

COMPUTER ETHICS

UN QUADRO CONCETTUALE

Fin dalla sua nascita, la *Computer Ethics* è stata una materia con diverse direzioni di ricerca: quelle che considerano l'informatica come un campo da studiare con gli strumenti classici della filosofia, quelle che ritengono necessaria una nuova disciplina dedicata ai dilemmi etici specifici legati ai computer, altre che attribuiscono la sua stessa fondazione al padre della cibernetica, Wiener. Questo articolo, dopo una breve introduzione storica, descrive la materia con un approccio da etica applicata per arrivare ad una definizione di una metodologia utile per i corsi universitari di *Computer Ethics*.

1. INTRODUZIONE

Forse il primo scienziato a riflettere sugli aspetti etici e sociali legati ai computer, ad individuare le connessioni tra Etica e *Information Technology* fu Norbert Wiener, professore al MIT negli anni '50 e padre della cibernetica. Egli infatti invitò a riflettere sulle rivoluzionarie conseguenze sociali che questa nuova tecnologia avrebbe prodotto. Nel 1948, nel suo libro sulla cibernetica scrisse: "... mi resi subito conto che eravamo in presenza di una tecnologia che, nel bene o nel male, avrebbe potuto avere potenzialità inaudite da un punto di vista sociale" [40]. Nel suo libro successivo *The Human Use of Human Beings: Cybernetics and Society*, dedicato esclusivamente a riflessioni sulla tecnologia, troviamo già i concetti fondamentali della *Computer Ethics* [41]. Secondo Wiener la diffusione dei computer nella società avrebbe portato a cambiamenti con conseguenze tali da toccare ogni aspetto della nostra vita.

Il primo a raccogliere l'invito a riflettere sulle conseguenze etico-sociali della tecnologia dell'informazione fu, nel 1968, Donn Parker,

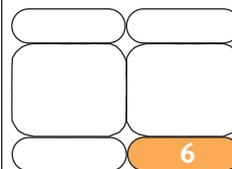
uno dei più noti ricercatori dello *Stanford Research Institute* (SRI) di Menlo Park. In uno degli articoli che segna un'altra tappa fondamentale nella storia della *Computer Ethics*, "*Rules of Ethics in Information Processing*", scrisse: "... sembra che quando le persone entrano nella sala computer lascino l'etica alla porta" [29]. Parker, raccolse e analizzò molti casi di attività legati ai computer e professionalmente poco etici e contribuì in modo sostanziale all'elaborazione del primo Codice Etico di Condotta Professionale della ACM (*Association for Computing Machinery*) la più antica associazione professionale di informatica. Dal 1973 questo codice venne adottato dalla ACM e, da allora, costituisce un punto di riferimento sostanziale.

Sempre negli anni '70 troviamo un altro professore del MIT, Joseph Weizenbaum, che lanciò un forte appello alla comunità scientifica per mettere in guardia dai rischi connessi con le applicazioni militati delle tecnologie dell'informazione [39].

La prima volta che il termine "*Computer Ethics*" venne usato, fu nel 1978, quando Walter Maner,



Norberto Patrignani



0

1

0

della Old Dominion University in Virginia, diede la prima definizione: "... campo di indagine che affronta i problemi etici creati, trasformati o aggravati dall'*Information Technology*" [24]. I suoi contributi attivarono il dibattito in molte università statunitensi a seguito del quale furono proposti agli studenti i primi seminari sul tema. Nel frattempo, i computer si diffondevano nella società e, con la rivoluzione del *personal computing*, con l'apparizione dei primi virus informatici nella nascente rete Internet, con le prime notizie riguardanti invasioni della privacy e disastri causati da malfunzionamenti dei computer, aumentò la consapevolezza delle conseguenze etico-sociali dell'*Information Technology*.

Arriviamo così al 1985, considerato l'anno di fondazione della disciplina *Computer Ethics*. Infatti in quell'anno James Moor, del Dartmouth College, pubblicò il suo famoso articolo *What is Computer Ethics?* [26] e Deborah Johnson, del *Rensselaer Polytechnic Institute*, il suo libro fondamentale *Computer Ethics* [15]. Nel 1983 nasceva a Palo Alto la *Computer Professionals for Social Responsibility* (CPSR), la prima organizzazione internazionale di docenti universitari, ricercatori e *computer professional* con la missione di portare all'attenzione pubblica le scelte critiche riguardanti le applicazioni dell'informatica e le loro conseguenze sulla società, sfatare i miti sull'infallibilità dei sistemi tecnologici e incoraggiare l'uso della tecnologia dell'informazione per migliorare la qualità della vita.

Tutte le energie della CPSR vennero dedicate a contrastare il progetto SDI (*Strategic Defense Initiative*), annunciato nel 1983 dal Presidente Reagan e più noto come *Star Wars*, dove decisioni molto critiche, come il lancio di missili intercontinentali, rischiavano di essere delegate ai computer.

Le ragioni della CPSR vennero espone nel famoso libro "*Computers in Battle: Will They Work?*" che rappresenta ancora oggi una pietra miliare nella denuncia dei rischi legati all'utilizzo dei computer in guerra [2].

La prima conferenza internazionale multidisciplinare sulla *Computer Ethics*, con la partecipazione di docenti di Informatica, *computer professional*, filosofi, sociologi, psicologi, giuristi, economisti, giornalisti e rappresentanti della pubblica amministrazione si tenne

nel 1991 a New Haven, negli USA. Nello stesso anno la materia *Computer Ethics* venne ufficialmente introdotta nei piani di studi di Informatica (*Computer Science*) delle università statunitensi [6].

Negli anni '90 emerse l'esigenza di avere, da questa disciplina, delle indicazioni anche pratiche, un'*etica applicata* che aiutasse a ridurre la probabilità del verificarsi di effetti imprevisti ed indesiderati derivanti dall'applicazione dell'*Information Technology* e a predisporre delle linee guida, dei codici etici per i progettisti di sistemi complessi che escono dai laboratori di ricerca per diffondersi nella società, offrendo servizi ed applicazioni al pubblico più vasto.

Nasceva così in Europa il *Centre for Computing and Social Responsibility* (CCSR, De Montfort University, UK). Il CCSR, diretto dai professori Simon Rogerson, Terry Ward Bynum e Donald Gotterbarn, oggi è un punto di riferimento mondiale per la ricerca e la formazione sui rischi ed opportunità dell'IT.

Il CCSR è anche l'organizzatore della conferenza internazionale sulla *Computer Ethics* che si tiene regolarmente ogni due anni (l'ultima, ETHICOMP 2008, si è svolta a Mantova, sotto la direzione di Mariacarla Calzarossa e Ivo De Lotto dell'Università di Pavia).

Oggi la *Computer Ethics* sta rapidamente evolvendo verso quella che potremmo definire *Global Information Ethics*: per la prima volta nella storia dell'umanità siamo interconnessi su scala planetaria. Internet ed il World Wide Web ci pongono di fronte ai problemi etici dell'informatica su scala globale: pensiamo per esempio al problema della legislazione nel *cyberspazio* (dove sono le frontiere?) oppure al *cyberbusiness* (la gestione di transazioni commerciali su scala planetaria), agli effetti sulle culture e tradizioni di una *Global Education*, per non parlare del *Digital Divide* tra Nord e Sud del pianeta.

Dal 1991 i corsi di *Computer Ethics* si sono diffusi in tutto il mondo nelle varie facoltà di *Computer Science*, diventando ormai una parte organica della cultura di base dei professionisti dell'informatica, per citare alcuni corsi: *Ethics and the Law on the Electronic Frontier* al MIT, *Computer and Information Ethics* a Stanford; in Europa, oltre al già citato CCSR in UK, abbiamo *Ethics of Computing* del Prof. Jacques Berleur

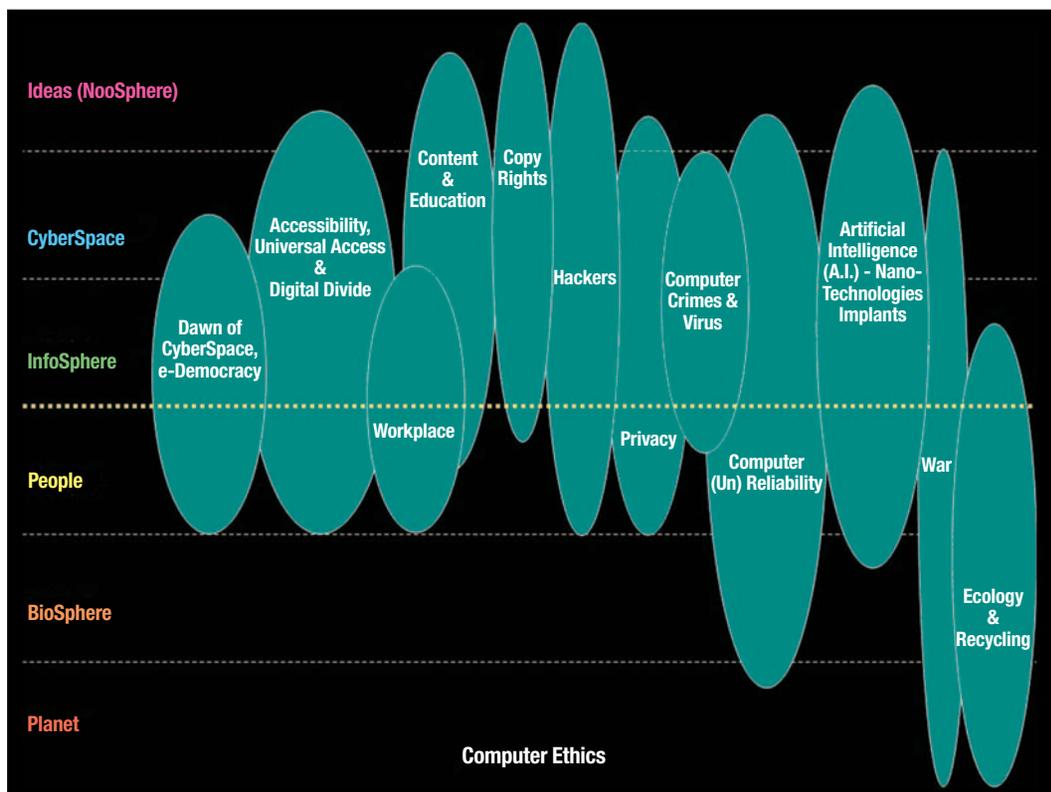


FIGURA 1
Un quadro concettuale per la Computer Ethics

(uno dei pionieri della materia in Europa) all'Università di Namur in Belgio, *Ethics of Information* di Luciano Floridi all'Università di Oxford. In Italia, il primo corso di *Computer Ethics* è stato introdotto dal Politecnico di Torino nel 2008, seguito dall'Università di Trento con *Ethics of Computing*. Al Politecnico di Milano abbiamo "Deontologia ed etica delle tecnologie dell'informazione" di Piercarlo Maggiolini. Questa materia è, per definizione, interdisciplinare (all'incrocio tra informatica, filosofia, giurisprudenza ecc.) e impone quindi un nuovo approccio che superi le tradizionali barriere tra tecnologi ed umanisti. Un esempio di eccellenza è lo storico dipartimento di *Science, Technology and Society* (STS) dell'Università della Virginia, diretto da Deborah Johnson. Cosa si intende per etica applicata all'*Information Technology*? Quali sono i principali argomenti e *critical issues* affrontati da questa nuova disciplina? La figura 1 offre una panoramica delle principali questioni emerse negli ultimi decenni. Esse pongono i responsabili dei sistemi informativi, i ricercatori, i *computer professional* e gli utenti finali, di fronte a veri e propri dilemmi etici e mettono in evidenza i punti di maggior vulnerabilità per la società dovuti sia

all'uso improprio o scorretto dei computer che al loro malfunzionamento.

2. UN QUADRO CONCETTUALE PER LA COMPUTER ETHICS

Questo quadro (Figura1) può essere semplicemente descritto nelle sue due dimensioni: la dimensione verticale (i "livelli") e la dimensione orizzontale (i "domini"). Ovviamente, come tutti i modelli, esso rappresenta una semplificazione della complessità del mondo reale, una semplice mappa qualitativa.

2.1. I livelli verticali

I livelli verticali rappresentano le diverse aree della realtà potenzialmente influenzate dai computer: dal mondo fisico reale (il pianeta, la biosfera, le persone) al mondo virtuale (l'infosfera, il ciber spazio, le idee). Vediamo una breve descrizione di ciascuno di questi "livelli".

2.1.1. IL PIANETA (*PLANET*)

Questo è il pianeta Terra, l'unico che abbiamo; nel modello proposto possiamo vedere che alcune aree hanno un impatto su questo livello più basso, come *Computer (Un)Reliability*, *War*

e, ovviamente, *Ecology & Recycling*. Quando analizziamo eticamente le azioni umane e le conseguenze delle tecnologie sviluppate dagli umani, dobbiamo includere anche gli ecosistemi e l'impatto a lungo termine nei confronti delle generazioni future [16].

2.1.2. LA BIOSFERA (*BIOSPHERE*)

Questo livello rappresenta l'intero mondo biologico vivente sulla Terra. Tutte le aree che hanno un impatto sul livello *Planet* hanno un impatto anche su questo livello immediatamente superiore; d'altra parte vi è un'area crescente nota come *Artificial Intelligence*, *Nanotechnologies*, *Implants* che cambierà il concetto di confine tra entità viventi / non-viventi (pensiamo ai *nano-bots*: macchine autonome a scala nanometrica in grado di muoversi all'interno del nostro corpo per applicazioni mediche come il trasporto di farmaci verso organi bersaglio; oppure pensiamo all'impianto di dispositivi miniaturizzati all'interno del nostro corpo in grado di interfacciare direttamente il sistema nervoso con l'esterno ecc.).

2.1.3. LE PERSONE (*PEOPLE*)

Questo livello rappresenta noi stessi, gli esseri umani; noi siamo toccati da tutti i "domini", le aree rappresentate con ellissi nella figura che riassume la *Computer Ethics*. La sfida per noi consiste nel ripensare l'intera disciplina dell'etica includendo nelle nostre analisi anche le speciali "macchine a stati finiti": i computer.

2.1.4. L'INFOSFERA (*INFOSPHERE*)

In questo contesto, con infosfera intendiamo il livello rappresentato dal sottile strato artificiale, costituito dalle tecnologie dell'informazione, che avvolge il pianeta. Esso rappresenta Internet, la Rete: l'insieme di hardware, software, computer, reti, router ecc. che costituisce il prezioso guscio attorno al pianeta che collega tutti noi, qualsiasi cosa, da qualunque punto del pianeta. Con le sue caratteristiche originali quali: standard aperti, architettura *peer-to-peer*, assenza di un punto centrale di controllo (e di guasto), neutralità (solo il mittente e destinatario conoscono i contenuti dei pacchetti di bit, la Rete si limita a smistare con efficienza i dati guardando solo agli indirizzi dei pacchetti), l'infosfera sta diventando talmente importante che, come il

pianeta Terra, dovremmo preservarla per le generazioni future.

2.1.5. IL CIBERSPAZIO (*CYBERSPACE*)

Questo nuovo livello, ancora in costruzione, è uno spazio virtuale al di sopra dell'infosfera, dove iniziamo a spendere gran parte della nostra vita [11]. Sono ormai innumerevoli gli esempi di applicazioni in questo spazio dove il confine tra mondo reale e virtuale si sta dissolvendo: social networks con avatar, realtà virtuali, videogame immersivi tridimensionali, giochi online multi-utente ecc..

2.1.6. LE IDEE "IDEAS" (*NOOSPHERE*)

Questo è lo strato al massimo livello di astrazione, probabilmente il più delicato. Esso rappresenta la risorsa più preziosa che abbiamo: la raccolta delle idee che fluiscono nelle menti umane, il pensiero umano nel suo insieme, l'eredità di conoscenza e saggezza dal passato ed il potenziale innovativo verso il futuro, la cosiddetta Noosfera [8]. Il libero flusso delle informazioni e l'approccio alla tecnologia tipico dell'etica hacker possono contribuire fortemente ad alimentare questo spazio (il *public-domain*) che è l'humus di una società davvero innovativa, come la società *knowledge-based* del futuro prossimo. Ecco perché il livello delle idee è toccato dagli ellissi dei domini *Copyrights* e *Hackers*.

2.2. I domini orizzontali

I domini orizzontali, rappresentati dalle ellissi della figura 1 (con le dimensioni approssimativamente proporzionali alla loro importanza o impatto potenziale), costituiscono una panoramica delle principali aree di criticità o di attenzione della *Computer Ethics*. La posizione verticale di una ellisse individua i livelli interessati da tale dominio. Esse rappresentano anche l'insieme delle questioni più critiche create o aggravate dai computer. Vediamo ora una descrizione dei principali interrogativi relativi a ciascun dominio.

2.2.1. DAWN OF CYBERSPACE, e-DEMOCRACY

Quali sono i nuovi scenari aperti dall'alba del cyberspazio? Quali sono le nuove metafore di cui abbiamo bisogno per sviluppare un uso appropriato di questo spazio? Come (e dove) usare questi nuovi strumenti di partecipazione alla vita pubblica, per discutere, per contri-

buire a dibattiti su questioni controverse, per confrontarsi con le pubbliche amministrazioni, per prendere decisioni, per votare? [4, 21]. La possibilità di avere identità multiple negli spazi virtuali sta aprendo diverse questioni etiche molto critiche: quale è la responsabilità sociale di un avatar? Quali sono le differenze negli aspetti di partecipazione e democrazia quando passiamo dal mondo fisico al mondo virtuale? Le tecnologie dell'informazione saranno "tecnologie di libertà" o "tecnologie di controllo", utopiche o distopiche? Esse espanderanno la partecipazione informata, la libertà e la democrazia, oppure diventeranno uno strumento per la manipolazione dell'opinione pubblica in una società a "controllo totale"?

In secoli di storia gli umani hanno sviluppato alcuni principi fondamentali che dobbiamo tenere presenti quando progettiamo applicazioni di "democrazia virtuale" o "iper-democrazia":

- ❑ la partecipazione diretta (non necessariamente mediata da rappresentanti);
- ❑ la discussione di diverse opzioni (non solo il loro conteggio come nei sondaggi);
- ❑ l'ascolto, l'apertura alle opinioni delle altre persone, la tolleranza;
- ❑ l'opportunità e la capacità di sostenere la propria opinione di fronte agli altri (non solo la comunicazione della propria scelta, spesso ristretta a poche opzioni selezionate "da casa"). Può la partecipazione essere a distanza, anonima, senza contatto fisico? Ha senso una agorà virtuale?

Altre caratteristiche importanti:

- ❑ la comunicazione orizzontale (da-molti-a-molti, non solo comunicazione verticale da-uno-a-molti, come in televisione);
- ❑ l'assunzione di responsabilità per le conseguenze delle proprie scelte (non solo risposte anonime);
- ❑ la pazienza (la democrazia è un processo necessariamente lento, mentre la tecnologia rischia di accelerare drammaticamente i processi decisionali senza rispettare i tempi umani; eppure la democrazia è per-gli-umani, tra-gli-umani);
- ❑ la riflessione (la nostra mente richiede tempo, silenzio, se vogliamo avere strumenti critici per poter influenzare la realtà dobbiamo in qualche modo fermare gli input, non possiamo limitarci a ricevere passivamente milioni di messaggi, la nostra mente ha una

"banda" limitata che dovremmo rispettare). Quando progettiamo le applicazioni di *e-participation* dovremmo attentamente considerare tutte queste virtù della democrazia antiche e consolidate.

2.2.2. ACCESSIBILITY, UNIVERSAL ACCESS & DIGITAL DIVIDE

Quali sono le nuove barriere (economiche, culturali, sensoriali) che rischiamo di innalzare quando sviluppiamo l'*Information Society*? Come possiamo garantire l'accesso alle risorse di conoscenza usando dei criteri giusti ed inclusivi? Come possiamo evitare di imporre nuove restrizioni alle persone con disabilità, alle persone anziane? [36].

Come possiamo preservare la cosiddetta "neutralità della rete" di fronte alle pressioni ed al massiccio attacco proveniente dai proprietari delle principali tratte della Rete stessa (esempio, le grandi compagnie telefoniche) che vogliono arrivare a segmentare gli utenti offrendo servizi di traffico prioritari di prima classe? Se i pacchetti di prima classe avranno priorità negli snodi della rete, inevitabilmente verranno ritardati i pacchetti degli utenti in seconda classe.

Come possiamo governare e gestire Internet in modo equo ed etico? Come possiamo arrivare a definire una "Costituzione" per questo nuovo spazio virtuale? Come la discutiamo, approviamo (e facciamo applicare)? [33].

La sfida consiste nel trovare la giusta miscela tra i quattro principali strumenti per la *governance* di Internet:

- ❑ educazione (codici etici, *soft-laws*);
- ❑ leggi (vincoli legali internazionali, *hard-laws*);
- ❑ architettura tecnologica (evoluzione dei protocolli di rete, nuovi sviluppi tecnologici);
- ❑ mercato (autoregolazione) [19].

2.2.3. WORKPLACE

Quali nuovi problemi e rischi professionali introduce il computer nel luogo di lavoro? Come vengono coinvolti i lavoratori, gli utenti finali nella progettazione dei nuovi sistemi? [7].

Quali sono le principali responsabilità dei *computer professional*, dei progettisti? [12].

Una delle aree che richiedono più ricerca è, ad esempio, quella del cambiamento in qualità (e quantità) dei posti di lavoro quando un processo viene automatizzato, o quando la maggio-

ranza dei processi di un'organizzazione vengono eseguiti da un sistema ibrido dove i compiti sono svolti dalle persone e dai computer.

2.2.4. CONTENT & EDUCATION

Come selezionare, raccogliere, organizzare e diffondere i contenuti sulla rete? [18]. Se l'educazione è principalmente un processo di trasmissione di informazioni e conoscenze verso i nostri figli, chi seleziona i contenuti che verranno ereditati dalle future generazioni? Quale è il ruolo etico dei motori di ricerca in queste aree? [42]. E ancora, quale impatto avranno i computer sulle nostre capacità di apprendimento?

2.2.5. COPYRIGHTS

Come dovrebbero evolvere i meccanismi di incentivazione per gli artisti, per gli innovatori nel nuovo scenario della società della conoscenza? [20]. Se la tecnologia dell'informazione ha definitivamente cambiato le modalità con le quali possiamo copiare (la copia è indistinguibile dall'originale) e riutilizzare contenuti pre-esistenti, quali sono i nuovi modelli di business in grado di sostenere un'economia della conoscenza? Per quanto riguarda il software, cosa possiamo imparare dall'affermarsi del software *open-source* nei confronti del vecchio software proprietario? Le tecnologie dell'informazione sono forse lo strumento definitivo per, citando Newton [28] "salire sulle spalle dei giganti"?

2.2.6. HACKERS

Come dovremmo proteggere i sistemi dalle intrusioni? Come mettere a frutto l'etica *hacker* per il bene collettivo, per migliorare la sicurezza stessa dei sistemi e la loro affidabilità? [22]. Dobbiamo definire molto attentamente il confine tra un *hack* (per esempio, per mettere in evidenza un difetto o trovare un "baco") ed un reato informatico. La società dell'informazione ha bisogno di persone esperte e dotate di speciali capacità tecniche per poter provare e sollecitare i sistemi complessi in condizioni estreme.

2.2.7. PRIVACY

Come possiamo proteggere i dati sensibili nel ciberspazio? Dove è il limite tra la sicurezza /sorveglianza ed una società Orwelliana? Quali sono le implicazioni relative ai due approcci alternativi "*opt-in*" (un servizio non è sottoscritto se non esplicitamente richiesto dall'utente) e

"*opt-out*" (un servizio è accettato implicitamente dall'utente a meno che non richieda esplicitamente di essere rimosso)? [23].

Le applicazioni di *ambient intelligence* (negli USA viene usato il termine *ubicomp* per definire l'insieme di *ubiquitous computing* e *pervasive computing*), rappresentano una delle più grandi trasformazioni della storia dell'informatica. L'evoluzione verso il *disappearing computing* dove macchine intelligenti e sensori saranno attorno a noi, metterà l'ambiente stesso in grado di riconoscerci e di reagire alle nostre azioni. Le applicazioni *ubicomp* hanno l'immenso potenziale di migliorare le nostre vite, aumentando le nostre capacità comunicative (per esempio, visualizzando i livelli di attività o di variabili vitali di un familiare a distanza), automatizzando semplici compiti come riordinare medicinali scaduti, assistendo le persone con disabilità, mettendole in grado di partecipare pienamente alla vita sociale (per esempio, con convertitori testo-voce per chi ha problemi di vista), aiutando le persone anziane vulnerabili (ed esempio inviando un allarme quando cadono a terra o quando non prendono medicine vitali). D'altra parte, queste applicazioni hanno anche le potenzialità di condurci verso una società Orwelliana dove ogni azione di una persona viene controllata e registrata [14]: quali linee guida etiche dovrebbero essere usate da questi progetti *ubicomp*?

Dato che le nostre vite possono essere seriamente compromesse da errori nei database, come affronteremo i dilemmi etici (impliciti nella costruzione di database di grandi dimensioni come le banche dati del DNA) derivanti dalla necessità, da una parte, di assicurare il corretto funzionamento di una società democratica controllando i criminali e, dall'altra, di mantenere una società libera dalla sorveglianza? Come possiamo proteggere le nostre libertà civili da organizzazioni molto grandi e potenti, concentrate solo sulle loro missioni ed obiettivi, che usano il loro immenso potenziale tecnologico per controllare enormi quantità di comunicazioni, senza alcuna attenzione verso le conseguenze sociali? [5, 32].

2.2.8. COMPUTER CRIMES & VIRUS

Quale è la definizione di crimine informatico? Come possiamo proteggere i sistemi più importanti dai criminali informatici? [10]. Questo

dominio è separato da quello degli *Hackers* visto in precedenza in quanto gli *hacker* non sono da considerare, a priori, dei criminali¹. La questione più critica in questo caso è legata al fatto che i reati “senza vittime” (i tipici reati informatici sono “puliti”, raramente provocano direttamente dei danni fisici a persone). Questi reati stanno diventando diffusi che dovremmo educare molto attentamente le future generazioni di informatici per affrontare il problema dell’aumento incredibile di reati legati all’abuso dei computer [34].

2.2.9. COMPUTER (UN)RELIABILITY

Come possiamo migliorare l’affidabilità dei computer e proteggerci dai malfunzionamenti dei sistemi più critici per la vita umana? Perché il software è così inaffidabile? Chi e quando dovrebbe essere informato sui difetti più gravi nella sicurezza ed affidabilità delle applicazioni software? [27].

Chi è responsabile dei malfunzionamenti delle applicazioni *life-critical*? (pensiamo ai sistemi di guida automatizzata degli aerei, *fly-by-wire*, o delle auto, *drive-by-wire*, per non parlare delle applicazioni dove il software controlla apparecchiature ospedaliere). Sono responsabili i programmatori? I progettisti dell’hardware? Le aziende fornitrici delle apparecchiature? Gli utilizzatori?

Nell’ottobre 1985 nello storico gruppo di discussione su Internet *comp.risk* dedicato ai rischi ed affidabilità dei computer, apparve una definizione molto efficace del cosiddetto:

“Effetto Titanic: la gravità delle conseguenze di un malfunzionamento di un sistema è direttamente proporzionale alla convinzione del progettista che ciò non possa mai accadere”.

E del suo corollario: *“La quantità e qualità della ridondanza incorporata in un sistema è direttamente proporzionale al grado di consapevolezza riguardo ai malfunzionamenti”.*

Il dilemma etico qui consiste nell’evitare l’effetto Titanic.

¹ In genere la traduzione di *hacker* con “pirata informatico” usata da molti giornali non è propriamente corretta. Infatti letteralmente *hacker* andrebbe tradotto con “persona particolarmente esperta a programmare o a risolvere problemi con i computer”. Quando parliamo di criminali informatici il termine inglese più adatto è *cracker*.

2.2.10. ARTIFICIAL INTELLIGENCE

Quali sono le questioni profonde poste all’umanità dallo sviluppo dei robot (sia a scala umana che a scala nanometrica)? Perché delegare a macchine decisioni critiche per le vite umane? Quali questioni farà emergere l’arrivo dei *cyborg*, sistemi ibridi uomo-macchina? [17]. Dobbiamo iniziare a studiare un’etica per i robot come un’etica centrata sugli umani? Un’etica per gli umani coinvolti nello sviluppo dei robot? Come potremo costruire dei robot autonomi dotati di un “codice di condotta” (etica artificiale?) compatibile con lo sviluppo delle persone e della società? [37]. Quali saranno le questioni etiche più critiche quando avremo agenti artificiali a scala nanometrica (*nanobot*)? [1].

Come potremo affrontare aspetti come la nostra privacy (quando vi è qualcosa attorno e dentro di noi che raccoglie informazioni sui di noi), i reati informatici (chi sarà responsabile del controllo di queste nano-macchine?), l’affidabilità dei computer (come verranno provati i *nanobot*? Quali tipi di decisioni sarà in grado di prendere il software di cui sono dotati?), la longevità (saremo in grado di “ritirare” i *nanobot* per evitare l’effetto “vaso di Pandora”?) [31].

2.2.11. WAR

Quali sono le conseguenze dello sviluppo di armi “intelligenti” dove deleghiamo alle macchine la decisione finale di uccidere? [2]. Possiamo mettere nelle mani delle macchine il destino dell’umanità e del pianeta costruendo sistemi altamente computerizzati di difesa contro attacchi missilistici potenziali? [30]. Non abbiamo ancora idea delle conseguenze dello sviluppo di armi a scala nanometrica, dove avremo armi autonome dotate di sensori che rispondono a stimoli ambientali [3]; in questo caso le questioni etiche attraversano il confine degli umani ed arrivano a toccare anche l’ambiente.

2.2.12. ECOLOGY & RECYCLING

Come possiamo evitare o minimizzare i rischi ambientali e l’impatto dei cicli di produzione dell’hardware? [9]. Possiamo usare le tecnologie dell’informazione per minimizzare il nostro impatto sul pianeta? Possiamo pensare ad un approccio a ciclo-chiuso per il riciclaggio dei computer? La cosiddetta “legge di Moore”, il

raddoppio del numero di transistor in un chip ogni diciotto mesi, è sostenibile da un punto di vista ambientale? [35].

3. UNA METODOLOGIA PER L'ANALISI DI CASI DI STUDIO

Questo quadro concettuale viene attualmente sperimentato nell'analisi di casi di studio nel corso di *Computer Ethics* alla Scuola di Dottorato del Politecnico di Torino (Dottorato di Ricerca in Ingegneria Informatica e dei Sistemi). La metodologia usata parte dall'analisi di un caso reale, preso dalle notizie quotidiane o dalla letteratura, per poi studiarlo in dettaglio attraverso i seguenti quattro stadi.

□ **Scenario:** in questa fase viene effettuata una descrizione dettagliata del caso nel modo più completo ed obiettivo possibile.

□ **Stakeholders:** tutti i diversi "portatori di interesse" coinvolti vengono identificati con le loro (inter)relazioni.

□ **Ethical Issue(s):** ove vengono individuate le principali aree di attenzione (le ellissi viste prima) coinvolte nel caso in esame.

□ **Alternative scenario(s):** nella situazione descritta, come individuare le scelte giuste o sbagliate? Vi sono degli scenari alternativi possibili? Quale è il ruolo dei computer professional coinvolti nella progettazione delle tecnologie dell'informazione al centro dello scenario analizzato?

In genere, alla fine di questo processo, le questioni etiche più critiche vengono subito identificate. Per riuscire ad evitare (o perlomeno ad affrontare in qualche modo) tali questioni, vengono prodotte delle raccomandazioni a tre livelli:

□ **Education:** quali indicazioni possiamo fornire agli insegnanti, alle università che preparano le prossime generazioni di *computer professional*? Spesso, in classe, dopo discussioni approfondite, vengono identificati molti suggerimenti per gli esperti del settore.

□ **Guideline:** quali indicazioni possiamo fornire alle persone che definiscono i codici di condotta, le linee guida per le organizzazioni, le cosiddette *soft-laws*?

□ **Law:** quali raccomandazioni possiamo fornire a livello politico, alle autorità pubbliche, alle persone responsabili della definizione delle leggi, le *hard-laws*?

4. CONCLUSIONI

Le questioni identificate dalla *Computer Ethics* possono essere affrontate a molti livelli: a livello individuale, professionale e sociale. Un ruolo speciale spetta ai *computer professional*, nella definizione dei loro codici etici di condotta e nel fornire, al pubblico in generale ed ai decisori pubblici, tutte le informazioni sulle potenzialità, sui rischi e limiti delle tecnologie dell'informazione [13].

In Italia diverse università hanno introdotto corsi di *Computer Ethics* e questo contribuirà sicuramente alla formazione di figure complesse, persone che, oltre ad essere esperte, siano anche in grado di dare una giusta valutazione delle implicazioni sociali ed etiche della tecnologia dell'informazione.

Bibliografia

- [1] Allhoff F., Lin P., Moor J., Weckert J.: *Nanoethics: The Ethical and Social Implications of Nanotechnology*. Wiley-Interscience, 2007.
- [2] Bellin D., Chapman G.: *Computers in Battle: Will They Work?* Harcourt Brace Jovanovich, 1987.
- [3] Carrol-Mayer M., Fairweather N., Rogerson S., Carsten-Stahl B.: *Stealing a march on society: The Ethical Implications of the Nanotechnological Weapons Policy*. De Montfort University, Proceedings of Ethicomp2005.
- [4] Castells M.: *The Rise of the Network Society*. Blackwell, 1996.
- [5] Cauley L.: *NSA has massive database of Americans' phone calls*. USA Today, 10 May 2006
- [6] Computing Curricula, Social, Ethical and Professional Issues. *Communications of the ACM*, Vol. 34, n. 6, June 1991.
- [7] CPSR: *Computer Professionals for Social Responsibility*. Participatory Design Conference, MIT, 1992.
- [8] De Chardin T.: *The Phenomenon of Man*. Harper Perennial, 1976.
- [9] EU-WEEE: *EU Directive 2003/108/EC on Waste Electrical and Electronic Equipment*. (WEEE), 2003.
- [10] Forester T., Morrison P.: *Computer Ethics, Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press, 1993.
- [11] Gibson W.: *Neuromance*. Ace Books, 1984.
- [12] Gotterbarn D.: *Informatics and Professional Responsibility, in Computer Ethics and Professional Responsibility*. Ed. by Ward Bynum T., Rogerson S., Blackwell Publishing, 2004.

- [13] Gotterbarn D.: *Professionalism Issues*. Software Engineering Ethics Research Institute, Department of Computer and Information Sciences, East Tennessee State University, 2006.
- [14] Jean Camp L.: *Design for Privacy: Towards a Methodological Approach to Trustworthy Ubicomp Design*. Proceedings of Ethicomp2005.
- [15] Johnson, Deborah G.: *Computer Ethics*. Prentice-Hall; quarta ed. 2009, 1985.
- [16] Jonas H.: *Das Prinzip Verantwortung*. Insel Verlag, Frankfurt. English edition (1984): *The Imperative of responsibility. In search for an ethics for the technological age*. University of Chicago Press, 1979.
- [17] Joy B.: *Why the future doesn't need us*. Wired 8.04, 2000.
- [18] Koyle K.: *Access: not just wires*. CPSR Annual meeting, October 1994.
- [19] Lessig L.: *Code and other laws of cyberspace*. Basic Books, New York, 1999.
- [20] Lessig L.: *The future of ideas*. Random House, 2003.
- [21] Levy P.: *Collective Intelligence: Mankind's emerging World in Cyberspace*. Perseus, 1999.
- [22] Levy S.: *Hackers: Heroes of the Computer Revolution*. Anchor Press/Doubleday, 1984.
- [23] Lyon D.: *Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press, 1994.
- [24] Maner, Walter: *Starter Kit in Computer Ethics*. Helvetia Press (published in cooperation with the National Information and Resource Center for Teaching Philosophy), 1980. Originally self-published by Maner in 1978
- [25] Maner W.: *Unique Ethical Problems in Information Technology*. ETHICOMP95, 1995.
- [26] Moor J.H.: *What Is Computer Ethics?* In: Bynum, Terrell Ward, ed. 1985, *Computers and Ethics*. Blackwell, Published as the October 1985 Issue of *Metaphilosophy*, p. 266-75.
- [27] Neumann P.G.: *Computer-Related Risks*. Addison-Wesley, 1994.
- [28] Newton I.: *Letter to Robert Hooke*. 15 February 1676.
- [29] Parker, D.: Rules of Ethics in Information Processing. *Communications of the ACM*, Vol. 11., 1968, p. 198-201.
- [30] Parnas D.: *Why the SDI software system will be untrustworthy*. University of Victoria, 26 June 1995.
- [31] Patrignani N.: *NanoBots, the next frontier of Computer Ethics*. Ethics of Human Interaction with Robotic, Bionic, and AI Systems Workshop, supported by the ETHICBOTS European Project, Naples, 17-18 October, 2006.
- [32] Risen J.: *Bush Lets U.S. Spy on Callers Without Courts*. New York Times, 16 December 2005.
- [33] Rodotà S.: *Internet Bill of Rights*. Internet Governance Forum, Rio de Janeiro, 14 November 2007.
- [34] Rogerson S.: IS Security needs ethics. *ETHical in the IMIS Journal*, Vol. 12, n. 4, 2002.
- [35] Soesterberg: *Trans-Atlantic Network for Clean Production Meeting*, Soesterberg. The Netherlands, May 1999.
- [36] UN-WSIS: *Geneva Declaration of Principles*. World Summit on Information Society, 2003.
- [37] Veruggio G.: *A Proposal for Roboethics*. First International Symposium on ROBOETHICS, 30-th - 31-st January 2004, Villa Nobel, Sanremo, Italy.
- [38] Ward Bynum T.: *The Foundation of Computer Ethics*. AICEC99, 1999.
- [39] Weizenbaum, J.: *Computer Power and Human Reason: From Judgment to Calculation*. Freeman, 1976. Trad.it. "Il potere del computer e la ragione umana. I limiti dell'intelligenza artificiale", EGA-Edizioni Gruppo Abele - 1987.
- [40] Wiener, Norbert: *Cybernetics: or Control and Communication in the Animal and the Machine*. Technology Press., 1948.
- [41] Wiener, Norbert: *The Human Use of Human Beings: Cybernetics and Society*. Houghton Mifflin, 1950. (Second Edition Revised, Doubleday Anchor, 1954).
- [42] Winograd T.: *Speech at The Ethics and Politics of Search Engines Panel*. Santa Clara University Markkula Center for Applied Ethics, Santa Clara University Center for Science, Technology, and Society, February 27, 2006.

NORBERTO PATRIGNANI, Docente di Computer Ethics alla Scuola di Dottorato del Politecnico di Torino. Laureatosi con lode in Informatica presso l'Università degli Studi di Torino, dopo molti anni nell'Information Technology (1975-1999: ricercatore Olivetti a Ivrea; 1999-2004 analista METAGroup, Stamford, USA) si è concentrato sulle implicazioni sociali ed etiche dei computer, collaborando a progetti di ricerca e innovazione ed insegnando in diversi atenei italiani (Università di Trento, Statale e Cattolica di Milano). Collabora con la EU Commission, DG Science & Society ed è responsabile della sezione Etica dell'IT del Centro Studi Politeia di Milano.
E-mail: norberto.patrignani@unicatt.it