, "Spaghetti hacker", pag.297, op. cit.
[16] Fino ad un paio d'anni fa, il triste primato della pirateria informatica a livello mondiale, nel ramo della duplicazione illegale di software, era appannaggio di una regione della Cina Meridionale, il Guandong. In seguito a fortissime pressioni degli USA su Pechino, il fenomeno pare sia stato stroncato, tuttavia ultime rilevazioni fanno pensare che in realtà esso si sia "solo" spostato nelle vicine province di Macao ed Hong Kong. Una spinta per tale "trasloco" sembra essere venuta da convenienze legate ai diversi codici penali, in quanto la pena prevista ad Hong Kong per tali reati prevede appena due mesi di prigione e 650$ di multa. (Fonte: "Hong Kong, il nuovo covo dei pirati informatici", d'A. Maselli, su Computer Valley n. 24 di marzo'98, pag.19).

Alcune caratteristiche particolari sono collegate a tale fenomeno: la notevole difficoltà tecnica della rilevazione degli attacchi, la rapidità d'evoluzione della tecnologia ed una diffusa resistenza psicologica ad affrontare il problema.

La difficoltà tecnica di rilevazione degli attacchi è dovuta a diverse ragioni, la principale delle quali è rappresentata dal fatto che, a differenza di qualsiasi altro bene, l'informazione può essere rubata senza che il legittimo proprietario ne perda la piena disponibilità e possa, così, accorgersi del furto subito. La rapidità con cui si evolve la tecnologia dell'informazione induce un'altrettanto veloce obsolescenza di soluzioni difensive e d'analisi di rischio[17]. Ciò ha creato un vero e proprio mercato della sicurezza telematica con corsi di formazione, congressi e pubblicazioni.

Esiste, tuttavia, una diffusa resistenza culturale e psicologica ad affrontare il problema delle intrusioni nei propri sistemi informatici, e soprattutto a far conoscere agli altri l'esistenza e la natura degli attacchi subiti, come se si trattasse di fatti vergognosi o disdicevoli. Spesso è proprio questo il primo passo da compiere per fronteggiare un crimine informatico, rassicurare la vittima e convincerla a fornire elementi sul caso.

Alcuni dati, qui riportati in ordine cronologico, invitano a riflettere sulla realtà del crimine informatico, e sulla difficoltà della sua rilevazione:

- Nel 1995, nei soli USA, su un campione di 325 aziende sono state riportate perdite d'informazioni per 5milioni di dollari. Da questo gli autori della ricerca hanno immaginato che le perdite potenziali per tutta l'industria americana potessero superare i 100milioni di dollari annuali[18];

- In un test del 1996, sponsorizzato dal Dipartimento della Difesa USA, su un totale di 8932 sistemi attaccati, l'88% è stato penetrato con successo ed in meno del 5% dei casi l'attacco è stato rilevato[19];

[17] Il calcolo necessario per rompere gli algoritmi di cifratura, ad esempio, è in continuo calo, grazie alla disponibilità di calcolatori sempre più veloci, potenti ed economici.
[18] Più di 170miliardi di lire. Fonte: FTI (Forum per la Tecnologia dell'Informazione), ***Osservatorio sulla criminalità informatica. Rapporto 1997***, pag.27, op. cit.
[19] Fonte: vedi nota precedente, pag.24, op. cit.

- Nel 1996 il Pentagono ha ammesso che, negli anni precedenti, vi sono stati almeno 250mila tentativi di penetrazione nei suoi elaboratori tramite i propri computer. Ben il 65% di questi tentativi è riuscito, ma meno dell'1% è stato individuato durante l'operazione stessa[20];

- Una ricerca americana, eseguita dal Computer Security Institute (CSI) in collaborazione con l'FBI, ha rilevato che nel 1997 il 60% delle aziende, nel mondo del lavoro, nella pubblica amministrazione e nelle università, hanno denunciato intrusioni ai sistemi di sicurezza interni dei propri computer, con un aumento del 22% rispetto al 1996. Le perdite economiche, considerando che solo il 17% degli attacchi via computer vengono denunciati alla polizia, supererebbero nel '97 i 142 milioni di dollari[21].

- La stessa ricerca, aggiornata a metà 1998, modifica di poco i dati del '97: in leggero aumento le violazioni dei sistemi di sicurezza (64% degli intervistati a parità di campione), con un +16% rispetto all'anno precedente. In leggero calo le perdite economiche, che ammonterebbero a 136 milioni di dollari[22].

- Secondo alcuni dati della Prince Warehouse, aggiornati ad inizio '98, il 73% delle aziende che commercializzano i loro prodotti tramite il Web, utilizzando software appropriato, ha lamentato di essere stata vittima d'episodi di spionaggio industriale o di violazione della sicurezza. L'indagine comprende le aziende di c.ca 50 paesi diversi[23].

Sempre più concreta appare la possibilità che le grandi organizzazioni criminali abbiano ormai acquisito il know-how tecnologico necessario a fare dell'informatica un mezzo prezioso per i loro affari, come teorizzato da C. Serra e M. Strano, nel citato ***Nuove frontiere della criminalità***. Secondo tali autori l'uso dell'informatica costituirebbe una struttura di supporto, usata quotidianamente per la

[20] Fonte: un ufficio federale del governo americano, il General accaunting office, che ha rilasciato tali dati nel mese di maggio 1996.
[21] Più di 240 miliardi di lire. Fonte: dati rilevati sul sito Internet www.galileo.it, nella sezione Archivio Dossier, inseriti nell'articolo di D. Vulpi ***La legge del Web***.
[22] Fonte: ***La triste parabola del pirata travel*** di R. Stagliano, pubblicato il 29/1/'99 sul sito www.caffeeuropa.it.
[23] Fonte: ***Aziende, gli hacker sono i dipendenti***, articolo privo d'autore pubblicato su Computer Valley n.44, pag.19, del 17settembre'98.

gestione e la movimentazione di grossi capitali. Sarebbero ormai completamente informatizzate alcune attività tipiche della criminalità organizzata, come il traffico di droga, il gioco d'azzardo, le scommesse illegali[24], i prestiti usurari, lo sfruttamento della prostituzione, l'immigrazione clandestina, il riciclaggio di denaro sporco e la contabilità coperta delle aziende.

"Tecnologia criminale cibernetica", stando alla definizione degli autori sopra citati, sarebbe ormai stata acquisita anche da organizzazioni eversivo-terroristiche, da cui la necessità di misurare il potenziale militare di un'organizzazione terroristica non più solo in termini canonici (armamenti, esplosivi, lotta armata…), ma anche con riferimento alla dimestichezza o meno con la navigazione nelle reti informatiche, e la conoscenza dei nodi nevralgici di queste ultime[25].

Altro settore di spicco della criminalità informatica è quello collegato alle aziende, le quali non devono più guardarsi solo da tentativi d'intrusione esterna nei confronti delle loro banche-dati, ma spesso corrono il rischio maggiore in seguito al comportamento dei propri dipendenti.

La figura dell'insider, precedentemente descritta, costringe ormai le aziende a ripetuti controlli onde evitare furti o frodi di vario tipo da parte dei dipendenti, dal fornire all'esterno le password d'entrata, quando non addirittura le informazioni copiate facilmente su un dischetto, fino al furto di ***tempo-macchina*** impiegando i computer per finalità personali[26]. Un'indagine della Prince Warehouse riporta che, in un campione d'aziende intervistate, ognuna delle quali aveva avuto dei problemi di spionaggio industriale e di sicurezza, ben il 58% dei casi ha rivelato i dipendenti interni come principali responsabili di tali problemi[27].

[24] E', infatti, possibile collegarsi con un sito che accetta scommesse clandestine, anche effettuando tale collegamento da una nazione dove il gioco d'azzardo è considerato un crimine, basta che tale sito si trovi fisicamente in una nazione dove il gioco d'azzardo è consentito. Alcuni paesi, come ad esempio i Caraibi, potrebbero così divenire dei "paradisi virtuali".
[25] Gli autori ricordano, ad esempio, l'attacco dell'organizzazione chiamata Falange Armata ai sistemi informatici d'alcuni istituti di credito, tra cui la Banca d'Italia, avvenuto nell'ottobre del 1995.
[26] A lungo questa è stata la causa delle infezioni di virus informatici da parte di molte aziende, tramite giochi o programmi di vario tipo usati dai propri dipendenti.
[27] Fonte: vedi nota n.23.

L’insieme di tali settori (grandi organizzazioni criminali, rischi di tipo eversivo o legato alla criminalità aziendale), unito ad una micro-criminalità dovuta alla facilità di reperimento dei mezzi e delle conoscenze necessarie, costituirebbe per la polizia telematica italiana un fenomeno in espansione nella nostra penisola. Tale incremento è spesso collegato dagli addetti ai lavori allo sviluppo della cosiddetta informatica alternativa, dai quali essa è considerata godere di una manodopera gratuita e spontanea in tutto il mondo.

Tale informatica, malvista alle multinazionali che l’accusano di un mancato guadagno di miliardi, si avvallerebbe di vasti circuiti distributivi di programmi shareware e di pubblico dominio, sorretti dalla spontaneità di giovani appassionati. Milioni di ragazzi, grazie ai compatibili, avrebbero scoperto la possibilità di inventare, provare e fare scambio di nuove soluzioni tecniche. Questi scambi oggi avverrebbero in prevalenza in rete, mediante BBS telematiche, malviste dalla polizia informatica a causa dell’assenza di regole che pare regnarvi.

Il fenomeno della criminalità informatica, qualunque sia la sua matrice, sembrerebbe dotato di modalità di procedimento autonome, nei confronti delle quali non basta più agire in seguito agli avvenimenti ma si deve puntare maggiormente sulla prevenzione delle stesse. Le intrusioni appaiono articolate in alcune fasi tipiche: raccolta d’informazioni utili e necessarie all’azione, primi tentativi d’intrusione per provare i collegamenti (password, codici d’accesso, esplorazione del sistema), penetrazione definitiva con assunzione dei privilegi del system manager ed attuazione dello scopo criminale, cancellazione delle proprie tracce.

Gli scopi possono essere tra i più diversi, secondo le capacità tecniche dell’hacker, il tempo a disposizione, le difese del sistema ed i danni che si vogliono provocare o meno. E’ possibile limitarsi a leggere informazioni o sottrarle, utilizzare impropriamente risorse elaborative per motivi personali, usare il computer come ponte per altri collegamenti, danneggiare le registrazioni o alcune parti del sistema ospite, inserire un comunicato. La successiva cancellazione del proprio passaggio, onde evitare di poter essere rintracciati, è forse l'opera di più difficile realizzazione da

parte di un hacker, ed è quella che qualifica la differente abilità dei criminali informatici[28].

Le abilità di un hacker si sposano con le difese del sistema da affrontare, e tanto le prime necessitano di continui aggiornamenti su come penetrare in nuovi computer (la rete contiene vari siti dedicati a tale scopo), quanto le seconde richiedono la stessa attenzione. Un vero e proprio "mercato" italiano della sicurezza informatica è venuto alla luce negli ultimi anni, e più di un'azienda si è specializzata nell'installare sistemi di protezione "ad hoc" per le esigenze del cliente[29].

Le maggiori difficoltà contro le quali si sono scontrati gli operatori di tale mercato hanno riguardato, ed in parte ancora riguardano, l'incapacità delle aziende di considerare le difese come una globalità organizzativa, come un investimento e non come un costo. Il massimo livello di sicurezza è stato spesso individuato, erroneamente, con la massima sofisticazione adottata, e non con il suo punto più debole.

Altri fattori che hanno reso a lungo vita facile ai pirati informatici sono stati: una scarsa attenzione dedicata alla gestione delle password, unita alla mancanza di sensibilizzazione tra i dipendenti verso le possibili forme di ***social engineering*** [30], uno scetticismo verso tali tipi di reati, la scarsa propensione delle imprese colpite a denunciare i crimini subiti per evitarne un ritorno in pubblicità negativa, fenomeno noto con il termine di "numero oscuro".

Dall'inizio degli anni'90 non sono mancati i casi d'intervento da parte della sezione ***Criminalità Informatica*** dello SCO (Servizio Centrale Operativo della Polizia di Stato), dal luglio'96 divenuta NOPT (Nucleo Operativo di Polizia delle Telecomunicazioni), alcuni in collaborazione con le polizie straniere, altri rimasti all'interno del nostro stato. Più che un'analisi approfondita delle singole indagini,

[28] Un conto è non lasciare tracce in seguito ad una semplice lettura dei dati, un altro è farlo dopo aver danneggiato la metà del sistema e lasciato un messaggio.
[29] L'argomento sarà approfondito nel paragrafo n.3 di questo stesso capitolo.
[30] Il ***social engineering***, comunemente nota come "ingegneria sociale, è una tecnica di hacking e phreaking che consiste, spacciandosi per altre persone, nell'ottenere informazioni riservate come password o specifiche tecniche su linee telefoniche o altro". Tecniche d'ingegneria sociale sono "parlare in fretta, farsi passare per un altro, compiere impersonificazioni e raggiri". (Vedi B. Sterling, ***Giro di vite contro gli hackers***, pag.90, op. cit.).

appare interessante una possibile categorizzazione delle stesse, onde individuare i settori maggiormente esposti agli interessi della criminalità informatica.

Un ramo importante delle operazioni ha riguardato indagini relative a truffe a compagnie telefoniche, le quali hanno sempre avuto un rapporto difficile con gli hacker o presunti tali. Mediante tecniche più o meno articolate[31], più di una volta questi sono venuti in possesso di password, account e dati riservati di vario tipo, mediante i quali non è difficile evitare di pagare qualsiasi collegamento in rete o farlo pagare a qualcuno di specifico[32], usare computers della Telecom come base per successive operazioni d'intrusione telematica, o dedicarsi ad attività più "banali" come la clonazione di telefoni cellulari.

Occorre però precisare che non sempre, a meno di non identificare impropriamente, con questo termine, chiunque commette un reato telematico, si sono individuati degli hacker dietro a tali operazioni; ad esempio nell'estate del '91 erano alcuni fornitori di contratti SIP-Videotel a truffare i propri clienti usando i codici ceduti a questi come "strettamente personali".

Naturalmente intrusioni informatiche non avvengono solo a danno di compagnie telefoniche, ma spesso colpiscono anche aziende, industrie, banche, università, in pratica qualunque computer "rischi" di contenere dati interessanti o controversi. Al riguardo sono numerosi i casi di pirateria informatica relativi ad operazioni economiche di tipo bancario, come la ricettazione di codici di carte di credito (operazione Ice-Trap'95), la duplicazione di carte Bancomat (operazione Bancomat'93), la simulazione d'attività telematiche ad opera di una filiale inesistente (operazione Banca sicura'95). Altre volte il settore era affine, come in una truffa alla previdenza dove un dipendente interno (dunque non un hacker) costruiva situazioni fittizie sulla base di casi reali (operazione Inps'90).

Più di una volta, durante queste operazioni, gli inquirenti hanno dimostrato l'uso di BBS, bacheche telematiche, come luogo di ritrovo e di scambio

[31] Dall'uso di moderni sistemi d'intercettazione ad una buona ingegneria sociale, fino al più banale passaparola.

[32] L'ultimo caso, in ordine di tempo, ha riguardato un famoso numero verde del Viminale, l'167-113-113, come traspare dai numerosi articoli che, nel novembre del'98, si sino occupati della vicenda (tra gli altri vedi ***Hacker scrocconi con un 167 del Viminale*** d'A. Usai, pubblicato su www.repubblica.it il 4/11/'98, e ***Pirati di Internet al Viminale*** di E. Vinci, sul quotidiano "La Repubblica" del 5/11/'98.

d'informazioni da parte di criminali informatici, i quali riescono con questo sistema ad organizzare complesse truffe senza doversi mai incontrare tra loro[33]. Tramite BBS si sviluppa anche una delle attività criminali più inquietanti, relativa al traffico d'immagini pornografiche aventi come soggetto dei minori. Questa tematica risulta particolarmente attuale in seguito alle rivelazioni effettuate dalla polizia telematica, nei primi giorni di settembre'98, in merito ad un traffico d'immagini sequestrate in 21 Paesi diversi, dalla Germania al Giappone.

Tale operazione, definita "Operation Cathedral", avrebbe colpito diverse organizzazioni internazionali di pedofili che si appoggiavano ad Internet per offrire agli utenti, a caro prezzo, i loro servizi. Pare che siano state sequestrate più di centomila immagini pornografiche, un'ingente quantità di dischetti (c.ca 2600), numerosi computer e videocassette. Altri casi simili, seppure con un raggio d'azione più ridotto, avevano riguardato l'Italia nel'95 e nel'97 [34], a dimostrazione di come i siti pornografici rappresentino un mercato molto ambito, che sarebbe stimato nel '98 per una cifra pari a 1700miliardi[35].

Un altro settore preda dell'interesse della pirateria informatica è rappresentato dal mercato del software, anche questo capace di un giro d'affari di miliardi. Si tratta di software illegale, più precisamente copie pirata di programmi ufficiali vendute ad un prezzo molto minore degli originali. Come precedentemente citato[36], diverse nazioni hanno acquisito un'abilità tale in questo campo da essere considerate delle vere e proprie "esperte" nella duplicazione illegale di software. E' necessario specificare che la legge italiana punisce la duplicazione abusiva solo a scopo di lucro, e che tale concetto ha provocato più di un problema nell'interpretazione dei casi originatesi.

Altre modalità d'effettuazione di crimini informatici riguardano l'utilizzo di virus, sui quali saranno fornite maggiori informazioni nella sezione inerente le tecniche d'attacco degli hacker.

---

[33] Sull'evoluzione della comunicazione, dal "face to face" alla tastiera, vedi cap.1, par.1.
[34] L'operazione in questione, denominata Gift-sex, rimane famosa per via di una codifica della merce venduta come fosse del vino: più 6 gradi intendeva foto con bambini con più di sei anni, meno 6 gradi con bambini più piccoli.
[35] Fonte: dati pubblicati a cura di M. Manzi, su ***La Repubblica*** del 3/9/'98, pag.11.
[36] Vedi l'articolo "Hong Kong, il nuovo covo dei pirati informatici", nota n.13.

In relazione alle indagini svolte, ci limitiamo a menzionare l'operazione AIDS (1990), così chiamata perché una pubblicazione apparentemente innocua su tale argomento, distribuita tramite floppy disk, conteneva in realtà un virus che nascondeva parte del disco rigido, mentre appariva in sovrimpressione il conto corrente di una società panamense cui pagare un riscatto per ottenere l'antivirus necessario.

A volte i pirati informatici cercano soltanto di attirare l'attenzione, di usare uno spazio pubblico il più possibile in vista per rivendicare dei diritti o delle azioni precedenti[37]. Tuttavia, occorre distinguere quando atteggiamenti di questo tipo sono opera di hacker da quando quest'ultimi ne sono estranei.

Il 10 luglio scorso, ad esempio, chiunque si è collegato al sito del Gr1 verso le 13.00 è stato accolto da una voce maschile e giovane che, dopo il benvenuto al giornale radio, ha cominciato una lunga litania d'insulti e critiche a Windows'98, il nuovo sistema operativo della Microsoft (le cui vendite cominciavano in Italia proprio in quel giorno). L'hackeraggio subito dalla Rai è durato c.ca 4 minuti, ma i responsabili del sito ci hanno messo due giorni (causa il week-end) ad accorgersi del fatto.

Su ammissione del direttore dei sistemi informativi Rai, Giuseppe Biassoni, solo attraverso la trasmissione all'esterno della password d'entrata, nota esclusivamente a chi ha l'autorizzazione ad aggiornare il sito, era possibile spiegare l'accaduto, ragione per cui le indagini hanno cominciato a svolgersi all'interno dell'azienda, alla ricerca dell'ennesimo caso d'***insider*** [38]. Invece, il 30 luglio la redazione telematica di Repubblica ha ricevuto, on-line, l'ammissione di colpa dell'hacker reo confesso, che si scusava e si diceva pronto ad accettare le

[37] E' interessante notare una certa necessità di protagonismo latente in molti hacker, dovuta al fatto che molte delle loro azioni, senza un'adeguata pubblicità, resterebbero ignote al pubblico. A volte è stata proprio la ricerca "dell'applauso" che li ha traditi, come il noto hacker israeliano Ehud Tennebaum, soprannominato "Analyzer" che, dopo aver violato ben 11 diversi sistemi di comunicazione militare del Pentagono, è stato catturato perché aveva diffuso in Internet la propria fotografia per vantarsi del suo operato. Fonte: vedi nota n.6.

[38] Fonte: ***Hacker sul sito Rai "sostituiscono" il Gr1***, opera d'Annalisa Usai, pubblicato su www.repubblica.it in data 13/7/'98.

conseguenze del suo gesto. Ora il responsabile rischia dai tre agli otto anni, per un reato che si chiama "interruzione di servizio pubblico".[39]

Un caso simile, molto discusso, ha riguardato nel 1994 la banca-dati romana dell'Adn-Kronos. L'agenzia d'informazione restò isolata per un'intera giornata, ed il suo contenuto fu sostituito da un delirante comunicato della Falange armata, un gruppo estremista simbolo della strategia della tensione. I giornali si sbizzarrirono nella caccia all'hacker, senza pensare quanto sia lontano dall'etica hacker un comportamento del genere[40].

Il succedersi di tali indagini, considerate nel loro complesso, ha finito per attirare l'attenzione della stampa, che ha "scoperto" il filone della criminalità informatica, applicandovi con successo le regole pratiche che permettono di trasformare un "fatto" in una "notizia"[41].

Una ricerca ad opera di P. Guerra e B. Ferrario, riportata nel rapporto'97 del FTI[42], rivela che il 1994 è stato l'anno in cui la stampa ha cominciato a sfruttare seriamente il "pericolo hacker": ben 73 sono stati gli articoli pubblicati su 16 diverse testate, a differenza dei soli 12 articoli dell'intera annata precedente (che avevano interessato solo quattro testate).

Il trend positivo si è confermato nel 1995, anche se con un aumento più contenuto, che ha visto la pubblicazione di 78 articoli su 19 testate. Singolare l'annotazione che, nella scomposizione di questi dati, siano stati gli articoli pubblicati sui periodici ad aumentare (da 5 a 10), mentre l'attenzione dei quotidiani verso la criminalità informatica è rimasta invariata (68 articoli). Le rilevazioni del '96 hanno riguardato solo la prima metà dell'anno, ma permettono comunque di confermare un

[39] Tale reato sarà affrontato nel quarto paragrafo di questo capitolo. Le notizie sull'hacker reo confesso sono state tratte da "L'Arsenio Lupin dei giorni nostri" d'Annalisa Usai, pubblicato sul ***Venerdì di Repubblica*** n.550, in data 25/9/'98, dove si legge anche (pag.89) "…non sono un vero hacker, ma è stato facile: ho beccato un computer RAI che aveva poche protezioni. Da lì ho preso la password per entrare nel sito del Gr1… Penetrare nei sistemi informatici ti dà un'euforia che ti porta ad esagerare. Ho voluto provare anche io".

[40] Oscurare una banca dati di notizie pubbliche per un'intera giornata, privare l'opinione pubblica di comuni informazioni come quelle trattate da un'agenzia di stampa, soprattutto in assenza di "battaglie ideologiche" come, al limite, può essere considerata quella contro la Microsoft di Gates.

[41] "I valori/notizia sono criteri per selezionare, dal materiale disponibile alla redazione, gli elementi degni di essere inclusi nel prodotto finale…, sono cioè delle regole pratiche comprendenti un corpus di conoscenze professionali che… spiegano e guidano le procedure lavorative redazionali". Vedi: M. Wolf, ***Teorie delle comunicazioni di massa***, pag.197, Bompiani, Milano, 1994 (XI ediz.).

[42] FTI, ***Osservatorio sulla criminalità informatica. Rapporto 1997***, op. cit.

leggero aumento sia riguardo gli articoli pubblicati sui quotidiani, che quelli riguardanti i periodici.

In particolare, nei sei mesi considerati, quasi il 30% della totalità degli articoli pubblicati (14 su 47) ha trovato spazio sul quotidiano “La Repubblica”, il più attento a proporre ai suoi lettori casi reali o presunti di criminalità informatica.

3.3. Gli strumenti della criminalità informatica e le possibili difese: il “guardie e ladri” della rete.

Con la parola “attacco”, in ambito informatico, s’intende un tentativo finalizzato a sovvertire le misure di sicurezza di una macchina. Se un utente cerca di diventare “root”, ovverosia di acquisire i privilegi dell’amministratore del sistema provando tutte le password possibili, si sta chiaramente verificando un attacco. Gli hacker, coltivando le più svariate finalità e motivazioni, fanno di queste conoscenze una vera e propria “scienza”, passando diverse ore a studiare ed a mettere in pratica differenti tipi d’attacchi. Le probabilità di cogliere in flagrante un pirata informatico sono molto basse, sia nel caso che egli sia un utente regolare del sistema, sia che provenga da un’altra macchina collegata in rete. Senza dilungarsi eccessivamente in particolari tecnici, saranno di seguito esaminati i più comuni tipi d'attacco, non solo in Italia ma anche nel resto del mondo, e le conseguenze più dirette di tali azioni.

Una delle tecniche più usate è il ***network sniffing***, che permette d’ascoltare, o meglio “annusare” il passaggio dei dati lungo la rete, con la successiva cattura di quelli cercati. Infatti, quando un calcolatore in rete vuole mandare un’informazione ad un altro computer, costruisce un “pacchetto” con l’indirizzo di quest’ultimo e lo spedisce in rete. Le varie macchine che sono attraversate dal pacchetto lo “sentono”, ma lo ignorano perché non contiene il loro indirizzo, a differenza del destinatario che legge il pacchetto e lo elabora. E’ tuttavia possibile alterare tale funzionamento mediante lo sniffing, che permette ad un calcolatore di leggere automaticamente tutti i pacchetti che transitano sullo spezzone di rete cui la macchina è connessa, estraendone le informazioni più interessanti (es. password) per gli hacker.

Mediante lo ***spoofing*** si falsifica la provenienza dei pacchetti, facendo così credere ad una macchina che sia un altro il reale mittente delle informazioni. Tale tecnica d'attacco è particolarmente efficace in presenza di protocolli che autenticano una connessione basandosi solo sull'indirizzo della macchina chiamante. In altre parole, una certa operazione viene o meno permessa in base all'indirizzo del calcolatore che ne richiede l'esecuzione.

Una categoria particolare d'attacco è definita ***denial of service*** o "rifiuto di servizio". Tali attacchi non sono finalizzati a violare la sicurezza di un sistema, bensì ad impedire che quest'ultimo possa effettuare dei servizi. Un protocollo che si presta molto ad attacchi di questo tipo è l'ICMP (Internet Control Message Protocol), i cui pacchetti sono facilmente falsificabili. Un attacco di questo tipo, finalizzato a rendere inutilizzabile la rete per un calcolatore o per un'intera organizzazione, è il ***network flooding***, il quale agisce saturando la capacità di gestire il traffico sulla rete.

L'***E-Mail bombing*** è una tecnica che prevede il bombardamento, con migliaia di messaggi di posta elettronica, della casella di un utente, per provocare un crash nel server. Una delle possibili conseguenze risulta, per il malcapitato, l'impossibilità di prelevare e visionare la propria posta elettronica non ancora scaricata al momento dell'attacco. Tuttavia tale tecnica può causare danni peggiori.

Sovraccaricando il computer del server di differenti richieste, in maniera che non possa più svolgere attività di discernimento, si può obbligarlo a fornire sempre pareri positivi a prescindere dalla domanda posta. Nel caso in cui tale computer fornisca (o meno) l'accesso ad una rete telematica in base all'invio di una password, è così possibile indurlo a consentire l'accesso anche in mancanza della password corretta.

Altre tecniche d'attacco sono le ***logic bomb*** e le ***time bomb***, programmi che vengono introdotti clandestinamente nei computer e provocano diverse conseguenze (danneggiamento del software, esecuzione d'istruzioni surrettizie) in concomitanza con circostanze o situazioni stabilite in anticipo[43].

[43] Simili sono i ***trojan horse***, o "cavalli di Troia", programmi che sembrano svolgere un compito ma in realtà nascondono al loro interno un altro compito non esplicito, che può attivarsi od essere attivato in un secondo momento.

Altro sistema è il ***breakage***: il termine indica la frazione di dollaro (o di sterlina) che si è soliti non computare nel calcolo degli interessi. Tale sistema illecito fu applicato dal programmatore di una banca di New York per dirottare, grazie ad un apposito programma da lui creato, l'ammontare di tutti i decimali di dollaro sul proprio conto, ricavando una somma cospicua.

La gravità di un incidente informatico non è solo in funzione dei danni arrecati a dati e programmi presenti sulla macchina attaccata, ma anche delle operazioni eseguite dall'hacker per garantirsi un eventuale accesso in futuro. L'operazione più comune per raggiungere tale scopo, ma anche la più temuta dal gestore del sistema, è la creazione di una ***backdoor***, una specie d'entrata di servizio segreta agli occhi di tutti tranne che a quelli dell'hacker.

Una volta installata, essa permette all'intruso di divenire root sulla macchina in questione, ed a nulla serve la modifica delle password d'entrata o la soppressione di qualche account. Riuscire a trovare il punto esatto in cui essa è stata posta è una ricerca moto ardua, perché una backdoor ben fatta rappresenta la "firma" dell'hacker al suo lavoro, ed è il frutto di diverso tempo passato in studi ed applicazioni.

Proprio l'esperienza nel settore fa la differenza fra un hacker alle prime armi ed uno più smaliziato, e può giocare a favore delle vittime degli attacchi informatici. Infatti, dopo essere diventato root ed aver installato o migliorato la propria backdoor, un hacker "professionista" sa che deve cancellare le tracce del suo passaggio, che inevitabilmente sono state lasciate. Esistono dei file, denominati file di ***log***, che registrano il passaggio nel sistema e le modifiche da questo subito, e che rappresentano il maggior pericolo per gli intrusi.

Riuscire a cancellare del tutto le proprie tracce non è un'operazione facile, tanto che per riuscirci gli hacker utilizzano dei piccoli programmi scritti da loro stessi, definiti ***editor***, in grado di modificare il contenuto dei file di log interessati[44]. Se tale operazione non dovesse essere ben fatta, il sistema manterrà la traccia di tutti i comandi digitati dall'hacker, da quelli per divenire root fino a quelli che riguardano la backdoor. Il sogno d'ogni hacker è riuscire a scrivere un ***exploit***, cioè un programma

[44] Alcuni file di log vengono addirittura cancellati a mano, nelle righe inerenti l'intrusione che variano secondo il tipo d'attacco sferrato.

che sfrutta i bug[45] e le backdoor di un sistema, facendo assumere al pirata informatico i privilegi e le conoscenze di chi lo ha progettato.

Trovare i punti deboli di un sistema non è cosa da tutti, ci vogliono notevoli conoscenze di programmazione, una gran dose di volontà e di passione, un interesse per la programmazione ai limiti del feticismo. Alcuni paesi hanno una gran tradizione in questo campo, e non a caso sono delle vere e proprie "miniere di hacker": USA, Olanda e Germania soprattutto, ma anche Finlandia e Polonia.

L'autore di un exploit lo rende spesso disponibile a tutti, in rete, sia per chi vuole usarlo per proteggere meglio il proprio sito (imparando quali errori non commettere), sia per chi vuole "bucarne" altri. Negli ultimi anni sono stati veramente molti gli exploit scoperti, per tutti i tipi di piattaforme, e ogniqualvolta una software house faceva uscire la nuova versione di un programma con la correzione dei vecchi bug, dopo alcuni giorni emergeva dal "mare magnum" dell'hacking l'ennesimo exploit per la nuova versione.

Un tipo d'attacco particolare, che abbiamo preferito trattare a parte per la sua specificità, è quello mediante i virus informatici. Gli autori di tali virus non possono essere ridotti ad un'unica tipologia, quindi non sarebbe esatto definirli unicamente come degli hacker, anche se i contorni tra le due figure non sono molto netti ed a volte si è assistito a delle sovrapposizioni di ruoli.

Un virus[46] informatico, dal punto di vista scientifico, è una procedura automatica autoriproducente che, al momento dell'esecuzione, effettua più copie di se stesso, che a loro volta creano altre copie e così di seguito, all'infinito. Un virus non è un programma a sé stante, ma viene avviato solo in seguito all'esecuzione di un altro programma[47].

[45] Il bug è un errore di programmazione, una piccola "porta" attraverso la quale si può entrare in un sistema e prenderne i privilegi di root. I bug vengono a volte dimenticati dai programmatori che, nella fretta per la consegna di un nuovo software, non sempre si ricordano di eliminarli.
[46] L'uso di questo termine per definire tali procedure si deve a Fred Cohen, un ricercatore californiano, ed è piuttosto recente (il primo articolo di Cohen che ne parla è del 1984).
[47] A differenza di un virus informatico, ***batteri*** e ***vermi*** non necessitano di un programma ospite. I primi sono dei programmi in grado d'autoriprodursi, i quali non attaccano direttamente il software ma tendono a moltiplicarsi fino ad esaurire le risorse del computer, come l'intera capacità del processore, la memoria del sistema o lo spazio su disco. I vermi compiono un'operazione simile su una scala molto più vasta: sempre in grado d'autoriprodursi, si diffondono su tutti i siti di una rete cercando di portarla al blocco completo.

Le strategie tramite le quali i virus si diffondono sono sostanzialmente due: il virus può modificare o sostituire un programma eseguibile o una sua parte, in modo che eseguendo il programma il virus viene caricato in memoria; oppure il virus modifica il boot sector[48]di un dischetto e/o dell'hard disk in modo che, quando si avvia il sistema da quell'unità il virus viene eseguito e caricato in memoria. Esistono soltanto due modi in cui un virus può entrare in un sistema: eseguendo un programma eseguibile che è stato in precedenza infettato ed avviando il sistema da un dischetto che è stato in precedenza infettato.

Il primo elemento di un virus è in genere costituito da una ***routine di ricerca***, che gli consente d'individuare un'area in cui diffondersi, che può essere un settore del disco o un determinato gruppo di programmi. Il secondo elemento è costituito dalla ***routine di copia***, che consente di copiare il virus stesso nell'area individuata dalla routine di ricerca. Uno degli elementi essenziali del virus è costituito dalla ***routine d'infezione*** (o codice virale), in grado di svolgere operazioni dannose per il sistema, come eliminare record da un determinato file o impedire all'utente di accedere a determinate risorse. Infine, può esistere una ***routine d'antirilevamento***, inserita in vari punti del codice, che ha il compito d'impedire la rilevazione del virus.

Laboratori e centri di ricerca hanno già classificato più di diecimila virus, dal famoso ***Creeper*** (1970) fino al recente Hps[49] per Windows'98, che ha fatto la sua uscita pochi giorni dopo il nuovo software della Microsoft. I virus sono scritti di solito in ***Assembler***, un linguaggio difficile da usare ma estremamente potente, e sono in grado di diffondersi su altri calcolatori attraverso lo scambio di dischetti o le reti telematiche, dando così origine a vere e proprie epidemie.

Nei primi quattro mesi del 1998, l'80% delle aziende americane infestate da un virus lo hanno contratto dalla rete, mediante file di posta elettronica contenenti documenti Word[50]. Tali file, infatti, sembrano essere un terreno fertile per i "macro-virus", una nuova generazione di virus che grazie a reti multipiattaforma è ora in

[48] Il primo settore del disco, che contiene un piccolo programma che viene eseguito quando si avvia il sistema da quel disco.
[49] L***'Hantivirus Pulmonary Syndrome***, inserendosi nei file di Winsows'98, causa un'inversione casuale degli elementi grafici presenti sullo schermo, come se all'improvviso il monitor si rovesciasse all'ingiù.
[50] Tali dati sono rintracciabili nell'articolo "Virus in Rete" di C. Gerino, pubblicato su Computer Valley n.32 del 21/5/98.

grado di contagiare anche dei sistemi operativi che sembravano immuni a tale rischio (es. il mondo Macintosh).

I macro-virus colpiscono i fogli elettronici, i programmi di presentazione multimediale (es. Power Point), i file di help e le nuove "librerie" di Windows. Riguardo al nostro paese, le statistiche elaborate da Euros-SecurityNet evidenziano alcuni fattori indicativi: i virus attivi in maniera efficace sarebbero c.ca 60, ma il 90% delle infezioni scoperte derivano solo da 15 di questi. Su un totale di 60, solo 6 sono dei macro-virus, ma questi ultimi sono stati responsabili solo del 48% delle infezioni censite. Rispetto agli 89 virus censiti nel 1996, si può notare un calo del 32%, che pare determinato sia dal cambiamento realizzato nel modo di lavorare e d'installare programmi[51]che dalla crescente diffusione di Windows 95 e Windows NT.

Nel campione esaminato dalla SecurityNet ogni azienda ha avuto almeno due casi d'infezione nel 1997, il che fa supporre ad un totale nazionale di c.ca 200mila infezioni l'anno, il 42% delle quali provenienti dalla rete. Se si sono ridotte le "infezioni" provocate dall'introduzione in azienda di programmi non ufficiali (es. videogiochi), sono in aumento quelle causate dai citati macro-virus.

Tale crescita sembra essere dovuta a due ragioni particolari: l'utilizzo, da parte di tale forma d'infezione, della posta elettronica come veicolo di contagio, e l'estrema semplicità di programmazione di un file di macro-virus[52]. Non vi sono più regioni italiane esenti dal fenomeno "virus", anche perché è cresciuta la diffusione dei sistemi informatici sul territorio nazionale. Ovviamente la distribuzione segue la presenza dei calcolatori sul territorio, quindi il nord resta la zona più colpita anche se la singola regione più a rischio è il Lazio (che da solo ha raccolto il 31% dei casi) [53].

Una novità emersa nel panorama italiano è la diffusione di falsi virus, definiti "Hoax", degli allarmi lanciati periodicamente in rete che indicano rischi di possibili infezioni attraverso la diffusione di semplici messaggi di posta elettronica. In alcuni casi l'effetto degli Hoax virus è stato equivalente all'attivazione di vere e proprie

[51] Tale installazione avviene oggi sempre più mediante CD-ROM, notoriamente meno a rischio di contaminazioni.
[52] In relazione ai contagi esclusivamente tramite macro-virus, le statistiche dell'International Security Association parlano di un notevole aumento, vicino al 48%. Fonte: ***Si diffonde il "Macro-contagio"***, di L. Tremolada, pubblicato su www.repubblica.it in data 17/9/'98.
[53] Vedi nota n.50.

infezioni, in quanto gli utenti più sprovveduti, dopo aver ricevuto tali messaggi, hanno bloccato attività aziendali in corso e perso intere giornate lavorative per verificare l'esistenza o meno di contagi.

Le aziende che subiscono maggiormente gli effetti dannosi dei virus sono quelle della Pubblica Amministrazione, mentre le più protette sono le banche e gli Istituti finanziari. Anche se pare in aumento l'attenzione al rischio virus, SecurityNet ha lanciato l'allarme sulla crescita dei virus a livello mondiale: pare che alla fine del '98 ve ne saranno c.ca 13mila, e che la produzione del '97-'98 sarà quella con più durata nel tempo. I maggiori produttori di virus si confermano gli USA, mentre Sud America ed Europa dell'Est stanno recuperando "importanti" posizioni.

Nel settembre del 1994 si è svolto a Rio de Janeiro il XV Congresso internazionale di diritto penale, una sezione del quale è stata dedicata al computer crime ed ai rischi originati dai crimini informatici. Al termine dei lavori di tale sezione, è stato stilato un documento indicante una serie di misure ritenute indispensabili, tra le quali: un'implementazione della sicurezza volontaria da parte degli utenti, un'imposizione di misure di sicurezza obbligatorie in settori di particolare importanza, sviluppo e promozione di un'etica informatica presso tutte le strutture della società, formazione ed istruzione di personale investigativo (pubblico e privato) e giudiziario[54].

Tali indicazioni sono state pienamente raccolte da una serie d'istituzioni pubbliche e private, che negli ultimi anni si sono mostrate particolarmente attive contro la criminalità informatica. Un punto di riferimento per gli utenti italiani, vittime d'intrusioni informatiche mediante la rete, è il CERT-IT (Computer Emergency Response Team Italiano), un organismo senza fini di lucro che svolge attività di ricerca e sviluppo nell'ambito della sicurezza dei sistemi informatici. Fondato nel 1994 presso il Dipartimento di Scienze dell'Informazione dell'Università degli Studi di Milano, il CERT-IT è stato ammesso dopo appena un anno di vita al Forum of

[54] Altri punti riguardavano: creazione ed implementazione di normative, politiche e linee guida da parte dei Governi nazionali in materia di sicurezza, sviluppo della cooperazione con le vittime per denunciare i computer crime. Fonte: FTI, ***Osservatorio sulla criminalità informatica. Rapporto 1997*** op. cit.

Incident Response and Security Teams (FIRST), un consorzio internazionale formato da c.ca 60 team provenienti da tutto il mondo, di cui è l'unico socio italiano[55].

Fino al 1996 il CERT-IT è stato finanziato dal Dipartimento di Scienze dell'Informazione. In seguito al mancare di tale finanziamento, tale organizzazione ha dovuto mettere le proprie conoscenze al servizio dei clienti tramite consulenze, tutorial sulla sicurezza, interventi in appoggio di strutture colpite dalla criminalità telematica. Se contattato, ad esempio in merito ad un incidente informatico[56], il CERT-IT provvede ad individuare il tipo d'incidente ed a suggerire eventuali contromisure momentanee o definitive, a fornire informazioni inerenti varie misure di sicurezza da adottare secondo le necessità dell'utente, ad individuare eventuali punti nella sicurezza di vari prodotti software, a sviluppare programmi per diverse funzioni di controllo e monitoraggio.

Dal 1994 al 1997, il numero degli incidenti registrati al CERT-IT non ha avuto una tendenza regolare. Dai 35 casi del '94 si è saliti ai 164 del '95, per scendere nel '97 a 103 infrazioni, con il coinvolgimento totale di 492 diversi calcolatori[57]. Le stime del '95 indicano nei mesi di luglio e agosto il minimo numero d'infrazioni, mentre ottobre e dicembre sono i periodi di maggior "lavoro" per gli hacker. I principali obiettivi sono Enti Profit (45%) e banche dati di diverse Università (40%). Le finalità di tali infrazioni consistono nel semplice curiosare (37%) e nel furto di dati (29%). Le tecniche più usate sono state lo sniffing (35%), la ricerca di bugs nei sistemi operativi (24%) e lo spoofing (16%).

Sulla totalità dei casi del 1997, il 66% ha una provenienza accertata, in netta prevalenza d'origine straniera. Solo 24 casi su 103 hanno una sicura origine italiana, ed in prevalenza riguardano università ed istituti di ricerca. Analizzando gli obiettivi degli attacchi, alla ricerca di una preferenza o di una logica di scelta, si è notato che

[55] Nato nel 1990, il FIRST è la più grande struttura internazionale che si occupa del problema della gestione degli incidenti informatici. I membri effettivi del FIRST sono Incident Response Team ammessi a farne parte solo dopo un processo di selezione, che ne verifica la qualità e l'adeguatezza.
[56] Tale contatto può avvenire anche riempiendo un questionario, fornito in rete presso il sito www.cert-it.it, dove sono reperibili anche diverse informazioni sulle attività di tale organizzazione, consigli su sicurezza, privacy, tecniche di protezione e numerosi altri argomenti, inerenti a come difendersi dai pirati telematici.
[57] Tali stime si sono ottenute incrociando i dati provenienti dall'articolo "***… e l'Italia sta a guardare***" di D. Bruschi (reperibile al sito www.inews.it, luglio '98) con quelli trovati in: FTI, ***Osservatorio sulla criminalità informatica. Rapporto 1997***, pag.104-106, op. cit.

spesso non esiste un disegno preciso, ma semplicemente si sfrutta l'individuazione casuale di una macchina poco protetta.

Il CERT-IT conclude le sue rilevazioni sul '97 affermando che in Italia esisterebbe una scuola di hacking di buon livello, che usa tecniche avanzate che presuppongono solide basi di conoscenza. Tuttavia, il fenomeno non sembra aver ancora assunto le connotazioni tipiche della criminalità informatica in altri Paesi, in quanto sono ancora rare le intrusioni informatiche operate con finalità strettamente commerciali, finalizzate al furto o alla deliberata alterazione di dati e flussi aziendali.

L'impronta delle indicazioni sorte al Congresso di Rio non si ferma all'opera del CERT-IT, ma permane in numerose altre attività presenti in rete. Più di una società, ad esempio, ha organizzato il proprio sito con una serie di proposte inerenti complessi sistemi di difesa a più livelli contro le intrusioni informatiche, secondo le esigenze del cliente. Inoltre tali società offrono un aiuto ai singoli cittadini anche per applicare correttamente le regole innovative fissate dalla legge sulla privacy (L.675/96), favorendo dibattiti ed approfondimenti tra gli interessati in apposite rubriche telematiche.

Un vero e proprio Club sul Computer Crime è sorto ad opera dell'IPACRI, con l'arduo compito di costituire un patrimonio d'informazioni, a disposizione delle aziende aderenti, mediante la raccolta di notizie riguardanti azioni criminose perpetrate o tentate ai danni d'Aziende di credito ed Istituzioni finanziarie. Il Club si propone anche di promuovere ricerche, studi, progetti ed iniziative per la concreta individuazione di strumenti di difesa. Gli attuali membri del Club, circa un centinaio, rappresentano una significativa quota del Sistema Bancario Italiano.

Curiosità ha destato, nel giugno del'98, l'iniziativa di un'azienda americana di gettare un guanto di sfida ai pirati dell'informatica, mediante il lancio di un sistema di sicurezza comprendente anche una polizza contro aggressioni di hacker. L'ISCA (International Security Computer Association) ha annunciato di offrire la polizza nell'ambito del suo servizio TruSecure, che prevede pagamenti fino a 250mila dollari (più di 420milioni), qualora un hacker riesca ad entrare nel network informatico di un cliente che ha seguito i parametri forniti dall'azienda.

Il costo complessivo del TruSecure è di 40mila dollari l'anno, e tale servizio consiste in una serie di procedure cui il cliente si deve attenere per mantenere alti standard di sicurezza. In effetti, l'ISCA non vende un solo prodotto, ma un insieme di prodotti e comportamenti certificati come aderenti ai propri standard di sicurezza. Tale azienda è stata la prima nel mondo a fornire un servizio d'assicurazione contro gli hacker[58].

Al termine di questa panoramica sui "nemici" della criminalità informatica non poteva mancare un accenno ai rivali istituzionali degli hacker, coloro che rappresentano la legge nella "frontiera" telematica. Dal 1989 al 1996, infatti, nell'ambito del Servizio Centrale Operativo della Polizia di Stato ha operato la sezione ***Criminalità Informatica***, costituita per contrastare fenomeni criminali nei settori emergenti dell'informatica e dei mezzi di telecomunicazione.

Nel luglio del 1996, tale sezione è divenuta il NOPT, Nucleo Operativo di Polizia delle Telecomunicazioni, collocato nella struttura dell'Ispettorato Generale di Pubblica Sicurezza presso il Ministero delle Comunicazioni. Il NOPT è oggi il nucleo centrale con competenza nazionale per il contrasto del fenomeno criminale informatico e telematico, ed opera in ambito regionale attraverso le squadre dei 19 Compartimenti della Polizia Postale, cui sono assegnati operatori specializzati nel settore dell'informatica e delle comunicazioni.

Il Nucleo si avvale di tecnologie d'avanguardia e di metodologie d'indagine, studiate per l'attività investigativa in ambito telematico, e vede i suoi investigatori dedicare una parte importante del proprio tempo all'individuazione di nuovi strumenti di contrasto a fenomeni criminali, quest'ultimi capaci di cambiare in tempi brevissimi. Gli abusi dell'informatica, delle reti e di tutti gli strumenti elettronici che possono essere impiegati per commettere reati non sono combattuti solo attraverso l'uso meccanico di mezzi continuamente aggiornati, ma il NOPT s'impegna da tempo nel tentativo di prevenire la diffusione di tali fenomeni. All'interno di tale impegno si colloca la costante attività d'avvicinamento a settori industriali, commerciali, del credito e dei "comuni" utenti telematici, allo scopo di diffondere un'etica di

[58] Fonte: ***Una sfida in piena regola ai pirati dell'informatica***, pubblicato privo d'autore sul sito www.puntoinformatico.it, in data 16/06/98. Da notare una particolarità: secondo l'ISCA, gli hacker non possono essere riformati, motivo per il quale nessuno degli esperti ISCA proviene dal mondo della pirateria.

comportamento che rispetti le ragioni dell'evoluzione tecnologica consentendo anche la prevenzione degli abusi ed il contrasto del crimine.

Maria Cristina Ascenzi, commissario capo di Pubblica Sicurezza nonché direttrice del NOPT, dichiara: "Il nostro è un lavoro complesso, di gran difficoltà, perché i criminali sanno nascondersi bene nella Rete e noi dobbiamo inventare ogni giorno nuovi strumenti. Per prevenire, per reprimere, ma non certo per censurare Internet… Siamo dei poliziotti-hacker, dobbiamo avere la loro curiosità e le loro stesse competenze per capire e scovare i passaggi dei criminali nella Rete… Non è con le segnalazioni degli utenti che riusciamo a stroncare le vere organizzazioni criminali, ma con i metodi di tutte le polizie… Sappiamo bene che prima o poi i commercianti di pornografia minorile passano su certi siti, e lì li aspettiamo…[59]".

Le segnalazioni degli utenti, tuttavia, non rivestono un'importanza puramente marginale, tanto è vero che alcune questure hanno creato una pagina Web di comunicazione con i cittadini. Questi ultimi, spesso restando anonimi, fungono da "anticorpi naturali" della rete, fornendo utili informazioni reperite durante la navigazione del Web, come liste di newsgroup sospetti o sigle particolari riferite al traffico di materiale vietato[60].

3.4. Aspetti legali dell'hackeraggio e della criminalità informatica.

La L.547 del 23/12/1993, "Modifiche ed integrazioni al codice penale in materia di criminalità informatica", ha colmato un vuoto normativo nell'ordinamento giuridico italiano, introducendo una disciplina in tale materia.

In assenza di una normativa espressa, in passato la Magistratura aveva tentato, mediante un'interpretazione più estensiva possibile, di ricomprendere le

[59] L'intervista è tratta dall'articolo ***Il poliziotto-hacker alla caccia dei criminali***, opera d'Annalisa Usai e pubblicato in rete il 13/2/98 sul sito www.repubblica.it

[60] Al riguardo vedi l'interessante articolo d'Annalisa Usai intitolato ***Poliziotti, manette online***, pubblicato a pag.94 del ***Venerdì di Repubblica*** n.550, del 25/9/'98.

tipiche ipotesi di criminalità informatica nelle fattispecie di reato riconosciute e disciplinate, fino a quel momento, dal Codice Penale.

Così facendo, si è ritenuto a lungo che norme esistenti, soprattutto nel settore della tutela del patrimonio e della fede pubblica, fossero di per sé sufficienti a reprimere i comportamenti illeciti emergenti nel settore informatico. Il tentativo della Magistratura, tuttavia, non ha sortito esiti positivi, data l'inadeguatezza delle norme del C.P. ad esprimersi su una tematica in così continua evoluzione, ed il legislatore ha finito per essere costretto a adottare una specifica disciplina, definita anche "Legge Conso".

In tale disciplina si sono creati una serie di reati che tengono conto delle più diffuse condotte criminose nel settore informatico, come l'accesso abusivo, il danneggiamento, la frode informatica, l'intercettazione fraudolenta, il falso informatico, lo spionaggio, l'attentato ad impianti di pubblica utilità, la detenzione e diffusione abusiva di codici d'accesso e la violenza sui beni informatici. Tali reati sono andati ad integrare il codice penale in una serie d'articoli, ed hanno anche modificato alcune norme processuali in materia d'intercettazione ampliando gli strumenti investigativi a disposizione delle forze di polizia.

Prendiamo in esame le novità più significative previste dalla L. 547 nel ramo dei reati telematici, riportando in sede successiva i commenti e le critiche. Tale legge ha previsto, come reato, l'***accesso non autorizzato a sistemi informatici o telematici***, collocandolo all'interno dei reati contro l'inviolabilità del domicilio[61]. L'accesso abusivo (art.615 ***ter*** del C.P.) è stato introdotto per ovviare alla difficoltà concettuale di applicare ai "beni informatici" il reato di furto, in quanto essi, diversi dai beni materiali, non sono suscettibili di sottrazione e spossessamento. Infatti, la possibilità che ci si accorgesse dell'illecita presa di conoscenza di dati o programmi, non provocando tale illecito l'assenza di questi ultimi ma solo una loro veloce copia, era divenuta molto difficile da accertare.

[61] La previsione che l'accesso abusivo ad un sistema informatico fosse da vietare era già presente nelle linee guida del Consiglio d'Europa, con le quali i Governi erano invitati a prevedere e punire questa figura criminosa.

Il reato d'accesso abusivo è configurabile esclusivamente nel caso di sistemi informatici, o telematici, protetti da dispositivi di sicurezza: si vuole così limitare la possibilità del crimine al caso in cui la presenza d'appositi meccanismi indichi chiaramente l'altruità del sistema, e la conseguente volontà del gestore di riservarne l'accesso alle sole persone da lui autorizzate.

La legge, colpendo il semplice accesso illegittimo a sistemi informatici, ha modificato la precedente considerazione che il comportamento degli hacker, quando non provocasse danno ai sistemi, non potesse avere rilevanza penale. Il reato d'accesso abusivo è punito con la reclusione fino a tre anni, e in presenza di determinate condizioni[62] prevede una serie d'aggravanti.

La legge n.547/93 considera come ***danneggiamento informatico*** ogni ipotesi di distruzione o deterioramento non solo di sistemi informatici (o telematici) e programmi, ma anche d'informazioni o addirittura di semplici dati[63].

Tale specificazione ha cercato di mettere ordine nel difficile campo della "consistenza" materiale o meno del software, che tanto aveva fatto penare i giuristi. La sanzione a tale reato prevede la reclusione da sei mesi a tre anni, con un'aggravante (fino a quattro anni) se il fatto è commesso con abuso della qualità d'operatore di sistema (chiunque abbia la facoltà d'accesso ed uso al sistema).

Una particolare forma di danneggiamento è considerata l'immissione nel sistema di ***virus***, vale a dire programmi con la specifica funzione di bloccare il sistema, distruggere i dati ivi contenuti o danneggiare l'hard disk. Chiunque diffonde un virus al fine di danneggiare un sistema informatico (o telematico), d'interromperne o alterarne il funzionamento, è penalmente responsabile a prescindere dal danno effettivamente causato e dall'intenzionalità della condotta[64]. La pena prevede una reclusione fino a due anni, ed una multa fino a 20milioni.

[62] Si può raggiungere un massimo d'otto anni se l'accesso riguarda sistemi informatici o telematici d'interesse militare, relativi all'ordine pubblico, alla sicurezza pubblica, alla sanità, alla protezione civile, se il fatto è commesso da un pubblico ufficiale con abuso di poteri e se il colpevole, per commettere il fatto, usa violenza su cose o persone, o è palesemente armato.
[63] Art.635 ***bis*** C.P.
[64] Art.615 ***quinquies*** C.P. Tuttavia è d'obbligo ricordare che non commette reato colui che, per ragioni di studio o interesse verso i sistemi di prevenzione, raccolga e/o custodisca programmi virus.

L'articolo 640 del Codice Penale descriveva il reato di truffa quando chiunque, tramite artifizi o raggiri, inducendo taluno in errore, procurava a sé o ad altri un ingiusto profitto con altrui danno. La legge sul computer crimes, sviluppando tale concetto, ha introdotto la ***frode informatica***, definendola come l'alterazione del funzionamento di sistemi informatici (o telematici) o l'intervento abusivo su dati, informazioni e programmi in essi contenuti o ad essi pertinenti[65].

La frode informatica, che per essere giudicata tale deve procurare il profitto ed il danno della formula originale, è punita con la reclusione da sei mesi a tre anni e con la multa da 100mila lire a 2milioni (anche qui sono previste aggravanti, in particolare se il fatto è commesso con l'abuso della qualità d'operatore del sistema).

Un altro settore facilmente esposto a comportamenti criminosi riguarda la ***fraudolenta intercettazione, l'impedimento o l'interruzione di comunicazioni relative a sistemi informatici e telematici***, nonché la rivelazione al pubblico, con qualsiasi mezzo d'informazione, del contenuto delle comunicazioni stesse[66].

Questo reato è punito con la reclusione da sei mesi a quattro anni, tuttavia sono possibili delle aggravanti in situazioni particolari, ad esempio se il reato è commesso da un pubblico ufficiale, da un operatore del sistema o da un investigatore privato (reclusione fino a cinque anni). E' altresì punita, con la reclusione da uno a quattro anni, l'installazione d'apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art.617 ***quinquies*** C.P.).

La L.547/93 ha introdotto il reato di ***falso informatico***, vale a dire la falsificazione di un documento informatico. Per arrivare a ciò si è dovuta specificare la nozione di "documento informatico", inteso come qualsiasi supporto informatico contenente dati, informazioni o programmi specificatamente destinati ad elaborarli[67]. In questo senso tale documento non è il prodotto dell'elaboratore, ma la sua natura va attribuita ai "supporti" di qualunque specie contenenti dati, informazioni o

[65] Art.640 ***ter*** C.P. Comportamenti tipici iscritti a tale reato sono, ad esempio, programmare l'afflusso sul proprio conto corrente d'arrotondamenti percentuali provenienti da altri c.c. ed il pagamento di assegni a vuoto.
[66] Art.617 ***quater*** C.P.
[67] Art. 491 ***bis*** C.P.

programmi. Il reato di falso informatico, quindi, si attua con l'alterazione, la modifica o la cancellazione del contenuto di comunicazioni informatiche o telematiche[68].

Affinché sia presente tale reato, si richiede il fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno. La pena prevista va da uno a quattro anni (con possibili aggravanti). Grazie alla nozione di documento informatico, è stato possibile estendere il reato relativo all'inviolabilità dei documenti segreti. In base alla nuova legge, quindi, costituisce reato la rilevazione del contenuto di documenti informatici segreti o il loro utilizzo al fine di procurare profitto a sé o ad altri con danno altrui[69]. Per tale reato è prevista una pena fino a tre anni ed una multa da 200mila lire a 2milioni.

Altri reati previsti dalla legge Conso riguardano la violenza su beni informatici, l'attentato ad impianti di pubblica utilità, la detenzione e diffusione abusiva di codici d'accesso e la violazione di corrispondenza. Il reato di "esercizio arbitrario delle proprie ragioni mediante violenza sulle cose"[70] è stato esteso ad una possibile violenza su un programma o su un sistema informatico o telematico. Si vuole così evitare il rischio che azioni violente, con il fine di esercitare diritti che si potrebbero far valere in tribunale, rendano inservibili programmi o sistemi informatici. Il reato è punito con una multa fino a 1milione.

Il legislatore ha anche esteso il reato di "attentato ad impianti di pubblica utilità" nei confronti di chi compie azioni dirette a danneggiare o distruggere sistemi informatici (o telematici) di pubblica utilità, vale a dire dati, informazioni o programmi in essi contenuti o ad essi pertinenti[71]. Nel senso voluto dal legislatore, l'oggetto del reato deve avere una rilevanza tale da far sì che un attentato allo stesso sia fonte d'immediato pericolo per l'ordine pubblico o per gli interessi socio-economici della collettività. La pena prevista è una reclusione da uno a quattro anni (fino ad otto con aggravanti).

Tipicamente relativo all'operato degli hacker è il reato di ***detenzione e diffusione di codici d'accesso***, previsto all'art.615 ***quater*** del Codice Penale. Tale

[68] Art.617 ***sexies*** C.P.
[69] Art.621 C.P.
[70] Art.392 C.P.
[71] Art.420 C.P.

reato sanziona l'abusiva acquisizione, riproduzione, detenzione e diffusione di codici d'accesso a sistemi informatici o telematici protetti da misure di sicurezza (es. password). Per configurare tale reato è richiesto che gli atti siano posti in essere con lo scopo di procurare a sé o agli altri un profitto, o di arrecare ad altri un danno. La sanzione consiste nella reclusione fino ad un anno, e nella multa fino a 10milioni (il limite si estende a due anni e 20milioni in presenza d'alcune aggravanti).

La disposizione prevista dal Codice Penale all'art.616, relativa alla violazione, sottrazione e soppressione della corrispondenza epistolare, telegrafica e telefonica, è stata estesa con la nuova legge alle comunicazioni informatiche e telematiche. Chiunque viene a conoscenza del contenuto di una comunicazione di questo tipo, che sia destinata ad un'altra persona, la devia per esaminarla, rivelarla ad altre persone o distruggerla, è così punito con una reclusione fino ad un anno ed una multa da 60mila lire ad 1milione (fino a tre anni di reclusione se dalla rilevazione del contenuto deriva un danno a qualcuno).

La legge Conso ha integrato o modificato alcune norme processuali in materia d'intercettazione, con la necessità di effettuare un raccordo con le novità apportate al Codice Penale.

La nuova legge consente all'Autorità Giudiziaria d'intercettare un flusso di comunicazioni relative a sistemi informatici (o telematici), o intercorrenti tra più sistemi, nel caso s'indaghi sui reati relativi all'art.266 del Codice di Procedura Penale, tra i quali giova ricordare delitti concernenti sostanze stupefacenti o psicotrope, armi e sostanze esplosive, contrabbando, associazione mafiosa, strage ed attentati alla sicurezza degli impianti di pubblica comunicazione.

La nuova legge ha anche modificato alcuni punti dell'art.268 del C.P.P., secondo cui è ora consentito al pubblico ministero disporre che le operazioni d'intercettazione siano compiute anche mediante impianti appartenenti a privati[72], è consentito ai difensori delle parti esaminare gli atti, ascoltare le registrazioni e prendere cognizione dei flussi di comunicazioni informatiche, ed il giudice deve disporre la trascrizione delle registrazioni da inserire nel fascicolo per il dibattimento.

[72] Ciò permette ad un agente di polizia, ad esempio, d'intercettare il traffico di comunicazioni di una BBS mediante il proprio computer e dalla propria abitazione, rendendo più agevoli certe indagini.

Numerose le critiche ricevute dalla L.547/93, sia in relazione alle forme d'espressione che ai concetti espressi mediante tali forme. S. Chiccarelli e A. Monti[73] la definiscono una legge sugli strumenti e non sugli esseri umani, eccessivamente permeata in tutte le sue norme di "sistemi telematici, programmi e documenti informatici, codici d'accesso…". Secondo questi autori, quanto più tale legge cerca di descrivere un reato addentrandosi in classificazioni terminologiche e modalità esecutive, tanto più genera norme confuse ed inapplicabili.

I termini di "riservatezza informatica", "spionaggio informatico" e "danneggiamento informatico" attribuiscono un risalto ingiustificato al nuovo mezzo, come se la presenza o meno di qualche microchip o semiconduttore modifichi i termini della questione. Perché, si domandano gli autori, è punita la detenzione e la diffusione di codici di accesso a prescindere dall'utilizzo o meno degli stessi? O la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico anche se effettivamente non utilizzati?

Un'altra questione che sembra stare molto a cuore a S. Chiccarelli e ad A. Monti riguarda l'art.615 ***ter*** del C.P., e precisamente il suo sancire che va punito il semplice fatto di essersi introdotti in un sistema, protetto da misure di sicurezza, a prescindere da qualsiasi intento od operazione effettivamente compiuta dall'agente, con aggravanti se dal fatto deriva un danno alle macchine o a dati e programmi. Gli autori confrontano il testo della 547/93 con il CFAA (Computer Fraud and Abuse Act), l'omonima legge americana per la quale è necessario più di un semplice accesso in un sistema telematico per violare la normativa.

Il CFAA, infatti, prevede e punisce tre diversi tipi d'accesso, tutti legati alla commissione d'azioni aggiuntive alla semplice penetrazione del sistema (scopo fraudolento, atti che intenzionalmente danneggiano un computer o si traducono nell'impossibilità di utilizzarlo causando un danno pari a 1000dollari in un anno, comportamenti che originano la stessa conseguenza pur non essendo deliberatamente pericolosi). Perché, si domandano gli autori, ciò che negli USA è considerato condizione ***sine qua non*** per punire l'accesso abusivo in Italia rende le pene più pesanti?

[73] S. Chiccarelli e A. Monti, ***Spaghetti hacker***, op. cit.

Inoltre, proseguono Chiccarelli e Monti, se è tanto importante proteggere l'integrità dei computer, perché non sono previste punizioni per chi non adotta le dovute precauzioni di sicurezza, o per chi produce sistemi o programmi intrinsecamente vulnerabili o malfunzionanti? L'ultimo aspetto pesantemente criticato dai due autori, relativo alle novità introdotte dalla legge Conso, riguarda le indagini e le intercettazioni informatiche, ree di strangolare i diritti dei cittadini.

L'art.266 ***bis*** del C.P.P. giustificherebbe, di fronte alla presenza di un qualunque sistema informatico sospettato dei reati citati in tale articolo, la richiesta d'intercettazione telematica, con pesanti conseguenze per la sfera privata del malcapitato. Siamo sicuri, sembrano chiedersi in conclusione gli autori, che tale sistema sia utilizzato solo di fronte a prove certe di colpevolezza, e non per individuare le prove stesse?

Accuse d'eccessiva severità, rivolte alla L.547/93, sono sorte anche da vari partecipanti al convegno ***Diritto alla Comunicazione nello scenario di fine millennio***, svoltosi a Prato nel febbraio del 1995. L'autore Raf Valvola Scelsi, redattore della rivista "Decoder" e nome noto nel ramo della cultura cyberpunk-underground, ha visto in questa legge una volontà molto ferrea di disciplinare il comportamento del corpo sociale, con pene molto pesanti nei confronti di comportamenti di carattere trasgressivo, più che per reati veri e propri.

Dal Convegno è emerso anche come, il non aver trattato e approfondito in alcun modo, da parte della L.547, la tematica delle BBS e dei relativi Sysop, rischi di lasciare la materia in balia di libere interpretazioni, alcune delle quali molto discutibili (es. identificazione certa dell'utente, trasformazione del Sysop in una sorta di pubblico ufficiale, riconoscimento dell'esistenza delle BBS, da parte dello Stato, attraverso una dichiarazione più o meno burocratica, dura e vessatoria).

Altri interventi legislativi completano il panorama all'interno del quale agisce la criminalità informatica, tutti con l'intenzione di rendere la vita più difficile ai pirati del ciberspazio.

Nell'aprile del '97, ad esempio, è stata presentata alla Camera dei Deputati una proposta di legge[74] relativa ad Internet, all'interno della quale si proponeva di raddoppiare le pene previste per i reati di pornografia, pedofilia, terrorismo e traffici criminali, quando commessi mediante reti telematiche. Un'altra "freccia" nell'arco della polizia telematica è la L.518/92, relativa al copyright ed alla tutela giuridica del software.

Tale tematica necessita di un approfondimento e di una trattazione particolare, in quanto rappresenta uno dei campi dove è maggiore l'attività della criminalità informatica, e dove l'evoluzione tecnologica fa sorgere in continuazione nuove domande. Inoltre, la normativa del '92 ha sollevato un vespaio di polemiche, creando in alcuni casi più problemi di quanti ne abbia risolti. Ad una breve analisi della legge, unita ad una serie di dati sulla pirateria del software in Italia, farà seguito una panoramica sulle critiche e sulle difficoltà d'applicazione della legge stessa.

Il decreto legislativo n.518, emanato il 29/12/1992, risponde alla necessità d'attuazione di una direttiva europea - precisamente la n.250 del '91 - relativa alla tutela giuridica dei programmi per elaboratore. In tale decreto si paragonano i programmi per elaboratore a delle opere letterarie, richiedendo per i primi la medesima protezione applicata a queste ultime (per le quali è fatto esplicito riferimento alla Convenzione di Berna, sulla "protezione delle opere letterarie ed artistiche", ratificata e resa esecutiva con la L. 399/'78) e sancendo così l'inviolabilità del diritto d'autore.

Il decreto precisa che restano esclusi da tale tutela le idee ed i principi alla base di qualsiasi elemento di un programma, compresi quelli alle origini delle sue interfacce. Il termine "programma" comprende anche il materiale preparatorio per la progettazione del programma stesso. Dovendo fare chiarezza in merito ai rapporti tra lavoratore dipendente e datore di lavoro, il decreto specifica nell'art.3 che "…qualora un programma per elaboratore sia creato dal lavoratore dipendente nell'esecuzione

[74] Precisamente la n.3530, iniziativa del deputato Stagno d'Alcontres.

delle sue mansioni o su istruzioni impartite dal suo datore di lavoro, questi[75] è titolare dei diritti esclusivi d'utilizzazione economica del programma creato".

Viene in seguito citato un elenco di diritti esclusivi, conferiti da tale legge al proprietario del programma. Questi diritti[76] rappresentano delle attività soggette all'autorizzazione di tale proprietario, salvo il caso in cui si dimostrino essere azioni necessarie per l'uso del programma da parte del legittimo acquirente.

Proprio su tale "necessità" vertono alcune difficoltà in sede applicativa, dovute all'impossibilità di dimostrare, sempre con la dovuta certezza, quando queste azioni siano indispensabili all'uso del programma e quando rientrino nella violazione dei citati diritti. La legge dichiara che "l'autorizzazione del titolare dei diritti non è richiesta qualora la riproduzione del codice del programma, e la traduzione della sua forma…, compiute al fine di modificare la forma del codice, siano indispensabili per ottenere le informazioni necessarie per conseguire l'interoperabilità, con altri programmi, di un programma per elaboratore creato autonomamente…[77]". Come traspare dalla nota, l'applicazione di tale legge richiede un'elevata competenza tecnologica, ed affronta situazioni dove è oggettivamente difficile delineare un confine netto tra legalità ed illegalità.

L'art.6 della 518/'92 prevede che la SIAE si occupi di tenere un registro pubblico speciale sui programmi per elaboratore. In tale registro deve essere registrato il nome del titolare dei diritti esclusivi d'utilizzazione economica del programma, e la sua data di pubblicazione, "intendendosi per pubblicazione il primo atto d'esercizio dei diritti esclusivi". Le modalità di registrazione devono essere regolate mediante relative tariffe[78].

---

[75] L'interpretazione corrente di tale passaggio vede il "questi" riferito al datore di lavoro, in realtà la forma usata non sembra corretta perché pone il rischio d'incomprensioni. Ci si domanda perché non sia stato utilizzato il termine "quest'ultimo".

[76] Riproduzioni di qualunque tipo, operazioni di caricamento, visualizzazione, esecuzione, trasmissione e memorizzazione del programma stesso, traduzioni, adattamenti e trasformazioni, qualsiasi forma di distribuzione al pubblico. Vedi art.5 del citato D.L.518/'92.

[77] A patto che tali attività siano svolte dal licenziatario, che le informazioni necessarie per conseguire tale interoperabilità non siano già rapidamente accessibili in altro modo, che tali attività siano limitate alle parti del programma originale necessarie per conseguire tale interoperabilità. Vedi art.5 del citato D.L.518/'92.

[78] E' importante notare come tale registro non abbia nessun compito di certificazione implicita o esplicita della paternità del programma, ma serva solo a tenere la traccia del trasferimento dei vari diritti sul software. Fonte: S. Chiccarelli e A. Monti, ***Spaghetti Hacker***, pag.175, op. cit.

L'art.10 riassume il senso dell'intero decreto legge, delineando i suoi reati e le sue pene: "Chiunque abusivamente duplica, a fini di lucro, programmi per elaboratore, o, ai medesimi fini e sapendo o avendo motivo di sapere che si tratta di copie non autorizzate, importa, distribuisce, vende, detiene a scopo commerciale, o concede in locazione i medesimi programmi, è soggetto alla pena di reclusione da tre mesi a tre anni e ad una multa da £ 500.000 a £ 6.000.000.

Si applica la stessa pena se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria, o l'elusione funzionale, dei dispositivi applicati a protezione di un programma per elaboratore[79]".Tale legge s'inserisce in un quadro generale che vede l'Italia come uno dei paesi al mondo con il più alto "tasso di pirateria" di software, superiore al 50% (vale a dire che ogni due programmi che girano sui computer, uno è illegale) [80].

La BSA (Business Software Alliance), potente associazione internazionale che riunisce tutti i produttori di software[81], ha denunciato per il '97 la perdita di 100miliardi di I.V.A. non pagata sul mercato italiano, ed ha intrapreso da tempo una politica di visite "a sorpresa" presso imprese ed aziende, onde verificare la situazione in merito alle copie clandestine di programmi software. Una massiccia campagna pubblicitaria d'avvertimento, intrapresa dalla stessa BSA, invita a prevenire tali controlli verificando la regolarità del software installato "prima che sia troppo tardi". Tale verifica può essere effettuata rivolgendosi ad un rivenditore di fiducia o direttamente alla BSA, mediante un numero verde, la quale provvederà ad inviare un kit di verifica gratuito.

Si calcola che c.ca 10mila imprese abbiano subito tale controllo, in seguito al quale sono state intraprese c.ca 400 iniziative legali nei confronti di possessori di programmi privi di licenza. Una media elevata se si pensa che, in tutta Europa, le azioni legali sono state 4000.

---

[79] Citato testualmente. L'intero D.L. è reperibile in rete al sito www.interlex.com, alla sezione "Fonti normative e documenti".

[80] Negli USA tale fenomeno si aggira intorno al 27%. Fonte: ***Software pirata*** di A. Usai, su Computer Valley n.33 del 28/5/'98.

[81] Fondata nel 1988 per volontà delle principali aziende multinazionali produttrici di software, il suo operato è oggi supportato da 22 produttori, tra i quali la Microsoft, Adobe System, Autodesk, Lotus, Novell, Symantec, Bentley, Filemaker e Finson. Tali aziende rappresentano oltre il 90% del mercato italiano, con un fatturato di 600miliardi di lire l'anno. Fonte: vedi nota precedente.

Il 59% delle aziende non in regola si trova nel Nord Italia, il 23% al Centro ed il 18% al Sud. La regione dove maggiormente si registra tale fenomeno è la Lombardia (25%), seguita da Lazio e Veneto (entrambe al 12%). A servirsi maggiormente di software "copiato" sono le imprese dei servizi (37%), seguite dagli studi professionali (22%) e dalla produzione industriale (21%) [82].

Come precedentemente accennato, tale legge ha suscitato una serie di reazioni molto critiche da parte della "popolazione della rete", sia in merito ai contenuti sia alle modalità d'espressione degli stessi. Viene contestata, ad esempio, l'assoluta mancanza di considerazione nei confronti d'alcuni programmi, come quelli ***shareware*** o di ***public domain***, che costituiscono una legittima, generosa ed efficace alternativa di distribuzione al software commerciale.

Uno dei punti più controversi riguarda la differenza fra "scopo di lucro" e "profitto", due ipotesi che dovrebbero distinguere chiaramente tra la presenza o meno di reato. Il fine di lucro sembra essere la chiave di tutto: se non c'è attività economica dietro la riproduzione del software, allora tale azione non può essere reato.

Una recente sentenza del Pretore di Cagliari[83] ha affermato chiaramente quest'importante differenza: se la legge punisce soltanto la duplicazione a scopo di lucro (vale a dire un accrescimento del proprio patrimonio), ed il non pagare i diritti su un programma genera solo un profitto (cioè una mancata spesa), allora la duplicazione a scopo personale non è reato.

Altre critiche hanno accusato tale decreto di essere stato emanato su pressione delle case di produzione di programmi, le quali si arrogherebbero tutti i diritti sul software, godendo degli interventi delle forze dell'ordine a smuovere situazioni che, altrimenti, le vedrebbero costrette in interminabili cause civili. Infatti, risulta quantomeno anomala una situazione dove la violazione di un contratto, in pratica un accordo tra privati, è automaticamente sanzionata con una norma penale. Inoltre, appare criticabile che chi visiona un programma per curiosità, bisogno di

[82] Fonte: vedi nota n.80.
[83] Fonte: ***Il Sole-24 ore*** del 2/10/'97. La sentenza è datata 26/11/'96.

conoscenza o motivo di ricerca scientifica, non sia autorizzato a farlo prima di aver pagato le royalties al produttore.

L'autore Raf Valvola Scelsi, già critico nei confronti della L.547/'93, intravede nel D.L. 518/'92 l'affermazione d'istanze di tipo monopolistico e d'egemonia del mercato americano su quello italiano, assieme ad una svalutazione del lavoro vivo e ad una sua sussunzione operata da parte del capitale[84].

A parziale giustificazione delle controversie sorte in seguito alla legge sul copyright, riportiamo un esempio di quanto sia difficile legiferare in merito, e di come altri paesi abbiano difficoltà ben maggiori del nostro. In Argentina, la Suprema Corte ha stabilito che il software per elaboratori elettronici non può essere tutelato dalle leggi sul diritto d'autore, considerate dai giudici troppo antiquate per trovare applicazione in un campo così innovativo.

Si pensi che sul 70% del software commercializzato in Argentina non risulta pagata alcuna royalty, il che si traduce in c.ca 165 milioni di dollari annui di mancati ricavi per gli sviluppatori. La maggiore preoccupazione dei produttori di software è che tale sentenza faccia fiorire in quel paese l'attività dei pirati informatici, di coloro che copiano il software e lo mettono in vendita senza pagare i diritti d'autore. Il rischio è che la sentenza argentina sia "copiata" anche da altri paesi del Sud America, trasformando tale continente nella terra del software illegalmente clonato e venduto al resto del mondo[85].

[84] Vedi Strano Network, ***Nubi all'orizzonte***, pag.38, op. cit.
[85] Fonte: ***Argentina, copiare software è legale***, articolo pubblicato privo d'autore su Computer Valley n.37 del 25/6/'98.

Figura 3 **Il criminale informatico ed il suo raggio d'azione**

Tipo di crimine	Tecnica usata	Riferimento legislativo	Riferimento sociale	Autore
Intrusioni informatiche con varie finalità (curiosità, spionaggio, operazioni economiche…).	Spoofing E-Mail bombing Exploit Breakage	L.547/'93 art.615 C.P.	La vittima prova disagio e vergogna, diffidenza verso i propri dipendenti, si teme la reazione dei clienti.	Hacker Cracker Insider
Truffe a compagnie telefoniche.	Sniffing Spoofing E-Mail bombing	L.547/'93 art.640 C.P.	Scarsa percezione del crimine nel far pagare i propri collegamenti alle compagnie, frequenti casi d'insider, diffidenza dei maggiori clienti verso le compagnie stesse.	Phreaker
Utilizzo della rete per il ***traffico di pedofilia***.	Utilizzo di BBS segrete, password, backdoor d'entrata.	Proposta di L.263, approvata giugno'98.	Cresce la diffidenza verso la rete, aumentano i controlli alle BBS, rischi per privacy e diritto alla comunicazione.	***Estraneo***[86]
Duplicazione e ***traffico illecito di software.***	Varie: per la sprotezione, la duplicazione, la distribuzione del software pirata.	L.518/'92.	Aumenta la difficoltà nel percepire tale costume come reato, aumentano i controlli a sorpresa (BSA), più attenzione per l'informatica "alternativa".	Cracker Courier Supplier
Attentato alla rete o a singoli sistemi tramite ***virus***.	Varie per la creazione e la distribuzione (es. floppy disk) dei virus.	L.547/'93 art.615 C.P.	Maggiore attenzione ai "contatti" tramite la rete, i floppy disk, la provenienza dei programmi; sviluppo mercato d'antivirus. Rischi di fobie collettive.	Cracker
Installazione e/o utilizzo di strumenti per ***intercettare, registrare, impedire, modificare comunicazioni informatiche e telematiche***.	Sniffing Spoofing Denial of service E-Mail bombing	L.547/'93 art.617 C.P. (ed altri).	Diffidenza verso qualsiasi tipo di comunicazione telematica, fobia del "big brother watching you", rischi per la privacy e per lo sviluppo d'alcuni servizi in rete (es. di tipo economico).	Hacker Phreaker

Fonte: Nostra elaborazione sulla base delle informazioni bibliografiche.

[86] Non è possibile inserire una categoria di hacker all'interno di questo tipo di crimine, in quanto totalmente estraneo a qualunque comportamento fra quelli approfonditi in questo lavoro. L'unica possibilità, come spesso erroneamente effettuato dai media, riguarderebbe l'inserire nel termine "hacker" chiunque perpetui un crimine per via telematica, ma allora la classificazione effettuata non avrebbe senso.

4. La Rete e gli Hacker: il binomio imperfetto

"Net.gener@tion, generazione della Rete, è il nome che si dà la generazione che ha deciso di cambiare volto al mondo, costituendosi come comunità informatica, comunità via cavo."
Luther Blisset, "Net.gener@tion".

4.1. L'ambiente di "lavoro" dei pirati telematici.

Questo capitolo ha l'intenzione di fornire le conoscenze di base relative alla rete, in quanto "ambiente di lavoro" per gli hacker, e di mettere in luce alcune conseguenze di questo equivoco binomio. Tutto ciò con la consapevolezza di una necessaria brevità, ma con la speranza di una sufficiente chiarezza e logicità di percorsi.

Il matrimonio tra informatica e telecomunicazioni ha generato la telematica, una disciplina che vede il suo settore di competenza nell'utilizzo delle tecnologie informatiche nel campo delle telecomunicazioni. Esempi d'applicazioni telematiche sono i fax, gli sportelli bancomat, i terminali di lettura delle carte di credito. Le reti telematiche connettono tra loro, tramite cavi telefonici e cavi a fibra ottica, un numero illimitato di computer, situati anche a grandi distanze; ciò semplifica l'agire di molti hacker, in grado di effettuare operazioni illecite in vestaglia e dalla propria camera da letto.

I computer collegati in rete, pur avendo caratteristiche hardware e sistemi operativi diversi, sono in grado di riconoscersi e di comunicare tra loro, grazie all'adozione d'alcuni protocolli comuni. Un protocollo è un insieme di regole che permettono tale riconoscimento e comunicazione[1]. Con il termine di "Internet" (con la

[1] McGraw-Hill, ***Professione Internet***, supplemento n.2 del quotidiano "La Repubblica", Gruppo Editoriale l'Espresso SPA, Roma, 1998

lettera iniziale in maiuscolo) s'intende, comunemente, l'insieme di tutte le migliaia di reti basate su tali protocolli comuni, il più famoso dei quali è il TCP/IP (Transfer Control Protocol/Internet Protocol), originariamente sviluppato dall'ARPA, un ente americano facente capo al Dipartimento della difesa.

Tale protocollo permette la commutazione dei pacchetti, vale a dire la suddivisione e l'invio di tutti i dati in vari pacchetti, ognuno con il proprio "indirizzo di destinazione"; in questo modo la rete non è mai interamente occupata solamente da un invio, ma tutti i computer possono inviare e ricevere i propri pacchetti che, alternativamente, trovano sempre la possibilità di transitare[2]. Per capire come si è arrivati a tutto questo occorre fare un passo indietro, alla realtà della Guerra Fredda e delle numerose ricerche che essa portò a sviluppare negli USA anni'60. Una di queste, il progetto ARPAnet, nacque dalla necessità di rendere periferica la rete di telecomunicazioni, in modo che la distruzione di un singolo nodo di collegamento non influenzasse gli altri, in grado di continuare a gestire il complesso flusso di dati.

L'assenza di un nodo centrale sembrò favorire tale scopo, e la sperimentazione cominciò nel 1969 ad opera dei militari, cui si unirono, in breve tempo, università ed enti di ricerca. Nel '72 i nodi erano già divenuti 37 ed il network andava perdendo le iniziali caratteristiche, svolgendo prevalentemente compiti di trasmissione di dati fra università. Nel 1983 si distaccò la sezione militare, gettando le basi per l'evoluzione della rete verso la situazione attuale[3].

Durante gli anni '80 questa rete, comunemente nota come NFSNet, ha cominciato ad espandersi molto velocemente: migliaia d'università, compagnie di ricerca, agenzie governative, aziende e semplici hobbisti hanno trovato il modo di utilizzarla e di esservi presenti. Ciò è stato possibile grazie al potenziamento dei backbone[4]. Nel 1986 NFSNet è arrivata in Italia, ma il fenomeno era ancora limitato ad ambiti universitari o privati, lontano dal grande pubblico.

Le modalità d'accesso alla rete, infatti, risultavano ancora poco intuitive e poco accessibili ad utenti occasionali.

---

[2] Per vedere come possono intervenire gli hacker sul transito di pacchetti vedi cap.3.3
[3] McGraw-Hill, ***Professione Internet***, op. cit.
[4] Linee dorsali che formano la struttura base del network

E' d'obbligo una specificazione: per "accesso alla rete" s'intende un semplice collegamento ad Internet, mentre "essere presenti in rete" vuol dire avere un proprio spazio (una o più pagine, definite "sito"), memorizzato in qualche computer ed accessibile agli utenti connessi.

Dal 1990 si è assistito ad una massiccia invasione di software e servizi dedicati ad un uso meno specialistico della rete; tra questi il servizio "gopher", e soprattutto il WWW (World Wide Web), hanno disegnato la struttura di Internet come oggi la conosciamo. Il gopher è stato il primo strumento a permettere un salto di qualità nell'interfaccia di Internet: esso prende il nome dalla mascotte dell'università del Minnesota (simile alla marmotta, in Italiano è denominato citello) dove, nel 1991, è stato sviluppato[5]. Tale strumento consente di muoversi all'interno della rete usando solamente i tasti "cursore" ed "invio", usando il protocollo TCP/IP ed il servizio client/server. Il gopher ha permesso di mettere un po' d'ordine in rete, e da una sua evoluzione ipertestuale è nato il WWW.

Creato dal CERN di Ginevra nel 1989, ma diffuso al pubblico solo all'inizio del 1993, il WWW è un'interfaccia ipertestuale che usa il linguaggio HTML, esplorata grazie ai programmi navigatori; in altre parole, è una veste grafica che ci presenta i documenti collegati tra loro mediante un linguaggio, in grado di gestire immagini, suoni e pagine grafiche. Quest'interfaccia consente di accedere alle informazioni nel modo più semplice possibile, puntando il cursore e cliccando con il mouse su dei "link", collegamenti ipertestuali che rimandano da una pagina all'altra di un documento, o direttamente da un documento ad un altro; si evita così di usare la tastiera per accedere ai servizi della rete. Il Web, noto anche come "la tela del ragno" è, per analogia, la rete, visto che il WWW rappresenta l'interfaccia più diffusa di Internet.

Tale rete è quindi formata da un insieme di calcolatori che prendono il nome di "host" o nodi (ogni host è un computer che ospita altri computer sulla rete; il provider, come vedremo, è un host), e di reti o network che costituiscono le infrastrutture di comunicazione cui gli host sono connessi.

[5] A. Arata, ***Navigando: guida introduttiva al mondo della Rete Internet***, Flashnet, Roma, 1996

L'architettura su cui si basa la rete è di tipo client/server: il client è la parte attiva che richiede i servizi e ne usufruisce tramite il proprio p.c., il server è il soggetto che risponde a tale richiesta diffondendo i servizi che realizza in proprio, o che sono svolti da altri server di cui esso è un client. Client e server sono indipendenti, vale a dire possono esistere su due calcolatori differenti.

La caratteristica saliente in Internet è che, una volta entrati, il costo del collegamento è del tutto indipendente dalla distanza; infatti, il solo costo telefonico da sostenere è quello fra il proprio telefono ed il punto scelto d'ingresso in rete, o provider. Il provider è la società che garantisce l'accesso alla rete tramite abbonamento, connettendo il computer dell'utente ad Internet mediante un nome ed una password scelti dall'utente stesso[6]. Dal punto di vista tecnico ciò avviene attraverso uno strumento, definito modem, in grado di trasformare il segnale digitale del computer in quello analogico del telefono al momento del contatto con la rete; viceversa, dal segnale analogico a quello digitale, quando attraverso la rete si raggiunge un altro computer.

Per accedere alle molteplici applicazioni di Internet è ideale possedere un modem veloce, che permetta di risparmiare tempo nei viaggi in rete, quindi di pagare meno la telefonata al proprio provider. Per avere la massima velocità possibile è consigliabile usare le linee ISDN (Integrated Services Digital Network), una rete digitale capace di trasportare diversi servizi trasmettendo dati sotto forma di bit, possibile da usare in maniera tradizionale grazie alle centrali di commutazione. Per ricevere il servizio è necessario che il modem sia in grado di allacciarsi alla rete ISDN, che il tradizionale apparecchio telefonico sia digitale e che si firmi un nuovo contratto con la Telecom (infatti, l'utente si troverà a possedere due canali, potendo telefonare e navigare contemporaneamente).

La navigazione all'interno del Web è permessa da particolari programmi, denominati browser, che hanno il compito di leggere e presentare documenti ipertestuali, costruiti mediante il linguaggio HTML. Il gran merito dei browser è stato rendere la comunicazione più semplice ed accessibile per tutti, hacker compresi, sfruttando un intuitivo sistema di codici ed icone. La particolare natura del linguaggio

[6] Come si ricorderà, una delle prime imprese di un qualunque hacker consiste spesso nel collegarsi in rete scaricando la spesa su ignari aziende, ree di non aver sorvegliato abbastanza sui propri codici d'accesso.

HTML, che non si occupa direttamente di come il testo debba essere visualizzato, aumenta ulteriormente l'importanza del browser, che procede autonomamente a visualizzare le pagine prodotte con tale linguaggio.

Ciò determina che le pagine Web siano visualizzate in modo differente secondo il browser usato, tuttavia quantità e qualità d'informazione restano sostanzialmente invariate. Senza addentrarci nella "guerra" fra browser che sta infiammando il mercato, ci limiteremo ad affermare che i due modelli più famosi ed utilizzati sono Netscape Communicator e Microsoft Internet Explorer, distribuiti in continuo aggiornamento ed in versioni adatte ai diversi sistemi operativi.

Possiamo definire un URL[7] come lo strumento attraverso il quale è possibile individuare la locazione di un altro computer in rete; più precisamente esso permette al nostro browser di accedere a qualsiasi file di un server Web. Ogni URL è formato da tre differenti parti: il formato di trasferimento, il nome dell'host (la macchina dove è collocato il file che cerchiamo), il percorso del file. Gli indirizzi IP identificano i computer connessi ad Internet: essi sono rappresentati con numeri a 32 bit, dichiarati in una sequenza composta da quattro cifre decimali separate da un punto, comprese tra 0 e 255.

Ad esempio 199.170.0.150, indirizzo molto noto agli hacker, corrisponde al server dell'F.B.I., un sito più volte "bucato" dai pirati informatici. La parte sinistra del numero indica una sottorete di Internet, ulteriormente precisata via via che ci si sposta verso destra, fino ad identificare un determinato host all'interno di quel network.

Tale concetto è stato semplificato dall'introduzione del DNS [8], un sistema d'indirizzamento simbolico che ripartisce l'intera rete in domini, suddivisi in sottodomini, a loro volta costituiti da livelli sempre più specifici, fino ad identificare l'host cercato. Il DNS consente di nominare un indirizzo in forma logica (host name), più agevole rispetto ad una sequenza complicata di numeri, ed è usato sia per accedere ai siti Web che per gli indirizzi di Internet.

[7] Sigla d'Uniform Resource Locator (Fonte: McGraw-Hill, ***Professione Internet***, op. cit.)
[8] Sigla di Domain Name System (Fonte: McGraw-Hill, ***Professione Internet***, op. cit.)

In genere, ogni utente di Internet possiede almeno un proprio indirizzo logico, diverso da altri tipi di indirizzi. Tali riferimenti sono costituiti da due parti principali: il nome dell'utente e quello del dominio, separati dal termine @ (si legge "at", cioè "presso"). Il nome dell'utente può essere di qualsiasi tipo, a patto che non ve ne sia uno uguale, di un altro utente, registrato presso lo stesso dominio; presso grossi provider ciò può diventare un problema, in quanto l'omonimia è molto più facile di quanto si creda, il che spiega l'utilizzo sempre più frequente d'acronimi, sigle e termini inventati.

Il dominio s'identifica generalmente con il nome del provider, cui viene aggiunta una sigla rappresentante il suffisso indicativo di un'organizzazione o di una collocazione geografica (es. ".com" per organizzazioni commerciali, ".it" per indicare il dominio nazionale italiano). Il numero dei singoli domini, nella parte dell'indirizzo loro riservata, dipende dal numero degli intermediari necessari per far recapitare la posta alla propria casella postale.

Non esiste un controllo centralizzato di Internet: gli organismi di sorveglianza delle varie nazioni si limitano ad assegnare (dietro pagamento di una certa tassa [9]) gruppi d'indirizzi agli enti o società che ne facciano richiesta, ed a registrare il loro "domain name", ossia la parte finale dell'indirizzo logico. In Italia tale compito è svolto dall'ente GARR[10], che gestisce anche la rete universitaria (GARR-Net). Per il resto, sono gli organi di gestione delle varie reti pubbliche e private ad esercitare, in maniera più o meno restrittiva, un controllo sull'uso che di esse viene fatto da parte degli utenti.

A livello di connessione, vige la politica di una "interconnessione totale e libera": ogni rete può essere attraversata dal flusso dei dati proveniente da altre reti. Il vantaggio reciproco è quello dell'interconnessione totale: offro il passaggio dei dati ai miei "vicini" e in cambio ho lo stesso servizio, potendo raggiungere anche reti con cui non sono direttamente connesso[11]. In tal modo si realizza la copertura globale a livello planetario. I costi della rete sono dovuti alla sua gestione tecnico-amministrativa, ai calcolatori ed agli altri apparati che ne consentono il

[9] Il pagamento della tassa è un contributo alla gestione tecnica della rete complessiva
[10] Vedi cap.2, par.3.
[11] Il vantaggio per gli hacker, inutile dirlo, è un'estrema libertà d'azione.

funzionamento, ed al noleggio delle linee fisiche di comunicazione attraverso cui passano i dati.

4.2. Servizi, utenti, pubblicità: come si articola l'ambiente.

Definita la rete ed esaminato, a grandi linee, il suo funzionamento, è ora nostro interesse fornire una breve panoramica dei principali servizi che essa offre, analizzando anche dove esiste il rischio hacker e dove, invece, questi pirati sono confusi con altre figure. I servizi che prenderemo in considerazione sono: la posta elettronica, le mailing list, i newsgroup, il sistema di prelievo dei file tramite FTP, i canali chat ed i motori di ricerca.

L'E-Mail è un servizio di messaggeria interpersonale, che permette di comunicare scambiandosi messaggi di diversa tipologia (file testuali, immagini grafiche, database …) tra interlocutori anche molto distanti tra loro. Mittente e destinatario, ovviamente, devono essere entrambi connessi in rete, possedere l'opportuno programma applicativo di E-Mail ed un proprio indirizzo di posta elettronica. I tempi d'invio e di risposta sono alquanto ristretti, praticamente immediati, sia che s'inoltri un messaggio ad un singolo interlocutore, sia simultaneamente ad un gruppo di questi. L'E-Mail utilizza il sistema "store and forward", ovverosia immagazzinamento ed inoltramento, attraversando vari computer prima di raggiungere quello cui è destinato il messaggio[12].

Il nostro indirizzo di posta elettronica è così paragonabile ad una casella postale, collocata nel calcolatore cui richiediamo la possibilità di accedere in rete, lo stesso dove sono memorizzati i messaggi che ci vengono inviati da altri interlocutori. Il server del provider effettua così un compito di segreteria, in attesa che il nostro p.c. inoltri domanda per scaricare i file di posta. Tutte le operazioni d'invio e ricezione vengono effettuate al solo costo della connessione, il che si traduce in un notevole risparmio se confrontato con il costo del telefono.

[12] G. Alessio, ***L'Internet***, SEAM, Roma, 1997.

Il successo dell'E-Mail è altresì rappresentato dal fatto che, anche in Italia, si stanno ormai diffondendo biglietti da visita che riportano il proprio indirizzo di posta elettronica.

Il problema della privacy, connesso alla posta elettronica, ha aperto un forte dibattito in seguito alla violabilità o meno dei messaggi e delle caselle postali, da parte d'estranei non autorizzati. E' qui utile sottolineare che non occorrono particolari capacità per "sbirciare" nella posta altrui, e che sarebbe sbagliato attribuire tale comportamento "in toto" al fenomeno hacker. Certo, un hacker potrebbe leggere la vostra posta elettronica più facilmente di un semplice utente troppo curioso, ma non occorre essere un hacker per farlo, né tale operazione comporta questa qualifica[13].

Il fenomeno dello "spamming", che consiste nell'invadere le caselle postali con messaggi pubblicitari, è oggetto di disputa fra chi considera la pubblicità come un'informazione al consumatore, con pieno diritto di cittadinanza nella posta elettronica, e chi considera la propria casella E-Mail come strettamente personale, quindi inviolabile[14].

Senza addentrarci in questa disputa occorre considerare, a differenza di quanto accade con i volantini nella cassetta delle lettere, che la spesa per scaricare i messaggi pubblicitari dalla propria casella elettronica è a carico del destinatario, il quale vede allungarsi il tempo di connessione al provider nell'attesa che tutta la posta sia scaricata. Per garantire la riservatezza del contenuto dei propri messaggi, invece, esistono dei software per la crittografia a doppia chiave, cioè dei programmi che codificano i messaggi e ne permettono la decodifica solo se si è in possesso della specifica chiave di decrittazione.

La posta elettronica fornisce anche l'opportunità di entrare in contatto con gruppi di vari interessi: è sufficiente inviare un messaggio di "sottoscrizione" ad una mailing list, e si riceveranno automaticamente gli aggiornamenti sugli argomenti trattati e sull'organizzazione della lista. Le mailing list sono spesso gestite da software (listserver) in lingua inglese, i quali modificano l'indirizzario relativo agli utenti del proprio archivio a seconda che si sottoscriva, o si annulli, un abbonamento.

[13] Che abbiamo visto essere relativa a comportamenti ben più pericolosi (vedi cap 3.3).
[14] Al riguardo vedi ***E-Mail, attenzione si, fobia no*** di E. Novari, pubblicato su www.internos.it il 29/1/'99.

Il listserver riceve tutti i messaggi di posta elettronica spediti dal gruppo e li invia a ciascun iscritto, in modo che tutti ricevano una copia del messaggio mediante la spedizione di una sola di queste.

I newsgroup sono forum di discussione basati su messaggi di posta elettronica. I diversi partecipanti inviano messaggi che possono essere letti da ogni frequentatore del gruppo, il quale può scegliere se rispondere privatamente o pubblicamente. Tali gruppi d'incontro permettono un confronto su argomenti d'interesse comune e sono simili ad una bacheca pubblica, dove le persone lasciano e ricevono dei messaggi. Ogni newsgroup possiede molte decine di queste bacheche, ciascuna dedicata ad un determinato argomento. A volte è possibile incontrarvi hacker, ma un vero pirata del ciberspazio, in genere, cerca di passare inosservato, mentre chi sbandiera le proprie imprese in pubblico è più probabilmente un "newbie" del settore a caccia di pubblicità.

Usenet (abbreviazione d' ***User's Network***) è un insieme di newsgroup distribuiti in tutto il mondo, basato su computer chiamati "news server", continuamente sincronizzati onde permettere a tutti di rispondere ai messaggi più recenti. I newsgroup di Usenet sono suddivisi in circa venti classificazioni principali, denominate top-level. Altre categorie top-level di newsgroup sono riferite a realtà nazionali. I newsgroup, in genere, non sono ufficialmente organizzati mediante l'uso di precise regole da seguire. Tuttavia, con gli anni, si è formato un codice di comportamento implicito e ufficioso, fondamentale da conoscere per chi vuole partecipare alla vita del gruppo.

Tale codice, definito netiquette [15] richiede, tra le altre cose, una giusta attenzione verso l'ironia espressa nei messaggi e l'educazione con cui rispondere agli stessi. Infatti, spesso originate da incomprensioni o ambiguità, non è difficile imbattersi in vere e proprie guerre di messaggi, definite "flamewars"[16]. La struttura canonica di una flamewar, a causa delle insicurezze sull'identità altrui che rendono eccessivamente suscettibili, si sviluppa attraverso un "botta e risposta" che si sposta progressivamente dal messaggio all'utente. Inizialmente critiche e insulti riguardano ciò che una persona scrive, i suoi commenti, le sue idee, successivamente

[15] Vedi cap.1.3.
[16] F. Berardi, ***Ciberfilosofia***, op. cit.

l'aggressione verbale colpisce la persona in sé ed i suoi valori. E' ipotizzabile che gli hacker non seguano con molta attenzione la netiquette, tuttavia raramente figurano tra gli imputati all'origine di una flamewars.

Il protocollo FTP (File Transfer Protocol) permette l'accesso a qualsiasi tipo di file, con il successivo trasferimento sul proprio hard disk (questo procedimento viene chiamato download) [17]. Risulta possibile anche l'operazione inversa, ovverosia l'invio di file su macchine remote (upload). Per trasferire i file con FTP è necessario possedere un programma adatto, chiamato FTP Client, installato sul proprio computer e opportunamente configurato. Quando si desidera trasferire un file da un sito remoto, basta collegarsi con il computer che lo ospita per visionare tale file; tuttavia, non essendo possibile ricordare tutte le User ID e le password corrispondenti, molti siti FTP offrono la possibilità di un accesso anonimo, digitando "anonymous" come User ID ed il proprio indirizzo di mail come password.

Gli utenti di Internet possono comunicare tra loro mediante mezzi sincroni e asincroni. Analizzati i principali mezzi asincroni, come la posta elettronica e i newsgroup, occorre soffermarci brevemente su quelli sincroni. Si possono utilizzare dei servizi on-line, siti Web e Telnet dedicati alla comunicazione, anche un apposito client per accedere ad una delle reti che ospita IRC, Internet Relay Chat. IRC è uno standard nato nel 1988 in Finlandia, che permette agli utenti di comunicare tra loro in ***real time*** mediante l'invio di messaggi con la tastiera.

Per partecipare ad una conversazione IRC occorre dotarsi di un qualunque programma client adatto, collegarsi ad Internet ed entrare in una delle svariate reti IRC. Ognuna di queste è formata da una serie di server in continua comunicazione tra loro: la scelta di un server determinerà il collegamento ad una specifica rete.

Uno dei problemi maggiori, per chi naviga in rete, è rappresentato dal riuscire a rintracciare le informazioni desiderate tra le oltre 20 milioni di pagine Web usufruibili su Internet. Tale ricerca è semplificabile grazie ad alcuni strumenti in grado di sondare siti Web, siti Gopher e newsgroup. I due principali strumenti di ricerca sono le directory Web ed i motori di ricerca.

[17] McGraw-Hill, ***Professione Internet***, op. cit.

Le prime sono elenchi organizzati per argomenti, all'interno dei quali è possibile navigare per trovare il sito che interessa. I motori di ricerca sono più efficienti, perché organizzano l'indagine seguendo le personalizzazioni indicate dall'utente. Alcuni motori hanno criteri di ricerca più dettagliati, consentendo di utilizzare gli operatori booleani "and", "or" e "not" per effettuare una ricerca mediante parole chiave. Una delle prime operazioni effettuate dai "newbies", volenterosi d'emulare le "imprese" dei pirati del ciberspazio, è il cercare, mediante tali motori, più informazioni possibili al riguardo[18].

La dimensione del fenomeno Internet è ormai planetaria: si calcola che oggi la "ragnatela telematica" colleghi circa 46.000 reti minori, estese in più di 120 nazioni con più di 90 milioni d'utenti. In Italia, le ultime ricerche non sono ancora riuscite ad effettuare una stima unanime, tanto che la scienza di contare gli utenti della rete produce spesso numeri molto diversi tra loro. Riferiamo qui i risultati d'alcune ricerche che si sono occupate di questo fenomeno[19], nel tentativo di provare a descrivere l'ambiente dove si formano i nostri smanettoni, prima di affrontare il ***mare magnum*** del Web.

La Nua, una società irlandese di consulenza sui nuovi media con sede a New York, stimava la popolazione italiana di navigatori, a gennaio 1998, a c.ca 700.000 utenti. Tuttavia, tale società non spiegava nei particolari la metodologia usata, difetto comune a molti sondaggi in questo settore.

Livraghi ha pubblicato sul suo sito Gandalf le stime di una ricerca condotta dall'Eurisko, secondo la quale, usando una definizione "estesa" d'utente, in Italia navigavano, ad aprile '98, poco più di 800.000 persone, di cui circa il 40% dalla propria abitazione. Tale stima considerava, di questi navigatori totali, circa 200.000 come abituali, con un incremento annuo dell'utenza italiana intorno al 40%. Livraghi concludeva la sua analisi prevedendo che presto, in Italia, vi sarebbero stati un milione d'utenti, che giudicava troppo pochi per raggiungere un livello europeo.

[18] Basta andare su un qualsiasi motore di ricerca (es. Altavista, il cui sito è www.altavista.com), e digitare come parola chiave ***hacker***, per essere letteralmente invasi da un elenco di siti contenenti informazioni al riguardo.
[19] I dati forniti nelle successive ricerche sono stati pubblicati nell'articolo "Internet, quanti sono i navigatori italiani ?", ad opera di M. Mandò, apparso sul sito www.repubblica.it di "La Repubblica", il 28/4/'98.

Ben diverse sono le opinioni di Raimondo Boggia, presidente dell'Osservatorio Alchera[20], il quale sonda continuamente il "mercato" della rete. Gli utenti saltuari (coloro che hanno navigato almeno una volta, individualmente o con altre persone), che nel settembre 1997 risultavano essere c.ca 2.348.000, nella primavera del'98 avrebbero raggiunto i 5milioni. Gli utenti "regolari", invece, stimati in 1.871.000 nell'autunno del'97, nella primavera successiva sarebbero divenuti c.ca 2,5 milioni[21].

Tutti i ricercatori concordano, tuttavia, sul fatto che il vero problema delle rilevazioni è il modo in cui si leggono i dati e la difficoltà nel definire chi è l'utente: se tale deve essere considerato solo il possessore di un indirizzo di posta elettronica, o l'abbonato ad un fornitore di connettività, rischiando di tagliare fuori una fetta consistente d'utilizzatori composta di studenti, familiari, colleghi.

Un'altra ricerca, condotta dall'Explorer Group su un campione di 15 mila individui, rappresentanti la popolazione italiana dai 15 anni in su nel periodo novembre'97-marzo'98, ha stimato che i navigatori italiani fossero 1.845.000, quasi il 4% della popolazione. Secondo l'Explorer, oggi oltre un milione di persone nel nostro paese usa Internet per lavoro. Gli utenti italiani sarebbero giovani adulti tra i 25 e i 44 anni, in prevalenza di sesso maschile, con cultura medio alta, per i quali la rete rappresenterebbe non solo un'opportunità di lavoro, ma anche di studio ed intrattenimento. Colpisce il dato sull'utenza casalinga: essa si aggirerebbe sui 900 mila, tra cui 100 mila sarebbero coloro che usano Internet anche sul lavoro. L'uso prevalentemente per lavoro o per studio (71%) è quasi pari a quello per finalità ludiche (63%), meno attenzione attira la possibilità di fare acquisti (9%).

Secondo i dati appena forniti, Internet si può considerare come il fenomeno comunicativo di fine millennio, e naturalmente tale aspetto non poteva sfuggire al mondo economico; dal 1991, quando le aziende in USA hanno visto aprirsi le porte della rete per fini commerciali, la presenza della pubblicità è andata aumentando fino alle ultime stime, che giudicano un terzo dei navigatori essere utenti "profit". Tale utenza commerciale, se da un lato ha consentito di espandere e migliorare i servizi, dall'altro è fonte di diverse conseguenze: lo spamming, la creazione di siti dedicati ad

[20] Vedi il sito www.alchera.it.
[21] Questi ultimi dati sono stati forniti dal settimanale Computer Valley, anno 2°, n.44, del 17/9/'98.

un particolare argomento dove, per cercare le poche informazioni utili, le si deve filtrare attraverso pagine e pagine di pubblicità, il problema dei costi, i cookies, le attenzioni “interessate” da parte degli hacker, che spesso individuano nelle maggiori aziende e società i “mulini a vento” contro i quali portare avanti le proprie battaglie.

Attualmente la maggioranza delle informazioni presenti su Internet è gratuita, e permette a molti utenti delle vere e proprie passeggiate esplorative anche in settori diversi dalla loro professione. Il timore dei “vecchi” utenti della rete è che, un’eccessiva diffusione di servizi a pagamento, non solo ne stravolga lo spirito anarchico, ma la trasformi in qualcosa di simile a Compuserve o Dialog, sistemi presso i quali un utente si collega solo quando ha bisogno di specifiche news, e che abbandona appena trovata l’informazione desiderata per non incorrere in costi aggiuntivi. Fintanto che i singoli utenti resteranno in grado di comunicare condividendo informazioni ed idee, la comunità della rete non dovrebbe temere nessuno stravolgimento culturale.

Il termine “cookie”, se tradotto alla lettera, ha il significato di biscotto, di dolcetto; tuttavia, riportato alla realtà della rete, assume una fisionomia molto poco dolce. Esso identifica un’informazione inviata da un server ad un qualsiasi navigatore a lui collegato, che viene memorizzata nel computer ricevente per essere poi restituita alla successiva connessione. Una sorta di strumento per scambiare informazioni tra due punti collegati in rete. I cookies vennero introdotti alla fine del 1995, in occasione dell’uscita del browser Netscape 2, con lo scopo di non interrompere il contatto d’informazioni tra browser e server fra una sessione e l’altra. In pratica servono al gestore del servizio per ottenere informazioni sugli utenti che visitano il proprio sito.

Proprio questa è l’importanza e la pericolosità di tale strumento, che consente di registrare vari tipi di dati relativi al navigatore, ed utilizzarla nei collegamenti successivi. Grazie a questa tecnologia, il provider può disegnare una particolareggiata mappa contenente le scelte effettuate nel corso della nostra navigazione, rilevando i siti più frequentati. Se manipolati per registrare indebitamente informazioni personali sui visitatori, i cookies innescano un processo che va ad interessare la nostra privacy, dando adito ad interpretazioni controverse.

Inoltre, i cookies non sono identificabili da parte dell'utente, a meno che questi non possieda uno speciale programma che funge da filtro.

Come evidenziato nel terzo capitolo, le aziende restano l'obiettivo preferito da parte d'intrusioni hacker. Se alcuni di questi sembrano così vendicarsi della "mutazione" genetico-economica subita dalla rete, altri violano data-base aziendali per motivi tra i più disparati: curiosità, eccesso di protagonismo, ricerca di password e codici d'accesso per scaricare sull'azienda in questione il costo della connessione, tentativi d'accesso abusivo per avvertire poi l'azienda stessa sull'inefficacia delle proprie difese informatiche (sperando d'essere assunti in prima persona per migliorarle).

4.3. Quando gli hacker non c'entrano: altri problemi della rete.

Per gli utenti inesperti, così come per i suoi denigratori, la crescita caotica della rete e l'impossibilità di trovarvi disposte in modo ordinato le informazioni cercate sarebbero caratteristiche deprecabili; tali caratteristiche, sommate all'imposizione di una nuova modalità di comunicazione apparentemente più distaccata e meno naturale, portano alcuni soggetti citati a negare l'utilità di questo nuovo mezzo.

Scambiare il disagio personale di fronte ad un luogo nuovo – nel quale occorre del tempo per orientarsi – per una qualità negativa del luogo stesso è un errore cognitivo diffuso. In un'epoca in cui l'innovazione tecnica concorre in larga misura a mutare ininterrottamente gli orizzonti delle attività umane, tale visione potrebbe essere registrata come il sintomo di una sana opposizione inconsapevole allo status d'individui eterodiretti[22]. Inoltre, l'opposizione nei confronti di Internet è anche una forma estensiva della diffidenza verso i computer, come concorrenti della forza lavoro umana, causa prima dell'accelerazione subita dall'attività lavorativa,

[22] Per un approfondimento del concetto d'etero-direzione vedi D. Riesman, ***La folla solitaria***, Il mulino, Bologna, 1956.

forma di “conoscenza d’élite” mediante la quale si accede ad un mondo privo di regole e popolato di gente poco raccomandabile[23].

Per l’ambivalenza che la contraddistingue – Internet esibisce le caratteristiche di un sistema autopoietico, cresciuto in seno ad una società totalmente amministrata – la rete è la punta avanzata delle sperimentazioni nel campo delle tecnologie dell’informazione, ed insieme un’entità che sfugge, per ora, al controllo di chi vorrebbe imporle regole d’uso. La possibilità di navigare nella rete è ritenuta un segno di progresso, tanto più evidente se si tiene conto che solo il 3% della popolazione mondiale dispone della possibilità d’accedervi[24].

La rete veicola una massa molto eterogenea di contenuti applicando dei valori discutibili come la velocità, la quantità, l’autoreferenzialità, l’omologazione, l’opulenza e la potenza, caratteristiche che nei precedenti capitoli abbiamo visto non appartenere ***in toto*** all’etica hacker.

Viceversa, su Internet non sembrano figurare la semplicità, la facilità d’uso, l’approfondimento delle fonti e dei contenuti (queste ultime due carenze fanno mancare il fattore più importante dell’informazione, quello qualitativo). Chi passa parte del suo tempo a pensare ed a scrivere, se potesse raddoppiare la velocità del suo p.c. non riuscirebbe a pensare, a scrivere, a comunicare più velocemente attraverso la rete[25]. Ciò a sottolineare che nello sviluppo della rete si esaltano spesso le novità più futili, ma in grado di colpire maggiormente la fantasia dell’utente.

Mancando piani di sviluppo in ordine alla natura e all’organizzazione dei contenuti, e potendo chiunque mettervi le informazioni che preferisce, il carattere enciclopedico di Internet oscilla tra il caos e l’ordine toccando tutti i gradi intermedi. Così, accanto a progetti organici di raccolta e diffusione del sapere, si effettuano

[23] Alla formazione di questa tecno-fobia, più spesso una vera e propria Internet-fobia, contribuiscono non poco gli altri media, la televisione in primis. A volte sembra in corso una vera e propria “guerra alla rete”, della quale sottolineare gli aspetti più negativi ed appariscenti. Una delle conseguenze di tale fenomeno è l’utilizzo improprio del termine ***hacker***, accostato dalla televisione a qualsiasi criminale informatico (dal trafficante d’organi al distributore di materiale sulla pedofilia, categorie estranee al fenomeno hacker come descritto in questo lavoro).
[24] L. De Carli, ***Internet. Memoria e oblio***, Bollati Boringhieri, Torino, 1997. Tale fenomeno rende la rete partecipe della teoria dei ***Knowledge-gap*** (scarti di conoscenza), descritta nel cap.1, nota n.16.
[25] C. Stoll, ***Miracoli virtuali***, Garzanti, Milano, 1996.

spontanee immissioni d'informazioni realizzate al solo scopo di appagare l'aspirazione ad avere un posto nel ciberspazio.

Tuttavia, la gran quantità di dati isolati fornita dalla rete manca di un vero e proprio significato, che Internet non riesce ad esprimere. Non basta fornire dei dati se questi mancano di un contesto d'applicazione, d'interrelazioni tra loro, e l'utente non conosce le esperienze che li hanno generati. Contesto, interrelazione, esperienza, sono delle "costruzioni sociali", dei "frame" di riferimento attraverso i quali solo gli esseri umani riescono ad insegnare le connessioni esistenti tra singole unità d'informazione.

Nonostante questo, vi è chi ha cominciato ad investire grosse somme per l'acquisto d'archivi d'immagini, col proposito di tradurle in formato digitale e disporne per la diffusione in rete. Simili operazioni sono state progettate per dischi e libri, con la conseguenza che il digitale sarà presto una forma d'essere della quale non si potrà fare a meno, pena il rischio di restare ai margini del rapido e profondo mutamento in atto[26]. Archivi e biblioteche potrebbero essere destinati all'oblio se non saranno trasferiti su un supporto magnetico, convertendo la loro natura analogica in digitale. In seguito a tale analisi sorge spontaneamente il dubbio su chi sceglierà - secondo quali criteri - cosa tramutare in digitale, e chi avrà il compito di rendere possibile l'accesso a tali nuovi archivi informatici.

L'immediatezza della rete è la conseguenza di una mediazione politica, da cui si evince che non diventerà digitale tutto indiscriminatamente, bensì ciò che sarà determinato da quei rapporti di forza, molto poco virtuali, che influenzano il nuovo ordine mondiale. Se l'ingresso nella rete sarà determinato dal profitto, e prevarrà il desiderio di poter fare a meno di tutte quelle colture che la storia dell'Occidente ha vessato, relegandole ad espressioni primitive, si avrà il momento propizio per "cancellare archivi, cancellare colture, fare roghi di libri senza nemmeno toccarli, inventarsi una tradizione[27]".

Scalpore e curiosità ha provocato, di conseguenza, il "Progetto Gutenberg" del professore di "testo elettronico" Dott. M.Hart dell'Illinois Benedictine College: la

[26] Vedi nota n.24.
[27] L. De Carli, ***Internet, memoria e oblio***, pag. 124, op. cit.

creazione di una grandissima biblioteca on-line che nel 2001 avrà scannerizzato 10mila libri, scaricabili dalla rete[28]. Negli anni dal '71 al '93 sono stati scannerizzati c.ca 200 libri, ma le tecnologie permettono oggi una velocità di riproduzione molto superiore. I fautori ad oltranza del Web, se sollecitati sul problema della responsabilità della scelta di un testo invece che di un altro, rispondono che tale problema non si pone in quanto un giorno saranno disponibili in rete tutte le pubblicazioni. Molti autori, tuttavia, esprimono seri dubbi su tale epilogo.

Clifford Stoll[29] manifesta le sue perplessità sulla possibilità che il "Progetto Gutenberg" fornisca testi veramente completi in ogni loro singola informazione, ed individua il maggiore ostacolo nel fatto che le persone che scrivono libri vogliono giustamente essere pagate per il loro lavoro, e ciò è difeso dal diritto d'autore. Il copyright[30], sostiene Stoll, non è un problema, come alcuni teorici del Web (e l'etica hacker) lo considerano, ma la soluzione di un'altra questione di primaria importanza, in pratica il giusto difendere gli sforzi e le spese di chi crea un'opera.

Se gli archivi e le biblioteche digitali decidessero di non far pagare per i libri elettronici, rischierebbero di mettere fuori mercato gli editori in un regime di libera concorrenza; viceversa si priverebbe la gente di molta informazione che oggi può essere ottenuta gratuitamente. Quello appena descritto è solo uno dei paradossi creati dalle possibilità offerte dalla rete.

Il problema dell "information overload", cioè del sovraccarico informativo che coglie l'utente che si rivolge ad Internet alla ricerca di qualcosa, è all'origine di un altro dibattito. Naturalmente, i teorici della rete mettono in risalto la possibilità che su Internet si possa trovare di tutto, fedeli al detto "Ask, the Net knows"[31]. Tuttavia, pochi evidenziano che la nostra capacità di recepire ed assorbire la conoscenza non

[28] Nel magazzino elettronico del "Progetto Gutenberg" i file usano lo standard Ascii, leggibile da praticamente tutti i p.c. sul mercato. L'idea di tale progetto è stata imitata in tutto il mondo, dal progetto "Athena" (opere svizzero-francesi) al "Runenberg" (paesi scandinavi), dai "Artfl" e "Abu" (opere francesi) all'italiano "Progetto Manuzio". Per gli interessati si vedano i siti www.gutenberg.net e www.liberliber.it. (da S. Minardi, ***La biblioteca globale che vive sulla rete***, pubblicato a pag.14 di "Computer, Internet e altro", allegato a "La Repubblica" in data 21/1/1999).
[29] C. Stoll, ***Miracoli Virtuali***, op. cit.
[30] Vedi cap.3, par.4.
[31] Il detto si riferisce al fatto che se non si capisce qualcosa, o non si riesce a trovare un'informazione, si può lanciare una richiesta d'aiuto in posta elettronica. Si troverà sicuramente qualcuno che sa dove e come trovare quel che serve, o nel peggiore dei casi può suggerire a chi inoltrare quella domanda (G. L. Giorda, ***Inviati nel cyberspazio***, Asca, Milano, 1996).

è infinita, di conseguenza le nostre attenzioni sono fortemente selettive. In tutto questo s'inserisce il rischio, molto elevato su Internet, della ridondanza, che alla lunga porta alla noia percettiva.

T. Maldonado[32] giudica gli umani poco capaci di sopportare la sovrabbondanza d'informazioni, e ritiene che la consapevolezza di questa incapacità ci abbia fatto munire di una protesi intellettuale: il computer. Destinato a depersonalizzare le funzioni di ricezione, elaborazione ed immagazzinamento dell'informazione, oggi il computer fornisce la possibilità di ripersonalizzare tali funzioni, riportandoci al punto di partenza.

Di fronte alla possibilità, almeno teorica, di raggiungere tutte le fonti d'informazione si preferisce minimizzare alcune conseguenze poco piacevoli, come il rischio di essere investiti da una valanga d'informazioni non richieste, e l'impossibilità di scindere quelle di cui si ha bisogno dalle altre.

Nicholas Negroponte - il profeta di "Essere digitali"[33] e riconosciuto "guru" del MIT, il fantascientifico Massachussets Institute of Technology - sembra risolvere il problema dell'informaton overload con un paradosso: per mettere ordine nel caos d'informazioni basterà aggiungere altri dati più specifici, inerenti all'informazione da riordinare. L'informazione "sull'informazione" acquisterà così maggior importanza dell'informazione originaria, permettendo di risparmiare il tempo di dispendiose analisi, ricerche e selezioni[34]. Al quesito su chi, e secondo quali criteri, analizzerà ed organizzerà l'informazione, Negroponte risponde con la figura degli "agenti intelligenti", divenuti ormai un simbolo delle nuove tecnologie.

Tali agenti saranno dei software dotati di una loro personalità, in grado di riconoscere espressioni tipicamente umane, programmati per conoscere il loro utente, le sue necessità, i suoi messaggi verbali e non. Le interfacce di tali programmi saranno così ben fatte da non essere neppure notate. I "maggiordomi digitali" saranno numerosi, risiederanno sia nella rete sia presso di noi,

[32] T. Maldonado, ***Critica della ragione informatica***, Feltrinelli, Milano, 1997
[33] N. Negroponte, ***Essere digitali***, op. cit.
[34] N. Postman, nell'opera "Technopoly" (Bollati Boringhieri, Torino, 1993) ha messo in guardia sul rischio di un circolo vizioso: più tecnologia, più informazioni, più controllo sulle informazioni, più tecnologia per migliorare tale controllo (l'epilogo si raggiunge quando la scorta d'informazioni non è più controllabile).Negroponte, tuttavia, sembra ignorare tale rischio.

risponderanno al telefono, raccoglieranno le news, gestiranno la posta elettronica, il tutto dopo essersi fatti un modello di ognuno di noi.

C. Stoll giudica gli "agenti intelligenti" come una fantasia germogliata nella "terra di domani" del MIT, abbastanza credibile da generare cospicui finanziamenti per ricercatori di gran nome. Tuttavia, secondo tale autore, la gente non ha bisogno di programmi che le dicano cosa le piace, bastano amici, recensioni ed un'occhiata di persona; inoltre gli individui sono complessi e non esiste nessuno i cui gusti siano così semplici da essere predetti da un programma[35].

P. Breton appare molto scettico verso tale eventualità, accusa Negroponte di rifarsi un po' troppo ad Asimov, e pone l'accento sui rischi di un individualismo profondo ed inquietante. L'uomo, così informato, vivrebbe sempre più nel "suo mondo", separato sistematicamente dagli altri individui, coltivando il germe di una nuova xenofobia, simile ad una corrente riemersa dagli abissi dell'orrore[36].

S. Turkle - insegnante di sociologia della scienza al MIT, quindi collega di Negroponte - affronta la questione con il tipico punto di vista del ricercatore scientifico. Secondo l'autrice dell'opera "La vita sullo schermo", dalla domanda "Come riporre fiducia in un programma per gestire questioni così importanti?", si è passati a chiedersi "Chi, se non un programma, potrà mai avere il tempo, la conoscenza e l'esperienza per fare tale lavoro?". La gente – conclude la Turkle – è ancora preoccupata dal fatto che un simile agente possa arrivare a sapere troppo, ma ora guarda alla tecnologia perché progetti sistemi veramente sicuri[37].

Il fenomeno "agenti intelligenti", inoltre, ponendosi lungo il processo che tende ad inserire sempre più software e microchip all'interno della nostra vita quotidiana, origina due ordini di dipendenza problematica: quella dai "buoni esperti" del settore[38] (es. tecnici di riparazione) e quella dai "cattivi esperti" (es. gli hacker). Questi ultimi,

[35] C. Stoll, ***Miracoli virtuali***, op. cit.
[36] P. Breton, ***L'utopia della comunicazione***, UTET, Roma, 1995.
[37] S. Turkle, ***La vita sullo schermo***, Apogeo, Milano, 1997.
[38] Sull'origine di tale dipendenza vedi: gli scritti sulla specializzazione dei saperi, e sulla settorialità delle conoscenze, cui porta la moderna divisione del lavoro (opere di Durkheim, Tonnies, Comte e Spencer), e la teoria di M. De Fleur, nota come T***eoria della dipendenza dal sistema dei media***, nello specifico del controllo di tale sistema sulle risorse funzionali ad obiettivi di tipo cognitivo.

se a parole combattono l'aumento di tale dipendenza[39], in realtà vedono così aumentare un possibile raggio del proprio campo d'azione, sia pratica sia psicologica.

4.4. Internet incontra il sesso: pornografia, pedofilia, sesso virtuale e cambiamenti di genere in rete.

Il rapporto d'ogni utente con la rete genera degli spazi, ora più tecnici ora più psicologici, all'interno dei quali le proprie difese sembrano venire meno. Tali spazi pongono il soggetto davanti a dei "rischi interattivi", dove il pericolo deriva dal contatto tra il proprio sé e le asperità di un universo eterogeneo e sconosciuto. Quando tale rapporto si sovrappone ad una sfera ad alta tensione emotiva come quella sessuale, ecco riapparire i nostri incubi sotto forma di "nudità telematiche", nel doppio significato di sentirsi nudi, indifesi di fronte ai pericoli della rete (es. gli hacker), e di dover decidere come gestire il proprio rapporto con il nudo sul Web, in tutte le forme in cui questo si presenta.

La criminalità informatica, intesa nel senso più ampio di "pratica d'operazioni illegali in rete" tanto caro agli altri media, non è estranea a questo campo; tuttavia, onde evitare confusione di ruoli, occorre effettuare delle precisazioni in merito, cercando d'individuare responsabilità e di fornire qualche esempio.

Intervenendo al convegno "Diritto alla comunicazione nello scenario di fine millennio"[40], la sysop della rete Cybersex BBS di Bologna, Helèna Velena, sottolineava un impegno da parte della stampa nostrana a far credere che Internet fosse invasa da pornografi e pornografia. In realtà - continuava la stessa organizzatrice della BBS emiliana - solo lo 0.2 % di quello che passa in Internet riguarda sesso e pornografia, mentre decine sono le iniziative giuridiche e politiche per censurare la rete con questa scusa. Quest'intervento, nonostante siano passati

[39] Vedi l'intervista a S. Wernèry, cap.2.2.
[40] Convegno avvenuto a Prato nel febbraio del 1995, i cui atti sono raccolti nel testo "Nubi all'orizzonte", di Strano Network, Castelvecchi, Roma, 1996.

quasi quattro anni e sia stato effettuato da una "parte in causa", sembra molto attuale in seguito ad alcuni recenti avvenimenti[41].

H. Rheingold giudica il sesso come la prima cosa, verso cui si concentra il pensiero della gente, quando nasce un nuovo strumento di comunicazione; solo più tardi ci si accorge delle altre possibilità che tale strumento fornisce[42].

Il "Communications Decency Act", la legge americana del febbraio '96 che aveva proibito la circolazione di materiale osceno su Internet mediante censura e controllo dei contenuti, è stata dichiarata anticostituzionale dalla Corte federale di Philadelphia nel giugno dello stesso anno, con una sentenza che ha sancito l'assoluta prevalenza della libertà d'espressione in rete[43]. Quale significato attribuire a tale sentenza?

In realtà, senza voler approfondire questioni storiche e morali relative a pornografia e pedofilia, si ha da più parti la sensazione che la rete sia usata come capro espiatorio, e che dietro molte campagne di stampa serpeggi una citata e strisciante Internet-fobia. Dati più recenti[44] descrivono il Web come meno "pericoloso" di una qualsiasi edicola, dove basta alzare gli occhi per essere sommersi da copertine di riviste e videocassette hard situate in bella mostra, più semplici da individuare e sbirciare di molti siti telematici; ciononostante, raramente si discutono proposte per chiudere le edicole o vietare l'affissione d'alcuni cartelloni al limite della decenza (e spesso oltre).

Nello scorso agosto, il Parlamento si è invece dimostrato molto solerte nell'approvare, senza la dovuta discussione, una legge nella quale il mezzo telematico è (tristemente) citato con molto riguardo.

---

[41] Vedi "Operation Cathedral", cap.3, par.2.
[42] H. Rheingold, ***Comunità virtuali***, Sperling&Kupfer, Cuneo, 1994.
[43] G. Alessio, ***L'Internet***, op. cit. E' da ricordare che l'iniziale approvazione di tale legge provocò la famosa campagna del nastro azzurro, in difesa del "free speech". Inoltre, un discusso intervento del presidente Clinton ha reso necessario l'esame del caso da parte della Corte suprema degli Stati Uniti, la quale ad un anno di distanza ha sostanzialmente confermato la prima sentenza.
[44] Sia G. Livraghi, i cui articoli sono rintracciabili presso i siti www.gandalf.it e www.interlex.com, che C. Gerino (vedi Computer Valley n.44, settembre '98), ritengono che il totale del materiale relativo a pornografia, pedofilia ed argomenti a sfondo sessuale (compresi articoli che ne parlano, libri, settimanali…) non superi il 12% del traffico totale della rete.

Considerata una legge d'emergenza ed approvata all'unanimità, nella n.269 del 3/8/'98, intitolata "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù", si può leggere all'art.3 che "Chiunque distribuisce, divulga o pubblicizza***, anche per via telematica***, materiale pornografico…o notizie finalizzate all'adescamento o allo sfruttamento sessuale di minori di anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da cinque a cento milioni" (corsivo nostro).

Si converrà che la forma usata suona particolarmente infelice, a tratti quasi demonizzante. In realtà, i casi di molestia sessuale a minori scoperti su Internet si contano a poche decine addirittura in un paese, come gli Stati Uniti, dove la comunità on-line è ormai composta da 60-70 milioni di persone. Inoltre, dati statistici sull'identità dei responsabili di violenze sessuali contro i minori, rivelano che solo nel 2% dei casi sono chiamate in causa figure estranee alla famiglia ed al riferimento sociale della vittima[45].

Lo scambio attraverso Internet di videotape, foto e filmati pedofili non è così agevole come i media si sono affrettati a descriverlo. Sarebbe molto più facile, avendo i contatti giusti, acquistare questo materiale per posta, mentre la rete si è già dimostrata uno dei modi più semplici per individuare i trafficanti ed i loro clienti, se hanno l'imprudenza di usare un sistema di comunicazione così verificabile e trasparente. La L.269/'98 ha reso tale traffico ancora più difficile, permettendo alla polizia d'installare dei "siti trappola" e di procedere ad intercettazioni telefoniche quando ritenuto opportuno.

Altra caratteristica di tale legge è rappresentata dall'obbligo, per gli Internet provider, di svolgere una funzione di controllo e di censura sui contenuti da loro veicolati, pena la chiusura ed il sequestro dei server. Tale obbligo è stato paragonato, in un convegno sull'argomento[46], ad una situazione di responsabilità penale, per le Poste italiane, di fronte ai pacchi bomba inviati dagli squatter ai

[45] Vedi il sito www.pacse.censis.it., sviluppato dalla fondazione Censis, con il contributo dei Ministeri degli Interni e di Grazia e Giustizia.
[46] Il convegno è stato organizzato a Roma, dai radicali, negli ultimi giorni dell'ottobre '98, e l'articolo di riferimento è "Pedofilia & Internet, una caccia alle streghe" d'Annalisa Usai, pubblicato sul sito www.repubblica.it/Internet il 27/10/'97.

magistrati di Torino. Tale paragone aveva lo scopo di dimostrare l'impossibilità, da parte dei provider, di svolgere la funzione loro assegnata.

Oggi Internet è un mezzo in grado di veicolare diversi contenuti, ed inevitabilmente alcuni di essi possono rappresentare un rischio; tuttavia, spesso il problema maggiore è dato dall'ignoranza, dalla superficialità, dalla carenza di comunicazione, dal non voler affrontare certe problematiche.

La sociologa S. Turkle, all'interno del già citato "La vita sullo schermo"[47], affronta tale questione assieme a tutte quelle legate al non semplice rapporto tra il sesso e la rete. Tale autrice afferma con sicurezza che la rete, come ogni ambiente dove gli adolescenti tendono a radunarsi, rappresenti un luogo dove possono subire molestie o abusi psicologici, reciproci o causati da adulti. Tuttavia, ella ritiene che il panico dei genitori sui pericoli del ciberspazio sia troppo spesso legato alla loro scarsa familiarità con esso. Molte delle paure nutrite per i propri figli, prosegue la Turkle, trovano spazio nelle cose sconosciute che si sente di non poter controllare: ai nostri giorni è Internet il grande sconosciuto[48].

Non è necessario che i genitori divengano dei tecnici esperti, ma dovrebbero imparare abbastanza sui network informatici, in modo da poter discutere con i propri figli su chi e che cosa si trova "là fuori", e da organizzare una serie di regole di sicurezza fondamentali[49]. Quando si legge di un adolescente che ha subito violenza da un adulto conosciuto sulla rete, sono proprio queste regole basilari che sembrano essere venute a mancare. I bambini che reagiscono meglio ad una cattiva esperienza su Internet sono quelli che hanno la possibilità di parlarne con i genitori.

Inoltre, anche se la Turkle non vi accenna apertamente, mi preme aggiungere che sarebbe bello che Internet – ma anche il computer in generale – non fosse un posto dove "parcheggiare" i propri figli per tenerli occupati. In alternativa, prima di tale eventualità (comunque non un'abitudine), sarebbe utile che si fosse trascorso

[47] Vedi nota n° 37.
[48] Quello che G. Livraghi descrive, nell'articolo ***Alice nel paese delle ipocrisie*** come "Questa cosa un po' misteriosa, che pochi conoscono e capiscono, popolata d'androidi, di mostri, di tecnomani assatanati che praticano il ***sesso virtuale***…". Vedi il sito www.gandalf.it
[49] Tali regole figurano come conseguenza del passaggio da una socializzazione di tipo verticale, legata ad agenzie formali, ad una di tipo orizzontale, più prossima ad agenzie informali. Per una chiara ed esauriente dinamica di tale processo vedi M. Morcellini, ***Passaggio al futuro***, F. Angeli, Milano, 1992.

del tempo insieme davanti a quello schermo per giocare, spiegare e condividere certe esperienze, in maniera che l'adolescente non rischi di doverle fare interamente da solo.

La rete può divenire uno strumento subdolo, e l'estrema libertà di comunicazione che essa incarna può rivelarsi uno stimolo per degli usi distorti della stessa. Si pensi a quei due studenti della Bocconi che per mesi hanno adoperato la rete per lanciare infamanti messaggi porno su una ragazza di 26 anni, "rea" di aver interrotto una relazione con uno di loro. In questo caso, il crimine informatico è uscito dalla dimensione "ottusa" di titolo di reato "contro l'inviolabilità del domicilio e dei segreti", ed ha compreso anche quello contro la persona e la sua libertà[50].

Occorre sottolineare, ancora una volta, come l'atto appena descritto debba essere considerato giustamente criminale, ma eluda totalmente categorizzazioni in stile hacker o simili. Si tratti di traffico d'immagini di minori, uso del mezzo telematico per violare la libertà della persona, o principio d'adescamento di giovani tramite il computer, non basta l'uso di tale mezzo per avvicinare tali pratiche a quelle dei pirati del ciberspazio, totalmente estranei a tali comportamenti.

Il sesso virtuale[51], vissuto in rete, consiste in due o più partecipanti che s'inviano descrizioni di atti fisici, affermazioni verbali e reazioni emotive, relative alla propria identità (che, come sappiamo, nel cyberspace vede l'unico limite nella fantasia dell'utente). In rete, non solo tale attività appare normale, ma per molte persone costituisce l'epicentro dell'intera esperienza on-line.

Su Internet si hanno rapporti sessuali con soggetti che possono essere o meno del proprio sesso, possono fingere di essere del sesso opposto, possono addirittura descriversi come personaggi non umani (animali, figure fantastiche, oggetti). Risulta molto semplice avere delle avventure virtuali, anche se possono condurre a significative complicazioni, in quanto persone e coppie diverse le affrontano in modi anche molto differenti tra loro.

[50] Fonte: ***"Tentata violenza via Internet", due denunce per stupro virtuale*** di C. Fusani, pubblicato su ***La Repubblica*** in data 19/7/'98.
[51] "…nessuno ha mai capito cosa sia, ma proprio perché non esiste è facile parlarne a vanvera e colorirlo come si vuole". Vedi l'articolo citato nella nota n.48.

Infatti, il sesso virtuale pone la questione di quello che si ritiene essere il centro del sesso e della fedeltà. Si tratta dell'atto fisico? Del sentimento d'intimità emotiva con una figura diversa dal partner ufficiale? Dove risiede l'infedeltà, nella mente o nel corpo? Molta gente, coinvolta nel netsex, dice di rimanere continuamente sorpresa dal grado di coinvolgimento fisico ed emotivo raggiunto. Ciò dimostra la validità della tesi secondo cui il 90% dell'attività sessuale avviene nella nostra mente. Non si tratta di un'idea nuova, ma il netsex l'ha resa più comune.

Sempre secondo la Turkle, il sesso on-line e il cambio di sesso virtuale fanno parte della storia più ampia di quanti utilizzano gli spazi virtuali per costruire la propria identità reale, non solo quella in rete. Ciò risulterebbe sempre più evidente per bambini e adolescenti, man mano che raggiungono l'età per partecipare al mondo della cultura on-line. La vita sessuale su Internet degli adolescenti, come ci viene descritta dalla sociologa americana, sembrerebbe sottoposta ad una minore tensione che nella vita reale, in quanto la possibilità di "scollegarsi" è sempre a portata di mano.

4.5. Privacy, sicurezza, commercio elettronico e vulnerabilità fisica: come difendersi da hacker e scoiattoli.

La comunicazione mediante reti telematiche presenta dei rischi, in parte dovuti alla giovane età del mezzo utilizzato, in parte a delle caratteristiche intrinseche al mezzo stesso. Contemporaneamente, le reti si presentano come depositarie di un numero sempre maggiore d'informazioni, alcune delle quali vanno assumendo un carattere fortemente privato. Alla luce di quanto descritto, appare inderogabile un esame di queste zone d'ombra, onde esaminare la gravità effettiva di tali rischi, e verificare il "contributo" degli hacker, quando presente.

Le incognite maggiori, per un utente di Internet, sembrano riguardare - da quanto analizzato nei capitoli precedenti - la difesa della propria privacy, intesa come protezione d'informazioni riservate, ed una serie di rischi legati alla sicurezza della rete, come la difesa dagli accessi e dalle interruzioni di servizio non autorizzate.

Il diritto alla privacy è uno dei temi più importanti del ciberspazio, in quanto pochi media, al pari della rete, sono così suscettibili di controlli ed intrusioni nella sfera personale dei soggetti che li adoperano. L'identità stessa dei soggetti, non solo la loro indipendenza, viene minacciata da tali rischi. La privacy, infatti, non è solo un meccanismo che permette alle persone di regolare in modo flessibile l'accesso al sé, ma anche uno strumento importante per definirne i limiti e le frontiere. Quando la permeabilità di queste frontiere è ben controllata, si sviluppa una percezione sicura della propria individualità.

L'invasività degli spazi elettronici di comunicazione mette in crisi il senso di controllo dell'attore sulla sua interazione con l'ambiente, da cui si evince che i nuovi mezzi di comunicazione non sembrano particolarmente idonei a consentire agli attori una definizione, ed un controllo, delle frontiere fra gli altri ed il sé[52]. L'attuale filosofia di sviluppo di tali mezzi, che esalta l'obiettivo di guadagnare un accesso più ampio possibile ad informazioni potenzialmente rilevanti, ha comportato per ora un sacrificio in termini di privacy.

Tuttavia, vi è una tesi[53] secondo la quale i computer, che sembrano essere la causa dell'enorme espansione della raccolta di dati personali alla fine del ventesimo secolo, in realtà non lo sono. La raccolta dei dati sarebbe uno dei numerosi processi in atto già da tempo, che le tecnologie dell'informazione avrebbero reso più efficiente, più diffuso ma meno visibile (quindi più pericoloso).

A riprova di ciò, alcuni autori[54] riportano una vicenda reale avvenuta negli USA, dove un'azienda produttrice di gelati vendette il data-base con le identità dei suoi acquirenti più giovani all'esercito, che lo usò anni più tardi per inviare le chiamate di leva. L'accordo fu scoperto quando un giovane consumatore di gelati, che si era divertito ad inventare delle identità diverse dalla sua, grazie alle quali aveva ricevuto dei gelati in omaggio, si vide recapitare anni più tardi le singole chiamate alle armi di tutte le persone che si era inventato, residenti presso il suo domicilio.

[52] Per approfondire la tematica del controllo delle frontiere fra gli altri ed il sé vedi, tra gli altri, G. H. Mead (***Mind, self, society***, 1934), E. Goffman (***La vita quotidiana come rappresentazione***, 1959, trad. italiana del 1969), e P. L. Berger e T. Luckmann (***La realtà come costruzione sociale***, 1966, trad. italiana del 1969).
[53] Vedi D. Lyon, ***L'occhio elettronico***, op. cit.
[54] Vedi Stoll (1996, op. cit.) e Lyon (1997, op. cit.).

La tesi sulla raccolta dei dati come processo in atto già da tempo non deve essere confusa con quella che, riferendosi alla situazione attuale di Internet, cita il problema della privacy e del trattamento dei dati come un fastidio inevitabile, e comunque sicuramente temporaneo. Le tematiche analizzate nei capitoli precedenti hanno sottolineato che, ogni volta che si prende parte ad una transazione commerciale (ma su Internet basta molto meno), è probabile che l'informazione sia registrata e venduta ad altri senza che il soggetto lo sappia, e per scopi che non si sarebbe mai aspettato.

S. Sansavini, redattore di una BBS di Firenze, nel citato "Nubi all'orizzonte" di Strano Network, si dichiara convinto che sia impossibile garantire il rispetto della privacy sulla comunicazione e sulla circuitazione d'informazioni, tanto da giungere ad una dicotomizzazione tra violazioni "legali" ed "illegali" della stessa[55]. Tale posizione, che giudica ipocrita anche il solo riferimento al rispetto della privacy, ci appare disfattista e poco costruttiva.

L'attuale sistema telematico presenta la possibilità di ricostruire le parole, le scelte, i gusti, le spese del singolo utente, e gli hacker non sono estranei a continue violazioni di banche-dati e transazioni, unite a tentativi d'entrare in possesso di password e codici d'accesso; tuttavia, se sotto alcuni aspetti tali possibilità restano tali, sotto altri esistono strumenti in grado di elevare la nostra soglia di sicurezza e relativa tranquillità.

Il nostro vivere si muove continuamente tra apertura ed isolamento, tra comunità e privato; gli stessi processi che potrebbero sembrare vincolanti (es. risalire al proprietario di un numero di previdenza sociale dal numero stesso inserito in una banca dati), sono quelli che ci permettono di partecipare alla vita della società (es. il numero in questione ci garantisce il sussidio di disoccupazione).

Secondo C. Stoll [56], i diversi sistemi di computer mantengono profonde incompatibilità tra loro, e sfruttarli per dei confronti incrociati richiederebbe

[55] La violazione legale riguarderebbe, ad esempio, il pagamento tramite bancomat al casello autostradale, che permette ad una banca ed alla Società autostrade di avere a disposizione informazioni su tutti i passaggi autostradali dei suoi clienti. La violazione illegale della privacy riguarda, invece, il furto d'alcuni computer, avvenuto presso l'ospedale Careggi di Firenze, contenenti i dati di persone affette da AIDS. Tali persone hanno in seguito subito dei ricatti da parte d'anonimi.

[56] C. Stoll, ***Miracoli virtuali***, op. cit.

un'eccessiva perizia di programmazione. Inoltre, i data-base sulle persone invecchiano con facilità se non sono continuamente aggiornati, e le fonti commerciali non sono molto attendibili. L'autore conclude che tenerci sotto controllo sarà molto difficile, ed il nostro privato sarà sempre coperto dalla semplice oscurità e dal costo eccessivo per farvi luce.

Di diverso avviso sono P. Breton e D. Lyon. Il primo si limita, nella sua opera "L'utopia della comunicazione", ad avvisare i lettori che le reti di domani potranno servire a schedare le persone ed a ridurre la loro libertà; il secondo approfondisce i meriti della questione nell'opera "L'occhio elettronico". La visione espressa in quest'opera, vale a dire un ridimensionamento dell'allarmismo inerente la "società della sorveglianza", pare incupirsi al momento di trattare l'uso dei data-base nell'immagazzinamento e nell'elaborazione dei dati personali.

L'autore, a differenza di C. Stoll, appare più spaventato dall'uso del controllo informatico incrociato, che rischierebbe di intrappolare tutti nella rete telematica. A creare preoccupazione figura l'eventualità che un soggetto, individuato come colpevole tramite un controllo informatico incrociato, sia considerato tale fino alla dimostrazione della sua completa innocenza. Incredibilmente, il "Privacy Act" (la legge americana sulla privacy) non è stato pensato per coprire questi casi, perché possono essere sempre giustificati dai controllori come attività di routine.

A coloro che sono identificati nel corso di questi controlli, infatti, viene negato il procedimento legale dovuto, che darebbe loro la possibilità di presentare prove contrarie prima che siano intraprese procedure di punizione. Inoltre, le leggi che tutelano la protezione dei dati negli USA tendono a regolare solo le banche dati governative, lasciando pressoché immutate ampie fasce di sorveglianza commerciale[57]. L'autore sottolinea la tendenza ad "autosostentarsi" da parte dei sistemi di sorveglianza, vale a dire il modo in cui le organizzazioni dipendono sempre più dal raffronto di dati personali tratti da altri archivi, invece che da forme di richiesta diretta al soggetto stesso.

[57] Lyon riporta che nel 1991 la Lotus era in procinto di lanciare sul mercato un nuovo software gestionale su CD-ROM che, al solo premere un tasto, avrebbe rivelato nome, indirizzo, stato civile e reddito presunto di 80 milioni di capifamiglia americani. Ancor prima che il software fosse lanciato ufficialmente, pare che la Lotus fu bersaglio di tante lamentele da dover ritirare il prodotto.

Lyon considera le leggi sulla privacy “terribilmente” importanti, non fosse altro perché istituzionalizzano giuridicamente l’idea che non si debba permettere che la sorveglianza cresca senza ostacoli. Tuttavia l’autore è convinto che quanto è possibile ottenere tramite le contromisure legali sia “cronicamente limitato”, perché la legge è inadeguata al compito di regolare le pratiche per la sorveglianza elettronica.

Per limitare il grado d’indiscrezione, insito negli strumenti per la navigazione, conviene utilizzare degli “anonimizzatori”. Il servizio d’anonimato può cancellare l’indirizzo di posta elettronica dell’utente, sostituendolo con un’identificazione anonima, in modo che non sia possibile riconoscere in lui l’autore dei messaggi inviati ad un determinato sito. Tale funzione viene svolta da “ripetitori anonimi” come ***anon.penet.fi***, che ricevono messaggi di posta elettronica regolarmente firmati e li riproducono in forma anonima, inviandoli ad altri utenti.

Volendo visitare i propri siti preferiti, senza che tale attività sia controllata, il più famoso “anonimizzatore” resta il celebre, a volte un po’ lento, www.anonymizer.com, per ottenere i benefici del quale é sufficiente inserire l’indirizzo della pagina che s’intende visitare nell’apposita casella. Ci pensa Anonymizer a prelevarne il contenuto ed a renderlo a noi disponibile.

Inoltre lo stesso sito permette di inviare messaggi di posta elettronica in modo del tutto anonimo, fornendo lo stesso servizio dei ripetitori anonimi precedentemente citati. Solo in caso di reato da parte dell’utilizzatore del servizio, il gestore del sito è obbligato dalla legge a fornire la vera identità del responsabile del reato, scoraggiando in questo modo eventuali malintenzionati che potrebbero sentirsi protetti dall’anonimato stesso.

Una nuova insidia è rappresentata dal “doubleclick.net”, un ulteriore indirizzo Web che consente alle aziende abbonate di fare pubblicità mirata verso i “navigatori”. Il meccanismo di funzionamento è molto semplice, tuttavia al limite della legalità, almeno per la legge italiana. Ogni volta che ci connettiamo ad un sito di nostro interesse, il quale ha contratto un accordo con “doubleclick.net”, riceviamo un cookie che registra alcuni nostri dati sul server della “doppio click” (dove ci colleghiamo, per quanto tempo, quali sono i nostri siti preferiti, cosa cerchiamo nelle pagine

contattate). Tali dati, se ben utilizzati, si rivelano molto utili per effettuare della pubblicità "mirata".

Questo sistema, al limite della legge, riesce a trovare applicazione in Italia, in quanto la normativa italiana sulla privacy vieta sì la raccolta d'informazioni, riguardanti le preferenze dei soggetti interessati senza che questi lo sappiano, ma non si può applicare ai siti dislocati in altre nazioni extraeuropee. Anche in seguito a questo tipo di "servizi", si è da più parti effettuata richiesta per una modifica degli standard dei cookies, al fine di renderli più sensibili alla privacy personale.

La posta elettronica pone due ordini specifici di problemi. Il primo riguarda i filtri per i messaggi che si ricevono al proprio indirizzo, il secondo le procedure d'autenticazione e di sicurezza in relazione ai messaggi inviati. I filtri sono degli strumenti dichiaratamente difensivi che, comportandosi in maniera analoga ad una segreteria telefonica, consentono all'utente di filtrare ed eliminare informazioni indesiderate. I filtri di tipo "dummy" o "bozo" sono dei programmi "killfile": se un utente, ad esempio, riceve messaggi sgradevoli da parte di un altro membro del suo newsgroup, inserirà l'indirizzo di quella persona nel filtro ***bozo***, e quest'ultimo farà scomparire dal computer dell'utente i messaggi provenienti da quell'indirizzo[58].

I ***cancelbots*** hanno invece un effetto più aggressivo, e sono solitamente usati contro i "pappagalli", ossia gli utenti che disseminano nel cyberspace messaggi inutili o inappropriati, spesso per scopi pubblicitari. Strumenti elettronici simili ad una sorta di "missile Patriot", i ***cancelbots*** percorrono il ciberspazio distruggendo tutte le comunicazioni superflue. Alcuni molestatori, tuttavia, sono molto abili, e riescono a mandare messaggi in forma anonima o spacciandosi per qualcun altro.

Alcune tecniche[59] permettono di arrivare ad intasare una casella postale con milioni di messaggi, bloccando il traffico dell'utente che li riceve. In casi come questi è importante avere un buon rapporto con il proprio fornitore, l'unico che può risolvere

[58] La questione relativa ai software-filtro è più complessa di quanto si crede: di recente, è stata sollevata addirittura dall'American Civil Liberties Union, che ha ritenuto incostituzionale la decisione di una biblioteca di Loudon County (Virginia) di usare il software ***X-Stop*** per filtrare i siti accessibili dai propri terminali, messi a disposizione del pubblico. Fonte: ***Un filtro poco democratico***, da Computer Valley n.46 del1/10/'98, pag.23.
[59] Vedi cap.3, par.3.

intasamenti o molestie simili, anche contattando uno dei tanti "investigatori" che operano sul Web.

Anche se le operazioni effettuate, dal punto di vista strettamente tecnico, possono essere simili, è necessario non confondere l'hacker con il "comune" molestatore: raramente, infatti, uno smanettone perde tempo ad infastidire un privato, in quanto estraneo alla sua etica. Diverso il rapporto con le aziende o le multinazionali, nei confronti delle quali scattano diverse percezioni del proprio comportamento (es. "sindrome di Robin Hood", vedi il primo capitolo).

I messaggi inviati a mezzo posta elettronica possono subire pericolose intercettazioni d'informazioni, ed i blocchi di dati inviati da un p.c. all'altro rischiano di essere intercettati come accade per una comune telefonata. La soluzione più comune, per ovviare a questo tipo di problemi, è data dalla crittazione dei messaggi, anche se nessun algoritmo di crittografia è ritenuto sicuro al cento per cento, come dimostrano alcuni programmi di decrittazione basati sulla "forza bruta", distribuiti in rete da vari hacker.

Uno tra i software più comuni per la crittografia è il PGP (Pretty Good Privacy), prelevabile alla pagina www.pgp.com., che offre funzioni di codifica e firma digitale. Alcune inquietanti scoperte sulla reale sicurezza delle release più recenti portano a garantire, però, solamente la completa affidabilità della versione DOS 6.3i, meno amichevole nell'interfaccia di gestione rispetto ad altre versioni. Inoltre, esiste la possibilità, da parte di supervisori, d'inserire nella versione 5.5 di PGP una sorta di "superkey", in grado di decrittare tutti i messaggi generati. In tal modo, un amministratore di rete potrebbe tranquillamente esercitare una funzione di controllo su tutta la corrispondenza presente sul network locale. Il PGP è utilizzato anche dal CERT-IT nei suoi servizi anti-hacker, dal questionario telematico alla diffusione dei dati sulle infrazioni[60].

Altri modi per cifrare i messaggi sono il DES (Data Encryption Standard) e la steganografia[61]. Quest'ultimo è un procedimento molto utile quando è proibito spedire messaggi crittografati, ma è permesso spedire testi, immagini, fotografie e

[60] Vedi cap.3, par.3.
[61] Strano Network, ***Nubi all'orizzonte***, op. cit.

simili purché in chiaro (come avviene sulla rete Fidonet). L'idea consiste nel trasformare un'immagine, un disegno o qualunque altra cosa, in una sequenza di numeri alfanumerici. Tali numeri, letti da un punto di vista umano, non hanno nessun significato, ma restano informazioni che possono essere spedite come se fossero un normale messaggio (tale procedimento è definito ***uuencoding***).

Grazie all'immersione di un file di testo, crittografato o meno, in un'immagine di tipo ***bitmap*** (dove ogni singolo pixel dell'immagine vede leggermente modificata la propria ***palette*** di colori, per ospitare le informazioni del messaggio che si vuole nascondervi), è possibile spedire un'immagine che ad occhio nudo sarà praticamente uguale all'originaria. Nel mentre questa sarà divenuto un contenitore per il suo vero contenuto, vale a dire il messaggio crittografato al suo interno.

Con la steganografia, in pratica, è quindi possibile prendere un messaggio, sottoporlo a crittografia tradizionale, prendere un'immagine qualsiasi, immergere il messaggio crittografato in tale immagine, sottoporla al processo d'***uuencoding***, e spedirla come normale messaggio. A questo punto, chiunque voglia verificare il contenuto del messaggio può tranquillamente farlo: si vedrà l'immagine, ma non che contiene un testo crittato. I programmi di steganografia sono di pubblico dominio, liberamente distribuibili e duplicabili a piacere, e questo per esplicito volere di chi li ha scritti. Sono anche dei programmi di cui sono disponibili le "sorgenti", quindi chiunque può modificarli per le proprie specifiche esigenze e può imparare a sua volta a farne di nuovi.

I sistemi di codificazione possono usare due tipi di crittografia: a chiave simmetrica ed a chiave asimmetrica. Nel primo caso per la codifica si usa la stessa chiave usata per la decodifica, nel secondo si usano due chiavi diverse ma legate fra loro[62]. Quest'ultimo sistema è alla base delle tecniche a chiave pubblica, dove la propria chiave viene suddivisa in una privata ed in una pubblica. Solo il proprietario conosce la propria chiave privata, mentre tutti possono venire a conoscenza della sua chiave pubblica, rintracciabile in una sorta di pagine gialle o resa disponibile in altri modi. Naturalmente, è praticamente impossibile ricavare la chiave di decodifica conoscendo solo quella di codifica e l'algoritmo di cifratura.

[62] V. Ahuja, ***Sicurezza in Internet e sulle reti***, McGraw-Hill, Milano, 1996.

Un utente A, che desideri inviare un pacchetto codificato all'utente B, può utilizzare la chiave pubblica di B per codificare il messaggio, che sarà decifrato da B usando la propria password privata. Poiché soltanto B conosce la propria chiave privata, nessun altro utente è in grado di decifrare il pacchetto. Inoltre, in alcuni sistemi a chiave pubblica è possibile codificare i dati utilizzando una qualsiasi delle due chiavi, mentre l'altra viene utilizzata per la decodifica.

L'utilità di questo metodo è chiarita dall'algoritmo a chiave pubblica RSA[63], che consente di effettuare la codifica, e l'autenticazione, usando entrambi le chiavi. I tre obiettivi da raggiungere sono: protezione e segretezza del messaggio, per essere sicuro delle quali il ricevente deve decrittare con la sua chiave privata, e autenticazione del mittente, per ottenere la quale il mittente stesso deve codificare con la sua chiave privata. L'unico procedimento, in grado di assicurare tali obiettivi, prevede la codifica, da parte di un utente A, con la sua chiave privata e con la chiave pubblica di B, e la decodifica di B con la sua chiave privata e con la chiave pubblica di A.

La firma digitale ha lo scopo di dimostrare l'autenticità e l'origine dei dati, ed è quindi diversa dalla codifica che serve alla loro protezione e riservatezza. Vari programmi, come il PGP (Pretty Good Privacy) o il PEM (Privacy-Enhanced Mail) offrono entrambe le funzioni. La firma digitale permette tali funzioni grazie all'utilizzo di una chiave privata nota solo all'utente che la possiede, che comprende un valore di controllo in grado di sancire l'identità del mittente. In questo modo si evitano alcuni spiacevoli inconvenienti, come l'ordinazione di un qualsiasi oggetto in nome di qualcun altro (poi costretto a pagarlo), o la "non ricusazione" (cioè il negare di aver inviato dei dati, se li si ha inviati, o di averli ricevuti, se li si ha ricevuti). In entrambi i casi la firma digitale consente di risalire all'identità del mittente.

Un sistema di firme digitali deve essere in grado di verificare anche la data e l'ora della firma, il contenuto del documento al momento della firma, deve poter essere verificato da terze parti (in modo da risolvere eventuali controversie) mediante un elaboratore ed un programma apposito.

[63] Tale algoritmo è stato sviluppato da Rivest, Shamir e Adleman (1978), ed è molto comune su Internet.

Tale contenuto, poi, deve poter essere contraffatto solo se chi effettua tale operazione è a conoscenza della sua chiave di cifratura (ma se la chiave che l'ha generata è la stessa, non è più dimostrabile che la firma in questione sia falsa). Inoltre, la firma digitale deve avere la stessa valenza d'autenticità di quella autografa.

Nell'archivio predisposto da ogni autorità di certificazione dovrà esservi, per ogni possessore di chiavi, un certificato (la firma digitale apposta alla chiave pubblica dell'autore) che, confrontato con la firma apposta al termine di un documento, permetta di identificare quelle firme come uguali o meno. L'uso di una chiave può essere revocato se il soggetto dichiara di aver smarrito la propria chiave privata, e ciò rende la chiave passiva. Esistono anche dei limiti temporali d'attività, ed attualmente i certificati emanati hanno una validità di circa due anni, a causa della veloce evoluzione tecnologica.

Come si può facilmente intuire, privacy e sicurezza rappresentano due requisiti fondamentali nella lotta alla criminalità informatica, per assicurare agli utenti di poter effettuare con tranquillità acquisti o trasmettere pagamenti in rete. Tali requisiti devono essere garantiti mediante alcuni servizi. Deve esistere un servizio che consenta il trasferimento sicuro di differenti modalità di pagamento, dalle carte di credito agli assegni elettronici, dalle carte di debito al denaro digitale. Oltre a ciò, un meccanismo di pagamento sicuro deve offrire una distribuzione a tre vie dei dati privati, vale a dire deve mettere in contatto un privato, la sua banca ed un esercizio commerciale (evitando che un criminale si sostituisca ad uno dei tre soggetti, più spesso il primo).

Altro servizio fondamentale deve essere la garanzia dell'integrità dei dati trattati, onde assicurare la privacy nelle transazioni. E' stata elaborata una serie di soluzioni per ovviare a tali necessità, alcune delle quali sono di seguito trattate; tuttavia, la continua ricerca in corso le rende superabili in tempi molto rapidi.

Il sistema ***SSL*** (Secure Sockets Layer), sviluppato dalla Netscape Communication, è realmente sicuro quando sia il browser sia il server in collegamento usano software Netscape. La sua qualità è nel saper riconoscere l'origine di un documento su qualsiasi server, proteggendone i diritti d'autore. L'informazione che il server utilizzato è sicuro viene trasmessa mediante la lettera

“s”, posta all’inizio o alla fine del termine col quale tale indirizzo comincia. Il sistema SSL utilizza la crittografia a chiave pubblica.

Il metodo ***First Virtual*** non usa sistemi di crittografia e non fa circolare il numero della carta di credito su Internet. Tale metodo consiste nella compilazione di un modulo, anche mediante uno pseudonimo, e nell’indicare una password di lunghezza non superiore agli otto caratteri. Tramite l’E-Mail, questo sistema invia un codice d’identificazione a dodici cifre e un numero telefonico da chiamare per comunicare tale codice assieme al numero della carta di credito. In seguito viene notificato sull’E-Mail il Virtual Pin, cioè il codice di carta di credito con cui fare acquisti on-line. La conferma dell’acquisto avviene mediante la posta elettronica.

Il ***Cybercash Wallet*** è il sistema della Cybercash che usa dei certificati crittati. Tali certificati vengono scambiati in rete tra acquirente e venditore, e sono garantiti da una serie di banche autorizzate alla loro emissione. Se si effettua una spesa tramite questi certificati, questa viene addebitata sulla propria carta di credito, i cui numeri non viaggiano in rete ma vengono custoditi dalle banche che hanno emesso i certificati stessi.

Il servizio ***SET*** (Secure Electronic Transaction), sviluppato da grandi multinazionali dell’informatica (IBM, Microsoft, Netscape …), garantisce l’integrità del messaggio e l’autenticazione dei dati finanziari, usando il sistema RSA Data Security di crittografia pubblica (lo stesso analizzato in merito all’uso delle due chiavi, pubblica e privata). Tale soluzione prevede che i dati della carta di credito del cliente passino al venditore in busta digitale (busta con informazioni protette), per evitare che si possa vedere il numero della carta.

Il venditore passa a sua volta la busta, assieme all'identificazione digitale, al proprio ***acquirer*** (istituzione finanziaria con la quale ha aperto un conto e che elabora la transazione per l’autorizzazione e il pagamento) per la verifica. Questi apre la busta e sottomette le informazioni della carta di credito all’istituto che l’ha emessa per l’approvazione. L’approvazione è comunicata all’aquirer, al venditore ed al cliente.

Critiche sferzanti al commercio elettronico sono state portate da C Stoll, nella sua opera “Miracoli virtuali”. Egli ritiene che i prodotti venduti con questo sistema non saranno diversi dalla “robaccia” pubblicizzata sulle televisioni commerciali, e dichiara a più riprese che la figura del negoziante resterà insostituibile, a causa di tutto ciò che può offrire in più rispetto alla “fredda transazione telematica”. Molti dubbi sono espressi sulla sicurezza e sulla validità delle transazioni commerciali effettuate in rete, così come sulla capacità delle persone di rinunciare all’acquisto di un oggetto “vedendolo, sentendolo e toccandolo”. In breve Stoll ritiene che la cyber-vendita sarà un fiasco. Sempre il testo di Stoll riporta due vicende che, al termine di questo capitolo dedicato agli sforzi prodotti per rendere la rete più sicura ed affidabile, dovrebbero far riflettere.

Nel dicembre del 1987 uno scoiattolo scavò una buca lungo una linea telefonica, disabilitando il ***NASDAQ Stock Exchange***, vale a dire il sistema che permette alla Borsa di Wall Street di funzionare. Alla fine del 1994, il sistema di computer della stessa borsa fu bloccato da un altro scoiattolo, questa volta nel Connecticut.

Perché, si chiede Stoll, un centro mondiale del capitalismo è alla mercé di un paio di roditori? La risposta del critico è solo in parte basata sull’ilarità: egli rileva l’estrema compattezza del sistema, mirata a renderlo più robusto, attendibile, espandibile, utilizzabile mediante precise linee di condotta cui ci si dovrebbe conformare, le quali non sono ancora state recepite dagli hacker e, naturalmente … dagli scoiattoli.

Figura 4

Vere e presunte responsabilità degli hacker

Problematica	Responsabilità degli hacker	Responsabilità d'altri soggetti
Violabilità della privacy dell'utente privato: messaggi telematici, caselle postali.	Ridotta partecipazione al problema, comportamento estraneo all'etica hacker.	Diversi soggetti possono violare tale privacy: sysop, utenti curiosi e smaliziati, polizia telematica…
Flamewars	Gli hacker, pur senza seguire la netiquette, non sono i principali imputati di tale problema.	In potenza, ogni chat può diventare una flamewars. Non si può descrivere un responsabile-tipo.
Aumento utenza profit: pubblicità, spamming, doubleclick, cookies, banche-dati sui gusti dei navigatori.	Alcune tecniche si avvicinano a quelle usate dagli hacker, ma questi non hanno alcuna relazione con tale problematica.	Il Web, apparentemente gratuito, trova nella pubblicità un sostegno prezioso alla sua espansione. Fenomeno destinato ad aumentare.
Scarsa sicurezza transazioni economico-commerciali; false ordinazioni e casi di "non ricusazione".	Diretta responsabilità hacker (qui meglio definiti come cracker o insider) in tutti i casi, esclusi quelli di "non ricusazione".	La "non ricusazione" è stata una possibilità sfruttata da diversi soggetti, dediti alla fornitura e/o la ricezione d'informazioni.
Violazione e manipolazione di data-base d'aziende ed università; ingegneria sociale.	Diretta responsabilità hacker nella violazione ed ingegneria sociale, cracker ed insider nella manipolazione.	L'aumento dei fenomeni d'insider ha portato più attenzione nelle assunzioni ed un maggiore controllo sulle attività dei dipendenti.
Scaricamento di connessioni private su grandi aziende ed università; truffe a compagnie telefoniche.	Diretta responsabilità degli hacker, qui classificati come phreaker nelle azioni contro le telco.	Negli anni'90 diverse indagini hanno rivelato casi d'insider, o d'operatori che truffavano i propri clienti.
Interruzione di programmi d'informazione, manipolazione di news e comunicati.	Diretta responsabilità degli hacker, qui spesso identificabili in newbies a caccia di pubblicità.	
Information overload ed agenti intelligenti.		Tale problematica, nata con la rete, è intrinsecamente legata alla sua struttura ed alle sue funzioni.
Commercio d'immagini relative alla pedofilia; molestie sessuali a minori adescati in rete.		Vere e proprie organizzazioni trafficano in immagini e propongono contatti con minori; molestie ed adescamenti sono provocati da singoli utenti non classificabili.
Stupri virtuali e violenze via Internet, intesi come crimini contro la persona e la sua libertà.		Impossibile proporre una categorizzazione di tali malintenzionati, vista l'eterogeneità dei soggetti che navigano in rete.
Duplicazione illegale di software e libera distribuzione in rete dello stesso (warez).	Probabile responsabilità hacker in assenza di fine di lucro, cracker et altri in presenza dello stesso.	
Progettazione e realizzazione di virus informatici, infezione di software circolante in rete.	Spesso dietro tale problematica si nasconde un cracker, ma tra questi e chi crea virus non esiste una precisa sovrapposizione.	Diversi possibili soggetti: dipendenti informatici licenziati, studenti in cerca di pubblicità, idealisti in rivolta contro le multinazionali…
Informatizzazione d'attività tipiche della criminalità organizzata (es. traffico di droga).		La criminalità organizzata, in tutte le sue forme, ormai padrona del know-how tecnologico necessario.

Fonte: Nostra elaborazione sulla base delle informazioni bibliografiche.

5. L'hacker in posa: tra metodologia e percezione

"Come sapere se il gatto è vivo o morto?
Si lascia in una condizione virtuale
finché non si apre la scatola".
Da una lezione di "Metodologia e Tecnica della ricerca sociale", tenuta dal Dott. Nobile il 27/11/'95.

Definita in chiave teorica la figura dell'hacker, la sua storia ed il suo ruolo, questo lavoro si propone di effettuare una ricerca sperimentale che "fotografi" tale soggetto all'interno di un immaginario collettivo, che ci fornisca la reale percezione di tale fenomeno da parte di chi popola il suo mondo, di chi lo affronta, di chi lo teme.

Il passaggio da una fase teorica ad una sperimentale, unito alla particolarità del soggetto di studio, presenta incognite organizzative, dubbi metodologici e rischi operativi propri di uno scenario nuovo, tanto innovativo da richiedere un procedimento analitico in stretta relazione con le modalità di manifestazione del soggetto stesso. Se già la famosa analisi del gatto di Schrodinger[1] poneva problemi d'oggettività sull'osservazione dei fenomeni, e si trattava di fenomeni semplici da rilevare, si può immaginare la difficoltà relativa allo studio di sensazioni, esperienze, percezioni soggettive di un pericolo spesso "invisibile" come l'hacker informatico.

Le novità relative a tale fase sperimentale del lavoro non riguardano solo l'oggetto di studio ma anche le modalità d'indagine utilizzate, a partire dallo strumento principe di rilevamento rappresentato da Internet, più precisamente dall'uso di una casella postale elettronica[2] per inviare e ricevere dati ed informazioni.

[1] Vedi citazione in alto a destra. Si tratta di un noto esperimento del premio Nobel per la fisica (1933), che prevedeva di mettere un gatto in una scatola, collegare elettricamente quest'ultima mediante due fili, uno dei quali passante per un'ampolla di veleno, e d'immettere casualmente degli elettroni in uno dei due fili. Schrodinger rivelò che, senza aprire in seguito la scatola, lo scienziato non avrebbe mai potuto sapere se il felino fosse morto o vivo, ed usò quest'esempio per sottolineare quanto l'osservazione del reale dipendesse dall'osservatore.
[2] Che risponde alla sigla di novafra@iol.it

L'ipotesi originale della ricerca è rappresentata dall'idea che il fenomeno hacker, nel nostro paese, sia percepito in maniera molto diversa tra i singoli utenti che definiremmo "normali", nel senso che usano la rete per scopi più o meno personali (hobby, professione, ricerca…) che non hanno nulla in comune con il fenomeno studiato, e gli "addetti ai lavori", cioè coloro che si trovano frequentemente in contatto con i pirati del ciberspazio, e che vedono la propria attività influenzata di continuo dal comportamento di questi ultimi (es. magistrati, agenti di polizia, esperti di sicurezza informatica, avvocati, giornalisti del settore).

L'analisi della bibliografia, e la vasta componente teorica del lavoro che n'è derivata, hanno contribuito a formare tale ipotesi e ad orientare il proseguo della ricerca in questa direzione. Come trapelato nei capitoli precedenti, si ha da più parti la sensazione che gli hacker nostrani, più noti come smanettoni[3], abbiano contribuito alla creazione di un "mercato della sicurezza" in grado di muovere notevoli capitali, il tutto senza che tale movimento d'interesse sia giustificato dall'effettiva pericolosità del fenomeno.

Vista l'impossibilità di confermare altrimenti tale ipotesi di ***distonia percettiva***, questo lavoro ha tentato di costruire una base di confronto tra le diverse figure dell'utente medio e dell'addetto ai lavori. Nonostante la presenza di un'ipotesi di base, che inserirebbe questo lavoro tra le analisi di tipo esplicativo (che partono da una teoria e cercano di confermarla), la ricerca che ci proponiamo di effettuare vuole descrivere la percezione degli utenti della rete senza lasciarsi distrarre od influenzare da tale base teorica, con la prontezza di sottolineare le diversità, rispetto alle nostre attese, se queste dovessero rendersi concrete.

Nel rapportarci ad un'utenza non specializzata sorgono problemi di diversa natura, relativi a fattori di reperibilità dei soggetti, rilevamento delle loro conoscenze mediante uno strumento che ne permetta una quantificazione, affidabilità delle risposte ricevute e possibilità di collegarle tra loro onde ricevere un'idea completa ed attuale della percezione analizzata. Ma il fattore che, all'origine dell'organizzazione del lavoro, ha rappresentato la maggiore incognita, è stato l'utilizzo del mezzo

[3] Vedi cap.2 e 3.

telematico per rilevare sensazioni ed esperienze dell'utenza della rete, a cominciare dalla problematica definizione dello stesso concetto d'utente[4].

L'interrogativo originario riguardava la possibilità di assegnare un nome ed un "volto" ad un soggetto, l'utente telematico, che sfugge per principio a tale categorizzazione, in quanto seguace dell'anonimato, del cambiamento d'identità e, a volte, di genere. Stratificare un campione che si attenesse a precise caratteristiche, senza la possibilità di controllare l'effettiva partecipazione degli utenti al campione stesso, è parso inutile, ed ha avuto come prima conseguenza la crescita in termini numerici del bacino d'utenza della ricerca, fissato inizialmente in c.ca 400 unità. Ad ognuna di loro, per essere giudicata idonea a far parte del campione, inizialmente è bastato avere un proprio recapito di posta elettronica e la capacità di rinviare autonomamente il documento di rilevazione ricevuto.

Il lavoro di reperimento degli indirizzi e-mail è avvenuto, in un primo tempo, navigando in rete a caccia di siti che trattassero almeno parzialmente l'argomento "hacker", e seguendo la dinamica del "campione a valanga", secondo la quale si chiede ad ogni soggetto disponibile di fornire l'indirizzo d'altre persone che potrebbero rientrare nel nostro campione, oppure gli si domanda d'inviare lui stesso il documento di rilevazione alle persone in questione (che, nel nostro caso, ha spesso rappresentato il procedimento di maggior successo). Altre caratteristiche del nostro campione sono il suo essere non probabilistico (non tutte le unità d'analisi, infatti, hanno la stessa possibilità d'entrare a farne parte), ed il suo avere una rappresentatività difficile da valutare (anche se la citata espansione a 400 unità aiuta, in parte, a diluire tale problema).

Tale metodologia è stata solo una delle conseguenze dell'utilizzo di un mezzo così innovativo per sondare le opinioni di un campione. Sull'uso del modem nei sondaggi ci sono sembrate molto interessanti le considerazioni di L. Ricolfi, riassunte nello scritto ***Incertezza e verità. Un confronto fra tecniche telematiche di sondaggio*** [5]. L'autore si riferisce alla tecnica CAMI (Computer Assisted Modem Interview), da lui sperimentata e confrontata con altre tecniche di sondaggio più comuni. I risultati finali di tale confronto assegnano alla rilevazione attraverso il modem una maggiore

[4] Vedi cap.4, par.2.
[5] Inserito nel testo "Lo strabismo telematico" di F. Di Spirito, P. Ortoleva, e C. Ottaviano, UTET, Roma, 1996.

fedeltà, vale a dire più vicinanza a quelli che sono i veri pensieri degli intervistati, rispetto a sondaggi telefonici od effettuati di persona.

Sembra che il modem, consentendo un diverso tempo di risposta ed un assoluto anonimato, permetta agli intervistati di essere realmente se stessi, di professare le proprie opinioni anche quando scomode o controcorrente. Ricolfi rileva che tale strumento induce ad una comunicazione priva di convenzioni, di comportamenti prescritti, di valutazioni di facciata, il tutto a discapito della certezza e della prevedibilità delle risposte. Infatti, se le valutazioni ottenute con il modem hanno il pregio delle fedeltà, queste sono anche più instabili, hanno una maggiore varianza temporale, risultano meno attendibili rispetto a quelle telefoniche.

Ricolfi pone l'accento sullo stretto legame tra fedeltà ed incertezza, e lo ripropone all'inverso per il mezzo telefonico, il quale fornirebbe risposte più certe ed attendibili, ma anche più lontane da fedeltà ed accuratezza. L'incertezza relativa alle risposte ottenute via modem non dipenderebbe solo dal mix di fattori accidentali che influenzano la risposta, ma anche dal grado di autonomia e riflessività del rispondente. Una risposta vera, fedele, "…richiede riflessione, e la riflessione richiede tempo. Il tempo della riflessione aumenta l'incertezza, perché allontana gli stereotipi. Ecco perché, con il modem (che consente all'intervistato di scegliere il momento in cui rispondere e di riflettere, su ogni domanda, tutto il tempo che desidera) non solo diminuiscono le risposte conformiste o stereotipate ma aumenta anche l'incertezza. L'incertezza è il prezzo della verità".[6]

In conclusione al suo intervento, Ricolfi ammette che l'unico problema della tecnica CAMI riguarda l'ampiezza del campione. Poiché la sua maggiore fedeltà "costa" incertezza, egli suggerisce di sovradimensionare leggermente i termini numerici del campione, in modo da evitare una perdita d'efficienza nelle stime. Altre caratteristiche di questa metodologia riguardano, in genere, un'alta impersonalità dell'intervista ed un basso costo della ricerca, se si esclude le spese iniziali per il computer, il modem e l'abbonamento alla rete[7].

[6] Vedi "Lo strabismo telematico", op. cit., pag.215.
[7] Ma Ricolfi sconsiglia questa tecnica se non si possiede già un computer ed un collegamento alla rete.

L'area coperta tramite modem risulta più estesa di quella copribile, a parità di tempo e di spesa, da altri strumenti. La rapidità di rilevazione, unita ad un maggiore controllo sui tempi della ricerca, completa i fattori positivi di tale metodologia. In quanto ai possibili svantaggi, detto dei problemi relativi ad una stratificazione del campione, resta da sottolineare l'incertezza relativa alla provenienza della risposta e ad una sua veridicità.

Della provenienza, grazie ai dati che correlano una risposta telematica, si possono conoscere la data d'invio e la casella postale di riferimento, ma naturalmente nulla è dato sapere sulla reale presenza della persona che invia tali informazioni. In merito alla veridicità, come in precedenza argomentato, prendiamo per buoni gli studi e le affermazioni di Ricolfi sulle ricerche tramite CAMI (Computer Assisted Modem Interview), ricordando che a noi è stato sufficiente sapere, almeno all'inizio, che l'intervistato fosse un navigatore ed avesse un indirizzo e-mail.

Altri possibili svantaggi, ai quali si va incontro con questo strumento di ricerca, sono rappresentati da un'elevata mortalità del campione (compensata solo in parte dall'utilizzo del campionamento a valanga), dalla possibilità che molti questionari siano inutilizzabili (per mancanza di una risposta, scelta di più alternative di risposta ad una domanda che ne contempla una sola…) e da una necessaria limitazione nella formulazione delle domande e delle scelte di risposta.

Alla luce di ciò, il ruolo dell'osservatore nella nostra ricerca appare più vicino alla concezione di Durkheim (un ruolo strumentale, un osservatore passivo) che a quella di Weber (l'osservatore conserva i suoi valori, ed i concetti che ne derivano hanno un ruolo arbitrario nella ricerca). L'hacker si mostra qui come un oggetto, sempre più vivo e reale man mano che la ricerca va avanti e lo definisce meglio. La metodologia usata, ed i risultati ottenuti, quasi si fondono in una fotografia che lascia l'hacker in posa, sullo sfondo, finalmente reale e non più sfuggente ed invisibile.

Anche in seguito a tali precisazioni, il nostro documento di rilevazione è stato articolato in un questionario d'otto domande, le prime sette relative al fenomeno in questione e l'ultima all'età del soggetto intervistato[8]. Le domande relative agli hacker

[8] Caratteristica priva anch'essa di riscontri pratici, tuttavia organizzata in una semplice classificazione per fasce (vedi in seguito).

sollevano questioni su diverse aree problematiche: l'andamento del fenomeno, eventuali esperienze del soggetto in questo campo, l'idea che l'intervistato si è fatto della figura del "pirata telematico", della sua reale pericolosità, di come le sue gesta vengono riportate dai media, il possibile futuro del triplice rapporto di dipendenza uomo-rete-hacker. Sono tutte domande a risposta multipla, articolate in modo da non fornire un numero troppo elevato di diverse risposte (massimo nove, ma accade solo nella settima domanda), all'interno delle quali è sempre data la possibilità che il soggetto non abbia le idee chiare su un argomento o non voglia rispondere.

Fedeli ai postulati di P. Bordieu[9], secondo i quali è errato supporre che tutti abbiano un'opinione su tutto, che esista un consenso pubblico sui problemi e che le opinioni della gente si equivalgano, si è considerato basilare fornire tale possibilità, riscontrabile nella formula "non sa/non risponde" che chiude ogni insieme di risposte (tranne la domanda sull'età, dove logicamente è prevista solo la possibile risposta "non risponde"). Tale articolazione permette di individuare le aree problematiche del fenomeno sulle quali gli intervistati non si sono fatti un'idea precisa, ma anche le domande che potrebbero necessitare di una diversa presentazione, in quanto un alto numero di "non sa/non risponde", relativo alle prime rilevazioni, farebbe sorgere seri dubbi sull'idoneità della domanda in questione così formulata.

La prima domanda[10] è relativa alla percezione dell'andamento del fenomeno, ed è già indicativa delle conoscenze del soggetto, perché un'iniziale non risposta farebbe sorgere dei dubbi sull'interesse di questi per l'argomento, aumentando la possibilità di risposte simili in seguito. L'intervistato è chiamato a scegliere fra tre alternative: il vedere tale fenomeno in aumento, stabile, oppure in calo.

La domanda successiva[11] interroga l'intervistato su un suo eventuale contatto, diretto o meno, con il fenomeno in questione, ed è indicativa dell'effettiva vastità o meno del fenomeno studiato. Secondo l'ipotesi iniziale, la maggioranza delle risposte a tale domanda dovrebbe essere di segno negativo, a dimostrazione di una

[9] Vedi il famoso articolo ***L'opinione pubblica non esiste***, pubblicato nel 1976 all'interno della rivista trimestrale "Problemi dell'informazione" (ed. Il Mulino, Bologna).
[10] "Lei giudica l'andamento del fenomeno hacker, nel nostro paese: in aumento, stabile, in calo, non sa/non risponde".
[11] " Ha mai avuto, direttamente (es. violazione della sua casella e-mail) o indirettamente (es. tentativo da parte d'estranei di superare il firewall della sua azienda), contatti con il fenomeno hacker, negli ultimi anni? Si, no, non sa/non risponde".

sopravvalutazione del problema da parte degli addetti ai lavori. La stessa articolazione delle risposte non permette contatti per vie anomale o "sentito dire": o si è entrati in contatto o ciò non è avvenuto, al massimo si può non esserne sicuri (e la risposta sarà inserita nella citata "non sa/non risponde").

In seguito[12], si approfondisce l'immaginario collettivo relativo al soggetto di studio, cercando d'identificare la caratteristica più adatta a descrivere il comportamento dell'hacker italiano. Tale domanda, in stretto rapporto con la settima[13] relativa all'attività con la quale s'identifica maggiormente l'operato di un hacker, dovrebbe fornire un chiaro quadro di riferimento sulla percezione del fenomeno, e consentire un riscontro della veridicità di entrambe le risposte. Infatti, se la caratteristica più ricorrente dovesse dimostrarsi, ad esempio, la curiosità, tale risultato mal si collegherebbe ad una prevalenza d'identificazione dell'hacker in comportamenti di "danneggiamento informatico" o "immissione di virus in rete", mentre ci aspetteremmo una maggiore connessione con pratiche abusive d'accesso ed intercettazione.

La terza domanda, inoltre, è la prima a consentire all'intervistato di esprimere più a fondo una propria opinione mediante l'uso dell'alternativa "altro", cui fa seguito la possibilità di specificare un'opzione diversa da quelle fornite con le normali risposte. L'analisi delle eventuali scelte di questo tipo, pur comportando qualche problema di classificazione e trattamento del dato, siamo certi che si dimostrerà alquanto interessante per una completa definizione della percezione del fenomeno, nonché per una sottolineatura da parte del campione d'alcune differenze che sono state volutamente lasciate "nell'ombra".

Il riferimento è alla classificazione del cap.3.1. tra hacker, cracker, phreaker, insider, courier, supplier e lamer, e nella curiosità di riscontrare la presenza di tale distinzione nelle conoscenze dell'utente testato: se l'analisi successiva dei dati riporterà tali distinzioni, ad esempio mediante una distribuzione delle percentuali tra

---

[12] Terza domanda: "Quale caratteristica ritiene più adatta a descrivere il comportamento di un hacker italiano: astuzia, curiosità, aggressività, eccesso di protagonismo, mancanza di rispetto verso gli altri, altro (specificare), non sa/non risponde".

[13] Settima domanda: "In quale delle seguenti attività identifica maggiormente l'operato di un hacker: accesso abusivo, danneggiamento informatico, creazione ed immissione di virus in rete, truffe e frodi informatiche,

diverse risposte tale da suggerire la contemporanea presenza di queste figure, l'utenza avrà dimostrato un'elevata sensibilità e conoscenza del fenomeno.

La quarta domanda[14] è forse la più tecnica, in quanto richiede di esprimere un giudizio sulla pena che la L.547/'93 prevede per il reato d'accesso abusivo in qualunque sistema con delle difese informatiche. I diversi pareri contrari, riportati in sede teorica[15], potrebbero far prevedere una risposta orientata ad un giudizio d'eccessiva severità verso la pena in questione, tuttavia la tecnicità della domanda potrebbe anche far salire il numero di "non sa/non risponde". Anche qui, comunque, le risposte non permettono molte alternative: si può considerare la pena eccessiva, giusta, oppure leggera, altrimenti si sceglie di non rispondere.

La quinta domanda[16] analizza un rapporto di cui si è parlato molto nella prima parte di questo lavoro, vale a dire quello tra i media ed il fenomeno degli hacker. Le due variabili prese in considerazione, nella formulazione delle risposte a tale domanda, sono state la conoscenza del fenomeno (giudicabile giusta o scarsa) e l'attenzione verso la realtà dei fatti (definibile come presente o assente). L'incrocio di queste variabili arriva a proporre quattro diverse possibili risposte, alle quali si è aggiunta la consueta "non sa/non risponde". Se le problematiche, all'interno del rapporto media-hacker, dovessero seguire le tesi riportate nella prima parte di questo lavoro, ci si dovrebbe aspettare una maggiore propensione del campione a fornire delle risposte più critiche verso la conoscenza del fenomeno da parte delle fonti d'informazione e sull'attenzione rivolta da queste alla realtà dei fatti.

La sesta domanda[17] prende in considerazione il possibile andamento futuro del rapporto di dipendenza uomo-rete, ed il conseguente rischio portato dal

---

intercettazione abusiva (compresa violazione e-mail), duplicazione e traffico illecito di software, detenzione e diffusione illegale di codici d'accesso, altro (specificare), non sa/non risponde".

[14] "Per il reato d'accesso abusivo in qualunque sistema con delle difese informatiche, la L.547/'93 prevede una reclusione (in assenza di possibili aggravanti) fino a tre anni. Lei ritiene tale pena: eccessiva, giusta, leggera, non sa/non risponde".

[15] Vedi cap. 3.4.

[16] "Secondo lei, in Italia, i media trattano il fenomeno hacker: con la giusta conoscenza del fenomeno e la dovuta attenzione verso la realtà dei fatti, con la giusta conoscenza del fenomeno ma senza la dovuta attenzione verso la realtà dei fatti, con scarsa conoscenza del fenomeno ma con la dovuta attenzione verso la realtà dei fatti, con scarsa conoscenza del fenomeno e senza la dovuta attenzione verso la realtà dei fatti, non sa/non risponde".

[17] "In relazione al rapporto Internet-hacker nel nostro paese, lei ritiene che il prossimo futuro vedrà: una maggiore dipendenza dell'uomo dalla rete ed un aumento della pericolosità del fenomeno hacker, una minore dipendenza dell'uomo dalla rete ma un aumento della pericolosità del fenomeno hacker, una

fenomeno hacker. Le due variabili, incrociate secondo lo stesso meccanismo della domanda precedente, hanno quindi immaginato una possibile futura ***dipendenza dell'uomo dalla rete***, giudicabile maggiore o minore rispetto alla situazione attuale, rapportata ad una modifica della ***pericolosità del fenomeno hacker*** rispetto a come viene percepito oggi.

La seconda variabile prevede una percezione di tale pericolosità come un possibile aumento o una riduzione. Oltre alla citata "non sa/non risponde", tale domanda consente di svincolarsi dalle scelte precostituite grazie alla risposta "altro", correlata da una successiva specificazione della diversa proposta. Tuttavia, a differenza della terza e della settima domanda, la formulazione più "chiusa" del quesito dovrebbe portare ad una minore scelta di questa possibilità.

L'ultima domanda[18], come precedentemente accennato, chiede all'utente di inserirsi in una delle fasce d'età precostituite, onde fornire al ricercatore una possibile stratificazione del campione per fasce d'età decennali, che partono dai ventun anni (un'intera fascia considera l'età precedente) ed unificano, in una sola opzione di risposta, l'età superiore ai sessanta. Tale divisione, nella consapevolezza di una sua parzialità, ci consente d'analizzare l'utenza in base ad un suo possibile rapporto "lavorativo" con la rete, permettendoci anche di dividere l'immaginario collettivo degli utenti più giovani, più sensibili a sollecitazioni di film e fumetti sulla figura dell'hacker informatico, da quello di navigatori più "esperti".

Secondo le intenzioni del ricercatore questo lavoro, abbinato a tale innovativo strumento di sondaggio, al termine della rilevazione e dell'analisi dei dati raccolti dovrebbe fornire un quadro esauriente di come l'utente, non specializzato nel settore degli hacker, giudichi la pirateria informatica e vi si rapporti. La completa percezione di tale fenomeno, per inserirsi all'interno dell'ipotesi di partenza della ricerca, dovrà in seguito essere confrontata con la valutazione del fenomeno da parte degli "addetti ai lavori", vale a dire del personale qualificato che si trova quasi quotidianamente a contatto con la realtà degli hacker nel nostro paese.

---

maggiore dipendenza dell'uomo dalla rete ma una riduzione della pericolosità del fenomeno hacker, una minore dipendenza dell'uomo dalla rete ed una riduzione della pericolosità del fenomeno hacker, altro (specificare), non sa/non risponde ".

[18] "Il questionario è rigorosamente anonimo. Ci riserviamo solamente di chiedere la sua età: meno di 21 anni, tra 21 e 30 anni, tra 31 e 40 anni, tra 41 e 50 anni, tra 51 e 60 anni, più di 60 anni, non risponde".

Tale valutazione dovrà essere composta da una lettura comparata d'alcune interviste, realizzate "face to face" o per via telematica, ponendo questioni di più ampio respiro rispetto al citato questionario. I soggetti di tali interviste dovranno essere delle figure di spicco rappresentanti diversi settori di riferimento le quali, fedeli al criterio di significatività[19], potranno sostenere il confronto con un numero assai maggiore d'utenti telematici.

Tali settori, giuridico, tecnico-informatico, e del controllo telematico, rispecchiano tre diversi riferimenti dell'universo hacker, tra loro complementari: ***il giurista***, che si occupa dell'aspetto legale degli atti compiuti dal pirata informatico***, il tecnico della sicurezza***, che lavora sui sistemi difensivi e cerca di renderli più difficili da superare, ed ***il poliziotto telematico***, che dà la caccia alla criminalità informatica e si trova ad affrontare l'hacker quando il comportamento di quest'ultimo si avvicina ad un'azione criminale.

La realizzazione di tali interviste comporta delle difficoltà differenti rispetto a quelle precedentemente analizzate. La maggiore di queste riguarda la reperibilità di tali soggetti, legata ad una loro disponibilità a collaborare nel contesto di tale ricerca, al tempo limitato per l'effettuazione delle interviste, alla possibilità (da appurare caso per caso) d'utilizzare un registratore portatile onde poter riascoltare con calma le risposte ottenute. Altri svantaggi possono essere intravisti in una diversa costruzione del questionario, che assicuri di toccare le stesse aree problematiche sondate via E-Mail ma con accorgimenti diversi, e nella trasposizione dell'intervista per iscritto tramite sbobinamento (con il rischio di perdere molte sensazioni che soltanto il ***face to face*** è in grado di trasmettere).

I vantaggi derivati da questo tipo di rilevazione sono riassumibili in una maggiore profondità delle risposte, ed in possibili collegamenti e divagazioni dovute ad una forma della domanda più aperta al pensiero dell'intervistato. L'approfondimento è maggiormente qualitativo, e si affida ad un'analisi del dialogo che prevede più flessibilità, adattamento, ed una rielaborazione di quanto detto in base a motivazioni più o meno coscienti, a risposte più o meno sincere. L'aver ottenuto diverse impressioni relative a tematiche simili, consentirà di articolare le

[19] Tale criterio sottolinea la peculiarità di un soggetto a fornire dati ed informazioni inerenti ad una ricerca specifica.

singole interviste in una sorta di “tavola rotonda d’addetti ai lavori”, la quale ci auguriamo figurerà come uno dei momenti più interessanti dell’intero lavoro.

Dalla lettura complessiva degli interventi di questi esperti dovrà trapelare una visione del fenomeno hacker che, stando all’ipotesi di partenza, dovrebbe scostarsi notevolmente da quella fornita dagli utenti tramite il questionario telematico. Su queste eventuali differenze si argomenterà un’analisi finale del lavoro, tendente ad esporre le cause di un’eterogenea percezione del fenomeno e le possibili conseguenze.

6. Manette e smanettoni: il giudizio della rete

"La fetta di società che descrive questo libro sfugge a qualsiasi tipo di catalogazione e classificazione."
Da "Pianeta hacker", postfazione
al testo ***Spaghetti Hacker.***

6.1. Novità metodologiche nell'impostazione della ricerca.

L'esame analitico di un fenomeno complesso, sfuggente ed eterogeneo come l'hacking, se sviluppato in diretto contatto con l'oggetto di studio, comporta la difficile necessità di calarsi in etiche e mentalità molto diverse dalla norma. Quando lo stesso esame viene effettuato per via indiretta, vale a dire sondando la percezione del fenomeno in soggetti ad esso estranei, le difficoltà sembrano aumentare.

A prima vista sembrerebbe porsi un passaggio in più, una sorta d'analisi di come e perché alcune persone considerano o immaginano esserne altre, diverse da loro. In realtà si tratta sempre di sondare alcuni soggetti su un determinato tema, solo che questa volta tale argomento è costituito dall'operato di un'altra categoria di persone. La soluzione di questa metodologia, in apparenza complicata, richiede semplicemente un approfondimento che vada oltre l'esame in questione, e che permetta il formarsi di un background di conoscenze tali da poter leggere, con la giusta analisi critica, i risultati raggiunti.

Per tale motivo, in questo capitolo non ci limiteremo ad esporre i risultati della ricerca on-line precedentemente costruita[1], ed a fornire una qualche lettura incrociata degli stessi, ma potremo tentare anche un approfondimento soggettivo dettato da nostre personali convinzioni, onde evitare che qualcuno sposi totalmente ed acriticamente la tesi fornita dalla rete.

[1] Vedi capitolo precedente.

Rispetto alle fasi metodologiche precedentemente descritte, la messa in pratica del progetto di ricerca ha portato leggere novità di tipo organizzativo e procedurale. L'indagine on-line è durata c.ca 90 giorni, svolgendosi nei mesi di novembre - dicembre 1998 e gennaio 1999, con una leggera appendice ai primi di febbraio per recuperare alcuni giorni persi durante le festività natalizie. Il risultato è stato leggermente inferiore alle attese dal punto di vista quantitativo, raggiungendo un totale di 375 contatti, ritenuti comunque sufficienti a fornire le indicazioni ricercate.

L'utilizzo della rete è avvenuto per gradi, con uno sfruttamento progressivo delle sue potenzialità parallelo ad una maggiore confidenza con il mezzo stesso. Sono stati inseriti on-line dei riferimenti all'indagine, all'interno d'alcuni spazi Web messi gentilmente a disposizione dai siti www.internos.it e www.citinv.it, agli indirizzi www.internos.it/professioni e www.citinv.it/sociale/piazzetta.htm#Sono. Entrambi contenevano una presentazione della ricerca, dei suoi obiettivi e delle possibili modalità d'intervento da parte dell'utente interessato. Il primo sito prevedeva anche un link al secondo, dal quale si poteva facilmente accedere al questionario stesso tramite un altro collegamento. Tali riferimenti fornivano l'indirizzo[2] di posta elettronica cui recapitare il questionario, e la richiesta di rendere nota la ricerca ad altri utenti, onde tentare l'impostazione di un campione a valanga come spiegato nel precedente capitolo.

Consapevoli della necessità di un ulteriore intervento inerente la presa di contatto con l'utenza, si è iniziato un sistematico e capillare lavoro di ricerca d'indirizzi e-mail, cui far pervenire un messaggio[3] di collaborazione all'indagine. Al termine della ricerca si è potuto costatare l'alto tasso di mortalità dei messaggi inviati: le citate 375 risposte hanno rappresentato appena il 14% della totalità di tali messaggi, che hanno ampiamente superato le 2600 unità.

[2] Lo stesso, causa termine abbonamento, veniva cambiato durante la ricerca, creando l'obbligo di controllare contemporaneamente due diverse mail-box e di aggiornare il contenuto dei riferimenti on-line.

[3] Il messaggio conteneva il seguente testo: "Sono un laureando in Scienze della Comunicazione presso l'Università "La Sapienza" di Roma, con una tesi sul fenomeno "hacker" nella realtà italiana. Sto facendo girare in rete un questionario (che allego in attached), con l'obiettivo di sondare la percezione di tale fenomeno da parte degli utenti italiani. Lo stesso questionario, se l'attached dovesse porre dei problemi, è disponibile all'indirizzo http://www.citinv.it/sociale/piazzetta.htm#Sono. Vi chiedo, se non abuso del vostro tempo, di compilare il questionario (poche brevi domande) e di rinviarlo al mio indirizzo e-mail. Se inoltre conosceste altri soggetti in grado di rispondermi, fornite pure loro il mio indirizzo e-mail ed una copia del questionario stesso, o l'indirizzo sovracitato dove poterli reperire. Vi ringrazio molto per la vostra preziosa collaborazione. Cordialmente, Novari Enrico". Ovviamente, l'indirizzo cui inviare il messaggio non viene specificato in quanto l'utente lo riceveva in calce alla mail.

I destinatari di tali messaggi di collaborazione hanno riguardato diverse categorie, non estranee al fenomeno studiato: società ed aziende interne al settore della sicurezza informatica, università e professori universitari, Pubblica Amministrazione, regioni, province e reti civiche, agenzie di stampa, quotidiani e periodici presenti in rete, singoli giornalisti che avessero pubblicato almeno un articolo sull'argomento, radio e televisioni con un proprio sito Web, enti ed associazioni il cui operato rivelasse interessi nel settore informatico, banche ed assicurazioni, webmaster e sysop il cui indirizzo fosse direttamente accessibile dalla rete, e-zine, newsgroup e mailing list vicine all'argomento di studio.

Lo svolgimento di tale lavoro ha imposto un continuo invio di messaggi, in gruppi di 15-20 unità, ed un parallelo compito di visione giornaliera della posta elettronica onde scaricare i questionari ed inserire nella matrice i dati ricevuti. Opinioni e commenti su tale attività d'utilizzo della rete, e del servizio di posta elettronica, sono rintracciabili al sito www.internos.it[4].

Il ricevimento soltanto parziale d'alcuni dati, dovuto a questionari incompleti nella forma (è capitato che la rete cancellasse parte degli attached inviati, o provocasse una ricezione incompleta da parte di chi scaricava il tutto dai siti precedentemente citati), o nel contenuto (assenza di talune o di tutte le risposte, presenza di notevoli incongruità tra alcune di queste, eccesso di risposte alla stessa domanda mediante la scelta di più di un'opzione contemporaneamente), ha imposto la non utilizzazione di alcuni di questi, per fortuna in numero irrisorio rispetto alla totalità delle ricezioni.

Al termine dell'impostazione pratica della ricerca, e subito prima di fornire i dati risultanti, è d'obbligo un ovvio suggerimento tecnico per chiunque voglia cimentarsi in analisi simili. Vista l'utilità di uno o più spazi di riferimento in rete, si consiglia d'inserirvi questionari compilabili direttamente on-line, tramite caselle su cui fare un semplice click con il mouse, prima d'effettuare un invio finale collegato tramite un link ad una matrice appositamente creata.

[4] Vedi cap.4 nota n.14.

Tale strumento di lavoro, in aggiunta e non in sostituzione di quelli comunque utilizzati, permette una più semplice collaborazione da parte dell'utenza ed una ricezione più rapida e sicura delle risposte fornite.

6.2. I risultati della ricerca: il momento dell'hacking in Italia.

I risultati del sondaggio sulla percezione del fenomeno hacking da parte degli utenti italiani hanno confermato solo parzialmente la tesi iniziale, evidenziando una serie di spunti ed interrogativi molto interessanti. Le opinioni ed i commenti in merito si alterneranno ad un'esposizione dei dati, sui quali saranno tentate anche delle letture incrociate in grado di arricchire ed ampliare il quadro di riferimento.

Cominciamo il nostro esame da un'analisi del campione, che ricordiamo essere di 375 elementi, i cui dati si riferiscono all'ottava ed ultima domanda del questionario. I problemi relativi a tale analisi on-line, analizzati nel capitolo precedente, non hanno impedito di ottenere dei risultati significativi, dai quali è stato possibile trarre interessanti conclusioni. La domanda conclusiva riguardava le fasce d'età in cui si divide il campione, e non può essere letta senza considerare le categorie che hanno composto il suo bacino d'utenza. Tali categorie, menzionate nella prima parte di questo capitolo, necessitano la presenza d'attori che conoscono la rete, padroneggiano i suoi strumenti ed hanno acquisito sufficienti basi informatiche sulle quali svolgere la propria professione.

Nessuna sorpresa, quindi, nel costatare che la fascia d'età più attiva all'interno del campione comprende coloro che hanno tra i 31 e i 40 anni (35,4%), seguita a breve distanza dalla fascia immediatamente più giovane con il 34,9% (soggetti tra i 21 e i 30 anni). Come facilmente ipotizzabile, la curva segue l'andamento di una campana, diminuendo sia nelle fasce successive (il 14,9% ha tra i 41 e i 50 anni, il 6,1% tra i 51 ed i 60) che in quella precedente (il 2,4%, pari a nove unità su 375, ha meno di 21 anni). Il campione è completato da un unico soggetto, con più di 60 anni, e da 22 elementi (pari al 5,8%) che non hanno voluto fornire la propria età.

In relazione alle fasce d'età il ricercatore, scaricando i dati, ha costatato delle relazioni interessanti, che vengono qui anticipate per fornire al lettore un quadro d'insieme, in seguito approfondito e verificato dalle singole domande.

Figura 5 **La composizione del campione**

Fasce d'età	N° di appartenenti	% di appartenenti
Meno di 21 anni	9	2,40%
Tra 21 e 30 anni	131	34,93%
Tra 31 e 40 anni	133	35,47%
Tra 41 e 50 anni	56	14,93%
Tra 51 e 60 anni	23	6,13%
Più di 60 anni	1	0,27%
Non risponde	22	5,87%
Totali	375	100%

Fonte: nostra elaborazione risultati della ricerca.

I più giovani[5], legati ad uno stereotipo diverso dell'hacker e, probabilmente, ad un vivere in maniera diversa la stessa rete, hanno avuto meno contatti con il fenomeno che giudicano tendenzialmente in aumento. Per loro i pirati telematici sono soprattutto astuti e curiosi, le pene che li riguardano sono eccessive e la rete finirà per legare fortemente a sé tutte le future attività dell'uomo. La figura dell'hacker, poco incline al rapporto con i media, viene completata da diverse e numerose attività, alcune molto fantasiose (es. creazione di virus) e poco presenti all'interno della realtà italiana.

[5] Possiamo inserire in questa categoria le prime due fasce d'età, fino ai 30 anni, previste dalla tabella.

Gli utenti più maturi[6], probabilmente a causa di un maggiore contatto diretto con il fenomeno, a prima vista sembrano conoscerlo meglio, ma sicuramente lo temono di più, come dimostra la severità del giudizio sull'operato degli hacker, sulle pene relative e sulle caratteristiche legate al comportamento. Rispetto al sotto-campione precedente il fenomeno è giudicato meno in aumento, tuttavia l'espressione di un parere negativo sui media nasconde solo in parte una dipendenza dagli stessi, spesso acritica, che la maggiore esperienza nel settore non permette di giustificare.

Figura 6 **Differenze valutative tra diversi sotto-campioni**

Sotto-campione più giovane	Sotto-campione più maturo
Ha avuto meno contatti diretti col fenomeno	Ha avuto più contatti diretti col fenomeno
Vede il fenomeno in tendenziale aumento	Considera il fenomeno più stabile
Principali caratteristiche: astuzia, curiosità	Carenza di rispetto, eccessivo protagonismo
La legge 547 determina delle pene eccessive	La legge 547 determina delle pene giuste
Attività hacker: accesso abusivo, creazione ed immissione virus, intercettazione abusiva	Attività hacker: accesso abusivo, danneggiamento informatico, truffe e frodi

Fonte: nostra elaborazione risultati della ricerca.

Il totale degli intervistati, interrogato sull'andamento del fenomeno nel nostro paese, si è così espresso: il 18,1% ha ammesso di non essere a conoscenza di tale andamento o di preferire una "non risposta", mentre l'81'8% ha scelto di fornire un'opinione personale al riguardo. Quest'ultima percentuale ha finito per delineare il seguente quadro: il 44,5% vede il fenomeno in aumento, il 33,8% lo ritiene stabile e solo il 3,4% lo considera in calo. Rapportando tali percentuali al totale dei rispondenti effettivi, senza considerare le "non risposte", il quadro risulta più chiaro: il 54,4% vede l'hacking in aumento, il 41,4% lo ritiene stabile, il 4,2% in calo.

[6] Appartengono a tale categoria le fasce d'età dalla terza alla sesta (31-più di 60 anni).

Figura 7 **Andamento del fenomeno hacker**

Giudica l'andamento del fenomeno hacker	% sul totale campione	% sui rispondenti
In aumento	44,5	54,4
Stabile	33,8	41,4
In calo	3,4	4,2
Non sa/non risponde	18,1	/

Fonte: nostra elaborazione dati della ricerca.

Nel capitolo precedente avevamo indicato tale domanda come già valido responso sulle conoscenze del soggetto, affermando che un'iniziale non risposta avrebbe fatto sorgere dei dubbi sull'interesse di questi per l'argomento, aumentando la possibilità di risposte simili in seguito. Il tema delle "non risposte", infatti, rappresenta un momento delicato d'ogni analisi sperimentale, ed il ricercatore si augura sempre che tale percentuale si mantenga bassa ed omogenea, permettendo confronti tra domande differenti.

All'interno di questa ricerca, l'analisi dell'alternativa "non sa/non risponde" individua una soglia sufficientemente omogenea (tra il 7,4% della settima domanda al 18,1% della prima), all'interno della quale sono possibili alcune correlazioni. Le maggiori percentuali di non risposta (intorno al 18%) hanno riguardato l'andamento del fenomeno ed il suo rapporto con i media, indice che in presenza di scarso interesse, questo ha seguito l'hacking anche nei suoi rapporti con diverse realtà.

Altre similarità di percentuale hanno riguardato: le caratteristiche comportamentali del soggetto hacker e le pene che dovrebbero regolarne il comportamento stesso (11,4%), l'aver avuto un contatto diretto con il fenomeno e l'immaginare una possibile relazione futura utente-rete-hacker (intorno al 9,8%). Inferiore resta la percentuale di "non sa/non risponde" relativa alla domanda sulle principali attività di un hacker (7,4%), tuttavia l'ampia scelta di alternative di risposta (ben nove) potrebbe aver influito su tale calo di percentuale.

La seconda domanda, relativa a possibili contatti diretti o indiretti tra l'utente intervistato ed il fenomeno hacker, ha visto esprimersi in merito c.ca il 90,4% degli intervistati, mentre il restante 9,6% ha ammesso di non poter essere certo se tali contatti vi siano stati o meno. Analizzando il citato 90,4% si scopre che sono certi di tale contatto il 29,3% degli intervistati, mentre il restante 61% (c.ca) si dice convinto del contrario. In pratica, quasi una persona su tre ha rivelato di aver subito l'iniziativa di un pirata telematico, in quanto giova ricordare che gli esempi presentati da tale domanda, come riferimenti al contatto in questione, riguardavano una violazione della propria casella e-mail ed un tentativo, da parte d'estranei, d'inserirsi all'interno del sistema informatico della propria azienda.

Secondo l'ipotesi iniziale, tale percentuale sarebbe dovuta essere significativamente inferiore, in quanto s'immaginava una sopravvalutazione del fenomeno dettata dagli interessi economici degli addetti al mercato della sicurezza. Il dato ottenuto, invece, rivela una presenza costante di soggetti che hanno dovuto realmente fronteggiare il problema.

Prima di proseguire occorre sollevare un interrogativo al quale si tenterà di fornire una risposta in seguito, ma che i lettori più attenti si saranno già posti. Se "solo" il 29,3% del campione ha affermato di avere avuto un contatto con uno o più hacker - esperienza che immaginiamo sia servita a farsi un'idea sul fenomeno e sull'operato di questa categoria di soggetti - da cosa derivano le supposizioni del restante 70,6% degli intervistati, visto che la soglia del "non sa/non risponde" non supera mai il citato 18,1%? Probabilmente, molti penseranno che una cultura generale sull'argomento derivi da un buon uso dei media, i quali a volte contengono riferimenti ed interviste relativi al fenomeno. I dati che ci apprestiamo a fornire, tuttavia, dimostrano che tale ipotesi presenta non poche difficoltà ad essere convalidata.

Infatti, di fronte alla domanda "Secondo lei, in Italia, i media trattano il fenomeno hacker…", ben il 57% del campione ha risposto "con scarsa conoscenza del fenomeno e senza la dovuta attenzione verso la realtà dei fatti", seguito da un 17,8% che ha preferito non rispondere. Le altre risposte hanno visto il 12% accusare i media sempre di scarsa conoscenza del fenomeno, moderata però dalla dovuta attenzione verso i fatti, l'8,2% denotare una giusta conoscenza del fenomeno ad onta

di una carenza d'attenzione ai fatti, e solo il 4,8% propendere per un corretto funzionamento delle fonti d'informazione, capaci di giusta conoscenza e dovuta attenzione. Sommando le risposte in base alla variabile "scarsa conoscenza", e riferendosi al solo totale di chi ha espresso una propria opinione, si ottiene che ben l'84% del campione considera molto insufficiente tale conoscenza del fenomeno da parte dei media.

Figura 8 **I media ed il fenomeno hacker**

Secondo lei, in Italia i media trattano il fenomeno hacker con:	%
Giusta conoscenza del fenomeno e dovuta attenzione verso la realtà dei fatti	4,80
Giusta conoscenza del fenomeno ma senza la dovuta attenzione verso la realtà…	8,26
Scarsa conoscenza del fenomeno ma con la dovuta attenzione verso la realtà…	12
Scarsa conoscenza del fenomeno e senza la dovuta attenzione verso la realtà…	57,06
Non sa/non risponde	17,86

Fonte: nostra elaborazione dati della ricerca.

L'interrogativo precedente suona ora con maggiore incisività: se il 70,6% del campione non ha avuto alcun tipo di rapporto con gli hackers, ma il 57% degli stessi giudica totalmente inaffidabili i media quando trattano tale argomento, come si è formata l'opinione espressa dagli utenti su tale tematica? In realtà, l'hacker come descritto dai media non si discosta molto da quello che traspare dalle risposte dell'utente intervistato, sintomo che le tanto criticate fonti d'informazione riescono comunque a "stingere" sui componenti del campione. Criticare le informazioni fornite dai principali mass media sembra ormai una costante, scarsamente supportata però da approfondimenti personali delle tematiche mediante fonti e strumenti differenti.

Un altro punto a favore di questa tesi è portato dalla risposta fornita dal campione in merito alla pena di reclusione fino a tre anni, conseguenza del reato d'accesso abusivo previsto dalla l.547/'93 Le opinioni presentate nel terzo capitolo, tendenti a giudicare tale reclusione come eccessivamente severa, sono state

incredibilmente smentite dal campione degli intervistati, che ha giudicato tale pena giusta per il 50,1%, eccessiva per il 26,4%, ed addirittura leggera per il 12%.

Gli utenti della rete hanno così giudicato con molta severità il reato di accesso abusivo in un sistema protetto da difese informatiche, nonostante due fattori tendenti a sminuire tale reato: non esiste, infatti, l'obbligo di porre delle difese informatiche a protezione dei propri dati, e la legge americana non sanziona minimamente il semplice accesso abusivo ma richiede, per intervenire con delle pene, un minimo di danno al sistema o ai dati contenuti[7]. La notevole severità con cui la rete ha giudicato tale abuso è maggiormente riscontrabile con delle percentuali parziali, relative solo ai soggetti che hanno scelto di esprimere una personale opinione sulla pena in questione. In relazione a tale sotto-campione, ben il 56,6% si è espresso ritenendo giusta tale pena, il 29,8% l'ha criticata come eccessiva, mentre il 13,5% l'ha considerata leggera.

Sommando questi dati, tra le persone che hanno voluto esprimere una loro opinione in proposito, più del 70% non interverrebbe sul reato di accesso abusivo se non per rendere la pena ancora più severa. Ciò testimonierebbe quanto gli hacker siano malvisti e temuti da molti utenti della rete, e sconfesserebbe gran parte dell'ipotesi posta alla base della ricerca stessa, tendente a ridurne l'effettiva pericolosità. Come non lasciar trapelare il dubbio, tuttavia, che dietro la giustificazione di tale pena vi sia un timore eccessivo del fenomeno, dettato da come lo stesso viene descritto ed analizzato dai tanto criticati (ed utilizzati) mezzi d'informazione?

La domanda, relativa allo sviluppo futuro del rapporto di dipendenza uomo-rete, connesso ad un possibile aumento o riduzione della pericolosità degli hacker, s'inserisce all'interno del quadro appena descritto, fornendo la possibilità d'interessanti scomposizioni di dati. Posto un 9,8% di non risposte già analizzato, del restante 90,1% poco meno del 54% intravede un aumento sia della dipendenza dell'uomo dalla rete sia della pericolosità del fenomeno hacker, ed il 22,6% mantiene tale idea di maggiore dipendenza uomo-rete pur immaginando una progressiva

[7] A meno che, com'è ovvio, non si sia entrati in un sistema informatico contenente dati d'eccezionale particolarità, come ad esempio quelli della NASA sullo scudo spaziale o dell'FBI sulle piste informatiche seguite dagli investigatori. Ma tali sistemi sono protetti da leggi "ad hoc", con pene commisurate al reato specifico. Vedi cap.3, par.4.

riduzione della pericolosità del fenomeno. La restante percentuale vede un 6,4% optare per una minore dipendenza uomo-rete ed un aumento della pericolosità del fenomeno, un 3,7% indicare un calo sia di dipendenza tecnologica sia di pericolosità degli hacker, ed un 3,4% scegliere possibili risposte alternative.

All'interno di tale percentuale, la maggior parte dei rispondenti (ipotizzabili pari al 2% del campione totale) prefigura una maggiore dipendenza tecnologica uomo-rete ma un andamento costante del fenomeno hacker, dovuto al progressivo miglioramento sia delle tecniche d'attacco sia di quelle di difesa. Altre risposte correlano il trend evolutivo di tali fenomeni con una serie di fattori: come la società si comporterà con gli hacker, se ci si abituerà alla rete ed in quanto tempo, quanto si deciderà d'investire sulla stessa con conseguente incremento di spese nel settore della sicurezza informatica.

Figura 9 **Crescita dell'hacker-fobia.**

Tipo di rapporto utente-hacker	% di risposta
Ha avuto, negli ultimi anni, contatti diretti (es. violazione casella e-mail) o indiretti (es. tentativo d'intrusione dall'esterno nel firewall aziendale) con il fenomeno hacker.	29,33%
Giudica l'andamento attuale del fenomeno, nel nostro paese, in aumento.	44,53%
Giudica giusta la pena di reclusione, fino a tre anni, per il reato di accesso abusivo in qualunque sistema abbia delle difese informatiche.	50,13%
Vede sicuramente un aumento della pericolosità del fenomeno hacker nel prossimo futuro.	60,26%

Fonte: nostra elaborazione risultati della ricerca.

Scomponendo le percentuali appena fornite, si scopre che c.ca il 76,5% prevede un progressivo incremento di dipendenza dell'uomo dalla rete (percentuale che sale all'85% calcolando solo i rispondenti), mentre il 60% indica l'hacking come un fenomeno che aumenterà la sua pericolosità nei prossimi anni (il che sale al 66% considerando solo i soggetti che hanno risposto). Tale percentuale rappresenta il

termine di una progressiva crescita dell'***hacker-fobia***, registrata nelle domande precedenti: il 29% ha ammesso di aver avuto dei contatti con il fenomeno, il 44% li considera attualmente in aumento, il 50,1% giudica idonee le pene che li riguardano, ed ora il 60% li immagina più pericolosi nel prossimo futuro, sia nel caso in cui la rete conduca l'uomo verso una maggiore dipendenza sia nel caso in cui questo non accada.

La terza domanda del nostro questionario indagava l'immaginario collettivo in merito alle caratteristiche adatte a descrivere il comportamento di un hacker nostrano. Premesso che l'11,5% degli intervistati ha affermato di non conoscere tali caratteristiche, andiamo ad analizzare la composizione del restante 88,5%. La caratteristica maggiormente riscontrata è la ***curiosità***, che riceve il 28,8% delle risposte, seguono l'***eccesso di protagonismo*** (20,5%) e la ***mancanza di rispetto verso gli altri*** (18,9%).

Le altre caratteristiche citate dalla domanda hanno raggiunto percentuali inferiori: indicativa solo quella relativa all'***astuzia*** (12%), mentre l'***aggressività*** è stata ritenuta saliente solo dal 4,3%. La possibile alternativa ***"altro (specificare…) "***, che permetteva di presentare caratteristiche diverse da quelle citate dal questionario, ha ottenuto solo il 4% delle risposte, all'interno del quale il campione ha voluto sottolineare l'intelligenza, il gusto del proibito, la conoscenza ed il divertimento, ma anche l'avidità, la mancanza di valori, la stupidità ed il senso di sfida verso le istituzioni.

Tali risultati vanno letti in stretta correlazione con quelli relativi alla settima domanda, foriera di diverse particolarità, alcune dovute al carattere strutturale della stessa, altre alle peculiarità dell'argomento trattato, vale a dire l'individuazione dell'attività che s'identificherebbe maggiormente con l'operato di un hacker. Ad esempio, una particolarità dei dati ricavati da questo quesito è dimostrata dal fatto che solo il 2,4% ha scelto una risposta alternativa a quelle fornite, opzione che rappresenta la percentuale minore tra le domande esaminate che contemplavano tale possibilità. Ma prima di approfondire il contenuto della risposta ***"altro (specificare…) "***, relativo alla settima domanda, forniamo tutti i dati sulle risposte alla stessa.

L'attività maggiormente correlata all'operato di un hacker è risultato l'***accesso abusivo***, con il 33,3%, seguito dal ***danneggiamento informatico*** (15,7%), l'organizzazione di ***truffe e frodi informatiche*** (15,4%) e la ***creazione ed immissione di virus in rete*** (12%). Completano il quadro una serie d'attività minori come ***duplicazione e traffico illecito di software*** (6,1%), ***intercettazioni abusive*** in rete (es. violazione e-mail, percentuale del 4,5%), ***detenzione e diffusione illegali di codici d'accesso*** (2,9%) e la citata ***altro***, pari al 2,4%.

All'interno di quest'ultima si è argomentato in merito ad una distinzione consueta, quella tra hacker e cracker, specificando che l'operato del primo si ferma alla visione di dati, senza scopi economici o di frodi, alla libera circolazione d'informazioni mediante l'abbattimento di barriere, alla creazione e diffusione gratuita di materiale informatico free (es. LINUX), ad una corretta contro-informazione informatica finalizzata alla protezione, allo studio ed alla crescita della rete. Il cracker, invece, sarebbe il vero autore di danni ed "inquinamenti" informatici.

Tale distinzione, in realtà estensibile anche ad altre voci di questa domanda, permette una classificazione che trova riscontro, in termini numerici, anche nelle altre risposte. Infatti, raggruppando le percentuali appena citate in base alla classificazione proposta da alcuni utenti intervistati, nonché secondo le principali teorie analizzate nei capitoli precedenti, la somma delle risposte relative al semplice accesso abusivo, all'intercettazione abusiva ed alla detenzione e diffusione illegali di codici d'accesso, dovrebbe fornire una percentuale legata alla percezione della figura dell'hacker, mentre dalla somma delle attività di danneggiamento informatico, creazione ed immissione di virus in rete, truffe e frodi informatiche, duplicazione e traffico illecito di software, risulterebbe il medesimo totale legato alla percezione della figura del cracker.

Lo svolgimento di queste operazioni porta ad una percentuale d'attività, legata all'hacker, del 40,8%, identica a quella che si ottiene sommando le prime due caratteristiche "positive" riferite allo stesso soggetto, cioè astuzia e curiosità, nella domanda sulle possibili origini del suo comportamento. Si suppone dunque che vi sia una connessione molto netta tra le caratteristiche d'astuzia e curiosità e le attività di accesso abusivo, intercettazione abusiva e detenzione e diffusione illegali di codici

d'accesso, tutte interne ad una visione dell'hacker come uno "spione telematico" che scarica i costi delle sue connessioni su malcapitate aziende e società.

Figura 10 **L'hacker ed il cracker visti dalla rete**

Hacker		***Cracker***	
Attività legate al soggetto	***%***	***Attività legate al soggetto***	***%***
Accesso abusivo	33,33	Danneggiamento informatico	15,73
Intercettazione abusiva	4,53	Creazione/immissione virus in rete	12
Detenzione e diffusione illegale di codici d'accesso	2,93	Truffe e frodi informatiche	15,46
		Duplicazione e traffico illecito di software	6,13
Totale	40,79	Totale[8]	49,32

Fonte: nostra elaborazione dati della ricerca.

Il totale relativo all'operato del cracker, invece, raggiunge il 49,3% inglobando al suo interno le figure dell'insider e del courier (all'interno di quest'ultima, con un po' d'azzardo, potremmo inserire tutte le sotto-figure legate al mondo del warez). Tale totale, molto vicino al 50,1% di chi reputa giusta la pena prevista per l'accesso abusivo, fa sorgere il dubbio che, in realtà, la figura realmente temuta non sia l'hacker, ma una sorta di criminale informatico dedito a danneggiamenti, infezioni via virus, organizzazione di truffe e frodi, diffusione illecita di software, erroneamente sovrapposto alla figura dell'hacker a causa della confusione fatta sull'uso di questo termine.

Tale ipotesi è suffragata anche dal possibile totale derivato, alla terza domanda, dalla somma delle caratteristiche più negative dell'hacker, cioè

[8] Questo totale considera, sotto la voce "cracker", tutte quelle attività a forte valenza negativa che vanno oltre l'accesso abusivo, ed ingloba al suo interno anche le figure dell'insider, del lamer e le sotto-figure legate al mondo warez.

aggressività, eccesso di protagonismo e mancanza di rispetto, la cui percentuale si avvicina al 44%, più alta rispetto al 40,8% legata ad astuzia e curiosità. La stessa relazione logica “pericolosità della figura/giudizio sulla pena” è applicabile anche con un procedimento inverso. Infatti, sommando la percentuale di quanti (sesta domanda) trovano il fenomeno hacker in calo, si ottiene il 26,4%, percentuale non a caso uguale a quella che giudica eccessiva la pena per il semplice abuso d’accesso.

Una diversa scomposizione e classificazione, che volesse contemplare tutte le diverse figure del lato oscuro del Web utilizzando i dati forniti dalla ricerca, vedrebbe l’hacker con una percentuale del 33,3% (accesso abusivo), stretta parente del 28,8% che si riferisce alla sua innata curiosità; il cracker al 27,7% (danneggiamento e creazione e diffusione di virus), anche questo non lontano dal 26,7% che ne caratterizza aggressività ed eccesso di protagonismo; l’insider al 18,4% (truffe e frodi informatiche, diffusione illegale di codici d’accesso), conseguenza del 18,9% legato alla sua mancanza di rispetto vero gli altri, tipica di questa figura e dei suoi difficili rapporti con i suoi datori di lavoro.

Figura 11 **L’insieme delle figure caratteristiche**

Figura	%	Caratteristiche	%
Hacker	33,3	Curiosità	28,8
Cracker	27,7	Aggressività ed eccesso di protagonismo	26,7
Insider	18,4	Mancanza di rispetto verso gli altri	18,9
Mondo Warez	6,1	Le precedenti, ma in minore concentrazione	/

Fonte: nostra elaborazione dati della ricerca.

Le diverse figure legate al mondo warez (courier, supplier…) si spartiscono il restante 6,1% legato al traffico illecito di software, per il quale occorrono probabilmente un po’ tutte le caratteristiche precedentemente citate, ma in minore concentrazione.

Tale incrocio di dati, unito ad una scomposizione percentuale piuttosto elevata con ben quattro risposte uguali o superiori al 12% (non a caso lo stesso avviene solo nella domanda sulla relazione caratteristiche-comportamento, mentre il quesito sulla pena per l'accesso abusivo vi si avvicina), sembrerebbe dimostrare che il campione ha recepito un'eterogeneità all'interno dell'insieme di comportamenti definito "hacking", ed è in grado di riconoscere tale differenziazione collegandola alle diverse caratteristiche comportamentali. Nonostante ciò, persiste un elevato timore del fenomeno, confermato anche dalla visione d'alcuni "addetti ai lavori", le cui interviste sono state riportate nel prossimo capitolo.

7. Tracce socio-telematiche: il vissuto dei protagonisti

"Pensi ancora che la colpa sia tutta mia?"
Dall'intervista on-line con
Raoul Chiesa (vedi allegati).

Esaminato il responso della rete, chiarita la percezione del fenomeno all'interno dell'immaginario collettivo di molti utenti direttamente coinvolti e non, l'obiettivo di questo capitolo è dar voce ai modem, alle tastiere, alle esperienze di chi vive quotidianamente il contesto "hacker". Quest'ultimo viaggio nell'universo del ***Web oscuro*** cercherà di far luce sui diversi momenti di una realtà in evoluzione, pulsante di dinamiche legate ad un contesto - l'Information Technology - che, per sua natura, sfugge ad un'analisi troppo ristretta nel tempo.

Durante questo lavoro, consci della difficoltà e della parzialità del metodo, si sono più volte tentate definizioni che aiutassero a far luce sulle diverse sfaccettature del fenomeno hacker, arrivando alla descrizione di differenti categorie, all'interno delle quali hanno stentato a ritrovarsi molti dei diretti interessati. Partendo spesso da esperienze personali, le pagine che seguono cercheranno di fare un po' d'ordine in merito, senza tuttavia privare il lettore della sensazione che tra gli stessi "addetti ai lavori" manchi una lettura univoca del fenomeno stesso.

Divergenze di lettura ed interpretazione dei fatti, tentativi più o meno riusciti di calarsi nei panni dei soggetti in questione, diverse esigenze legate al proprio ruolo sembrano acuire tali distanze. Tuttavia, riteniamo che la seguente analisi rappresenti il giusto tributo ad un fenomeno che vive di luce riflessa, che ha poche possibilità di farsi veramente conoscere, in quanto chi lo descrive raramente lo fa con cognizione di causa ed interpellando i diretti interessati.

7.1. Mutamenti generazionali ed aspetti significativi del fenomeno.

Coautore del testo ***Spaghetti hacker***, più volte citato all'interno di questa ricerca, Stefano Chiccarelli considera il mondo hacker troppo mitizzato dai media, accusati di basarsi su un modello americano poco reale, originato da film e notizie in grado di alimentare erroneamente l'immaginario collettivo. Questi ritiene, come accennato nei capitoli precedenti, che esista una via italiana all'hacking, gli "smanettoni", in quanto in Italia veri e propri hacker non esistono, o almeno, non nella figura di soggetti molto competenti, veri e propri programmatori dotati di grande esperienza, che vivono il loro lavoro in maniera molto viscerale[1].

Lo smanettone viene considerato un autodidatta, simile all'hacker nel suo approccio compulsivo alla macchina, ma dotato di minori capacità di programmazione e privo di gran genialità, solo in parte compensata da curiosità ed amore per la tecnologia. Chiccarelli ritiene che il tempo abbia assistito al succedersi di diverse generazioni di smanettoni, e che la principale differenza tra quest'ultima e le precedenti risieda nella mancanza d'ideologia.

Le intrusioni, al giorno d'oggi, non avrebbero più un valore etico, culturale, ma sarebbero solo una dimostrazione d'esibizionismo. Pur non potendo generalizzare, l'autore è convinto che manchi un progetto culturale di base, una politica comune, per questo non ha accettato la tendenza tutta italiana ad accomunare le realtà antagoniste al mondo dell'hacking, privo a suo dire di qualunque politicizzazione, ed unito solo nella passione per la tecnologia e la libera circolazione delle informazioni.

Riguardo alla possibile evoluzione di tale fenomeno in Italia, nel prossimo futuro, Chiccarelli spera che l'hacking sia capito, che la cultura della rete si espanda, rendendo note a tutti le differenze tra le varie figure che la popolano. Le aziende si renderanno sempre più conto dell'esigenza di sicurezza nello stare in rete, si creerà una cultura della "system security" e non ci saranno più innocenti immolati in nome della paura della rete.

[1] Vedi cap.2, nota n.27.

Di diverso avviso è il magistrato romano Giuseppe Corasaniti, uno dei maggiori esperti nel settore dei reati informatici, il quale giudica l'hacker come una figura di passaggio all'interno del panorama tecnologico italiano. Oggi, per un ragazzo di buona cultura informatica, non è difficile, ad esempio, "agganciare" un numero verde ed usarlo per fini illeciti, ma con dei controlli appropriati la quantità di queste bravate diminuirebbe sicuramente.

Tale figura non va mitizzata né sovraesposta, tuttavia, difficilmente troverà spazio nella rete globale se non imparerà ad accettare ed a rispettare regole ed interessi altrui. Il magistrato ama immaginare la rete come una grande autostrada dove tutti dovranno poter circolare, dove non potrà essere possibile tenere la velocità che si vuole solo per soddisfare il proprio piacere di guida e la propria libertà di movimento, e per la quale si dovranno dettare norme coerenti ed utili alla sicurezza di tutti, hacker e non.

Raoul Chiesa[2] riscontra una diversità enorme, di pensiero e d'azione, tra gli hacker dell'ultima generazione (a grandi linee dal '96 in poi) e la sua (fine anni '80). Oggi, girando in chat, dice di imbattersi frequentemente in ragazzini che, "parlando in chiaro" (senza usare sistemi di crittografia), si spacciano per hacker, scambiano codici, si vantano di aver "bucato" quel tale sito, senza sapere realmente di cosa parlano, senza conoscere tutto il background che tale fenomeno possiede, senza certezze sui loro interlocutori.

Chiesa, per approfondire tale differenza d'approccio, ricorda il citato "Hack-it98"[3] ed il diverso modo di viverlo da parte dei "vecchi" e dei "nuovi" hacker: durante le navigazioni on-line, i primi erano in disparte, più silenziosi, utilizzavano la rete come un mezzo per raggiungere importanti mainframe, non come uno scopo, e cercavano di evitare accuratamente pubblicità e spazzatura. I più giovani, noti come

[2] Arrestato nel 1995 in seguito alla famosa operazione "Ice-Trap" (vedi cap.3, par.2), oggi esperto di sicurezza e collaboratore del team di Mediaservice (www.mediaservice.net), Raoul Chiesa è forse il mito di un'intera generazione di hacker italiani. Le sue esperienze lo hanno portato ad essere un profondo conoscitore di tale mondo, nonché ad interpretare questo ruolo in prima persona, fino ad ammettere che essere hacker lo ha indubbiamente cresciuto, istruito, fornito di uno stile di vita, di particolarità e caratteristiche che ama ritrovare in altri come lui. Ridimensionati i numerosi capi d'accusa (eversione, associazione a delinquere, ricettazione, duplicazione illecita di software, clonazione di carte telefoniche, utilizzo abusivo di numeri verdi per collegamenti alla rete) in seguito al patteggiamento cui è stato costretto, oggi non è raro trovare on-line articoli e commenti che lo riguardano, nei quali non esita a prendere posizione per una diversa lettura del fenomeno rispetto a quella attuata dai media.

[3] Vedi cap.2, par.5.

newbies, parlavano invece liberamente, giravano, si vantavano, rendevano pubblica ogni loro conoscenza (o presunta tale) ed esperienza su come penetrare nei sistemi.

Ad “Hack-it98”, si è saputo dopo, c’erano anche agenti di polizia in borghese, ai quali non sarà certo sfuggito tutto questo parlare di codici e sistemi bucati, anche se la vecchia guardia, fedele al concetto “io so e sto zitto”, è riuscita a dare molto poco nell’occhio. Volendo utilizzare i concetti espressi nella ricerca[4], Chiesa vede gli hacker odierni più portati verso aggressività ed eccesso di protagonismo, mancanza di rispetto e danneggiamento informatico, mentre ai suoi tempi le caratteristiche più salienti erano astuzia e curiosità, accesso abusivo e detenzione illegale di codici d’accesso.

Di fronte ai concetti espressi dal magistrato Corasaniti, Chiesa non può naturalmente essere d’accordo, e li giudica un’assurdità: “E’ vero - egli dice - che gli hacker stanno diventando dei miti, ma tale trend andrà a terminare, ed oggi porta più svantaggi che vantaggi al fenomeno in questione”[5]. A suo avviso gli hacker sono dei pionieri, senza di loro un sistema operativo come LINUX non si sarebbe mai sviluppato né diffuso come ai giorni nostri, non saranno mai una figura di passaggio perché, dagli albori dell’informatica ad oggi, vi sono sempre stati.

“I primi - prosegue Chiesa – hanno gettato le fondamenta di luoghi come il MIT[6], hanno usato Arpanet quando c’erano quattro nodi, sempre spinti dalla voglia di conoscere più a fondo la rete ed i suoi segreti. L’hacker non vuole che la rete sia imprigionata da regole ed interessi, lo vogliono la “giustizia” ed il “mercato”, ma qualunque cosa questi ultimi useranno per aumentare le verifiche di sicurezza, saranno sempre delle cose informatiche. Come tali, l’hacker le aprirà e le capirà, e difficilmente ne resterà imbrigliato. La vera rovina della rete sono, e saranno, i diversi interessi che la stanno raggiungendo, soprattutto d’origine economica”[7].

Tony Mobily si considera un ex-hacker, dice di aver perso quella spinta che lo portava ad essere molto curioso, di aver mantenuto sostanzialmente tutte le capacità necessarie, tranne la volontà di farlo. Dall’Australia - dove oggi vive e lavora

[4] Vedi capitoli 5 e 6.
[5] Cfr.: allegato n.1.
[6] Vedi cap.2.1
[7] Cfr.: allegato n.1.

configurando server ed installando diversi programmi - rivela che ha potuto costatare l'assenza di particolari caratteristiche legate ad hacker di diversi paesi, e che vi è una netta differenza tra l'hacker e l'eroe immaginario che oscura la sua figura reale. I film, a suo avviso, non riescono mai a rendere la reale sensazione che prova un hacker ad esplorare un sistema:

> "Un esempio: un root si connette proprio in quel momento, mentre sei dentro con la password di un'altra persona, e ti sbatte una richiesta di talk, e quando ci parli ti chiede come stai, se hai risolto il problema del cane dal veterinario, ecc… E mentre tu ti rendi conto che l'utente cui hai fregato la password era un amico stretto del root, il root realizza che tu non sei quella persona… Questa è un'avventura, una cosa che ti carica d'adrenalina, una sfida che senti di poter vincere, una cosa che ci metterai due ore a raccontarla, ed a dire ai tuoi amici come tu sia riuscito a farglielo credere…Ma che in un film, semplicemente, non renderebbe l'idea"[8].

Prendendo in esame la recente produzione cinematografica, l'unico film che è riuscito ad avvicinarsi all'argomento, a suo avviso, è stato ***Nirvana*** di G. Salvatores, un'opera piena di riferimenti che soltanto un programmatore, o comunque un esperto di computer, ha potuto realmente capire.

Manlio Cammarata - noto giornalista ed esperto conoscitore di cultura telematica - giudica il fenomeno hacker molto variegato e sfuggente, e diffida dal tentativo di relegarlo in definizioni o classificazioni d'alcun genere. Egli ritiene la "pirateria telematica" (anche se, afferma, molti hacker si ribelleranno a questa definizione) come una "manifestazione di disagio psicologico e sociale che trova sbocco nell'attività in rete, piuttosto che in manifestazioni fisiche"[9]. Interrogato a proposito degli aspetti più significativi del fenomeno, egli ha citato la tendenza all'associazione segreta, al riconoscimento di capi carismatici, alla convinzione di agire per una nobile causa ed alla contestazione dell'ordine costituito.

Di fronte a tali aspetti, le reazioni dei partecipanti al fenomeno possono essere di tipo diverso, a seconda delle loro esperienze precedenti. Chiesa, ad esempio, le contesta, sottolineando quanta poca conoscenza del fenomeno esse implicano, e dando di questi "loschi figuri" una raffigurazione più umana:

[8] Cfr.: allegato n.1.
[9] Cfr.: allegato n.1.

> "Se tu fossi stato ad Hack-it98, avresti visto questi "loschi figuri" con un notebook appoggiato su un piano di legno, che stava in piedi per miracolo, con una connessione ISDN a 64Kper c.ca 80 persone, con i cavi per terra che appena c'inciampavi su non funzionava più nulla, a bere birre e rollare cannoni…parlando di hacking, security, Web…, insegnando ai ragazzini di Firenze, che passavano di lì per caso, di cosa si trattava, e cercando di fare cultura…senza interessi economici di parte"[10].

Tony Mobily, invece, si ritiene in accordo con la disamina di Cammarata, della quale cerca di approfondire alcuni punti. L'associazionismo si può ritenere comune in quanto è tale lo stare con persone che abbiano interessi e passioni simili, e questa reazione l'hacking l'ha sempre creata. Più che dei capi carismatici, in questi gruppi si finisce per avere dei "miti", dei "modelli" che si desidera raggiungere. La "giusta causa" dipende dalle persone: per Mobily sapere che un sistema, a seguito di una sua violazione e della successiva mail al root, sarebbe stato più sicuro, era piacevole, ma non era la ragione principale del suo gesto. L'immaginario collettivo agisce fortemente su tali descrizioni, tuttavia egli dice di non vedervi nulla di negativo.

Approfondendo il rapporto tra la rete e gli smanettoni, Tony Mobily non crede che il mezzo in questione possa essere fonte di una maggiore o minore aggregazione, lo ritiene solo un nuovo media da sfruttare, il cui uso dipenderà sempre e solo dall'utente, dalle sue attitudini personali, le stesse che influenzano la "famosa" etica hacker. Alla base di tale etica non vede caratteristiche psicologiche e comportamentali comuni, ideali e linee guida valide per tutti, ma una serie d'ingredienti fondamentali che, ben mescolati, possono portare una persona a fare esperienze di hacking.

Consapevole del rischio di dimenticarne qualcuno, egli ne cita una serie, ricordando che ognuna di queste qualità ha un intero mondo alle spalle: il fascino verso i computer e la voglia di passarvi del tempo davanti, la curiosità di sapere come sia possibile violarli, la disponibilità ad imparare e scoprire nuove tecniche e particolarità, la perseveranza, la volontà di fare qualcosa di proibito. Non essendo mai venuto in contatto con un'etica diffusa, Tony Mobily ha scoperto di averne una sua: bucare i sistemi, usarli magari per un po', e poi mandare una mail all'amministratore di sistema dicendogli di chiudere il bug. Egli ritiene impossibile

[10] Cfr.: allegato n.1.

tracciare una linea che separi persone etiche e non etiche, in quanto diversi gruppi di persone hanno differenti interessi, e non è possibile generalizzare[11].

Diverso è l'approccio al fenomeno da parte del suo principale antagonista, la polizia telematica, che ci ha fornito un quadro critico e completo al riguardo. Questo particolare corpo di polizia definisce genericamente come hacker colui che si diletta a cercare buchi nei sistemi informatici, al fine di accedervi ed avere il possesso dei dati in essi contenuti. Chi entra in questo mondo, secondo tale quadro psicologico, è spinto dal bisogno di fare nuove esperienze, si lega ai suoi compagni attraverso dei fili "telematici" che non lo faranno mai sentire solo, ma sempre partecipe di una realtà in grado di collegare la sua azione a quelle d'altri soggetti. Quasi tutti i pirati informatici, difatti, comunicano tra loro attraverso BBS, che in alcuni casi consentono o agevolano condotte punite dalla normativa in vigore, e che non servono solo a scambiare programmi pirata ma anche idee, opinioni e sfide.

Per loro la sfida al mondo dei "grandi", finalmente vulnerabile, è troppo allettante per non essere raccolta. Ancora più gratificante è il fatto che, con apparecchiature di bassissimo costo, riescano spesso a mettere in scacco sistemi che valgono decine o centinaia di milioni. In tal modo, iniziando da un'azione che mantiene il suo aspetto ludico anche se compiuta con uno strumento "da grandi", essi si sentono intelligenti, dimostrano a loro stessi di saper "battere" il mondo degli adulti, riescono a soddisfare una serie di bisogni legati alla loro età.

L'indagine psicologica della polizia individua tali bisogni nel fare nuove esperienze, nel ricevere riconoscimenti da parte degli adulti, nel liberare il proprio protagonismo e nel dimostrarsi più in gamba di tutti gli altri coetanei. Chi decide di entrare a far parte di questo universo non sembra iniziare le proprie esperienze d'intrusione casualmente, da un livello "zero", ma da quello più alto raggiunto dai colleghi, e seguendo lo stesso principio decide di mettere tutti gli altri al corrente dei risultati raggiunti.

Nonostante non ami molto parlare del proprio passato, se interpellato in merito all'etica hacker ed alle origini di certi comportamenti, R. Chiesa affermerà che

[11] "Quando parliamo di hacker non stiamo parlando di persone che si riuniscono per decidere cosa è giusto e cosa non lo è, tutto è vissuto in maniera fortemente individuale". Cfr.: allegato n.1.

alla base di ciò vi sono delle carenze, dei disagi psichici e sociali, e che qualunque etica si baserà, prima d'incontrare la tastiera, sull'origine socioculturale del soggetto e sulla sua formazione. I migliori hacker da lui conosciuti vengono descritti come delle persone strane, chiuse, solitarie, curiose ed intelligenti, per i quali l'hacking diventava una specie di droga, un isolarsi scegliendo "quella parte di mondo che ti accetta senza pregiudizi, che ti capisce, che ti ascolta". Persone rapite dalla conoscenza, dal sentirsi "diversi", dalla sfida, "che genera un'esaltazione interiore difficile da gestire".

Chiesa professa di essere sempre rimasto fedele ad una sua etica molto precisa, che ci tiene a rimarcare:

- mai far danni al sistema se non strettamente necessario, per evitare pericoli a te o ad altri di cui t'importa;
- rispettare, curare ed ottimizzare, dove possibile, il sistema che violi;
- mai far danni a singoli individui (privati ed utenze finali);
- rispettare il lavoro sistemistico altrui;
- se un sistema si dimostra realmente protetto (es. banner d'avvertimento, barriere particolari) rinunciare ad entrarvi.

"La rete - continua l'hacker - è il vero fenomeno d'aggregazione di questo fine millennio, può portare ad una diversa reazione solo in chi ha paura di confrontarsi, d'imparare. E' assurdo accusare Internet di far perdere alle persone il loro amore per la lettura e la scrittura, scaricare su di essa la nostra paura della globalizzazione. Il vero hacker non avrà mai di questi timori, userà la rete per formarsi quel background che si acquista solo con l'esperienza diretta, perché alla fine diviene una vera e propria ***forma mentis***, e non si può insegnare[12]".

Di fronte alle accuse d'imborghesimento che iniziano a colpire il fenomeno[13], Chiesa ha le idee molto chiare:

> "Allora… di base, un hacker hackera, e ha nel cuore il sogno (specie da ragazzino) di venir assunto da un grande per fare quello che sa fare meglio: bucare e di conseguenza proteggere. Era anche il mio sogno, e di molto di noi, prima di arrivare alla fase di piena maturità che io chiamo "lo stato". Solo che le aziende non si fidano degli hacker, non si pongono il problema della sicurezza informatica, e se lo fanno non l'affidano a te, ragazzino hacker, ma a professionisti per centinaia di milioni, quando tu ragazzino hacker con lo spirito pulito, lo faresti – meglio – per un decimo di quella somma, ringraziando a

[12] Cfr.: allegato n.1.
[13] Cfr.: allegato n.1.

> vita e "uccidendo" chiunque provasse a toccare quel sistema. Perché lo ami e lo rispetti, ti hanno dato una possibilità e tu te la giochi bene… Chi ha iniziato prima di me (gli albori, ITAPAC con la numerazione corta, era l'85, credo, io ho iniziato a cavallo tra l'86 e l'87), ad esempio i DTE222[14], o quelli dell'hacking a MC-Link, oggi sono i system manager di Flashnet S.p.A., oppure i più vecchi sono responsabili di sicurezza (e lo sanno fare) presso multinazionali farmaceutiche e banche…Gli altri, quelli come me, si sono divisi dalla parte lavorativa…io con le mie idee "strane e pazze", altri presso Telecom, Istituti, Università, sempre con compiti molto delicati, in possesso di quelle informazioni che solo 3-4 anni prima ci costavano notti e notti di lavoro (non autorizzato) per entrarne in possesso. Ma io continuo a sentirmi un hacker dentro, perché per me questo vuol dire libertà, sfida, essere più bravi, anche se adesso per me l'hacking è diventato un lavoro. Lo faccio per rendere i sistemi più sicuri, non per dimostrare che non lo sono. Gli ultimi, i newbies, continuano a sognare il posto nella grande azienda come sistemista, o il posto come system manager presso il provider Internet medio-piccolo, ed intanto spesso fanno danni senza saperlo. Io ho preso diversi ragazzi, hacker newbies, e li ho portati su quella che chiamo "retta via", insegnando loro gli obblighi morali che, per me, anche l'hacker ha"[15].

La tematica dell'imborghesimento ha destato un notevole interesse anche in Mobily, il quale giudica il sogno di non pochi hacker quello di essere pagati per fare ciò che è sempre piaciuto loro: "…stare davanti al computer e bucare gli altri". Tuttavia, avverte l'ex-hacker, è "un sogno che raramente si realizza, perché gestire la sicurezza di una ditta è una responsabilità importante, diventa consulenza, ed ha delle dinamiche particolari e contorte". Ci sono altri ex-hacker, da lui conosciuti, che oggi fanno i consulenti ed hanno scoperto quanto ciò sia difficile, ma continuano a farlo usando le loro abilità fino a perdere, forse, la definizione di hacker secondo il senso comune del termine. In realtà, conclude l'ex-hacker sull'imborghesimento, "l'essere hacker alla fine resta sempre, e spesso riemerge…dopo le ore lavorative"[16].

Aver superato la fase più acuta, aver mantenuto certe conoscenze perdendo l'assuefazione allo schermo, quella che ti fa considerare il computer un "angolino sicuro" nel quale rifugiarti, può essere considerata un'evoluzione dell'hacker verso un uso differente della rete. Mobily considera Internet una vera rivoluzione, uno strumento di cui non tutti hanno capito le grandi potenzialità, a partire dall'incredibile quantità d'informazioni disponibili. Pienamente consapevole delle ambiguità che tali potenzialità fanno sorgere (ad esempio il problema del copyright), egli immagina che alla fine pagheremo la rete con la pubblicità, in modo simile a come funziona per la televisione: la pubblicità sarà un'abitudine che non ci porterà eccessivi fastidi e,

[14] Vedi cap.2 par.3
[15] Cfr.: allegato n.1.
[16] Cfr.: allegato n.1.

nonostante la possibilità d'ignorarla con filtri e tecniche particolari, alla fine rientrerà nel comune utilizzo del Web.

Una nuova problematica - mai affrontata prima per l'assenza di un "parallelo" con il mondo reale - è quella della libertà d'espressione in rete, tanto cara agli smanettoni d'ogni epoca. In nome di tale libertà sono state abrogate delle leggi[17], e molti utenti esperti oggi s'interrogano sulle sue possibili conseguenze. Tony Mobily considera l'argomento un grosso problema, sottolinea che qualsiasi cosa sia messa on-line può essere letta da tutti, e che trattare un argomento senza dare noia a nessuno è veramente difficile.

Sollecitato al riguardo, R. Chiesa risponde in maniera sintetica, tuttavia la sua opinione è in controtendenza rispetto al pensiero di molti suoi "colleghi". Egli si professa contrario ad un'eccessiva libertà, non perché la ritenga ingiusta - anzi rivela di considerare la trasparenza il massimo in ogni situazione - ma perché immagina la massa incapace di gestirla. "Il mondo - conclude l'hacker - ha istituzioni, leggi, barriere…immaginiamo che servano a difenderci, anche se nessuno sa bene da che cosa"[18].

Sibillino appare, sull'argomento, il parere di Manlio Cammarata secondo il quale approfondire i rapporti tra cultura, etica e tecnologia è un'operazione da lasciare ai filosofi. "Solo una cosa è chiara - conclude il giornalista - quando un comportamento è previsto come reato dal codice penale, come tale va perseguito. L'hacker, quando la legge lo prevede, deve essere inserito nelle patrie galere"[19].

[17] Vedi cap.4 nota 43.
[18] Cfr.: allegato n.1.
[19] Vedi l'intervista inserita negli allegati.

7.2. Categorie, definizioni ed “ethical hacker”.

Raoul Chiesa, interrogato in merito ad una possibile definizione di hacker, risponde con un paragone che merita di essere citato testualmente:

> “L’hacker fa l’installatore d’antifurto: li installa, ma vuole capire come funzionano. Se ne porta uno a casa, lo ruba o se lo compra, ma se lo smonta, lo simula, lo ricostruisce, e poi capisce i difetti. L’appassionato, o il professionista d’informatica, fanno anche loro gli installatori d’antifurto: aprono la scatola e installano l’antifurto. Stop”[20].

Egli ama distinguere gli hacker non tanto dai “non-hacker”, quanto da chi continua a considerare il fenomeno un passatempo per ragazzini introversi e brufolosi. Hacker come sfida, curiosità, conoscenza della psicologia e dell’animo umano, una sorta di “novel-trovatore” sempre alla ricerca di cose nuove, fare hacking come studio della mentalità del sistemista, dell’utente, del responsabile di sicurezza.

Gli altri “personaggi” del Web si differenziano in modo netto: Chiesa giudica il cracker come “colui che sprotegge il software”, vale a dire ne elimina le difese installate dalla casa produttrice e lo studia in profondità; lo smanettone come “l’individuo che studia i p.c. da anni, li modifica, si fa le sue cose ***on his own***, per questo siamo tutti un po’ smanettoni”. Ultima figura di questa categorizzazione è lo ***script kid***, ritenuto una sorta di piccolo insulto, con il quale “si apostrofa chi è solo capace di scaricare dalla rete gli script[21] ed utilizzarli per penetrare nei sistemi”[22].

Tony Mobily considera l’hacker come un programmatore con attitudini un po’ particolari, con la voglia di far eseguire al sistema le istruzioni che questi ha scritto appositamente. Volendo approfondire il termine, egli individua tre classi di soggetti: i programmatori, chi utilizza tali programmi per migliorare effettivamente la rete e chi per scopi criminali. La prima classe è formata da “un insieme di persone molto ristretto, poco visibili ai media perché quasi mai allo scoperto, dediti alla ricerca d’errori di programmazione ed alla successiva pubblicazione sia dei bachi sia dei mezzi per chiuderli”.

[20] Cfr.: allegato n.1.
[21] Particolare tipo di programma.
[22] Cfr.: allegato n.1.

La seconda classe vede al suo interno “chi usa tali programmi per andare a bucare i sistemi, facendo come me una mail al root per avvisarlo sulle carenze delle sue difese informatiche”. L’ultima classe riguarda i “cattivi della situazione, coloro che usano gli stessi programmi della seconda classe per impadronirsi di dati ed informazioni, distruggere gli originali e fare danni ai sistemi per il puro gusto di farlo”[23].

Mobily ritiene che tutte le forme, più o meno gravi, di criminalità siano legate a quest’ultima categoria di soggetti, e che in Italia manchino i mezzi per mettere in evidenza la giusta distanza che separa le ultime due classi.

L’avvocato A. Monti, esperto del settore e coautore, assieme a S. Chiccarelli, del testo “Spaghetti hacker”, sostiene che tale termine non abbia mai voluto significare estremista in lotta contro il sistema, né delinquente di professione. In Italia, a suo avviso, non vi sono mai stati dei veri e propri criminali, solo molti appassionati d’informatica che hanno spesso approfittato di tutta la libertà concessa loro. Anch’egli, come Mobily in precedenza, rileva che nel nostro paese non si considera una differenza fondamentale, tra chi entra nei sistemi “solo per curiosità, per saggiare le proprie possibilità, uscendone senza aver toccato niente, e chi lo fa per creare danno o per ricavarne profitto”[24].

Di diverso avviso figurano Cammarata e Corasaniti, più preoccupati dal fenomeno e dai suoi effetti incontrollati. Il primo, dalle pagine on-line del sito www.interlex.com, ha più volte messo in guardia contro gli eccessi delle libertà telematiche, cercando di evidenziarne i rischi e le possibili ripercussioni. Gli hacker, secondo il suo parere, sono soggetti con la tendenza a commettere atti illeciti, molto pericolosi, e come tali devono subire una repressione atta a spingerli ad usare altre vie per far valere le proprie ragioni. Il rischio, causato da un’erronea interpretazione della libertà d’informazione, é di “consentire a chiunque di frugare nelle nostre tasche, nei nostri cassetti, di forzare la nostra porta di casa solo per informarsi di cosa c’è dentro”[25].

[23] Cfr.: allegato n.1.
[24] Cfr.: allegato n.1.
[25] Cfr.: allegato n.1.

Anche il magistrato Corasaniti individua, nella precarietà del rapporto libertà-sicurezza, la chiave di lettura di un difficile futuro per la rete globale delle comunicazioni. Egli accusa gli hacker di una mancanza di consapevolezza verso le conseguenze dei propri gesti, descrivendoli come soggetti poco inclini a valutare che "anche un gesto innocente come l'intrusione (e magari la copia dei dati) può fare danni eccome a chi li deteneva legittimamente, causando pregiudizio ad attività personali o economiche"[26].

Tale tematica appare fondamentale nella disamina del comportamento in questione: molti hacker, infatti, riducono il loro operato all'invio schiacciato per far partire un programma, al tasto spinto per entrare nel sistema, ed alla fine si smarriscono se messi di fronte alla propria responsabilità. Interrogato al riguardo, Chiesa considera tali soggetti dei newbies, e ci tiene a ricordare che:

> "Io hackero con l'intenzione di farlo, di entrare, di capire chi è quell'azienda, cosa fa, che reti adopera, di cosa si occupa, in che regione si trova, provo i cognomi comuni, guardo le ditte intorno, controllo in borsa con chi hanno partnership…il mio hacking è intenzionale, non mi limito a premere un tasto, anzi. Sono comunque d'accordo ad accusare l'hacker, spesso, di mancanza di rispetto e d'eccesso di protagonismo…a patto di accusare, della stessa mancanza di rispetto verso la propria azienda, il sistemista che non si protegge…punti di vista.(…) La gente comune si sente derubata della propria privacy se un hacker gli spia le mail, senza sapere che pochissimi hacker lo fanno perché non ce ne frega nulla, e c'è altro da fare di più carino che leggersi le mail altrui. Oltre a ciò io per primo considero le mail una cosa assolutamente riservata e personale, e divento nero se vedo persone spiare una mail altrui"[27].

Tony Mobily ritiene che spesso, mentre si fa hacking, non ci si rende conto di quello che si fa. Egli rivela di aver fatto dei danni una sola volta, per sbaglio, alcuni anni fa, finendo con il distruggere una directory piena di programmi. Il sapere che le sue azioni erano illegali, ammette, lo ha portato ad una tale condizione di stress da temere che potessero rintracciarlo e confiscargli il computer. Anche se oggi non crede di aver mai raggiunto un tale livello di "pericolosità", ammette:

> "So praticamente per certo che la polizia ha un nastro con una conversazione telefonica tra me ed un hacker, in cui parlavamo veramente di tutto…ma so anche per certo che quel nastro è stato archiviato. Quella telefonata, tra le altre cose, e lo stress che ho vissuto quando ho saputo che la polizia sapeva cosa avevo detto, è stato un motivo di gran

[26] Cfr.: allegato n.1.
[27] Cfr.: allegato n.1.

> riflessione per me. Aveva la polizia il diritto di registrare i miei fatti personali? Ma potevo dimenticare d'essere "fuorilegge"? Poteva questo giustificarli? Il fatto che qualcuno stesse ascoltando mi fa sentire ancora male, tuttavia non ho trovato una risposta a queste domande…"[28]

Ma come sono considerati gli hacker da parte della polizia telematica? Maria Cristina Ascenzi[29] - commissario capo di Pubblica Sicurezza e direttrice del NOPT - non è d'accordo con la definizione di "smanettoni", in quanto ritiene che molti utilizzino le capacità acquisite per azioni criminali, con il rischio "della solita indulgenza italiana per fatti gravi e pericolosi". Ella descrive lo scenario di questi ultimi anni costatando il calo degli accessi abusivi a grandi sistemi informatici, che un tempo rappresentavano il crimine principale, in quanto tali sistemi stanno cominciando a proteggersi, alcuni anche assumendo hacker ed utilizzando la crittografia[30].

Oggi, gli elaboratori che subiscono la maggior parte degli accessi non autorizzati, appartengono prevalentemente a privati o a piccole imprese, che non considerano la necessità di sicurezza in rete, preferendo affidarsi a compagnie assicuratrici che coprono eventuali danni economici causati da intrusioni abusive. "Una volta - termina l'Ascenzi - gli hacker erano meno furbi e ci sottovalutavano, arrivavano a parlarsi al telefono senza pensare minimamente di poter essere intercettati; oggi in Italia i veri hacker sono meno di un centinaio, gli altri sono lamer[31] che rubano le telefonate gratis per collegarsi alla rete, o copiano il software per giocare"[32].

La polizia telematica è solita inquadrare il soggetto hacker in due macro figure: l'adolescente ed il professionista. Il primo tipo, meno dannoso dal punto di vista economico e della riservatezza delle informazioni, si prefiggerebbe di superare le barriere di sicurezza solo per mettere alla prova la propria abilità, per sfruttare tutte le potenzialità dei sistemi, scaricando su utenti ignari il costo delle connessioni. Da questa figura è nata la definizione di "criminalità dei pantaloncini corti". Il secondo ha

[28] Cfr.: allegato n.1.
[29] Vedi cap.3, par.4.
[30] Vedi cap.4, par.5.
[31] Vedi cap.3, par.1.
[32] Vedi l'articolo ***Guardie e ladri***, di A. Masera, dal settimanale "Panorama Web" n°4, del 28/1/'99, pag.39.

come intento la violazione di un sistema informatico contenente informazioni riservate, per appropriarsene a diversi fini.

Individuata tale iniziale suddivisione, l'analisi psicologica operata dalla polizia approfondisce i diversi soggetti. Sulla base di quest'ultima si suppone che l'hacker adolescente svilupperebbe diversi comportamenti secondo altre variabili caratteriali, ad esempio, di tipo relazionale. I soggetti più introversi utilizzerebbero il computer come "finestra" verso il mondo esterno, raggiungendo forme di contatto ossessivo con il mezzo informatico[33].

I soggetti più estroversi, invece, potrebbero arrivare ad usare le proprie competenze tecniche per divenire leader di gruppi o per farsi assumere all'interno di società da loro precedentemente violate. L'hacker estroverso amerebbe inoltre rilasciare interviste, dialogare in tema di sicurezza, disinformazione ed incompetenza all'interno delle reti. Anche se con azioni singole o sporadiche, gli hacker adolescenti seguirebbero regole non scritte, che darebbero loro modo di attenersi ad una stessa linea di comportamento. Ultima sotto-categoria, interna a questa prima tipologia, è quella degli hacker "politici", coloro che lasciano nei sistemi messaggi di tipo ambientale o politico, o virus[34] dedicati ad argomenti similari. Al di là di tali particolari connotazioni, nei comportamenti di questi soggetti la polizia è solita individuare bisogni di leadership e protagonismo.

Più difficile, per le stesse forze dell'ordine, distinguere in via generale le motivazioni dell'hacker che si limita ad entrare in un sistema ed a comportarsi come ospite, da quelle più aggressive e dannose. Le situazioni più facilmente analizzabili sembrerebbero quella dell'impiegato licenziato, di colui che ha effettuato un colloquio di lavoro con esito negativo, o di chi utilizza le proprie capacità a scopo di lucro. Tutte queste motivazioni appartengono alla seconda tipologia precedentemente citata, quella dell'hacker professionista, vero obiettivo delle indagini informatiche.

[33] Ad esempio il non poterlo vedere spento ed il dover controllare, molto frequentemente, le BBS con cui si è soliti dialogare, per vedere se contengono nuovi messaggi.
[34] Come il "Cossiga Virus", il quale contiene scritte contro l'ex-presidente programmate ad apparire sul monitor ad una certa data.

All'interno di tale categoria figura l'insider[35], una sorta di versione telematica della "white collar criminality", la criminalità dei colletti bianchi. Tale definizione indica la dimensione sommersa della criminalità, quella parte di reati commessi da persone rispettabili nel corso della loro occupazione. In questi casi, la polizia attribuisce al crimine un significato profondamente diverso da quello tradizionale, descrivendo un'attività fortemente differenziata e non più relativa ad una minoranza deviante, ma ad una maggioranza considerata "normale".

Tale analisi psicologica sembrerebbe, in verità, eccessivamente definita per un fenomeno che sfugge a tali categorizzazioni. L'ampia fascia di comportamenti (uniti alle dirette conseguenze) possibili, e l'intricato intreccio di motivazioni, contribuiscono a disegnare situazioni di difficile analisi. Noto per le sue ricerche telematiche, spesso vere e proprie "cacce all'hacker", il famoso "samurai" Shinomura ha sintetizzato così un pensiero comune a molti: "Il maggior crimine di un hacker non è tanto il reato commesso in sé, quanto il contribuire a far nascere un clima di diffidenza verso le tecnologie della rete"[36].

Punti sul vivo da tale affermazione, che li inquadra come attori sociali negativi all'interno del sistema da loro scelto come ambiente "naturale", gli hacker non hanno tardato a ribellarsi. Chiesa non nasconde la propria amarezza:

> "Dico che è il contrario, che sono aziende come Microsoft a far crescere un clima ed un'opinione generale di "falsa sicurezza", quando in realtà sviluppano e sommergono il mondo di prodotti altamente sicuri ed inaffidabili. Sono stati gli hackers a sviluppare Arpanet e a farla diventare Internet. I primi system manager dei primi .edu. che ricevettero le connessioni dedicate ad Internet, giravano sui precursori di Altos e di Qsd. Oggi i migliori security men sono ex-hacker. (…) L'IBM ha utilizzato hacker di cui si fidava per verificare che, su 10 sistemi con on-line payment, 9 erano bucabili. In questi 9 sistemi ci sono le tue e le mie carte di credito. Se non li bucava un hacker, come lo sapevamo io e te che le nostre CC potevano essere rubate?"[37]

Tony Mobily, nonostante l'ammissione di aver perso la curiosità di un tempo, dimostra di aver mantenuto quello spirito e di considerare l'affermazione di Shinomura:

[35] Vedi cap.3. par.1.
[36] Cfr.: allegato n.1.
[37] Cfr.: allegato n.1.

> "…una pura idiozia. Le persone **dovrebbero** essere informate dei rischi della tecnologia. Devono sapere che, se mettono i loro dati on-line, un hacker può entrare e rubare tutto, distruggerli, ridistribuirli. (…) Cosa dovremmo fare? Chiudere gli occhi e far finta che i computer siano **sicuri**? O, peggio ancora, mettere in galera gli hacker perché fanno scoprire alle persone che in Internet nulla è chiuso a chiave? E' come voler mettere in galera le persone che dicono a tutti che il governo è corrotto… Bisognerebbe, invece, rendere consapevoli le persone delle insidie di un mondo, quello dell'Internet, in cui la stragrande maggioranza dei server può essere bucato in meno di quindici minuti, a causa della svogliatezza e dell'ignoranza dei "sysadmin". I dati importanti vanno in un hard disk _non_ connesso alla rete, a meno che non ti possa fidare **ciecamente** del tuo provider. Punto. Non so se questa cosa cambierà in futuro. Per ora è così"[38].

Chiccarelli, nella sua posizione d'esperto del settore, non si discosta dalle affermazioni appena citate. Lungi dall'addossare agli hacker alcun tipo di colpe, egli non pensa che essi abbiano potuto influenzare negativamente la rete, anzi si ritiene convinto che essi abbiano "fatto" la stessa. Le insicurezze del sistema, a suo avviso, non sarebbero dovute agli smanettoni ma alla rete, che si trova ad un punto d'evoluzione tale da non riuscirne a garantire la propria sicurezza.

Negli ultimi mesi[39] è andato "in onda", sul sito www.interlex.com, un interessante scambio d'articoli, contenenti commenti ed opinioni personali in merito alla partecipazione di gruppi hacker alle ricerche anti-pedofilia in rete, alle tecniche usate ed al rischio legato alle azioni di questi "vigilantes" telematici[40]. Rinviando alla lettura degli articoli stessi chi volesse approfondire la questione, rileviamo in breve che l'avv. Monti si è dimostrato molto preoccupato per l'emergere di tali associazioni di "ethical hacker", che dichiarano esplicitamente di voler effettuare "…azioni dirette alla commissione di una serie di reati, invocando a scusa il perseguire una giusta causa"[41].

Messi al corrente del rischio, i nostri interlocutori hanno fornito diverse impressioni. Raoul Chiesa considera tali associazioni "bande di ragazzini", e giudica rilevante il fatto che siano così a caccia di pubblicità da aprire siti Web sulla loro attività, e da partecipare a scambi d'opinione in rete.

---

[38] Cfr.: allegato n.1.
[39] Tra dicembre 1998 e gennaio 1999.
[40] Si tratta dei due articoli dell'avv. A. Monti ***Hacker contro pedofili: crociata o istigazione a delinquere?*** (datato 3/12/'98) e ***Hacker contro pedofili – "Un po' di spoofing è reato"*** (11/1/'99), intervallati dalla risposta di un hacker anonimo, intitolata ***Hacker contro pedofili: l'hacker risponde*** (8/12/'98).
[41] Fonte: vedi nota precedente, in particolare il primo articolo di A. Monti.

A suo avviso, se un hacker volesse rendere un servizio alla comunità virtuale cercherebbe meno notorietà, si comporterebbe secondo la propria etica senza cercare il plauso altrui. Le collaborazioni tra hacker e forze dell'ordine, per concludere, sono senz'altro possibili, ma non verranno mai rese note.

Corasaniti punta il dito verso queste "forme d'autotutela", che ci appaiono comprensibili quando, in realtà, corrono il rischio di causare equivoci e danni. Tali associazioni, secondo il magistrato, non sarebbero mai in grado di fornire quelle garanzie che caratterizzano l'intervento della polizia e della magistratura, anche se potrebbero svolgere un compito di denuncia se fosse assegnato loro un ruolo ben definito. Tony Mobily, invece, ritiene che tali associazioni non abbiano rigorosamente nulla a che fare con il mondo dell'hacking. Formate da soggetti che, semplicemente, hanno in comune di "non sopportare tutti la stessa cosa", l'ex-hacker le giudica tollerabili in quanto "… per ogni cosa tu faccia, a parte collezionare trenini, ci sarà sempre qualcuno che storce il naso"[42].

Ma la polizia come considera tali hacker "buoni"? Secondo quali modalità gestisce i rapporti con l'utenza privata della rete, organizzata sotto forma d'associazione o meno, quando quest'ultima segnala situazioni anomale o siti "sospetti"? Tali rapporti sono multiformi, svariando dal contatto con il privato cittadino che riceve al proprio indirizzo e-mail, inconsapevolmente, offerte di foto pornografiche, alla società commerciale che segnala genericamente l'indebito utilizzo del proprio account, sino ad arrivare a strutture pubbliche che hanno patito un attacco al proprio sistema informativo.

Sino ad ora, sia per le dimensioni del fenomeno sia per ovvi motivi di riservatezza, la Polizia di Stato non ha diffuso indirizzi di posta elettronica cui segnalare eventuali reati commessi con l'uso delle nuove tecnologie. I contatti sono sempre avvenuti seguendo i canali tradizionali, vale a dire l'intermediazione degli uffici territoriali quali Questure e Compartimenti di Polizia Postale.

[42] Cfr.: allegato n.1.

Le segnalazioni d'utenti della rete, che pervengono al Nucleo Operativo attraverso tali canali, vengono tutte vagliate, analizzate e verificate; spesso, però, tali indicazioni risultano troppo generiche, o indicano la presenza di siti coinvolti in attività illecite, ma residenti su server collocati in territorio estero, da cui l'impossibilità di agire in maniera diretta.

A causa della natura stessa delle azioni poste in essere da tale soggetto, la polizia non ritiene possibile considerare "buono" un hacker, per cui ha sempre dichiarato ufficialmente di non essersi mai avvalsa di tali collaborazioni. Viceversa, viene positivamente considerata qualunque segnalazione d'attività illecite da parte di normali utenti, a patto che non abbiano violato sistemi di sicurezza logica, per venirne a conoscenza.

7.3. Luci ed ombre della legge sul "computer crime".

La legge n° 547/'93, nota come "Legge Conso" ed ampiamente discussa nel terzo capitolo, è fonte ancora oggi di un aspro dibattito non solo tra chi ne paga, o ne ha pagato, le conseguenze, ma anche tra chi deve eseguirla e farla rispettare. Se era prevedibile, infatti, riscontrare al riguardo dei pareri negativi all'interno del fenomeno hacker, meno lo è stato ascoltare critiche severe in proposito da parte dello stesso apparato giudiziario.

Senza voler riesaminare i diversi articoli in cui si sviluppa tale impianto, per la cui operazione si rimanda al capitolo inerente, ci sembra qui interessante fornire le opinioni dei diretti interessati, premettendo che la polizia telematica si è astenuta dal voler fornire un giudizio unitario sulla legge stessa. Tale astensione è stata motivata dall'impossibilità di poter esprimere un'opinione univoca al riguardo, e dal fatto che rientra nei compiti di tale arma quello di sorvegliare la corretta applicazione dello strumento legislativo, non di esprimere un giudizio critico nei suoi confronti.

Nonostante la perizia, a volte eccessiva, nel descrivere i diversi reati e le possibili aggravanti previste, intere problematiche restano prive di qualsiasi

argomentazione, alimentando dei vuoti legislativi di difficile soluzione. Dopo aver fornito uno sguardo d'insieme, ogni diversa opinione cercherà di approfondire tali problematiche ipotizzando possibili soluzioni.

G. Corasaniti considera la legge 547 votata alla tecnica del "taglia e incolla", nel senso che avrebbe aggiunto gli aggettivi "informatica e telematica" a fattispecie tipiche del codice penale, evitando d'addentrarsi in una specifica analisi dei beni giuridici tutelati e dei comportamenti criminosi reali. Sembra essere stata concepita da persone assolutamente all'oscuro della realtà pratica dell'informatica[43], risultando inadeguata di fronte a molti interrogativi posti dalla rete. In pratica, secondo il magistrato romano, si è adeguato il codice penale aggiungendovi la dizione "informatica e telematica", e si è cercato di riproporre una serie di reati (attentato, esercizio abusivo delle proprie ragioni, accesso ed intercettazione illecita, frode) in tale nuova veste.

Nella sua esperienza di magistrato, Corasaniti non esita ad affermare che la "Legge Conso" andrebbe ripensata, riscritta da mani più attente ed in grado di distinguere tra il vero accesso illecito ad un sistema e quello che non lo è. Al posto di tutte le figure presenti nel testo, basterebbe prevedere solo il danneggiamento informatico, sia pure aggravato, e chiarire cosa s'intende per misura di sicurezza[44], visto che non esiste l'obbligo di proteggere i dati con sistemi di difesa appropriati, e che negli USA l'accesso abusivo viene punito solo di fronte alla presenza del danno[45].

Le pene, nella considerazione del giudice, sono spropositatamente alte per comportamenti magari innocui sul piano pratico, ed estremamente basse quando, come nel caso delle frodi internazionali, i danni sono enormi.

---

[43] "Per la rete vengono fuori paradossi inaccettabili, pregiudizi ed istanze di regolamentazione che non è regolamentazione ma sanzione di tutto. A volte si propongono normative per il livello tecnologico senza conoscere le tecnologie, e questo è un fenomeno ancora più pericoloso degli hacker". Tali concetti sono stati espressi dal Dott. Corasaniti alla presentazione del testo "Spaghetti hacker " (op. cit.), avvenuta il 19/11/'98 presso la biblioteca comunale P. P. Pasolini di Ciampino.

[44] "Mancano norme chiare sul concetto di misura di sicurezza, che evidentemente varia secondo i caratteri del sistema. Per la legge è la stessa cosa un sito Internet, uno sportello bancario, un newsgroup, una casella di posta elettronica, mentre a tutti è chiaro che occorrerebbe forse stabilire una scala di priorità, anche perché si può accedere (abusivamente) per ragioni diverse". Vedi intervista negli allegati.

[45] Vedi cap.3 par.4.

La legge, inoltre, non si pone per nulla problemi pratici d'enorme rilevanza, come il riferimento d'obbligo alla sede giudiziaria competente ed il tema delle intercettazioni. In merito alla competenza territoriale, nulla viene detto su chi debba occuparsi dell'azione criminale, vale a dire se la sede giudiziaria debba essere quella dove si trova il sistema danneggiato o quella da dove ha operato l'hacker[46].

Sulle intercettazioni il dibattito è molto acceso, e Corasaniti si limita a sottolineare come, il mutuare la norma da quelle telefoniche, abbia lasciato scoperti tutti i settori prettamente informatici. Qui le carenze riguardano l'accesso ai dati del server, a quelli identificativi delle comunicazioni usate in concreto, la durata della conservazione di tali dati, la cooperazione internazionale per identificare gli autori delle frodi, e la legge necessita di un'ulteriore disciplina che ritocchi anche il codice di procedura penale. Da notare che in Italia, rileva il giudice, il tutto è controllato dalla magistratura e non, come in altri paesi, dalla polizia[47].

Altro punto di discussione è l'equiparazione, effettuata da tale legge, del domicilio al nostro computer. In merito il giudizio di Corasaniti è meno critico, tuttavia non esclude che la tematica possa essere rivisitata e discussa. Egli considera il domicilio informatico la proiezione della nostra personalità, il luogo dove cittadini, imprese ed istituzioni conservano dati riservati, e non fa certo piacere "tornare a casa e trovarvi qualcuno che vi è entrato solo per assicurarsi che il sistema d'allarme funzionasse[48]". Incongruità e paradossi sembrano venire anche da una cattiva traduzione dall'inglese, come l'espressione "system operator" che è stata tradotta "operatore di sistema", figura di cui non si capisce la vera identità[49].

Nel complesso, rileva il magistrato, l'hacker esce mal rappresentato da questa legge, dove viene descritto in forma poco chiara e non riceve certezze in merito ai propri diritti. Ad esempio, manca un principio guida per decidere quando il materiale

[46] "Quello del luogo da cui ci si connette è un problema, se la frode avviene all'estero non c'è modo d'intervenire. Però l'incertezza per l'azione viene diminuita da una distinzione: se c'è danneggiamento (in questo caso si prosegue d'ufficio) o se serve una querela (questo è il caso del semplice accesso abusivo). Se in assenza di querela uno si limita ad accedere ad un sistema altrui all'estero, questi non sarebbe perseguibile. Oltre ad essere una mancanza della legge, questa è anche una grave carenza delle regole internazionali". Cfr.: allegato n.1.
[47] "Il rischio d'abusi da parte della polizia giudiziaria, tuttavia, è inevitabile in ogni attività, fa parte del gioco, succede anche quando siamo fermati per un banale controllo di polizia stradale". Cfr.: allegato n.1.
[48] Cfr.: allegato n.1.
[49] "Non si capisce se sia il Webmaster o chi sta alla tastiera e svolge un'attività di trattamento dei dati". Cfr.: allegato n.1.

confiscato può essere restituito, e quando deve servire a compensare le vittime dei danni subiti, provvedimento che spetterebbe al tribunale al termine del processo. Tuttavia, nel concludere tale analisi Corasaniti afferma di non condividere, a prescindere dalla riuscita o meno della legge 547, la posizione di chi pensa non esservi nulla di male a fare hacking, conseguenza di un malinteso senso della propria libertà in un momento storico particolare, dove è in gioco un'evoluzione economica e sociale a carattere globale e si rischia di veder pregiudicate occasioni importanti di lavoro e di sviluppo[50].

Più volte critico nei confronti degli hacker e del loro operato, Manlio Cammarata giudica molto complesso il discorso relativo alla "Legge Conso", a causa dello scontrarvisi d'esigenze investigative da un lato e diritto alla riservatezza dall'altro. In merito al problema delle intercettazioni, questi nota come in Italia si faccia un uso di questo mezzo più ampio rispetto ad altri paesi, con un livello di garanzie di segretezza sui contenuti intercettati che egli ritiene insufficiente.

S. Chiccarelli fa risalire l'accanimento giudiziario nei confronti degli hacker all'attuale vuoto legislativo, ben lungi dall'essere stato colmato dalla legge 547/'93. Quando la percezione di un fenomeno non è chiara, rileva il coautore di "Spaghetti hacker", la sua regolamentazione è confusa e contraddittoria. Un palese esempio di tale confusione è nell'assenza di chiarezza in merito a servizi privati mal configurati, che figurano come risorse lasciate libere a tutti perché all'entrata non viene richiesta alcuna password d'accesso. La legge non chiarisce se l'utilizzo pubblico di tali servizi rappresenta un reato, ne suggerisce un comportamento idoneo a rendere meno efficaci nuove forme d'attacco informatico come il Back Orifice[51], in grado d'introdurre dei file nell'hard disk, o di modificare quelli già presenti, senza che l'utente di quel p.c. se n'accorga.

Forte del suo ruolo d'avvocato, esperto conoscitore della legge 547 e dei suoi cavilli, A. Monti non le risparmia una critica severa. Il difetto fondamentale di questo strumento legislativo risiederebbe in un'assenza di simmetria, che finisce col punire l'accesso abusivo ma non la totale assenza di difese informatiche, siano esse di tipo

[50] "Non c'è per niente da scherzare, anzi occorre un impegno comune, una ricerca di regole deontologiche perché siano garantite libertà e sicurezza di chi lavora e opera on-line". Fonte: vedi intervista negli allegati.
[51] Vedi cap.3 nota n° 8.

tecnico o dovute alla carenza di sorveglianza da parte del sysop[52]. Monti accusa la legge di scaricare la responsabilità delle intrusioni sulla categoria degli hacker, salvando così quella dei tecnici (o presunti tali) di difesa informatica.

Sull'equiparazione p.c./domicilio informatico, il giurista non è pienamente d'accordo: egli non considera il computer casa propria, né il luogo dove vive o esprime la sua personalità. L'articolo sulle intercettazioni telematiche viene considerato "folle", conseguenza della totale mancanza di una teoria organica sulle indagini di polizia. Tale carenza si è tradotta, con il passare del tempo, in assurdi sequestri indiscriminati di materiale informatico[53], perché nel silenzio del codice gli operatori di polizia hanno spesso prelevato ogni tipo di materiale considerato "inerente" (ad esempio i tappetini del mouse) per tacere d'interi server bloccati alla ricerca di un file.

Monti conclude ponendo l'accento sull'irrisolto problema della reità (da ***res***) del dato informatico e del programma, che l'art.392bis c.p. afferma essere danneggiabile, ma l'art.624 c.p. dichiara non sottraibile perché non ***res***, mentre la normativa in materia di firma elettronica e documento informatico promette fieri scontri con la disciplina del documento informatico falso (art.491bis c.p.) [54].

Tony Mobily considera la legge sul computer crime molto dura nei confronti degli hacker, in misura maggiore rispetto agli altri paesi europei. Il suo giudizio, nei confronti del sistema italiano, non è dei più teneri:

> "In Italia si hanno le pene più dure, ma tanto non va mai in galera nessuno. E' un paese dalle tante, mostruose regole, mai applicate…I politici non sanno cosa fanno, ed i pochissimi che fanno le cose bene devono risolvere problemi più importanti di questo. Restano gli incompetenti, quelli pensano "..si, gli hacker... sono quelli che fanno i criminali, no? Si, quelli devono essere messi in galera" e poi fanno le leggi. Se questo non fosse vero, la legge sull'hacking in Italia non somiglierebbe tanto ad una barzelletta…sembra scritta da tecnici IBM degli anni '60"[55].

[52] "Se si riesce ad entrare in un sistema che poteva essere protetto, e che per l'ignoranza e l'incompetenza della persona preposta non lo era abbastanza, quest'impreparazione professionale non dovrebbe essere punita anche lei penalmente?". Cfr.: allegato n.1.
[53] Vedi cap.2 par.4.
[54] Fonte: ***Brevi note sulla recente giurisprudenza di diritto delle tecnologie*** di A. Monti, pubblicato il 10/11/'97 sul sito www.interlex.com.
[55] Vedi intervista negli allegati.

Interrogato in merito al giudizio di Monti sull'assenza di simmetria hacker/tecnici di difesa informatica, l'ex-hacker risponde sorprendentemente di non trovarsi d'accordo:

> "No, secondo me è assurdo punire la non-difesa. Il motivo, a mio parere, è molto semplice: se **non** sei difeso, qualcuno entrerà e creerà casini grossi. E se i casini grossi continuano per molto tempo, e tu sei un provider, alla fine chiudi. E' un sistema che s'autoregola, una specie di selezione naturale. No ha molto senso creare una legge per forzare la gente a proteggersi… Ed è per questo che, a mio parere, l'hacking fatto in modo "giusto" è fondamentale per aumentare la sicurezza in rete. E quello non dovrebbe essere punito. Se scopro le debolezze di un sistema, e mando una mail al root facendoglielo notare, e avvertendolo che non è stato abbastanza bravo da salvaguardare i dati privati dei suoi clienti, gli ho fatto sostanzialmente una consulenza gratis. Come dire: un host è un albergo. Appartiene a qualcuno, e le persone lo usano per (dormire) registrare i propri dati. L'oste (la persona) dovrebbe, in effetti, fare di tutto per chiudere la porta d'ingresso a chiave, per evitare che ladri entrino e rubino le cose dei suoi clienti. Ma se uno fa un test, vede che la porta era aperta, e gli lascia un bigliettino, dicendogli come deve chiuderla…non vedo come sia punibile per legge. Se poi, dopo la letterina, l'oste tiene la porta aperta senza tenere presente i consigli, per svogliatezza o per incompetenza, allora l'hacker avrebbe il **diritto** di dire questa cosa a tutti, di allarmare. E l'oste non dovrà lamentarsi della cattiva pubblicità…"[56]

Raoul Chiesa confessa di ritenere la legge 547 errata e dettata dalla necessità di uno standard con altri paesi europei. Tale necessità, però, non avrebbe coperto l'ignoranza del legislatore nel capire i reati, nell'effettuare le giuste distinzioni all'interno degli stessi, nel fornirne una comprensibile spiegazione a magistrati, avvocati e forze dell'ordine. Egli considera eccessiva la pena di tre anni per l'accesso abusivo, e fa risalire la mancanza di riferimenti alla sede giudiziaria competente all'impossibilità di basarsi su norme precedenti da cui trarre un esempio:

> "…la legge in materia non può prevedere cose di questo tipo, se non rifacendole per intero, e non basandosi, purtroppo o per fortuna, più sulle fondamenta delle normative italiane… quelle che ci legano a concetti che stanno cambiando o sparendo…lo spazio non c'è più in rete, la fisicità del reato non esiste. Devono affrontare un nuovo problema, nel paese con più leggi al mondo…auguri. Sono molto pessimista in merito".

Avendo a cuore la questione, memore della sua esperienza sfortunata, Raoul Chiesa narra la propria vicenda personale, finendo così per delineare ulteriormente carenze ed omissioni della "Legge Conso":

> "…io, accusato e condannato in base a svariati articoli del codice di procedura civile. Uno di questi recita: "Accusato di aver violato un sistema informatico protetto". Allora…

[56] Cfr.: allegato n.1.

1) se è protetto non ci entro
2) se era protetto lo era con dovute barriere, in questo caso io SONO colpevole perché quelle barriere mi avrebbero avvertito di trovarmi di fronte ad un sistema informatico il cui accesso è vietato se non autorizzati
3) se è protetto, l'azienda ha fatto del suo meglio per garantire la riservatezza dei dati custoditi, ed evitare attacchi e manomissioni (legge 675/'96)
4) in caso contrario l'azienda è colpevole di qualcosa (non so bene cosa, dovrei approfondire, lo farò, ma sempre della 675 si tratta)

Il sistema che ho violato in bankitalia.it e per il quale sono stato condannato (insieme ad altri sistemi) era un IBM Aix 3.2 (Unix) che:

1) non era protetto: ci sono entrato
2) nessun avvertimento, divieto (banner, etc…), barriere particolari, se non la richiesta di login/password.

Lei qui mi dirà: ecco, lei è stato condannato perché ha utilizzato login/password abusive. Non è andata così. Ma, per ora, facciamo finta di sì. Ok, c'era la login ROSSI con la password ROSSI. TU azienda sei colpevole. Io anche, ma – credo - di meno che se avessi trovato login ROSSI e password RGEw76zX. C'è un però…io NON ho immesso login o password…ho utilizzato un bug, che per chiarezza ora chiamerò CONOSCENZA. Fai molta attenzione a quello che segue: questa CONOSCENZA consiste nel fatto che l'IBM sbagliò la procedura di login sugli AIX versione 3.0 e 3.2.

Dando il comando "rlogin-f root" da un'altra macchina Unix connessa ad Internet (rlogin è il comando standard per entrare su un altro sistema "trustato" con lo user con il quale si è collegati dalla macchina di partenza: se io specifico uno user, mi chiede la password di quello user sulla macchina remota), gli Unix IBM 3.0 e 3.2 sbagliavano…NON CHIEDEVANO LA PASSWORD DI ROOT. Ti ritrovo root (utente con tutti i massimi privilegi) SENZA AVER TOCCATO O LANCIATO ALCUN PROGRAMMA, TOOLS, SENZA AVER INDOVINATO PASSWORD…senza nulla di nulla!!! Io scrivo un comando sulla MIA macchina, e mi ritrovo nella shell root di bankitalia.it! Ora…:

- IBM ha annunciato il suo bug OVUNQUE (cert, bollettini, advisores…)
- le maggiori organizzazioni di sicurezza, profit e no profit, hanno riportato il bug che è vecchio d'anni
- IBM gratuitamente distribuiva il patch, e informava gli utenti del potenziale rischio
- il compito di un system manager è solo quello d'informarsi (è pagato per questo) e applicare il patch (è strapagato per questo)
- enti come bankitalia (così come tante altre aziende) hanno contatti con IBM, Digital, etc…come mai nessuno ha patchato quel bug?

Mi si accusa, denuncia e condanna per aver fatto ciò, dando solo la colpa a me. Mi si sequestra e non mi si ridà un hard disk con 2 anni della mia VITA (hacking, lettere, appunti, ricordi, software…la mia vita) perché su quell'hard disk c'è il "corpo del reato" (la descrizione del bug in questione). Questo bug è pubblicato OVUNQUE su Internet, non l'ho rubato all'IBM ma l'ho scaricato dal CERT (Computer Emergency Response Team[57], sono dall'altra parte rispetto ad un hacker…loro i buoni e noi i cattivi).

- Migliaia di siti Internet riportano quel bug
- bankitalia mi chiede i danni (!) economici
- devo pagare le spese processuali perché sono stato OBBLIGATO a patteggiare, ed a non andare in discussione processuale e relativo dibattimento (pagandomi di tasca mia consulenti incapaci e periti altrettanto incapaci!).

……..Pensi ancora che la colpa sia tutta mia?"[58]

[57] Riferimenti al CERT-IT ed al suo operato sono presenti nel secondo capitolo (par.5), nel terzo capitolo (par.3) e nel quarto (par.5).
[58] Cfr.: allegato n.1.

7.4. Il difficile rapporto tra la stampa ed il mondo hacker.

Come più volte accennato all'interno di questo lavoro, gli hacker italiani hanno spesso accusato la stampa di resoconti parziali ed inesatti sul proprio operato, vedendo in essa una sorta di fedele alleata di un sistema che gli stessi, a modo loro, cercavano di mettere in difficoltà. Forse solo oggi, grazie a figure come Chiesa che si prestano a commenti ed interviste, l'universo hacker appare meno lontano ed incomprensibile, e sembra chiaro che continuare ad inneggiare alla "caccia al pirata informatico" nasconde una fobia ingiustificata.

Al riguardo, nella sua veste di giornalista Manlio Cammarata rileva quanto i suoi colleghi non facciano solo disinformazione in merito al fenomeno hacker, ma come si comportino allo stesso modo con tutti gli aspetti della società dell'informazione, e della rete in particolare. Chi scrive per la rete, prosegue il giornalista, la conosce e non la teme, mentre i cronisti della carta stampata, appena possono, parlano male del…nemico.

Sul rapporto stampa-smanettoni, Chiccarelli pensa che la prima abbia scritto spesso di fatti che non conosceva, senza interpellare minimamente i diretti interessati. L'autore si augura che, anche grazie al suo libro, la considerazione del fenomeno cominci a cambiare, la gente scriva meno per sentito dire e decida di approfondire maggiormente le fonti. I veri pericoli sembrano essere la caccia all'audience, nel senso che "il ragazzino brufoloso che mette in pericolo la sicurezza nazionale" ha sempre fatto vendere i giornali, ed una forte reazione della stampa tradizionale verso la rete, che da alcuni anni si cerca di screditare evidenziandone tutta la sua presunta ed estrinseca pericolosità[59].

In merito ad una differenza di toni, costatata a volte sullo stesso giornale tra la sua edizione cartacea e quella on-line, specialmente nei confronti di resoconti su operazioni di polizia relative alla rete, Chiccarelli dichiara di non essersi mai imbattuto nella palese manifestazione di tale differenza, tuttavia, non esclude che ciò possa accadere vista la differenza di pubblico a cui le diverse edizioni si rivolgono.

[59] "Un mezzo di comunicazione libero fa sempre paura, e gli hacker ci sono capitati nel mezzo". Cfr.: allegato n.1.

I toni usati dall'avvocato Monti sull'argomento risultano più duri, ed immaginiamo sia perché più di una volta, vista la sua professione, si sarà trovato a difendere soggetti duramente accusati dalla stampa. Egli dichiara che: "Le campagne di stampa contro gli smanettoni sono vergognose ed hanno stravolto parti, situazioni, fatti. L'Operation Cathedral[60]si è conclusa dopo tre mesi, con l'archiviazione e la chiusura del procedimento penale per l'inesistenza della notizia di reato. Chi ridarà la dignità e l'onorabilità alle persone finite sui giornali, date in pasto alle masse con il ***marchio di Caino***?"[61].

Più ironico appare in proposito il commento di Tony Mobily, che merita di essere citato testualmente:

> "Le persone hanno un problema fondamentale: leggono i giornali. Questo di per se non sarebbe un problema insormontabile. Il disastro comincia quando cominciano a **credere** ai giornali…
> Mi è successo una decina di volte, di leggere fatti di cui, in effetti, ero a conoscenza. Dieci volte su dieci, erano così distorti da diventare quasi comici. Non compatisco le persone per pensare che l'hacker sia un criminale. Il mare di stupidaggini che le bombarda tutti i giorni le giustifica al 100%. Un articolo che parla di hacker in modo corretto, si perde nel mare d'immondizia che lo circonda"[62].

Il suo non facile ruolo di "hacker pubblico" ha portato Chiesa ad avere contatti diretti con i media, e ad esporsi in prima persona scrivendo articoli per la rete. Interrogato sulla duplice connessione stampa-hacker e stampa-R.Chiesa, questi ha così risposto:

> "Mi capita molto spesso di leggere un articolo e di pensare *questo qui non ha capito proprio niente di hacker*, perché il giornalista deve scrivere di tante cose, non può avere una conoscenza profonda degli hacker. Pochi ce l'hanno, e ancora meno scrivono belle cose. (…) Molti giornalisti, quando pubblicano per Web hanno paura, non sanno a che target scrivono…quando lo fanno per la carta si, sono i *loro lettori*…il popolo del Web è strano, svariato…li spaventa. (…) Le domande che mi vengono poste più di frequente sono - perché lo hai fatto, perché lo fai, cosa ci si sente ad essere hacker, cosa vuol dire hacker, cosa fai quando entri in un sistema - …domande molto stupide, in genere. (…) Le domande che la gente non mi pone, ma a cui mi piacerebbe rispondere, riguardano cosa penso che succederà, cosa penso d'alcune morti sospette d'alto livello accadute in Europa, perché nascondono Echelon ed Enfopol, perché i media non ne parlano, perché condannano a morte gli hacker in Cina, perché i sistemi più protetti sono quelli delle case farmaceutiche, cosa ho visto in questi anni nei sistemi che bucavo? (…) Credo un hacker andrebbe fatto parlare, prima di tutto, si dovrebbe sentire cosa pensa e se ha cose

[60] Vedi cap.3 par.2.
[61] Cfr.: allegato n.1.
[62] Cfr.: allegato n.1.

interessanti da dire. (…) Ma non è che ogni hacker abbia delle cose interessanti da dire o sia per forza un genio. Ci sono tanti hacker stupidi in realtà, purtroppo. (…) A me piace scrivere in rete, anche se ritengo che gli argomenti sui quali ho qualcosa da dire si esauriranno a breve. Sto per terminare un secondo articolo[63] per Apogeonline, sul mio punto di vista riguardo alle normative italiane sui crimini informatici…poi si vedrà"[64].

[63] Il primo è stato ***Hacking in Italia, a first overview***, pubblicato su www.apogeonline.com in data 7/1'99.
[64] Cfr.: allegato n.1.

Gli spazi della coscienza

In questa vorticosa fine di millennio, dove è più importante muoversi in fretta che conoscere realmente la propria meta, lo spazio che ci circonda sembra subire continue trasformazioni.

Si riduce, fino a scomparire, se considerato come distanza fra le persone, sempre più in stretto contatto anche se lontane fisicamente. Viceversa, si ampliano a dismisura gli spazi della nostra fantasia, delle nostre fughe dalla realtà, dei nostri sogni. All'interno di queste dimensioni aumenta anche una nuova capacità operativa, preda d'avanguardie dello spirito prima ancora che del mercato, che riescono a tradurre la fantasia in realtà, la fuga in interesse, il sogno nel suo raggiungimento, il tutto in nome di ritrovate libertà di pensiero ed azione.

Pionieri del virtuale, illusionisti dello schermo, gli hacker rappresentano una di queste avanguardie, destinata per natura a fungere da battistrada delle nostre conoscenze. Il rischio, all'interno di questi percorsi dell'immaginario, è dato da una fuga in avanti delle abilità, mal compensata da un ritardo delle coscienze e delle connesse responsabilità.

Vivendo in loro compagnia per più di un anno, la mia tesi ha cercato di descrivere uno di questi nuovi spazi ed i soggetti che hanno scelto di percorrerlo. Se tale analisi, limitata in ristretti ambiti temporali, ha forzatamente dovuto porsi un limite di svolgimento, il lettore sappia che il viaggio non finisce con l'ultimo capitolo, ma prosegue quotidianamente negli spazi della nostra coscienza.

Allegati

Allegato n.1

Il presente allegato si compone degli stralci di cinque interviste, rilasciate tramite posta elettronica tra il dicembre ’98 ed il febbraio ’99, ed inserite nel settimo capitolo come note e commenti. Alcune interviste sono completate da una serie d’interventi, effettuati dai medesimi soggetti durante l’incontro per la presentazione del testo ***Spaghetti hacker*** di A. Monti e S. Chiccarelli, tenutosi a Ciampino il 19/11/’98

Dall’intervista al magistrato Giuseppe Corasaniti

Prima di entrare nei dettagli, vorrei una sua opinione sulla l.547/’93 nel suo insieme, come impianto organizzativo, predisposizione al problema dei crimini informatici e rapporto con la rete.

E’ una legge, la 547, che utilizza la tecnica del “taglia e incolla”, cioè aggiunge gli aggettivi “informatica e telematica” a fattispecie tipiche del codice penale, senza però addentrarsi in una specifica analisi di beni giuridici tutelati e di comportamenti criminosi reali. Sembra davvero essere stata concepita da persone all’oscuro della realtà pratica dell’informatica, di fronte alle tematiche di Internet tale legge è assolutamente inadeguata. E’ stato adeguato il codice penale incollando qui e lì la dizione ***informatica e telematica***, riprendendo i reati di attentato, esercizio abusivo delle proprie ragioni, accesso illecito, intercettazione illecita, frode informatica. Le pene sono spropositatamente alte per comportamenti magari innocui sul piano pratico, ed estremamente basse quando, come nel caso di frodi internazionali o di danneggiamenti ai sistemi, i danni sono enormi. Infine, la legge non si pone per nulla problemi pratici d’enorme rilevanza, come ad esempio chi debba essere il giudice competente. Sul problema delle intercettazioni, anche qui il legislatore ha usato il “cut and paste” mutuando le norma sulle intercettazioni telefoniche, mail vero problema è l’accesso ai dati del server, ai dati identificativi delle comunicazioni usate in concreto. Il tutto con molteplici problemi aggiunti, come la conservazione dei dati oltre un certo periodo o in caso di accertato illecito e la cooperazione internazionale per identificare autori delle frodi.

Si è a lungo discusso sulla scelta di equiparare il computer ad un domicilio: vorrei che lei approfondisse l’argomento sottolineando vantaggi e svantaggi di questa scelta.

Il domicilio informatico è la proiezione della nostra personalità, il luogo dove tutti, cittadini, imprese ed istituzioni, conservano i dati riservati, e non fa certo piacere tornare a casa e trovarvi qualcuno che vi è entrato solo per assicurarsi che il sistema d’allarme funzionasse. Molti ritengono che non c’è niente di male a schiacciare un tasto, smanettare e magari far partire un missile nucleare o divertirsi facendo acquisti a spese altrui o accrediti ai danni di un cinese, ma queste attività non sono innocue, sono illegali perché

offendono il patrimonio e la riservatezza di una persona. Non condivido le posizioni di chi, forse per un malinteso senso della propria libertà, pensa che non ci sia nulla di male nell'hacking… al contrario oggi più che mai è in gioco un'evoluzione economica e sociale a carattere globale, e rischiamo di vedere pregiudicate impensabili occasioni di lavoro e di sviluppo economico. Non c'è per niente da scherzare, anzi occorre un impegno comune, una ricerca di regole deontologiche perché siano garantite libertà e sicurezza di chi lavora e opera on-line.

Vorrei conoscere la sua opinione in merito alla pena di tre anni per l'abuso di accesso, considerando che non esiste l'obbligo di creare sistemi di difesa appropriati e che, negli USA, l'abuso di accesso non viene punito di per se, ma rappresenta un passaggio *sine qua non* perché si consideri un reato informatico.

La pena è inadeguata in via generale, ma soprattutto mancano norme chiare sul concetto di "pubblica sicurezza", che evidentemente varia secondo i caratteri del sistema. Per la legge è la stessa cosa un sito Internet, uno sportello bancario, un newsgroup, una casella di posta elettronica, mentre a tutti è chiaro che occorrerebbe forse stabilire una scala di priorità, anche perché si può accedere (abusivamente) per ragioni diverse.

L'art.266 della 547 crea il problema di una totale assenza di metodo riguardo le operazioni di polizia. E' giusto intercettare telefonate, mail, effettuate tracciati dei percorsi in rete di un cittadino solo perché "sospettato" di aver commesso un reato?

Appunto a ciò serve la disciplina della legge e del codice di procedura penale. Il tutto è controllato in Italia dal magistrato (e non come in altri paesi dalla polizia) con tutte le garanzie di legge, cioè Tribunale del riesame, ricorso per la cassazione e così via.

La legge 547 piò aver influito sulla percezione del fenomeno hacker da parte del pubblico, che se lo è visto descrivere, in diversi punti, in maniera più pericolosa di quanto si è (fin ora) dimostrato? Come esce da tale legge la figura dello "smanettone"?

Ne esce male, anche perché così come è descritta sul piano pratico non si tratta di una figura chiara. Non esiste l'hacker che gioca, se fa danni deve essere individuato e punito, come per ogni reato.

Come comportarsi quando viene fatta domanda della restituzione di materiale "a rischio" (hard disk, floppy disk, qualunque cosa raccolga informazioni il cui interesse non è venuto meno in seguito al passare del tempo)?

Difficile rispondere, bisogna verificare caso per caso e distinguere quelli che possono essere i rischi di una reiterazione di condotte criminali da episodi occasionali di "vandalismo" informatico per cui la lezione, a volte, basta e avanza. Occorre buon senso e competenza tecnica da parte di polizia e magistrati. Il discorso della restituzione è molto più complesso di quello che sembra, tutte le cose che servono a commettere reati (quindi anche il computer) potrebbero essere confiscate e dovrebbero servire a compensare le vittime dei danni (economici) subiti

Mi è capitato, nell'ultimo periodo, d'imbattermi in rete in articoli che puntavano a distinguere tra una sorta di "ethical hacker" (hacker etici, il cui obiettivo è il rendere

la rete più sicura) rispetto ad “hacker normali”. Avendo sempre pensato che la curiosità, la sicurezza di sé, la sfida, fossero componenti genetiche “proprie” del DNA di un hacker, tale categorizzazione mi ha lasciato un po’ perplesso. Tali “vigilantes” possono avere una reale utilità, secondo lei, o rischiano di scadere in forme di “farsi giustizia da soli” che allontanano dalla giustizia ordinaria?

Bisogna verificare caso per caso anche la sussistenza del dolo, ma intendiamoci, se sussistono le condizioni (quindi se il fatto è accertato e se sono accertati i danni) l’hacker “etico” rischia né più né meno dell’hacker ordinario. Normalmente è l’hacker a fraintendere, non la legge. L’hacker a volte non sembra molto consapevole che anche un gesto “innocente” come l’intrusione (e magari la copia dei dati) può fare danni eccome a chi li deteneva legittimamente, causando pregiudizio ad attività personali o economiche. Se ammettiamo l’esistenza di un etica hacker, è chiaro che anche queste forme d’autotutela, che ora ci sembrano comprensibili, finiranno per causare equivoci e danni, magari in assenza delle garanzie che invece devono caratterizzare l’intervento pubblico (di polizia e magistratura). Al contrario, essi potrebbero svolgere un ben definito ruolo di denuncia e di “smascheramento”, ma ripeto che i rischi sono tanti.

Come vede lo sviluppo futuro della rete nel nostro paese e come inserisce la figura dell’hacker all’interno di tale sviluppo?

L’hacker è una figura di passaggio, che non va mitizzata ne sovraesposta. Perché non ci deve essere spazio nella rete globale per chi le regole non le rispetta, e tanto meno rispetta gli interessi degli altri. In una rete, come in una grande autostrada, devono poter circolare tutti, ma tutti devono conoscere e rispettare le regole.

Intervento di Corasaniti presso l'incontro di Ciampino (19/11/'98).

"Per la rete vengono fuori paradossi inaccettabili, pregiudizi ed istanze di regolamentazione che non è regolamentazione ma sanzione di tutto. A volte si propongono normative per il livello tecnologico senza conoscere le tecnologie, e questo è un fenomeno ancora più pericoloso degli hacker. In rete c'è criminalità, c'è pedofilia, ma chi le effettua è e resta un criminale ed un pedofilo, persone che si possono identificare e sanzionare con leggi diverse dalla 547/'93. (…) Si è parlato del rischio d'abusi. Tale rischio da parte della polizia giudiziaria, tuttavia, è inevitabile in ogni attività, fa parte del gioco, succede anche quando siamo fermati per un banale controllo di polizia stradale.(…) Quello del luogo da cui ci si connette è un problema, se la frode avviene all'estero non c'è modo d'intervenire. Però l'incertezza per l'azione viene diminuita da una distinzione: se c'è danneggiamento (in questo caso si prosegue d'ufficio) o se serve una querela (questo è il caso del semplice accesso abusivo). Se in assenza di querela uno si limita ad accedere ad un sistema altrui all'estero, questi non sarebbe perseguibile. Oltre ad essere una mancanza della legge, questa è anche una grave carenza delle regole internazionali. (…) La legge è fatta così, ed io devo applicarla in questo modo, tuttavia non posso esimermi dal notare queste cose. Incongruità e paradossi vengono anche da una cattiva traduzione dall'inglese, come l'espressione ***system operator*** che è stata tradotta ***operatore di sistema***, figura di cui non si capisce se sia il Webmaster o chi sta alla tastiera e svolge un'attività di trattamento dei dati".

Dall'intervista al giornalista Manlio Cammarata

Lei ritiene che il fenomeno hacker, in Italia, abbia caratteristiche proprie, autoctone, che lo differenziano da quello statunitense? Giudica il fenomeno in crescita? Come delimiterebbe le categorie interne a tale fenomeno? Che genere di rapporto c'è tra gli hacker e la stampa?

Non so dare una risposta precisa alle sue domande, perché il fenomeno è così variegato e sfuggente da non consentire, a mio avviso, le definizioni e le classificazioni che lei richiede. A me sembra ovvio chiamare "pirateria telematica", anche se quelli che si considerano i "veri hacker" si ribellano a questa definizione, la manifestazione di un disagio psicologico e sociale, che trova sbocco nell'attività in rete piuttosto che in manifestazioni "fisiche". Per quanto riguarda gli aspetti quantitativi, o se gli italiani siano diversi dagli stranieri, chi può dirlo? Occorrerebbe una conoscenza generale del fenomeno, che è difficile avere dall'esterno, mentre dall'interno ciascun componente della "comunità" ha fatalmente una visione parziale e settaria. Metterei comunque in rilievo alcuni aspetti che mi sembrano significativi: la tendenza all'associazione (segreta), il riconoscimento di capi carismatici, la convinzione di poter agire per una nobile causa, la contestazione dell'ordine costituito e via discorrendo. Il fatto certo è che queste persone commettono atti illeciti, spesso molto pericolosi, quindi è necessaria la repressione. Per quanto riguarda la stampa, il problema non è tanto come i miei colleghi trattano il fenomeno hacker, quanto su come disinformano su tutti gli aspetti della società dell'informazione, e di Internet in particolare.

Fin dove sono accettabili soprusi, da parte della polizia, all'interno d'indagini che utilizzano intercettazioni telematiche?

Il discorso è molto complesso, perché si scontrano le esigenze investigative ed il diritto alla riservatezza. In Italia si fa un uso delle intercettazioni molto più ampio che in altri paesi. Il problema, a mio avviso, è nelle garanzie di segretezza dei contenuti intercettati, che devono essere molto più forti di quelle attuali.

Perché in alcuni giornali esiste una notevole differenza tra come certi argomenti (es. pedofilia ed operazioni di polizia collegate) sono trattati nell'edizione cartacea e come, invece, lo sono all'interno dell'edizione on-line?

Perché chi scrive su Internet la conosce e non la teme. Invece i cronisti della carta stampata, appena possono, parlano male del…nemico.

Vorrei avere un suo parere in merito allo sviluppo, nel prossimo futuro, della rete in Italia, e su come la figura dell'hacker potrà inserirsi in tale evoluzione.

Solo una cosa è chiara, quando un comportamento è previsto come reato dal codice penale, come tale va perseguito. L'hacker, quando la legge lo prevede, deve essere inserito nelle patrie galere. Si possono far valere le proprie ragioni, diffondere le proprie idee, contestare quelle degli altri, senza violare i siti altrui. Non è previsto, in nome della libertà d'informazione, consentire a chiunque di frugare nelle nostre tasche, nei nostri cassetti, di forzare la nostra porta di casa solo per informarsi di cosa c'è dentro.

Dall'intervista all'autore Stefano Chiccarelli

Può darmi una definizione di "smanettone" e dirmi in cosa, principalmente, si differenzia dalla figura dell'hacker?

Non amo dare definizioni, diciamo che lo "smanettone", per come lo interpreto io in ***Spaghetti hacker***, è quella persona con una passione viscerale per la tecnologia, che da autodidatta ha imparato moltissime cose sull'informatica. Più che per quello che sa, lo smanettone si distingue dall'informatico per il tipo d'approccio compulsivo e viscerale che ha con l'uso del PC e di qualsiasi altra tecnologia. Lo smanettone italiano si differenzia dall'hacker principalmente per le capacità di programmazione, è il livello diverso di capacità di programmare che differenzia lo smanettone dall'hacker. L'hacker vero, non il cracker, è un programmatore d'altissime capacità con uno skill di capacità in più.

Vi sono state realmente, come accenna il suo libro, generazioni di smanettoni? In cosa si differenzia, secondo lei, quest'ultima rispetto alle precedenti?

Io penso proprio di sì, sia come età sia come approccio ed ideologia. La differenza principale è la mancanza d'ideologia, molto più frequente oggi che nelle precedenti generazioni. Oggi le guerre, le intrusioni, non hanno un valore etico o culturale ma sono solo esibizionismo, non c'è più etica, non c'è un progetto culturale dietro. Certo, non si può generalizzare, tuttavia la tendenza principale è questa, mentre prima chi smanettava con la telematica era spinto da un bisogno di comunicare, di scambiarsi informazioni, ecc…

Come vede, nel prossimo futuro, l'evoluzione di tale fenomeno in Italia?

Penso che pian piano l'hacking sarà capito, la cultura della rete farà capire bene a tutti la differenza tra hacker, cracker, smanettone e script kid. Le aziende si renderanno sempre più conto dell'esigenza della sicurezza per stare in rete, si creerà una cultura della system security e non ci saranno più innocenti immolati in nome della paura della rete. Chiaramente tutto questo lo spero.

Crede che i nostri smanettoni abbiano delle colpe, che possano aver influenzato negativamente lo sviluppo della rete (es. rallentandolo o rendendolo più insicuro)?

Non penso che gli smanettoni abbiano influenzato negativamente la rete, anzi gli smanettoni della generazione delle BBS hanno FATTO LA RETE in Italia, contribuendo in maniera determinante al Net Bang del 1995. Le insicurezze della rete non sono dovute agli smanettoni, ma alla rete stessa, che si trova ad un punto d'evoluzione tale che non ne garantisce ancora la sicurezza. Gli smanettoni hanno solo evidenziato questa realtà.

Il rapporto stampa-smanettoni è sempre stato molto difficile, perché?

Non penso sia stato difficile, penso semplicemente che la stampa abbia scritto cose che non conosceva, senza interpellare minimamente gli smanettoni; forse soltanto ora le cose stanno un po' cambiando, forse anche grazie al nostro libro. Prima, semplicemente, scrivevano cose per sentito dire, senza conoscere l'argomento.

A chi giova darne un'immagine così negativa?

Penso che da un lato sia un fatto d’audience, nel senso che il ragazzino brufoloso che mette in pericolo la sicurezza nazionale fa vendere i giornali, dall’altro ci sia stata una forte reazione (come anche per la pedofilia) della stampa e dei media tradizionali per screditare la rete, e per evidenziarne tutta la presunta ed intrinseca pericolosità. Un mezzo di comunicazione libero fa sempre paura, e gli hacker ci sono capitati in mezzo

Intervento di Chiccarelli presso l'incontro di Ciampino (19/11/'98).

"Ci sono molte aziende che si spacciano per esperte di sicurezza informatica e poi si ritrovano bucate da un ragazzino di 17 anni. Il problema è un altro: manca l'informazione, non si riesce a dare credibilità a realtà competenti, mentre ce l'hanno personaggi che, di fatto, sono incompetenti. (…) Ci si è concentrati moltissimo sui server in rete, ma ciò sta portando a scoprirsi su altri lati: ad esempio il client sulla scrivania della segretaria nel quale si penetra con un semplice Back Orifice, ed allora tutti questi firewall cosa si montano a fare? Back Orifice viene installato grazie ad un errore di configurazione, ma la sua capacità d'introdurre dei file nell'hard disk, o di modificare quelli già presenti, lo rende molto pericoloso".

Intervento di Monti presso l'incontro di Ciampino (19/11/'98).

"Questo libro vuole dimostrare che in Italia di veri e propri criminali non ce n'erano, se poi secondo una legge certi fatti sono stati considerati reato, questo non vuol dire che i soggetti che li commettono siano automaticamente dei delinquenti. Chi fa la copia di un sistema operativo senza averne la licenza non è paragonabile ad un ricettatore o ad un ladro, anche se certe interpretazioni della legge consentono tale equiparazione. Ugualmente bisogna distinguere tra chi entra in un sistema solo per curiosità, per saggiare le proprie possibilità, uscendone senza aver toccato niente, e chi lo fa per creare danno o per ricavarne profitto. (…) Tra gli smanettoni ed il mondo dell'informazione c'è un pessimo rapporto: le campagne di stampa contro gli smanettoni sono vergognose ed hanno stravolto parti, situazioni e fatti. L'Operation Cathedral si è conclusa dopo tre mesi, con l'archiviazione e la chiusura del procedimento penale per l'inesistenza della notizia di reato, in quanto lo sfruttamento e l'induzione alla prostituzione di minori non erano nemmeno configurabili. Chi ridarà la dignità e l'onorabilità alle persone finite sui giornali, date in pasto alle masse con il ***marchio di Caino***? (…) Il difetto fondamentale della 547, che non credo sarà cambiato, è sul fatto che se è pericoloso e va punito l'accesso ad informazioni particolari si dovrebbe punire anche la mancata difesa e protezione delle stesse. Se si riesce ad entrare in un sistema che poteva essere protetto, e che per l'ignoranza e l'incompetenza della persona preposta non lo era abbastanza, allora quest'impreparazione professionale non dovrebbe essere punita anche lei penalmente? E' un problema di simmetria. Questa cosa nella legge non c'è, e probabilmente non ci sarà. Si butta la croce solo su una categoria di persone, gli hacker, salvando le penne ad un'altra, chi dovrebbe lavorare sui sistemi. (…) L'equiparazione tra il domicilio di casa ed il computer mi sembra un po' forte, c'è un problema concettuale: il computer non è casa mia. Casa mia è una cosa, il computer (un pezzo di ferro con un po' di silicio sparso in ordine più o meno coerente) un'altra. (…) Non c'è, se escludiamo l'articolo sulle intercettazioni telematiche che è di per sé folle, una teoria organica per le indagini di polizia. Questo si è tradotto, nel corso degli anni, in fatti assolutamente folli come sequestri indiscriminati di materiale informatico. (…) Ad una carenza del codice di procedura penale, si somma una scarsa preparazione d'alcuni componenti delle forze dell'ordine, che non possono nemmeno essere troppo criminalizzate per questo perché, dovendo occuparsi di tantissime cose diverse, è anche ragionevole che non abbiano un'onniscienza procedurale. (…) Se i dati oggetto dell'intrusione non sono personali ma sono quotazioni, listini prezzi, in quel caso non c'è un fatto penalmente rilevante ma si ricade soltanto nei problemi civili".

Dall'intervista all'hacker Raoul Chiesa

Che differenza c'è tra un hacker ed un semplice appassionato d'informatica?

L'hacker fa l'installatore d'antifurto: li installa, ma vuole capire come funzionano. Se ne porta uno a casa, lo ruba o se lo compra, ma se lo smonta, lo simula, lo ricostruisce, e poi capisce i difetti. L'appassionato, o il professionista d'informatica, fanno anche loro gli installatori d'antifurto: aprono la scatola e installano l'antifurto. Stop.

Il cracker, lo smanettone, lo script kid, tutte figure interne al mondo hacker. Particolarità e caratteristiche.

Il cracker è colui che sprotegge il software, lo duplica e cerca di guadagnarci sopra. Lo smanettone è l'individuo che studia i p.c. da anni, li modifica, si fa le sue cose ***on his own***, per questo siamo tutti un po' smanettoni. Lo script kid è una specie d'insultino, in genere riferito a chi è solo capace di scaricare dalla rete gli script ed utilizzarli per penetrare nei sistemi.

Taluni considerano l'hacker una figura di passaggio, da non mitizzare, per la quale difficilmente ci sarà spazio in futuro. Cosa ne pensa?

E' vero che gli hacker stanno diventando dei miti, ma tale trend andrà a terminare, ed oggi porta più svantaggi che vantaggi al fenomeno in questione. Gli hacker sono dei pionieri…e oltre. I primi hanno gettato le fondamenta di luoghi come il MIT, hanno usato Arpanet quando c'erano quattro nodi, sempre spinti dalla voglia di conoscere più a fondo la rete ed i suoi segreti. L'hacker non vuole che la rete sia imprigionata da regole ed interessi, lo vogliono la "giustizia" ed il "mercato", ma qualunque cosa questi ultimi useranno per aumentare le verifiche di sicurezza, saranno sempre delle cose informatiche. Come tali, l'hacker le aprirà e le capirà, e difficilmente ne resterà imbrigliato. La vera rovina della rete sono, e saranno, i diversi interessi che la stanno raggiungendo, soprattutto d'origine economica.

Libertà d'informazione e d'espressione come base dell'etica hacker, come libertà totalmente perseguibile senza limiti. Ma è davvero così? Da che punto in poi è meglio frenare questa corsa verso tali libertà, prendere delle precauzioni contro possibili "rischi"?

Io sono contrario ad un'eccessiva libertà. Non perché non credo sia giusto, anzi… la trasparenza è il massimo in qualunque situazione. Per il semplice fatto che la massa non saprebbe come gestirla. Si dovrebbe cambiare il mondo, no? Il mondo ha istituzioni, leggi, barriere…immaginiamo che servano a difenderci, anche se nessuno sa bene da che cosa.

Lei si è sempre comportato secondo una sua etica personale. Quali sono i punti principali di tale etica? Alle accuse, poste ai suoi colleghi, di mancanza di rispetto ed eccesso di protagonismo, cosa si sente di rispondere?

Mai far danni al sistema se non strettamente necessario, per evitare pericoli a te o ad altri di cui t'importa; rispettare, curare ed ottimizzare, dove possibile, il sistema che violi; mai far danni a singoli individui (privati ed utenze finali); rispettare il lavoro sistemistico altrui;

se un sistema si dimostra realmente protetto (es. banner d'avvertimento, barriere particolari) rinunciare ad entrarvi. Attenzione, però, si devono sottolineare alcune cose fondamentali. Io hackero con l'intenzione di farlo, di entrare, di capire chi è quell'azienda, cosa fa, che reti adopera, di cosa si occupa, in che regione si trova, provo i cognomi comuni, guardo le ditte intorno, controllo in borsa con chi hanno partnership…il mio hacking è intenzionale, non mi limito a premere un tasto, anzi. Sono comunque d'accordo ad accusare l'hacker, spesso, di mancanza di rispetto e d'eccesso di protagonismo…a patto di accusare, della stessa mancanza di rispetto verso la propria azienda, il sistemista che non si protegge…punti di vista. La gente comune si sente derubata della propria privacy se un hacker gli spia le mail, senza sapere che pochissimi hacker lo fanno perché non ce ne frega nulla, e c'è altro da fare di più carino che leggersi le mail altrui. Oltre a ciò, io per primo considero le mail una cosa assolutamente riservata e personale, e divento nero se vedo persone spiare una mail altrui.

Rete come fenomeno d'aggregazione o di disaggregazione? Perché?

La rete è il vero fenomeno d'aggregazione di questo fine millennio, può portare ad una diversa reazione solo in chi ha paura di confrontarsi, d'imparare. E' assurdo accusare Internet di far perdere alle persone il loro amore per la lettura e la scrittura, scaricare su di essa la nostra paura della globalizzazione. Il vero hacker non avrà mai di questi timori, userà la rete per formarsi quel background che si acquista solo con l'esperienza diretta, che alla fine diviene una vera e propria ***forma mentis***, e non si può insegnare.

Da più parti cominciano a colpire il fenomeno hacker accuse d'imborghesimento, di cercare più la poltrona della grande azienda e meno il bene reale della rete. Come si difende? (da mandare)

Allora… di base, un hacker hackera, e ha nel cuore il sogno (specie da ragazzino) di venir assunto da un grande per fare quello che sa fare meglio: bucare e di conseguenza proteggere. Era anche il mio sogno, e di molti di noi, prima di arrivare alla fase di piena maturità che io chiamo "lo stato". Solo che le aziende non si fidano degli hacker, non si pongono il problema della sicurezza informatica, e se lo fanno non l'affidano a te, ragazzino hacker, ma a professionisti per centinaia di milioni, quando tu ragazzino hacker con lo spirito pulito, lo faresti – meglio – per un decimo di quella somma, ringraziando a vita e "uccidendo" chiunque provasse a toccare quel sistema. Perché lo ami e lo rispetti, ti hanno dato una possibilità e tu te la giochi bene… Chi ha iniziato prima di me (gli albori, ITAPAC con la numerazione corta, era l'85, credo, io ho iniziato a cavallo tra l'86 e l'87), ad esempio i DTE222, o quelli dell'hacking a MC-Link, oggi sono i system manager di Flashnet S.p.A., oppure i più vecchi sono responsabili di sicurezza (e lo sanno fare) presso multinazionali farmaceutiche e banche…Gli altri, quelli come me, si sono divisi dalla parte lavorativa…io con le mie idee "strane e pazze", altri presso Telecom, Istituti, Università, sempre con compiti molto delicati, in possesso di quelle informazioni che solo 3-4 anni prima ci costavano notti e notti di lavoro (non autorizzato) per entrarne in possesso. Ma io continuo a sentirmi un hacker dentro, perché per me questo vuol dire libertà, sfida, essere più bravi, anche se adesso per me l'hacking è diventato un lavoro. Lo faccio per rendere i sistemi più sicuri, non per dimostrare che non lo sono. Gli ultimi, i newbies, continuano a sognare il posto nella grande azienda come sistemista, o il posto come system manager presso il provider Internet medio-piccolo, ed intanto spesso fanno danni senza saperlo. Io ho preso diversi ragazzi, hacker newbies, e li ho portati su quella che chiamo "retta via", insegnando loro gli obblighi morali che, per me, anche l'hacker ha.

Shinomura vi accusa non tanto per le vostre azioni, quanto per il clima di diffidenza verso la rete che contribuite a creare. Ammetterà che il vostro comportamento non genera un senso di sicurezza… (da mandare)

Dico che è il contrario, che sono aziende come Microsoft a far crescere un clima ed un'opinione generale di "falsa sicurezza", quando in realtà sviluppano e sommergono il mondo di prodotti altamente sicuri ed inaffidabili. Sono stati gli hackers a sviluppare Arpanet e a farla diventare Internet. I primi system manager dei primi .edu. che ricevettero le connessioni dedicate ad Internet, giravano sui precursori di Altos e di Qsd. Oggi i migliori security men sono ex-hacker. L'IBM ha utilizzato hacker di cui si fidava per verificare che, su 10 sistemi con on-line payment, 9 erano bucabili. In questi 9 sistemi ci sono le tue e le mie carte di credito. Se non li bucava un hacker, come lo sapevamo io e te che le nostre CC potevano essere rubate?

Gli hacker e la legge. Prima di esprimere un'opinione generale sulla 547 e, se vuole, sul suo caso personale, come risolverebbe la questione della sede giudiziaria? Si sta cercando di basarsi su norme precedenti da cui trarre esempi dimostratisi funzionali… (da mandare con qualche modifica)

La legge in materia non può prevedere cose di questo tipo, se non rifacendole per intero, e non basandosi più, purtroppo o per fortuna, sulle fondamenta delle normative italiane… quelle che ci legano a concetti che stanno cambiando o sparendo…lo spazio non c'è più in rete, la fisicità del reato non esiste. Devono affrontare un nuovo problema, nel paese con più leggi al mondo…auguri. Sono molto pessimista in merito. Riguardo al mio caso personale, se me lo consenti, ci terrei ad approfittare dell'occasione per raccontarti bene tutto quello che mi è successo, e perché. Allora …io, accusato e condannato in base a svariati articoli del codice di procedura civile. Uno di questi recita: "Accusato di aver violato un sistema informatico protetto". Allora…

- se è protetto non ci entro
- se era protetto lo era con dovute barriere, in questo caso io SONO colpevole perché quelle barriere mi avrebbero avvertito di trovarmi di fronte ad un sistema informatico il cui accesso è vietato se non autorizzati
- se è protetto, l'azienda ha fatto del suo meglio per garantire la riservatezza dei dati custoditi, ed evitare attacchi e manomissioni (legge 675/'96)
- in caso contrario l'azienda è colpevole di qualcosa (non so bene cosa, dovrei approfondire, lo farò, ma sempre della 675 si tratta).

Il sistema che ho violato in bankitalia.it e per il quale sono stato condannato (insieme ad altri sistemi) era un IBM Aix 3.2 (Unix) che:

- non era protetto: ci sono entrato
- nessun avvertimento, divieto (banner, etc…), barriere particolari, se non la richiesta di login/password.

Lei qui mi dirà: ecco, lei è stato condannato perché ha utilizzato login/password abusive. Non è andata così. Ma, per ora, facciamo finta di sì. Ok, c'era la login ROSSI con la password ROSSI. TU azienda sei colpevole. Io anche, ma – credo - di meno che se avessi trovato login ROSSI e password RGEw76zX. C'è un però…io NON ho immesso login o password…ho utilizzato un bug, che per chiarezza ora chiamerò CONOSCENZA. Fai molta attenzione a quello che segue: questa CONOSCENZA consiste nel fatto che l'IBM sbagliò la procedura di login sugli AIX versione 3.0 e 3.2. Dando il comando "rlogin-f root" da un'altra macchina Unix connessa ad Internet (rlogin è il comando standard per entrare su un altro sistema "trustato" con lo user con il quale si è collegati dalla macchina di partenza: se io specifico uno user, mi chiede la password di quello user sulla macchina

remota), gli Unix IBM 3.0 e 3.2 sbagliavano…NON CHIEDEVANO LA PASSWORD DI ROOT. Mi ritrovo root (utente con tutti i massimi privilegi) SENZA AVER TOCCATO O LANCIATO ALCUN PROGRAMMA, TOOLS, SENZA AVER INDOVINATO PASSWORD…senza nulla di nulla!!! Io scrivo un comando sulla MIA macchina, e mi ritrovo nella shell root di bankitalia.it! Ora…:

- IBM ha annunciato il suo bug OVUNQUE (cert, bollettini, advisores…)
- le maggiori organizzazioni di sicurezza, profit e no profit, hanno riportato il bug che è vecchio di anni
- IBM gratuitamente distribuiva il patch, e informava gli utenti del potenziale rischio
- il compito di un system manager è solo quello d'informarsi (è pagato per questo) e applicare il patch (è strapagato per questo)
- enti come bankitalia (così come tante altre aziende) hanno contatti con IBM, Digital, etc…come mai nessuno ha patchato quel bug?

Mi si accusa, denuncia e condanna per aver fatto ciò, dando solo la colpa a me. Mi si sequestra e non mi si ridà un hard disk con 2 anni della mia VITA (hacking, lettere, appunti, ricordi, software…la mia vita) perché su quell'hard disk c'è il "corpo del reato" (la descrizione del bug in questione). Questo bug è pubblicato OVUNQUE su Internet, non l'ho rubato all'IBM ma l'ho scaricato dal CERT (Computer Emergency Response Team, sono dall'altra parte rispetto ad un hacker…loro i buoni e noi i cattivi).

- Migliaia di siti Internet riportano quel bug
- bankitalia mi chiede i danni (!) economici
- devo pagare le spese processuali perché sono stato OBBLIGATO a patteggiare, ed a non andare in discussione processuale e relativo dibattimento (pagandomi di tasca mia consulenti incapaci e periti altrettanto incapaci!).

Pensi ancora che la colpa sia tutta mia?

Esaminiamo il rapporto stampa-hacker e stampa-R. Chiesa: chi scrive di hacking, secondi lei, come lo fa e perché? Quali sono le domande che le vengono poste più di frequente? E quelle cui vorrebbe rispondere, ma che non le vengono mai poste? Cosa si dovrebbe chiedere ad un hacker, prima di tutto? Le piace scrivere articoli che saranno pubblicati in rete?

"Mi capita molto spesso di leggere un articolo e di pensare ***questo qui non ha capito proprio niente di hacker***, perché il giornalista deve scrivere di tante cose, non può avere una conoscenza profonda degli hacker. Pochi ce l'hanno, e ancora meno scrivono belle cose. Molti giornalisti, quando pubblicano per Web hanno paura, non sanno a che target scrivono…quando lo fanno per la carta si, sono i ***loro lettori***…il popolo del Web è strano, svariato…li spaventa. Le domande che mi vengono poste più di frequente sono - perché lo hai fatto, perché lo fai, cosa ci si sente ad essere hacker, cosa vuol dire hacker, cosa fai quando entri in un sistema - …domande molto stupide, in genere. Le domande che la gente non mi pone, ma a cui mi piacerebbe rispondere, riguardano cosa penso che succederà, cosa penso d'alcune morti sospette d'alto livello accadute in Europa, perché nascondono Echelon ed Enfopol, perché i media non ne parlano, perché condannano a morte gli hacker in Cina, perché i sistemi più protetti sono quelli delle case farmaceutiche, cosa ho visto in questi anni nei sistemi che bucavo? Credo un hacker andrebbe fatto parlare, prima di tutto, si dovrebbe sentire cosa pensa e se ha cose interessanti da dire. Ma non è che ogni hacker abbia delle cose interessanti da dire o sia per forza un genio. Ci sono tanti hacker stupidi in realtà, purtroppo. A me piace scrivere in rete, anche se ritengo che gli argomenti sui quali ho qualcosa da dire si esauriranno a breve. Sto per terminare un secondo articolo per Apogeonline, sul mio punto di vista riguardo alle normative italiane sui crimini informatici…poi si vedrà.

Dall'intervista all'ex-hacker Tony Mobily.

Tu sostieni che è impossibile presentare, in un film, le sensazioni provate da un hacker nell'esplorare un sistema. Perché?

Un esempio: un root si connette proprio in quel momento, mentre sei dentro con la password di un'altra persona, e ti sbatte una richiesta di talk, e quando ci parli ti chiede come stai, se hai risolto il problema del cane dal veterinario, ecc… E mentre tu ti rendi conto che l'utente cui hai fregato la password era un amico stretto del root, il root realizza che tu non sei quella persona… Questa è un'avventura, una cosa che ti carica d'adrenalina, una sfida che senti di poter vincere, una cosa che ci metterai due ore a raccontarla, ed a dire ai tuoi amici come tu sia riuscito a farglielo credere…Ma che in un film, semplicemente, non renderebbe l'idea.

Che rapporti hai avuto con l'etica hacker?

Non credo di esservi mai venuto veramente a contatto. Io avevo una mia etica: bucare i sistemi, usarli magari per un po', e poi mandare una mail all'amministratore di sistema dicendogli di chiudere il bug. Ma forse è impossibile tracciare una linea e mettere da una parte le persone etiche da quelle non etiche. Spesso gli hacker sono isolati, io lo facevo sempre con i soliti 3 o 4 amici. Quando parliamo degli hacker non stiamo parlando di persone che si riuniscono per decidere cosa è giusto e cosa non lo è, tutto è vissuto in maniera fortemente individuale.

Gli hacker e le accuse d'imborghesimento.

Quello di essere pagati per fare ciò per cui prima si rischiavano le manette è un sogno che raramente si realizza. Infatti, gestire la sicurezza di una ditta diventa consulenza: ha dinamiche contorte e situazioni particolari. Ci sono ex-hacker che ora fanno i consulenti, hanno scoperto quanto è difficile e lo continuano a fare. Ma credo che non abbia niente a che fare con l'imborghesimento, anche perché l'essere "hacker", alla fine, resta sempre e spesso riemerge…dopo le ore lavorative!

Classi e categorie interne al fenomeno hacker. Come le definiresti e perché?

Io ritengo vi siano tre classi di soggetti: i programmatori, chi utilizza tali programmi per migliorare effettivamente la rete e chi per scopi criminali. La prima classe è formata da un insieme di persone molto ristretto, poco visibili ai media perché quasi mai allo scoperto, dediti alla ricerca d'errori di programmazione ed alla successiva pubblicazione sia dei bachi sia dei mezzi per chiuderli. La seconda categoria è formata da chi usa tali programmi per andare a bucare i sistemi, facendo come me una mail al root per avvisarlo sulle carenze della sue difese informatiche. Nell'ultima classe troviamo i cattivi della situazione, coloro che usano gli stessi programmi della seconda classe per impadronirsi di dati ed informazioni, distruggere gli originali e fare danni ai sistemi per il puro gusto di farlo.

Che livello di "pericolosità" hai raggiunto nelle tue escursioni da hacker? Ti sei mai sentito controllato, hai mai avuto contatti diretti con la polizia telematica?

So praticamente per certo che la polizia ha un nastro con una conversazione telefonica tra me ed un hacker, in cui parlavamo veramente di tutto…ma so anche per certo che quel nastro è stato archiviato. Quella telefonata, tra le altre cose, e lo stress che ho vissuto quando ho saputo che la polizia sapeva cosa avevo detto, è stato un motivo di gran riflessione per me. Aveva la polizia il diritto di registrare i miei fatti personali? Ma potevo dimenticare d'essere "fuorilegge"? Poteva questo giustificarli? Il fatto che qualcuno stesse ascoltando mi fa sentire ancora male, tuttavia non ho trovato una risposta a queste domande…

Come rispondi alle accuse di Shinomura che giudica gli hacker pericolosi a causa del clima d'insicurezza che sono riusciti a creare?

Una pura idiozia. Le persone **dovrebbero** essere informate dei rischi della tecnologia. Devono sapere che, se mettono i loro dati on-line, un hacker può entrare e rubare tutto, distruggerli, ridistribuirli. Cosa dovremmo fare? Chiudere gli occhi e far finta che i computer siano **sicuri**? O, peggio ancora, mettere in galera gli hacker perché fanno scoprire alle persone che in Internet nulla è chiuso a chiave? E' come voler mettere in galera le persone che dicono a tutti che il governo è corrotto… Bisognerebbe, invece, rendere consapevoli le persone delle insidie di un mondo, quello dell'Internet, in cui la stragrande maggioranza dei server può essere bucato in meno di quindici minuti, a causa della svogliatezza e dell'ignoranza dei "sysadmin". I dati importanti vanno in un hard disk **non** connesso alla rete, a meno che non ti possa fidare **ciecamente** del tuo provider. Punto. Non so se questa cosa cambierà in futuro. Per ora è così.

Hacker contro ethical hacker, cattivi scassinatori contro buoni vigilantes a caccia di pedofili. Ritieni che tali associazioni possano rendere realmente la rete più sicura?

C'è sempre qualcosa che da fastidio a qualcuno, dovunque. Per ogni cosa che tu faccia, a parte collezionare trenini, c'è qualcuno che storcerà il naso. Ma questo non ha assolutamente nulla a che fare con il mondo dell'hacking. Tali associazioni sono formate solo da gruppi di persone che non sopportano qualcosa.

La legge 547 dimostra che sono chiamati a legiferare soggetti spesso a digiuno delle conoscenze tecniche necessarie. Ti sei fatto un'opinione in proposito?

In Italia si hanno le pene più dure, ma tanto non va mai in galera nessuno. E' un paese dalle tante, mostruose regole, mai applicate…I politici non sanno cosa fanno, ed i pochissimi che fanno le cose bene devono risolvere problemi più importanti di questo. Restano gli incompetenti, quelli pensano "Si, gli hacker... sono quelli che fanno i criminali, no? Si, quelli devono essere messi in galera" e poi fanno le leggi. Se questo non fosse vero, la legge sull'hacking in Italia non somiglierebbe tanto ad una barzelletta…sembra scritta da tecnici IBM degli anni '60.

Ritieni che ci sia un'assenza di simmetria nella legge 547, vale a dire che si dovrebbero punire anche le aziende che non si difendono in maniera appropriata dagli hacker?

No, secondo me è assurdo punire la non-difesa. Il motivo, a mio parere, è molto semplice: se **non** sei difeso, qualcuno entrerà e creerà casini grossi. E se i casini grossi continuano per molto tempo, e tu sei un provider, alla fine chiudi. E' un sistema che s'autoregola, una specie di selezione naturale. No ha molto senso creare una legge per forzare la gente a

proteggersi… Ed è per questo che, a mio parere, l'hacking fatto in modo "giusto" è fondamentale per aumentare la sicurezza in rete. E quello non dovrebbe essere punito. Se scopro le debolezze di un sistema, e mando una mail al root facendoglielo notare, e avvertendolo che non è stato abbastanza bravo da salvaguardare i dati privati dei suoi clienti, gli ho fatto sostanzialmente una consulenza gratis. Come dire: un host è un albergo. Appartiene a qualcuno, e le persone lo usano per (dormire) registrare i propri dati. L'oste (la persona) dovrebbe, in effetti, fare di tutto per chiudere la porta d'ingresso a chiave, per evitare che ladri entrino e rubino le cose dei suoi clienti. Ma se uno fa un test, vede che la porta era aperta, e gli lascia un bigliettino, dicendogli come deve chiuderla…non vedo come sia punibile per legge. Se poi, dopo la letterina, l'oste tiene la porta aperta senza tenere presente i consigli, per svogliatezza o per incompetenza, allora l'hacker avrebbe il **diritto** di dire questa cosa a tutti, di allarmare. E l'oste non dovrà lamentarsi della cattiva pubblicità…

Il difficile rapporto tra gli hacker e la stampa. Credi che vi sia un accanimento particolare o gli hacker sono effettivamente come vengono descritti?

Le persone hanno un problema fondamentale: leggono i giornali. Questo di per se non sarebbe un problema insormontabile. Il disastro comincia quando cominciano a **credere** ai giornali…
Mi è successo una decina di volte, di leggere fatti di cui, in effetti, ero a conoscenza. Dieci volte su dieci, erano così distorti da diventare quasi comici. Non compatisco le persone per pensare che l'hacker sia un criminale. Il mare di stupidaggini che le bombarda tutti i giorni le giustifica al 100%. Un articolo che parla di hacker in modo corretto si perde nel mare d'immondizia che lo circonda.

Allegato n.2

Vengono di seguito forniti i link ad alcune pagine Web, reperibili all'indirizzo generico www.poliziastato.it, relative alla legge 547/'93, alle note procedurali che la riguardano, ed alle principali indagini informatiche svolte dalla polizia tra il 1990 ed il 1998.
Tali documenti consentono un approfondimento dei paragrafi legislativi redatti nei capitoli 3 e 7, tuttavia per chi volesse una maggiore completezza d'informazione sull'operato della polizia si consiglia l'esame dell'intero sito, rintracciabile al citato indirizzo.

- Commenti in merito alla legge 547/'93 come strumento legislativo (il link è www.poliziadistato.it/nopt4.htm
- Elenco articoli modificati dalla legge 547/'93 e relative note procedurali (il link è www.poliziadistato.it/nopt_leg.htm
- Elenco principali indagini informatiche relative agli ultimi anni (il link è www.poliziadistato.it/nopt5.htm

Riferimenti bibliografici

Testi

Alessio, G. – ***L'Internet*** – SEAM, Roma, 1997.
Arata, A. – ***Navigando. Guida introduttiva al mondo della rete Internet*** – Flashnet, Roma, 1996.
Artieri, G. B. – ***Lo sguardo virtuale –*** Franco Angeli, Milano, 1998.
Ahuja, V. – ***Sicurezza in Internet e sulle reti*** – McGraw, Roma, 1996.
Bender, G, e Druckrey, T. – ***Tecnocultura. Visioni, ideologie, personaggi*** – Urrà-Apogeo, Milano, 1996.
Berardi, F. – ***Ciberfilosofia*** – Castelvecchi, Roma. 1995.
Berger, P. L. e Luckmann, T. – ***La realtà come costruzione sociale*** – Il Mulino, Bologna, 1969.
Berretti, A. e Zambardino, V. – ***Internet, avviso ai naviganti*** – Donzelli, Roma, 1995.
Berzano, L. e Prina, F. – ***Sociologia della devianza*** – La Nuova Italia Scientifica, Roma, 1995
Breton, P. – ***L'utopia della comunicazione*** – UTET, Roma, 1995.
Chiccarelli, S. e Monti, A. – ***Spaghetti hacker*** – Apogeo, Milano, 1997.
Collins, R. – ***Teorie sociologiche –*** il Mulino, Bologna, 1992.
Cooley, C. H. – ***Human nature and the social order*** – Scribner, New York, 1902.
Crespi, F. – ***Le vie della sociologia –*** Il Mulino, Bologna, 1985.
De Carli, L. – ***Internet. Memoria ed oblio*** – Bollati Boringhieri, Torino, 1997.
De Kerckhove, D. – ***Brainframes*** – Baskerville, Bologna, 1993.
De Nardis, P. – ***L'equivoco sistema –*** Franco Angeli, Milano, 1991.
Di Spirito, F., Ortoleva, P. e Ottaviano, C. – ***Lo strabismo telematico –*** UTET, Roma, 1996.
Frosini, V. – ***Contributi ad un diritto dell'informazione*** – Liguori, Napoli, 1991.
FTI – ***Osservatorio sulla criminalità informatica, rapporto 1997*** – Franco Angeli, Milano, 1997.
Gallino, L. – ***Dizionario della sociologia –*** UTET, Torino, 1993.
Giorda, G. – ***Inviati nel cyberspazio*** – Asca, Milano, 1996.
Goffman, E. – ***La vita quotidiana come rappresentazione*** – Il Mulino, Bologna, 1969.
Hance, O. – ***Internet e la legge*** – McGraw-Hill, Roma, 1997.
Herz, S. C. – ***I surfisti di Internet*** – Feltrinelli, Milano, 1995.
Husserl, E. – ***La crisi delle scienze e la fenomenologia trascendentale –*** Nijhoff, Aia, 1954.
Ingrassia, G. e Paterna, G. – ***Comunicazione sociale: crimini e devianze nel postmoderno informatico*** – Giappichelli, Torino, 1989.
IPACRI (a cura di) – ***Computer crime, virus, hackers: metodi d'indagine e strumenti di protezione*** – Buffetti, Roma, 1989.
Izzo, A. – ***Anomia: analisi e storia di un concetto –*** Laterza, Bari, 1996.
Levy, S. – ***Hackers, gli eroi della rivoluzione informatica*** – Ed. Shake, Milano, 1996.
Lyon, D. – ***L'occhio elettronico –*** Feltrinelli, Milano, 1997.
Luhmann, N. – ***Sociologia del diritto –*** Laterza, Modena, 1977.
Luhmann, N – ***Sistema giuridico e dogmatica giuridica*** – Il Mulino, Bologna, 1978.
Luhmann, N. – ***Sistemi sociali –*** il Mulino, Bologna, 1984.
Luhmann, N. – ***La differenziazione del diritto –*** Il Mulino, Bologna, 1990.
Luhmann, N. – ***Sociologia del rischio*** – Mondadori, Bologna, 1996.
Luther Blisset – ***Net*** Gener@tion – Mondadori, Milano, 1996.

Macioti, M. I. – ***Il concetto di ruolo nel quadro della teoria sociologica generale –*** Laterza, Bari, 1993.
Maldonado, T. – ***Critica della ragione informatica –*** Feltrinelli, Milano, 1997.
Mansell, R. – ***Le telecomunicazioni che cambiano*** – UTET, Roma, 1996.
Mantovani, G. – ***Comunicazione e identità –*** Il Mulino, Bologna, 1995.
Mantovani, G. – ***L'interazione uomo-computer –*** Il Mulino, Bologna, 1995.
Mead, G. H. – ***Mind, self, society*** – University of Chicago Press, Chicago, 1934.
Morcellini, M. – ***Passaggio al futuro*** – F. Angeli, Milano, 1992.
Negroponte, N. – ***Essere digitali –*** Sperling & Kupfer, Milano, 1995.
Postman, N. – ***Technopoly: la resa della cultura alla tecnologia*** – Bollati Boringhieri, Torino, 1993.
Rheingold, H. – ***Comunità virtuali*** – Sperling & Kupfer, Cuneo, 1994.
Riesman, D. – ***La folla solitaria*** – Il Mulino, Bologna, 1956.
Scelsi, R. V. – ***Ciberpunk, antologia di testi politici –*** Ed. Shake, Milano, 1992.
Scelsi, R. V. – ***No Copy-right, nuovi diritti del 2000*** – Ed. Shake, Milano, 1994.
Serra, C. e Strano, M. – ***Nuove frontiere della criminalità: la criminalità tecnologica*** – Giuffrè, Milano, 1997.
Sterling, B. – ***Giro di vite contro gli hackers*** – Ed. Shake, Milano, 1993.
Stoll, C. – ***Il nido del cuculo*** – Sperling & Kupfer, Milano, 1990.
Stoll, C. – ***Miracoli virtuali: le false promesse di Internet e delle autostrade dell'informazione*** – Garzanti, Milano, 1996.
Strano Network – ***Nubi all'orizzonte*** – Castelvecchi, Roma, 1996.
Turkle, S. – ***La vita sullo schermo*** – Apogeo, Milano. 1997.
Wolf, M. – ***Teorie delle comunicazioni di massa*** – Bompiani, Milano, 1994.

Indirizzi Web citati all'interno della tesi

www.poliziastato.it
www.repubblica.it
www.caffeeuropa.it
www.galileo.it
www.cultdeadcow.com
http://beast.cc.emory.edu
www.cert-it.it
www.inews.it
www.puntoinformatico.it
www.interlex.com
www.internos.it
www.altavista.com
www.alchera.it
www.gutenberg.net
www.liberliber.it
www.gandalf.it
www.pacse.censis.it
www.anonymizer.com
www.pgp.com
www.citinv.it
www.apogeonline.com
www.the-watchers.demon.co.uk
www.mediaservice.net

Articoli citati all'interno del lavoro

Bordieu, P. – ***L'opinione pubblica non esiste*** – dal trimestrale "Problemi dell'informazione", pubblicato nel 1976.

Usai, A. –***Pedofilia & Internet, una caccia alle streghe*** – dal sito www.repubblica.it del 27/10/'97.

Monti, A. – ***Brevi note sulla recente giurisprudenza di diritto delle tecnologie*** – dal sito www.interlex.com del 10/11/'97.

Usai, A. – ***Il poliziotto hacker alla caccia dei criminali*** – dal sito www.repubblica.it del 13/2/'98.

Maselli, A. – ***Hong Kong, il nuovo covo dei pirati informatici*** – dal settimanale "Computer Valley" n.24, allegato a "La Repubblica" del 26/3/'98.

Anonimo – ***Internet devasta la privacy*** – dal sito www.repubblica.it del 16/4/'98.

Maselli, A. – ***Hacker reo confesso*** – dal settimanale "Computer Valley" n.27, allegato a "La Repubblica" del 16/4/'98.

Mandò, M. – ***Internet, quanti sono i navigatori italiani?*** – dal sito www.repubblica.it del 28/4/'98.

Livraghi, G. – ***Alice nel paese delle ipocrisie*** – dall'archivio del sito www.gandalf.it, primavera'98.

Anonimo – ***Gli hackers assalgono il Pentagono*** – dal sito www.repubblica.it, fine aprile'98.

Usai, A. – ***Tra privacy e libertà Internet in cerca di regole*** – dal sito www.repubblica.it del 8/5/'98.

Gerino, C. – ***Virus in rete –*** dal settimanale "Computer Valley" n.32, allegato a "La Repubblica" del 21/5/'98.

Usai, A. – ***Software pirata*** – dal settimanale "Computer Valley" n.33, allegato a "La Repubblica" del 28/5/'98.

Anonimo – ***Una sfida in piena regola ai pirati dell'informatica*** – dal sito www.puntoinformatico.it del 16/6/'98.

Anonimo – ***Argentina, copiare software è legale*** – dal settimanale "Computer Valley" n.37, allegato a "La Repubblica" del 25/6/'98.

Usai, A. – ***Hacker sul sito Rai "sostituiscono" il Gr1*** – dal sito www.repubblica.it del 13/7/'98.

Fusani, C. – ***Tentata violenza via Internet*** – dal quotidiano "La Repubblica" del 19/7/'98.

F.D.S. – ***Gli Italiani scoprono il Web –*** dal settimanale "Computer Valley" n.41, allegato a "La Repubblica" del 23/7/'98.

Bruschi D. - ***…e l'Italia sta a guardare*** – dal sito www.inews.it del luglio'98.

Anonimo – ***Hacker, assalto alla Microsoft –*** dal sito www.repubblica.it del 4/8/'98.

Anonimo – ***Aziende, gli hacker sono i dipendenti –*** dal settimanale "Computer Valley" n.44, allegato a "La Repubblica" del 17/9/'98.

Tremolada, L. – ***Si diffonde il Macro-contagio –*** dal sito www.repubblica.it del 17/9/'98.

Usai, A. – ***L'Arsenio Lupin dei giorni nostri –*** dal settimanale "Venerdì" di Repubblica n.550, allegato a "La Repubblica" del 25/9/'98.

Usai, A. – ***Poliziotti, manette on-line –*** dal settimanale "Venerdì" di Repubblica n.550, allegato a "La Repubblica" del 25/9/'98.

Vulpi, D. – ***Pirati o Robin Hood –*** dal sito www.galileo.it sez. archivio dossier '98.

Vulpi, D. – ***La legge del Web*** – dal sito www.galileo.it sez. archivio dossier '98.

Maselli, A. – ***Un filtro poco democratico –*** dal settimanale "Computer Valley" n.46, allegato a "La Repubblica" del 1/10/'98.

Usai, A. – ***Hacker scrocconi con un 167 del Viminale –*** dal sito www.repubblica.it del 4/11/'98.

Vinci, E. – ***Pirati di Internet al Viminale –*** dal quotidiano “La Repubblica” del 5/11/’98.
Ferrari, E. M. – ***Il Back Orifice, porta aperta nel p.c. –*** dal settimanale “Computer, Internet ed altro” n.7, allegato a “La Repubblica” del 19/11/’98.
Monti, A. – ***Hacker contro pedofili: crociata o istigazione a delinquere?*** – dal sito www.interlex.com del 3/12/’98.
Anonimo – ***Hacker contro pedofili: l’hacker risponde*** – dal sito www.interlex.com dell’8/12/’98.
Chiesa, R. – ***Hacking in Italia, a first overview –*** dal sito www.apogeonline.com del 7/1/’99.
Monti, A. – ***Hacker contro pedofili: “Un po’ di spoofing è reato”*** – dal sito www.interlex.com dell’11/1/’99.
Di Nicola, A. – ***I tecnodelinquenti fanno danni per miliardi –*** dal settimanale “Computer, Internet ed altro” n.14, allegato a “La Repubblica” del 21/1/’99.
Minardi, S. – ***La biblioteca globale che vive sulla rete –*** dal settimanale “Computer, Internet ed altro” n.14, allegato a “La Repubblica” del 21/1/’99.
Masera, A. – ***Guardie e ladri*** – dal settimanale “Panorama Web” n°4, allegato a “Panorama” del 28/1/’99
Novari, E. – ***E-Mail, attenzione si, fobia no*** – dal sito www.internos.it del 29/1/’99.
Casella, P. – ***Hacker, il nuovo cattivo di Hollywood –*** dal sito www.caffeeuropa.it del 29/1/’99.
Stagliano, R. – ***La triste parabola del pirata travel –*** dal sito www.caffeeuropa.it del 29/1/’99.

Ringraziamenti

Dopo più di un anno di lavoro, quattordici mesi per la precisione, siamo arrivati ai ringraziamenti. Sono tante le persone che mi hanno aiutato, in diversi modi, nel portare a termine questa tesi, che in alcuni momenti è sembrata essere quasi “di gruppo” per l’interesse e la partecipazione che è riuscita ad attirare.
Desidero ringraziare, inizialmente, tutti quelli che mi hanno sostenuto ed incoraggiato durante questi mesi, ed in particolare Francesca e Vincenzo per il tempo dedicato a seguire i tortuosi sentieri del mio pensiero, e Sergio per i preziosi prestiti culturali.
La rete è stata fonte di amicizie e collaborazioni, ed in proposito è d’obbligo un grazie particolare a Federica, Lidia e Jusy, per la rapidità e l’intelligenza delle loro risposte via mail e per lo spazio messomi a disposizione nei loro siti Web.
Un pensiero caloroso va a tutto il CDD, ed in particolare a Sandra, Cinzia, Giuseppe, Marco, Andrea e Federico, per i validi suggerimenti tecnici ed il provvidenziale aiuto nella ricerca on-line.
Un sentito ringraziamento va rivolto, in primis, al Professor Russi ed al Professor Marinelli, per l’attenzione e l’interesse dimostrato nei confronti del mio lavoro, nonché naturalmente alla Dott.ssa Barbara Mazza, che con pazienza e costanza ha saputo affiancare e sostenere il mio impegno durante questi lunghi mesi, contribuendo attivamente al buon esito raggiunto.

Enrico Novari