

Editoriale

... diamo i numeri

MONDO DIGITALE, rivista ufficiale di AICA (Associazione Italiana per l'Informatica e il Calcolo Automatico), nasce nel 2002 con l'obiettivo di seguire, documentare, approfondire e proporre a un pubblico specialistico e non, lo sviluppo del settore delle Tecnologie per l'Informazione e la Comunicazione nei diversi ambiti in cui queste trovano impiego e in cui diventano fattore trainante e innovativo.

Consentitemi di ripercorre *per numeri* la storia di questa rivista.

Dopo 40 numeri e quasi dieci anni di vita, siamo nel 2012: la rivista è stata ridisegnata, passando dal cartaceo al digitale, con l'obiettivo di mantenere tutti i contenuti che avevano caratterizzato fino a quel momento l'edizione cartacea arricchendoli però con quanto il supporto cartaceo non sarebbe stato in grado di offrire. Attraverso questa soluzione sono state messe a disposizione del lettore tutte le relazioni, i video e le interviste dei più importanti convegni organizzati periodicamente dalla Associazione.

L'evoluzione messa in atto non ha cambiato però la sua impostazione generale, sempre basata su articoli caratterizzati da breve, ma compiuta monografia dell'argomento trattato, con una esposizione rigorosa, ma accessibile anche ai non specialisti.

Il numero 61, l'ultimo del 2015, ha voluto introdurre una ulteriore novità: una duplice veste, ossia in digitale e su carta. Con tale scelta non si è voluto contraddire la profezia sulla "fine della carta", ma neppure ritornare al passato: questo numero consentirà di archiviare nelle nostre librerie la Rivista e documentare nel mondo "del sensibile" la nostra presenza e contributo. I due



media hanno infatti ciascuno i propri tratti distintivi e possono convivere proficuamente a vantaggio del lettore. E' stato pertanto deciso di offrire nel futuro, una volta all'anno, MONDO DIGITALE in duplice forma, diversificando questo numero "annuale speciale" anche in termini di contenuti. In particolare, questo numero "speciale" ha ospitato un articolo su una prospettiva fondamentale dell'era digitale, un problema filosofico sotto certi aspetti sconvolgente e cioè la "consapevolezza" delle macchine. L'autore? E' un ricercatore che ha fatto la storia delle Tecnologie Digitali: Federico Faggin, progettista nel 1971 del primo microprocessore al mondo, l'Intel 4004. Chissà che non si possa avere ogni anno un ospite di tale profilo!

Arriviamo al numero 63 e quindici anni di storia di MONDO DIGITALE, diretti per 47 numeri da Franco Filippazzi e, successivamente, da Viola Schiaffonati, con un Comitato Scientifico coordinato fino a oggi da Giulio Occhini.

E' un onore per me oggi, al numero 63, assumere il Coordinamento del Comitato Scientifico di MONDO DIGITALE, rivista che ho avuto modo di apprezzare durante questi 15 anni come lettore. Ringrazio il Comitato Direttivo di AICA per avermi proposto per questo incarico e ringrazio in particolare Giulio Occhini per aver seguito e guidato con passione (si è sempre potuta sentire nei suoi editoriali) il lavoro svolto durante i 62 numeri della Rivista.

Voglio rimanere sui numeri per richiamare alcuni fatti, eventi, persone, temi su cui fare brevi personali considerazioni legate alle tecnologie digitali nel nostro mondo di oggi.

Centosessanta sono gli anni trascorsi dal 1856, anno in cui nacque Nikola Tesla, ingegnere elettrotecnico, che darà un contributo fondamentale in molti campi della scienza e della tecnica, e grande visionario. Mi ha sempre colpito un suo articolo del 1926 su "The National Weekly" in cui scriveva: *Quando la logica wireless sarà perfettamente applicata, tutta la Terra sarà trasformata in un gigantesco cervello, ovvero in ciò che è in realtà: tutte le cose sono singole particelle di un unico e armonico insieme. E gli strumenti attraverso i quali l'uomo sarà in grado di fare questo saranno incredibilmente più semplici rispetto al nostro attuale telefono. L'uomo sarà in grado di portarne uno nel taschino del panciotto.*

Visionario? Forse non tutti indossano oggi il panciotto, ma sicuramente quasi tutti hanno un telefono in tasca o in borsetta. Quando il protocollo IPv6 introdotto nel 2008 sarà perfettamente integrato con tutti gli altri protocolli esistenti saranno inoltre disponibili un numero di indirizzi IP quasi impronunciabile e pari a 340.282.366.920.938.463.463.374.607.431.768.211.456, meglio scritto come 3.4×10^{38} . Pressoché impronunciabile è anche il numero di indirizzi IP per metro quadro della crosta terrestre: 655.570.793.348.866.943.898.599. Potremo avere in rete anche ogni singola lampadina di casa nostra e molto, ma molto di più. Non sarà senz'altro un "gigantesco cervello", ma avremo sicuramente una rete di dimensioni "impronunciabili": *l'Internet delle Cose evolverà nell'Internet di Qualunque Cosa? Si*

comincia già oggi a parlare di SPIMES, crasi di SPace+tiMES, termine con cui lo scrittore Bruce Sterling definisce oggetti rintracciabili attraverso lo spazio e il tempo per tutta la durata della loro esistenza. Abbiamo già assistito in questi ultimi anni a una evoluzione del Web: da un Web in cui *i dati sono altrove*, attraverso un Web in cui *le applicazioni sono altrove*, ad un Web in cui *le componenti fisiche del sistema sono massivamente distribuite e altrove*, fino a sfiorare temi fra il filosofico e fantascientifico in cui *noi siamo altrove* con i nostri avatar, ologrammi che chissà se potranno avere gradi di libertà d'azione anche in nostra assenza. Tutto ciò fa sorgere una domanda: e il fattore tempo? Quanto del nostro tempo dovrà essere dedicato a gestire tutte le informazioni derivanti da questo mondo interconnesso? Ci rimarrà tempo per...?

Sessanta sono gli anni trascorsi dal 1956, anno di quella che è nota come Conferenza di Dartmouth o più precisamente il *Dartmouth Summer Research Project on Artificial Intelligence*, in cui sono state buttate le basi di una disciplina – l'Intelligenza Artificiale - che oggi rappresenta un'opportunità di innovazione e sviluppo senza pari, sulla quale le aziende investono sempre più cospicuamente per la loro crescita e il loro sviluppo e per dei fattori di ordine sociale e culturale che non si erano mai verificati fino ad ora.

AICA, fino dalla fine degli anni '70 ha creduto in questa disciplina creando il GLIA (Gruppo di Lavoro su Intelligenza Artificiale), poi diventata associazione autonoma, l'AI*IA (Associazione Italiana per l'Intelligenza Artificiale). A questa disciplina possiamo ricondurre anche l'idea di un Web – il *Web Semantico* – che vive grazie ad *agenti intelligenti*, applicazioni in grado di comprendere il significato dei testi presenti sulla rete e perciò in grado di guidarci direttamente verso l'informazione ricercata, oppure di sostituirsi a noi nello svolgimento di alcune operazioni: *il noi altrove?*

Ho deciso di proporre una impostazione “per numeri” per rendere “visualizzabile” la dimensione consistente degli eventi che hanno/stanno caratterizzato il fenomeno della *Digital Transformation*, cioè la concretizzazione della trasformazione digitale nel mondo delle organizzazioni, ormai una realtà nel modo di operare delle imprese e delle pubbliche amministrazioni. Le diverse organizzazioni si trovano oggi a riconsiderare le proprie competenze interne e a promuovere un cambiamento culturale in logica digitale. La *cultura digitale* è fatto ormai diffuso non solo per i professionisti IT, ma anche per tutti i lavoratori: ricordo qui i temi delle competenze di e-leadership e quelle di cittadinanza digitale. AICA sta giocando un ruolo importante in questo scenario ed è stata parte attiva nella definizione di *cultura digitale* insieme all'Agenzia per l'Italia Digitale, Assinform, Assintel e AssinterItalia, attraverso l'Osservatorio delle Competenze Digitali.

Nello sviluppo delle nuove competenze digitali, il sistema formativo sarà chiamato a giocare un ruolo sempre più determinante: 35 sono le Azioni previste dal Piano Nazionale Scuola Digitale presentato a Ottobre 2015 dal MIUR, e scuola e università stanno rivedendo/adequando la propria offerta formativa, i

propri percorsi di studio alle richieste di un mercato del lavoro che necessita sempre più di professionalità digitali. AICA supporta il mondo della formazione a orientare i propri curricula IT con una propria originale proposta per il mondo delle professioni informatiche, sviluppando e-CFPlus, sistema di strumenti, servizi e certificazioni conforme a quanto indicato dall'European Competence Framework. Ha altresì riformulato la sua proposta per il mondo della scuola, individuando tre ambiti specifici rispettivamente per Licei, Istituti Tecnici e Istituti Professionali. Forse in questo momento scoperta è l'offerta per gli insegnanti.

Tutto questo è stato veicolato anche attraverso le pagine di MONDO DIGITALE.

Voglio concludere con un ultimo numero: 40.

Nel dicembre del 1976, circa 40 anni fa, ho iniziato la mia avventura nel mondo delle tecnologie digitali con una borsa di studio che mi ha aperto la strada nel mondo della ricerca. Vorrei partire da questa mia esperienza per dare un contributo, insieme a Viola Schiaffonati, affinché la Rivista possa giocare un ruolo sempre più consistente anche sul piano dell'innovazione, rendendola sempre più di interesse per i nostri giovani – per tradizione valenti - ricercatori.

Giovanni Adorni

Università degli Studi di Genova

La crittografia, uno snodo cruciale per la cybersicurezza

Angelo Luvison

Sommario

Da millenni, l'attività di intelligence è una funzione primaria delle agenzie governative dei più importanti Paesi. Ciò comporta l'impiego di sistemi di crittografia per la protezione di dati riservati, da un lato, e di crittanalisi per carpire tali informazioni, dall'altro. Più recentemente, la sicurezza informatica (cybersicurezza) è diventata un'esigenza di privati e di aziende, a cui si è opposto un incremento speculare dell'ingegno di malintenzionati nell'uso di tecniche crittografiche per fini disonesti, illeciti o illegali. L'articolo esplora alcuni aspetti del complesso problema privacy-sicurezza nel contesto del ruolo che la crittologia gioca in questi temi particolarmente caldi. Si introducono, in modo discorsivo e intuitivo, i principi di base dei sistemi a chiave pubblica, oltre a due recenti sviluppi in crittografia. Si accenna, infine, al cyber rischio dovuto al cosiddetto "fattore umano", se non adeguatamente governato.

Abstract

From millennia, the issue of intelligence has been a major concern of government agencies in many countries. Therefore, cryptology techniques have been emerging in the dual role of cryptography to protect private information and cryptanalysis to get non-authorized access to the same information. In recent times, cybersecurity objectives, as extended to both personal and business sectors, witnessed a dramatic soaring of cybercrime activities, especially malware. The paper investigates a number of items in the intertwined relationship between privacy and security in the framework of the increasing role cryptology is expected to play in the future. The principles of public-key systems and other recent developments of cryptography are introduced in simple tutorial form. A final issue is how to contain the cyber risk stemming from "the human factor", when not properly controlled.

Keywords: Cybersecurity, Public-key cryptography, British Intelligence (GCHQ) priority, Cryptanalysis and birthday attack, Zero-knowledge protocol, Human factor

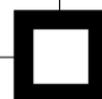
0

1

0

1

0



1. Introduzione¹

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files

(Bruce Schneier, crittografo statunitense)

Il tema della cybersicurezza è oggi particolarmente caldo poiché rappresenta uno snodo cruciale fra i diritti dei cittadini, l'azione di controllo dei Paesi e l'incalzare di nuove tecnologie. Da millenni, tanto in Occidente quanto in Oriente l'attività di intelligence – un tempo si chiamava “spionaggio”, un termine oggi considerato poco elegante – è fonte di occupazione (e preoccupazione) crescente per i principali governi [2]-[4].

La crittografia sembra oggi essere demonizzata da molti come causa rilevante dell'insicurezza della società e del genere umano. L'intera questione è posta con chiarezza da Juan Carlos De Martin del Politecnico di Torino. Su *Nova24*, l'inserito tecnologico del *Sole 24 Ore* (6 dicembre 2015), egli osserva: “Dopo l'11 settembre, le barriere che fino a quel momento avevano tenuto sotto controllo la tentazione securitaria furono in buona parte spazzate via, prima degli Stati Uniti e poi in Europa e in altre parti del mondo. [...]. Per i tecno-entusiasti – e per i politici che li assecondavano – il sacrificio della privacy di milioni di cittadini innocenti era il prezzo trascurabile da pagare se in cambio si poteva ottenere un sistema automatico di prevenzione degli attentati terroristici. In questo ordine di cose la crittografia non poteva che essere un nemico da combattere strenuamente: i bit, infatti, devono essere 'in chiaro' affinché l'intero approccio basato sulla sorveglianza di massa abbia senso. Ciò che è emerso dopo le rivelazioni di Snowden ha seriamente intaccato i presupposti del 'security complex'. [...]. [È] stato messo in evidenza che il semplice, ma incontrovertibile, fatto che indebolire la crittografia con l'obiettivo di intercettare più facilmente i terroristi rende ciascuno di noi, nonché le banche e tutte le istituzioni che usano la crittografia, più deboli nei confronti di tutti i criminali del pianeta. È davvero saggio andare in quella direzione? [...]. Eppure ormai non ci dovrebbero essere dubbi che la sorveglianza di massa è allo stesso tempo pericolosa e non risolutiva, che la crittografia è troppo importante per volerla indebolire e che la lotta ai terroristi richiede un mix sapiente di vecchie tecniche 'analogiche'? E di nuovi strumenti digitali usati in maniera mirata. Solo così è possibile sperare di essere sia rispettosi dei diritti alla base delle nostre democrazie, sia efficaci nel contrasto ai terroristi”.

Un chiarimento concettuale e terminologico può risultare, a questo punto, appropriato. È opportuno distinguere tra *security* (attinente alla protezione e alla privacy dei dati) e *safety* (concernente la sicurezza fisica, l'incolumità): proprio qui si articola il confronto dialettico tra le agenzie di intelligence per garantire la

¹ L'articolo è una continuazione del lavoro [1] del quale conserva lo stile comunicativo; i vari temi sono presentati seguendo un'esposizione parzialmente aneddotica e, soprattutto, narrativa, qua e là in tono leggero, in modo quasi ludico – anche se l'argomento è terribilmente serio, oggi come ieri e, ancor più, in futuro.

safety contro il terrorismo e l'esigenza dei cittadini e delle aziende a proteggere i loro dati, la propria cybersecurity (cfr. anche il paragrafo conclusivo). Data la polisemia della parola italiana "sicurezza", l'uso del lessico inglese, in certi contesti, può essere utile per evitare ambiguità.

Il punto di equilibrio non potrà che essere il frutto di una dialettica costruttiva tra diversi poli d'interesse, pur tenendo conto che l'intera "questione sicurezza" è resa molto articolata, quindi difficilmente componibile, in uno scenario caratterizzato da grande complessità, arduo da controllare, circolare e non lineare, quindi sensibile (vulnerabile) anche a piccoli input o fattori di cambiamento. I principali elementi tecnologici di questo scenario sono: le reti sociali, la raccolta e l'analisi di immense moli di dati (big data), l'Internet delle cose (che integra il mondo fisico con il digitale), i servizi di cloud computing e cloud gaming, nonché delle funzioni di rete virtuale e definite in software. Queste tecnologie – separatamente o nel loro insieme – favoriscono lo sviluppo di nuovi modelli di business, per esempio, basati su complesse piattaforme che legano la domanda e l'offerta, promuovendo la connessione diretta tra consumatori e altri gruppi, e sostituiscono le tradizionali catene del valore del prodotto [5]. In ogni caso, tecnologie e piattaforme si basano sulla condivisione dell'informazione, il che compromette la possibilità di un controllo diretto dei dati proprietari.

I progressi tecnologici hanno prodotto benefici incommensurabili per il nostro mondo, ma c'è una criticità evidente: i criminali sono spesso i più rapidi e innovativi ad adottare la tecnologia e i tempi moderni hanno condotto a crimini moderni. I malintenzionati di oggi sono in grado di rubare identità, prosciugare conti bancari online e azzerare server di computer. È davvero inquietante sapere che è semplice attivare le telecamere dei monitor per spiare le nostre famiglie, che i ladri sono in grado di analizzare i social media per determinare il momento migliore per entrare in casa e che i bioterroristi sono in grado di scaricare la ricetta di malattie epidemiche.

In ogni caso, un punto saldo per imprese e cittadini è rappresentato dalla consapevolezza della protezione – information security – che i moderni sistemi di crittografia possono dare. Quindi, il conflitto tra sicurezza e riservatezza degli individui, come pure delle imprese, e l'esigenza di contrastare il cybercrimine in tutte le sue forme rende più evidente non solo il ruolo delle tecniche crittografiche quanto anche la necessità ineludibile di un'attenzione maggiore al cosiddetto "fattore umano".

Nell'articolo si considera – ancorché in termini divulgativi (ossia senza formule), metaforici e con il ricorso all'analogia (immagini mentali) – il punto di svolta che ha aperto la strada ai sistemi più avanzati: la crittografia a chiave pubblica (paragrafo 2). Essa rappresenta il più recente passo verso la matematizzazione e la formalizzazione della crittologia, che può perciò rivendicare un proprio statuto di disciplina scientifica autonoma. Il paragrafo 2 è articolato in più punti, in particolare il 2.3 riassume la vicenda dell'ormai accertata priorità dei crittografi britannici nell'invenzione della crittografia a chiave pubblica, da loro chiamata cifratura non segreta [3]. Il paradosso del compleanno con il suo risultato del tutto controintuitivo rientra nella categoria delle sorprese che il

calcolo delle probabilità ci riserva. Uno dei più famosi ed emblematici attacchi di crittanalisi sfrutta proprio questo paradosso ed è oggetto del paragrafo 3. Nel paragrafo 4, si riferirà di due importanti recenti contributi da parte di ricercatori italiani, che continuano così una nostra tradizione secolare a partire da Leon Battista Alberti, Girolamo Cardano, Giovanni Battista della Porta per arrivare, nel Novecento, a Luigi Sacco [1]. Nel conclusivo paragrafo 5, si sottolinea la rilevanza del “fattore umano” nella cybesicurezza, oltre alla tecnologia crittografica. Il riquadro finale sviluppa alcune considerazioni sulla rappresentazione pubblica e mediatica dei servizi di intelligence degli USA e del Regno Unito. La bibliografia integra e completa quella già riportata in [1], benché alcuni riferimenti fondamentali siano necessariamente ripetuti in entrambi gli articoli.

2. La crittografia a chiave pubblica, ultima pietra miliare della crittografia

Siamo nani sulle spalle di giganti
(Bernardo di Chartres)

Se ho visto più lontano, è perché stavo sulle spalle di giganti
(Isaac Newton)

Nel precedente lavoro [1], abbiamo delineato i passi che, a giudizio degli studiosi, rappresentano altrettante pietre miliari verso la matematizzazione della crittologia contemporanea:

1. il principio di Kerchoff;
2. il cifrario a blocco monouso (*one-time pad*) di Vernam;
3. il fondamentale lavoro di Shannon sulle comunicazioni segrete [6].

(Per una discussione approfondita e analitica a livello universitario di questi e altri punti attinenti all'intera disciplina si consigliano i testi [7] e [8]). A proposito di Shannon, il cui centenario della nascita cade quest'anno, tra le varie motivazioni per celebrarlo adeguatamente, l'esperto di innovazione e comunicazione Pascal Zachary (su *IEEE Spectrum* di aprile 2016) avanza la seguente: “Shannon ha dimostrato che la tecnica ingegneristica crea nuove conoscenze tanto rapidamente quanto la scienza e che la pratica ingegneristica può *precedere* una teoria scientifica”. Una stoccata non indifferente alla credenza diffusa che l'applicazione viene sempre *dopo* la ricerca di base. L'avanzamento della tecnologia dell'informazione e delle comunicazioni (ICT), a partire da Shannon, Turing, John von Neumann e Norbert Wiener, è la prova evidente della correttezza di questa asserzione. (Un'altra vulgata corrente è, a nostro avviso, l'asserita separatezza statutaria tra matematica pura e matematica applicata – cfr. anche *infra*, nota 5).

La quarta, e più recente, scoperta basilare è la crittografia a chiave pubblica – o cifratura non segreta – il cui principio di funzionamento può essere ricondotto al seguente esempio, adattato dal divertente libro di enigmistica e giochi matematici [9]. La schematizzazione proposta è una fra le più semplici, intuitive

e, allo stesso tempo, istruttive, perché consente di comprendere la logica del principio che sta alla base del sistema²:

Alice vuole inviare un oggetto a Bob³. È un oggetto privato che non deve essere aperto da nessuno se non da lui. Alice decide di spedirlo in un cofanetto, ma l'unico modo per chiuderlo è di usare un lucchetto. Scambiarsi le chiavi sarebbe troppo rischioso. Però entrambi dispongono di lucchetti, ciascuno con la propria chiave. Come può Alice essere sicura che il prezioso contenitore possa essere aperto solo da Bob?

Prendete un po' di tempo per escogitare una possibile soluzione al quesito!

Se vi pare di avere riflettuto abbastanza, ecco la successione di passaggi per assicurare che lo scambio avvenga in modo sicuro:

1. Alice chiude il cofanetto con un lucchetto e lo invia a Bob.
2. Bob chiude il cofanetto con un altro lucchetto e lo rispedisce ad Alice.
3. Alice rimuove il proprio lucchetto e rispedisce il cofanetto a Bob.
4. Bob riceve il cofanetto (ora protetto solo dal lucchetto apposto da lui stesso) e lo apre con la propria chiave.

Nei passaggi tra Alice e Bob, nessuno è in grado di aprire il cofanetto – senza manometterlo – poiché non c'è scambio o distribuzione di chiavi (*no-key protocol*), ma solo andirivieni di lucchetti.

(Si può notare che i passaggi potrebbero essere ridotti se Alice e Bob si scambiassero i rispettivi lucchetti *a priori*, cioè prima dell'invio del messaggio. Tuttavia, questa soluzione presenta almeno una controindicazione, infatti si basa sull'aspettativa di una continuità temporale della relazione tra Alice e Bob, i quali nel futuro potrebbero non rimanere così amici... Sarebbe un po' come scambiarsi permanentemente le proprie chiavi di casa, anziché imprestarle per l'uso all'occorrenza).

Partendo da questo concetto, Adi Shamir ha sviluppato (intorno al 1980) il "protocollo a tre passi" per comunicare segretamente in un contesto che permette ad Alice di inviare un messaggio alla controparte Bob in modo sicuro e senza la necessità di scambiare, o distribuire, chiavi di cifratura (per un'elegante formalizzazione matematica del protocollo si può vedere [11]). L'idea di base è che ciascuna delle due parti, possedendo entrambe una chiave privata di cifratura e una privata di decifrazione, usa le proprie chiavi indipendentemente, prima per cifrare il messaggio e poi per decifrarlo. Sembrerebbe plausibile utilizzare in questo scambio la chiave di cifratura di Vernam, cioè una chiave scelta casualmente e utilizzata una e una sola volta (monouso) [1]. È facile però

² Sul Web sono disponibili molti tutorial utili e interessanti. Fra questi, suggeriamo la registrazione video della conferenza di James Massey [10], che riporta esempi di "trucchi" utilizzabili per verificare se la crittografia sia "scienza" (cioè, può provare ciò che sembra fare) oppure "magia" (cioè, quanto essa sembra fare, o essere, è frutto di mera illusione).

³ Gli studiosi della crittografia hanno il vezzo di illustrare il funzionamento dei vari schemi attraverso problemi che hanno come protagonisti due personaggi convenzionalmente denominati Alice e Bob.

provare che in tal caso il protocollo diventerebbe totalmente insicuro [10], [11]. È possibile, invece, ricorrere ad algoritmi più sofisticati che sfruttano i risultati della complessità computazionale applicati alla teoria dei numeri, in particolare dei numeri primi (cfr. i successivi punti 2.1 e 2.2).

Peraltro, il protocollo come descritto non fornisce alcuna forma di autenticazione del mittente, senza la quale lo schema sarebbe suscettibile dell'attacco da parte di un cosiddetto "uomo in mezzo", potenzialmente in grado di creare falsi messaggi, in sostituzione di quelli originalmente trasmessi.

Concetti di questo tipo, apparentemente ovvi e banali, hanno rappresentato il punto di partenza per prospettive del tutto inedite della crittografia scientifica negli ultimi quarant'anni.

A metà degli anni 1970, Whitfield Diffie e Martin Hellman, a partire da un'idea di Ralph Merkle, hanno sviluppato il concetto di *crittografia asimmetrica*, o *a chiave pubblica* [12]. Ogni utilizzatore tiene segreta la sua chiave di decifrazione e rende nota la sua chiave di cifratura in un elenco (*directory*) pubblico. La crittografia a chiave pubblica permette a due (o più) persone di comunicare in tutta riservatezza senza usare la stessa chiave: chiunque (Alice) desideri comunicare privatamente con un utilizzatore (Bob) la cui chiave sia in elenco deve solo leggere la chiave pubblica di Bob per cifrare il messaggio che unicamente Bob potrà decifrare con una chiave diversa, la propria chiave segreta.

Come prima, si può visualizzare il principio con un'analogia fisica, il funzionamento di una cassaforte meccanica o della cassetta postale di servizio:

1. Bob spedisce ad Alice il suo lucchetto aperto (non necessariamente su un canale sicuro).
2. Alice deposita il proprio messaggio in una cassaforte chiudendola con il lucchetto di Bob.
3. Solo Bob ha la chiave per aprire il proprio lucchetto, quindi per recuperare e leggere il messaggio inviatogli da Alice.

Le possibilità legate alle metafore esemplificate sono molteplici. Nel 1977, Donald Rivest, Adi Shamir e Leonard Adleman hanno proposto la crittografia a chiave pubblica basata sulla teoria della complessità e sulle proprietà dei numeri primi. Oggi, lo schema – denominato RSA dalle iniziali dei cognomi degli inventori – è comunemente impiegato per garantire la firma digitale, cioè l'autenticazione del mittente, oppure l'integrità del messaggio. Per consentire di svolgere queste funzioni in modo sicuro, tecniche di crittografia a chiave pubblica si trovano anche nei protocolli di Bitcoin, sistema dedicato alle transazioni commerciali-finanziarie che impiegano la e-currency, o moneta virtuale, bitcoin (dove la "b" iniziale della valuta dovrebbe essere scritta in minuscolo). Ulteriori approfondimenti e particolari operazionali su Bitcoin sono disponibili alla pagina Web <https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained>.

2.1 La sfida dell'RSA

L'obiettivo principale del progetto di un cifrario efficace è di rendere l'operazione (illegale) di decrittazione, o forzatura, praticamente equivalente alla soluzione di

problemi laboriosi (cioè complessi) dal punto di vista computazionale. Caso molto comune è oggi quello della fattorizzazione del prodotto n di due numeri primi p e q , dove n è costituito, per esempio, da 250 cifre decimali, benché il calcolo di n sia rapidamente effettuabile se p e q sono entrambi noti. L'operazione diretta (il prodotto) è facile, l'inversa (la fattorizzazione) tutt'altro: siamo nel campo della complessità computazionale⁴.

Prima di pubblicare i loro lavori in una rivista scientifica, nel 1977, Rivest, Shamir e Adleman scrissero a Martin Gardner – autore della celebre rubrica di “Giochi matematici” su *Scientific American/Le Scienze* – allo scopo di coinvolgere in modo rapido e capillare un uditorio più vasto di quello strettamente accademico. Nella sua rubrica, Gardner lanciò ai lettori la sfida, denominata RSA Factoring Challenge [13], di decrittare un messaggio che avrebbe richiesto la scomposizione in fattori primi di un numero di 129 cifre, impresa che all'epoca era considerata impensabile stante le macchine disponibili. “A new kind of cipher that would take millions of years to break”, era l'iperbolico titolo dell'articolo di Gardner. Ma nel 1994 gli sforzi congiunti di 1600 computer e di 600 utenti connessi a Internet per sei mesi, e coordinati dal matematico olandese Arjen Lenstra, permisero di trovare i due fattori per decrittare il messaggio originale: “The magic words are squeamish ossifrage” (“Le parole magiche sono gipeto schizzinoso”). La sfida si chiuse ufficialmente nel 2007 dopo che si era ottenuta la fattorizzazione di numeri di 160 cifre, anche se poi ci si è spinti oltre: oggi la barriera da superare è di 250 cifre.

Si può osservare che la vicenda capitanata da Lenstra rientra a buon diritto in quei casi che Michael Nielsen ne *Le nuove vie della scoperta scientifica* descrive come passaggi dall'intelligenza singola all'intelligenza connessa e collettiva grazie alla condivisione in rete dei risultati di ricerche scientifiche. Un altro esempio è quello dei matematici che nel “Polymath Project”, pilotato da Tim Gowers, collaborano e si confrontano online per trovare soluzioni a problemi ancora insoluti.

2.2 Turing e i numeri primi

La teoria dei numeri primi è dunque uno dei capisaldi dell'odierna crittografia a chiave pubblica, e di questa matematica Turing si è occupato a fondo prima e dopo la Seconda guerra mondiale. Perciò, Turing può essere considerato un precursore, sia pure in senso lato, della crittografia a chiave pubblica, sebbene non un contribuente diretto. Nel periodo bellico, ebbe invece, a Bletchley Park, il ruolo di crittanalista principe nel decrittare (forzare) la macchina tedesca Enigma [1].

L'inglese G. H. Hardy è spesso citato per aver sostenuto – in *Apologia di un matematico* (1940) – che questa branca della matematica pura è uno dei più ovvi esempi della sua inutilità pratica, una visione oggi alquanto datata⁵. A

⁴ Per esempio, i numeri primi sono correntemente usati nelle chiavi di cifratura dei PIN delle carte bancarie.

⁵ Nel documentario di Olivier Peyon dal titolo *Comment j'ai détesté les maths* (2013), Cedric Villani, noto matematico e direttore dell'Institut Henri Poincaré di Parigi, sostiene – d'accordo con molti altri studiosi contemporanei – che la distinzione tra matematica pura e matematica applicata è da considerare puramente accademica.

Oxford, Hardy era seguace di una concezione sostanzialmente platonica della matematica, secondo la quale essa e i suoi risultati costituirebbero “scoperte” ma non “invenzioni”; quindi la teoria dei numeri primi “è così e basta”, senza implicazioni ulteriori. Questa impostazione caratterizzò l'Università di Oxford fin dalla fondazione (verso la fine dell'XI secolo); infatti, il suo magistero filosofico-matematico fu opera di eminenti studiosi francescani quali Roberto Grossatesta e Ruggero Bacone nel XIII secolo e poi, all'inizio del successivo Trecento, di Guglielmo di Occam. Essi improntarono l'insegnamento oxoniano in modo fondamentalmente platonico, almeno fino al termine del medioevo [14]. È probabile che Hardy oggi si ricrederebbe vedendo i progressi della scienza dei segreti, consentiti proprio dalle basi di teoria dei numeri. Peraltro, Hardy non era autorizzato a sapere, per evidenti ragioni di sicurezza nazionale, che matematici, fisici, ingegneri stavano lavorando insieme in un team formidabile contro la presunta inviolabilità di Enigma.

2.3 Le priorità dei crittografi britannici

I due capisaldi della crittografia a chiave pubblica sono dunque il protocollo di scambio delle chiavi di Diffie-Hellman e il sistema di cifratura RSA, proposti entrambi in ambiente accademico, rispettivamente, nel 1976 a Stanford e nel 1978 al MIT.

Molto presto, peraltro, si diffuse la voce che entrambe le tecniche fossero già note, da anni, ai crittografi del governo britannico. Si è effettivamente accertato [3] che la loro scoperta, risalente all'inizio degli anni Settanta, è da attribuire al CESG (Communications-Electronics Security Group), il centro di sicurezza delle informazione del GCHQ (Government Communications Headquarter) – pressappoco l'equivalente britannico della NSA statunitense. Solo nel dicembre 1997, ne fu data la conferma ufficiale con il contestuale rilascio di un articolo sulla storia della scoperta, scritto nel 1978 dal suo artefice James Ellis [15]. Purtroppo, Ellis morì neppure un mese prima che la memoria potesse essere letta a un uditorio di crittanalisti dal collega Cliff Cocks il 18 dicembre 1997, dopo quasi tre decenni di segretezza tipicamente *British*.

“Cifratura non segreta” (*non-secret encryption*) è la locuzione adottata da Ellis per l'idea di risolvere il problema della distribuzione delle chiavi in crittografia [15]⁶. Il presupposto che due parti dovessero prima scambiarsi un segreto condiviso per poter comunicare in modo sicuro era sempre stato considerato come ovvio, fin dai tempi di Giulio Cesare. Ellis infranse questa convinzione con

⁶ In [15], Ellis riferisce di un documento intitolato “Final Report on Project C-43” dei celebri Bell Telephone Laboratories (BTL) senza, peraltro, fornirne informazioni aggiuntive utili all'identificazione. *En passant*, questo particolare ha incuriosito per anni la comunità crittografica per la possibilità che i ricercatori dei BTL avessero fatto importanti progressi sulla crittografia a chiave pubblica addirittura negli anni 1940. Il misterioso rapporto (del 1944) sulla cifratura del segnale vocale in realtà esiste ed è perfino disponibile online. È firmato da Walter Koenig Jr., l'ingegnere-capo del progetto; non è perciò chiaro perché Ellis parli di un “autore sconosciuto”. Il Progetto C-43 – commissionato dal National Defense Research Committee (NDRC) statunitense ai BTL fu sviluppato in parallelo, ma con nessuno o pochi contatti, con il più famoso Progetto X (o SIGSALY) sulla segretezza del linguaggio parlato, che vide impegnati anche Shannon e Turing (cfr. riquadro 2 di [1]).

l'ipotesi che il ricevente potesse giocare un ruolo nel processo di cifratura, un'idea decisamente rivoluzionaria.

La soluzione, equivalente a quella che oggi è chiamata crittografia a chiave pubblica, si basa sullo stesso concetto proposto da Diffie e Hellman, ma Ellis, come anche Diffie e Hellman, non riuscì ad arrivare a una realizzazione concreta dell'idea di base. Ellis, tuttavia, fu perseverante, senza curarsi dei dubbi avanzati da molti colleghi. Memorabile è il commento di Shaun Wylie (capo di Ellis ed egli stesso codebreaker a Bletchley Park durante la guerra): "Sfortunatamente non posso trovare niente di sbagliato in tutto ciò".

Tre anni dopo, nel 1973, il rapporto venne dato da esaminare all'appena assunto Cocks, il quale, in un tempo brevissimo, inventò l'algoritmo (oggi noto come RSA) che sarebbe stato concepito quattro anni dopo da Rivest, Shamir e Adleman. Malcolm Williamson, compagno di liceo di Cocks, fu contestualmente assunto nel GCHQ e pervenne, poco dopo, a quello che oggi conosciamo con il nome di protocollo di Diffie-Hellman. Quindi, entro il 1973, Ellis, Cocks e Williamson avevano ideato *in nuce* tutte le componenti della crittografia a chiave pubblica, che i ricercatori USA avrebbero messo insieme quattro anni dopo.

La comunità degli studiosi di crittografia, all'annuncio del 1997, fu subito in grado di riconoscere la priorità di quanto realizzato dai britannici: l'IEEE nella pagina "Milestones: Invention of Public-key Cryptography, 1965-1975" del suo sito (http://ethw.org/Milestones:Invention_of_Public-key_Cryptography,_1969_-_1975) tributa il giusto riconoscimento ai tre ricercatori britannici⁷. Tuttavia, non è inusuale per pubblicazioni che descrivono l'origine della crittografia a chiave pubblica continuare a sminuire, o ignorare completamente, la scoperta del GCHQ. Lo stesso Hellman, in occasione della ristampa nel 2002 del suo articolo di rassegna [12], nel nuovo commento retrospettivo non ha certamente seguito la norma di bon ton di menzionare i lavori prioritari del GCHQ. Questo disinteresse dei nordamericani verso altri si può riscontrare anche nello scarso o nullo riconoscimento della paternità dell'invenzione del telefono di Antonio Meucci (rispetto ad Alexander Graham Bell), nonostante che una risoluzione della Camera dei Rappresentanti USA l'abbia ufficialmente dichiarata nel 2002.

3. L'attacco del compleanno in crittanalisi

Corruzione, ricatti, inganni e metodi classici di intelligence e ingegneria sociale possono essere impiegati per ottenere informazioni riservate dalle persone – uomini o donne, indifferentemente. Per esempio, costringere qualcuno a rivelare la propria chiave segreta con minacce è illegale ma tecnicamente fattibile. Un altro tipo di attacco, meno aggressivo, è l'uso di telefonate o email capziose per carpire (*phishing*) le password a soggetti disattenti o ingenui.

Anche la lista degli attacchi contro i sistemi informatici non finisce mai [16]-[18]. Si possono usare metodi furtivi basati sull'overflow dei buffer o su *malware* – software malevolo – per rivelare chiavi segrete in sistemi di software.

⁷ Su proposta, peraltro, della sua Sezione britannica e irlandese: IEEE United Kingdom and Republic of Ireland Section.

Ransomware è un tipo di malware che, nella variante *crypto*, blocca il computer della vittima prescelta, cifrandone illecitamente e illegalmente le informazioni per impedirne l'uso finché la vittima non paga un riscatto (*ransom*) ai cybercriminali per avere la chiave di decifrazione che consente di accedere ai propri dati. Un esempio di ransomware è CryptoLocker (dal 2013), per il quale la chiave costa circa 300 euro. CryptoLocker agisce come la pesca a strascico: cifre relativamente basse ma un numero elevato di obiettivi potenziali. Nuovi ransomware si dimostrano ancor più esosi e aggressivi.

Decrittare le trasmissioni cifrate può dimostrarsi un gioco lungo, complicato e costoso. Altri attacchi informatici si basano allora su un'intuizione assai semplice: cercano di intrufolarsi con un virus in un PC o in uno smartphone. Un pezzetto di codice che, una volta installatosi, quatto quatto assume progressivamente il controllo del dispositivo aggredito e si appropria di tutte le informazioni sensibili.

Si potrebbe ritenere che questi attacchi alla sicurezza, specialmente quelli basati su logiche di ingegneria sociale e/o sull'implementazione del sistema di cifratura, siano sleali, ma il mondo della crittanalisi è caratterizzato da scarsissima correttezza: se qualcuno vuole attaccare un sistema informatico, sta già comportandosi in modo disonesto e infrangendo le regole. Se un opponente di solito prova ad attaccare il punto più debole di un sistema, allora chi vuole difendersi deve cercare di scegliere gli algoritmi più resistenti per avere una ragionevole sicurezza che l'azione illegale sia resa difficilmente praticabile e che, quindi, sia scoraggiata.

Vediamo ora i fondamenti matematici di uno degli attacchi di crittanalisi fra i più temuti: l'attacco del compleanno. In teoria della probabilità, il problema, o paradosso, omonimo riguarda la probabilità che almeno due persone di un medesimo gruppo compiano gli anni lo stesso giorno (non occorre che gli anni di nascita coincidano). Il paradosso, proposto nel 1939 da Richard von Mises – da non confondere con Ludwig von Mises, uno dei padri del neoliberismo – sta nel fatto che la “probabilità di collisione” è molto maggiore di quanto si possa intuitivamente immaginare. Infatti, in un gruppo di 23 persone tale probabilità è già del 50%; con 30 persone supera il 70% e il 97% con 50; il 99% di probabilità si raggiunge con 57 persone. All'evento certo, tenendo conto della possibilità di anni bisestili, si arriva con almeno 367 persone per il principio dei buchi della piccionaia (o legge delle cassette postali). La dimostrazione analitica della soluzione è reperibile in letteratura a diversi livelli di approfondimento, anche se è consigliabile il volume [19] per completezza di trattazione (oltre che per molti altri stimolanti quesiti probabilistici).

Questo problema ha ispirato la realizzazione dell'attacco del compleanno in casi in cui la firma digitale impiega funzioni crittografiche cosiddette *hash* (illustrate, per esempio, in [7]). In linea di principio, le funzioni (o algoritmi) *hash* in crittografia costituiscono un modo per assicurare la sicurezza dell'informazione. Esse sono tipicamente usate nelle firme digitali e nello stabilire connessioni sicure tra i siti Web. I dati, fatti passare in un algoritmo di *hash*, producono una successione di bit più breve; questa stringa opera come una sorta di *message*

digest (estratto del messaggio)⁸. Ogni cambiamento dei dati originali cambia la stringa dei bit estratti. La stringa risultante agisce perciò come impronta digitale dei dati, garantendo che nessuno abbia interferito con essi.

Le funzioni hash svolgono un ruolo essenziale in crittografia per verificare l'integrità di un messaggio, infatti, l'esecuzione dell'algoritmo su un testo anche minimamente modificato fornisce un estratto completamente differente rispetto a quello calcolato sul testo originale, rivelando così una tentata frode. Esse possono essere anche utilizzate per la creazione di firme digitali, in quanto, non richiedendo calcoli lunghi e complessi, permettono di realizzare rapidamente la firma anche per file di grosse dimensioni. È certamente più conveniente eseguire un hashing del testo da firmare per poi autenticare solo questo, evitando così l'applicazione di complessi schemi di crittografia asimmetrica su moli di dati molto grandi.

Si noti che il paradosso del compleanno si basa su coppie che "collidono" (stesso giorno di compleanno), ed è esattamente quello che si propone di ottenere l'omonimo attacco: trovare coppie diverse di sequenze binarie che collidono, ossia che producono lo stesso output. Le firme digitali possono essere vulnerabili a questo tipo di attacco, poiché i risultati del paradosso sono utilizzabili per generare un contratto fraudolento contro chi ha apposto la propria firma digitale a una versione corretta del contratto. Per evitarlo, la lunghezza dell'output della funzione hash deve essere sufficientemente grande, cioè resistente alle collisioni, così da rendere l'attacco computazionalmente impraticabile. Sulla base di approfondimenti teorici della robustezza rispetto a questo tipo di attacco, risulta che una funzione di hash dovrebbe avere una lunghezza di almeno 128 bit e, in un prossimo futuro, anche di 256 bit [7].

4. Riconoscimenti a studiosi italiani

Accenniamo qui a due recenti sviluppi in settori di frontiera della crittologia, che hanno visto il sostanziale apporto di ricercatori italiani, sia pure non da soli.

4.1 "Il re degli algoritmi di sicurezza"

Si è prima ricordato che gli algoritmi hash sono utilizzati in applicazioni crittografiche che garantiscono l'autenticità dei documenti digitali: per esempio, le firme digitali. Guido Bertoni, laureato al Politecnico di Milano, è uno degli inventori di SHA-3 (Secure Hash Algorithm-3), un inedito algoritmo hash di crittografia, anche conosciuto con il nome di Keccak – pronunciato "catch-ack" – e in [20] definito "Il re degli algoritmi di sicurezza".

Il National Institute of Standards and Technology (NIST) degli USA ha selezionato nel 2012, dopo una competizione durata cinque anni, l'algoritmo studiato dai ricercatori della STMicroelectronics Guido Bertoni, Joan Daemen, Gilles Van Assche e Michaël Peeters. La loro proposta ha superato altre 63 offerte ricevute dal NIST in seguito alla gara bandita nel 2007, quando si temeva

⁸ Hash significa letteralmente "polpetta fatta con avanzi di cibo sminuzzati".

che lo standard SHA-2 potesse essere minacciato entro breve tempo (preoccupazione poi rivelatasi eccessiva).

Keccak, basandosi su una generalizzazione del concetto delle funzioni hash crittografiche, non sembra suscettibile di forzature con metodi tradizionali. Inoltre, il progetto hardware lo rende particolarmente adatto a sistemi *embedded*, dedicati ad applicazioni speciali che richiedano chip di piccole dimensioni e con basso consumo di potenza⁹.

4.2 Il premio Turing 2012

Silvio Micali – laureato alla Sapienza di Roma e oggi al MIT – è stato insignito con la collega Shafi Goldwasser del “2012 A.M. Turing Award” per lavori fondamentali di scienza della crittografia basati sulla teoria della complessità e per metodi pionieristici di verifica delle dimostrazioni matematiche. Forse, stiamo per assistere a un nuovo balzo in avanti della disciplina, dopo Shannon, Turing e i sistemi DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA. Il conferimento del premio risulta ancora più significativo se si ricorda che il 2012 ha segnato l’anno del centenario della nascita di Turing.

Nella motivazione del premio appare anche il riferimento all’interessante caso dei protocolli di autenticazione a conoscenza zero (*zero-knowledge protocol* o *zero-knowledge proof*). Si tratta di protocolli raffinati che consentono di verificare l’identità del mittente, evitando l’impiego diretto dell’informazione d’identificazione, che potrebbe essere intercettata e successivamente utilizzata da un terzo protagonista per cercare di far credere di essere il mittente autorizzato.

L’idea di base della prova a conoscenza zero può essere visivamente illustrata ricorrendo alla “metafora della caverna spiegata ai bambini” [21]. La buffa caverna di figura 1 è formata da due tunnel A e B separati da una porta che può essere aperta solo usando una frase segreta, o password. Peggy¹⁰ vuole convincere Victor di essere a conoscenza del segreto d’accesso alla caverna senza però rivelarglielo. A questo scopo, Peggy raccomanda a Victor di restare fuori dal tunnel ed entra in uno qualsiasi dei due punti d’accesso. Ora, Victor avanza all’ingresso della caverna e chiede a Peggy di uscire o dal tunnel A o dal tunnel B. Peggy ci riesce aprendo, qualora necessario, la porta con la password. Peggy ha solo il 50% di probabilità di trovarsi già nel tunnel giusto e di non avere perciò bisogno della password. Ovviamente, la prova deve essere ripetuta più volte. Dopo N volte, la probabilità che Peggy goda solo di una fortuna sfacciata scende a 2^{-N} , diventa cioè esponenzialmente trascurabile. Peggy avrà così dimostrato a Victor di conoscere la chiave segreta senza avergliela rivelata¹¹. Ricorrendo a un significato secondario, ma non scomparso,

⁹ Per una descrizione tecnica aggiornata di Keccak si rinvia al link <http://keccak.noekeon.org/index.html/>.

¹⁰ In questo contesto, Peggy denota chi ha l’onere di provare l’affermazione e Victor chi la verifica.

¹¹ Anche gli scambi di crittocaluta bitcoin possono avvenire senza che gli indirizzi siano rivelati, usando la prova a conoscenza zero (<https://en.wikipedia.org/wiki/Bitcoin>).

dell'aggettivo qualificativo, potremmo dire che Peggy dimostra altresì di essere una persona "probabile"¹².

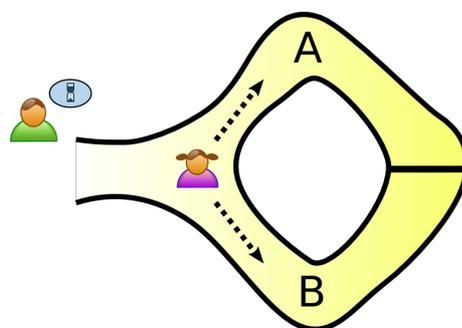


Figura 1.
Metafora della caverna in una "prova a conoscenza zero"
(Adattamento da Wikipedia).

È importante, infine, sottolineare che gli studi di Micali e Goldwasser sulla complessità computazionale possono trovare impiego, oltre che in crittografia, in altri settori importanti dell'informatica teorica.

5. Conclusioni: il fattore umano e la cybersicurezza

*Un giornalista chiese ad Albert Einstein di spiegare la formula del suo successo. Dopo una breve riflessione, Einstein rispose: "Se A è il successo, direi che la formula è $A = X + Y + Z$, dove X rappresenta il lavoro e Y il gioco".
"E Z cosa rappresenta?", chiese il giornalista.
"Tenere la bocca chiusa", replicò lo scienziato.
(Aneddoto tratto da [22]).*

Dopo lo scandalo metadati – la raccolta di informazioni personali da parte della NSA – risulta sempre più chiaro che la vera battaglia tra privacy e intelligence sta nella crittologia (crittografia e crittanalisi). L'antica arte crittologica – a partire, soprattutto, da Shannon e Turing – è diventata una disciplina autonoma dallo

¹² Può essere motivo di curiosità, ancorché marginale, il sottile quanto apprezzabile slittamento del significato dell'inglese "probable" che fino a circa due secoli fa designava argomentazioni "verificabili e persuasive" o "degne e meritevoli di approvazioni". Allora, per esempio, l'espressione "a probable doctor" denotava un medico autorevole in cui riporre fiducia. La questione è ben spiegata da Ian Hacking in *The Emergence of Probability*, a partire dall'apparentemente contraddittoria asserzione dello storico Edward Gibbon: "Such a fact is probable but undoubtedly false", frase che, tuttavia, acquista un senso compiuto quando *probable* sia inteso come "plausibile", "verosimile". Oggi, l'aggettivo qualifica un giudizio attendibile confortato da motivi ragionevoli ma non conclusivi. I linguisti direbbero che il "significante" *probable* è sempre lo stesso ma che il suo "significato" è cambiato nel tempo a partire dall'equivalente latino. Infatti, nel trattato di logica *De inventione dialectica libri tres* (1479) dell'olandese Rodolphus Agricola l'avverbio *probabiliter* equivaleva a "persuasivamente". Ovviamente, anche in italiano si è assistito a un analogo fenomeno diacronico per il senso di "probabile" e derivati.

statuto scientifico: non è quindi strano che la usino agenzie di intelligence, governi, aziende, cittadini, come pure, purtroppo, lestofanti e cybercriminali della peggior risma.

A questo punto, diventa opportuno fare due osservazioni. La prima è che questa contesa apre la strada alla ricerca su diritto e cybersicurezza, ben al di là delle facili analisi sinora condotte da spiriti passatisti e tecnofobi, per i quali la tecnologia (crittologia) è da condannare in linea di principio, nonostante che essa sia uno snodo fondamentale per garantire privacy e sicurezza informatica nella vita digitale di tutti gli utilizzatori di Internet.

La seconda è che la tecnologia da sola, pur necessaria, non è sufficiente; infatti, la cifratura è solo un aspetto della sicurezza nelle comunicazioni. Altrettanto importanti sono i nostri comportamenti, da come custodiamo i dispositivi che abbiamo a come ci proteggiamo con PIN e password. Già in [1] abbiamo accennato all'imprescindibilità del fattore umano. Per esempio, l'ingenuità comportamentale dei tedeschi si è intrecciata quasi indissolubilmente con la genialità del team di Turing nel portare a violare la potentissima macchina cifrante Enigma [23]. Oggi il fattore umano risulta, se possibile, ancora più cruciale [17], [18]. Nel monito di Einstein, all'inizio del paragrafo, sta tutta la saggezza per assicurare la privacy dei nostri dati sensibili proteggendoli, per esempio, da tecniche di ingegneria sociale. Saper "tenere la bocca chiusa" – essere cauti, attenti e riservati – è la chiave per tenere sotto controllo il fattore umano.

Da più parti è stato fatto notare che il maggior pericolo per la cybersicurezza non sia tanto l'ignoranza tecnologica quanto la presunzione di non essere nel mirino di malintenzionati. Nell'Internet delle cose e della casa intelligente, sensori, frigoriferi, televisori, smartphone, auto, gli oggetti più disparati sono dei computer collegati alla Rete e gestiti a distanza: nuovi ecosistemi rispettosi dell'ambiente ma che nascondono molti pericoli per privacy e sicurezza. Marc Goodman, autore dell'esauriente (circa 400 pagine) *Future Crimes* [17], osserva che l'attenzione dei cittadini nei confronti di privacy e sicurezza sta evidenziando la fragilità della tecnologia. Egli fornisce tutta una serie di dati statistici stupefacenti: il migliore software antivirus intercetta solo il 5% delle minacce online; l'80% degli hacker lavora per il crimine organizzato. Un esempio del 2013 sarebbe gustoso se non facesse rabbrivire, ed è quello dei ferri da stiro e dei bollitori cinesi, illecitamente equipaggiati con schede Wi-Fi, che consentirono a questi elettrodomestici di accedere alle reti domestiche dei loro acquirenti, diffondendo in tal modo virus e spam.

Goodman osserva che essendo ogni dispositivo connesso (nell'Internet delle cose), tutti noi risuliamo vulnerabili. Nel volume, oltre a investigare le incombenti minacce dei pirati tecnologici, propone una varietà di modi per ridurre i rischi. I protocolli comportamentali pratici e quotidiani suggeriti per difendersi dai pericoli più comuni sono consigli di buon senso, gli equivalenti di chiudere la porta di casa, non lasciare le chiavi inserite nell'avviamento dell'auto, ecc. Lo specifico protocollo normativo stilato da Goodman è sintetizzabile nell'acronimo-acrostico **UPDATE**: effettuare frequenti **Update**; utilizzare **Passwords** robuste di protezione; eseguire **Download** del software solo da siti ufficiali; usare i privilegi di **Administrator** con attenzione e parsimonia; spegnere (**Turn off**) il computer

quando non lo si usa; usare tecniche di cifratura (**Encrypt**) nella propria vita digitale per proteggere i dati sia localmente sia trasferendoli attraverso il Web. In questo modo – secondo Goodman – si può evitare più dell'85% delle minacce che incombono dalla Rete.

Nella direzione dei rischi legati al fattore umano, si muove anche il lavoro [18], specificatamente dedicato alla protezione delle reti informatiche di imprese e aziende. Gli autori enunciano e commentano con una certa ampiezza gli errori più legati a debolezze e pecche nel comportamento umano. Per mitigare l'impatto negativo di questo fattore – secondo l'articolo di *Harvard Business Review* – la cultura aziendale deve giocare un ruolo a tutto campo: dall'eccellenza (conformità) operativa e procedurale alla formazione mirata e continua del personale, dall'ispezione sia sistematica sia episodica dei mezzi e dei processi di calcolo alla responsabilizzazione dei dipendenti, ecc. Affinché il cambiamento culturale sia effettivo ed efficace, occorre che i vertici aziendali facciano empaticamente propri obiettivi condivisi di cybersicurezza, agevolandone il percolare in tutti i settori aziendali, dall'information technology alle risorse umane, in modo da garantire “a psychologically safe workplace” (Amy Edmondson, Harvard Business School).

Un'impresa può impiegare anche altri accorgimenti, come rilevare alterazioni significative nei pattern del traffico entrante nelle proprie reti; nel qual caso, occorre usare le tecniche matematiche più aggiornate di analisi dei big data (data science). Per una rassegna approfondita dei metodi, degli algoritmi e delle applicazioni nel settore “grandi moli di dati”, si segnalano i due aggiornatissimi fascicoli monografici dei *Proceedings of the IEEE* [24].

In definitiva, l'opposizione privacy-sicurezza pare essere una questione eccessivamente amplificata e semplificata, soprattutto dai mass media. Su *Nòva24* (20 marzo 2016), quanto al dilemma “liberi o connessi”, il giornalista esperto di nuove tecnologie, Luca De Biase, acutamente osserva: “Si può coltivare l'obiettivo di vivere in modo pieno la vita in rete e salvaguardare la libertà. Di certo c'è che la rete facilita la sorveglianza più che la privacy e che la raccolta di dati personali [Ndr, metadati] concentra il potere in poche grandi piattaforme private e pubbliche, lasciando i cittadini in una condizione di asimmetria informativa. La privacy è un obiettivo di libertà. La redistribuzione della conoscenza è un obiettivo di giustizia”.

La privacy quindi non è certamente morta, ma le scelte che facciamo oggi avranno conseguenze di portata enorme per il futuro. Secondo l'esperto informatico di Microsoft Jaron Lanier dovremmo evitare di parlare della privacy come di uno scambio in cui meno privacy corrisponde a più sicurezza quanto piuttosto dovremmo potere scegliere il livello di privacy desiderato [25]. Non è quindi ineluttabile che la privacy (o cybersecurity) individuale debba essere limitata a beneficio della sicurezza (nel senso di safety) collettiva.

È peraltro da notare che tanto le minacce quanto gli strumenti di protezione cambiano frequentemente interagendo in modo dinamico, accelerato e inarrestabile, perciò la sicurezza informatica, o privacy, assoluta è un obiettivo utopistico. Non c'è quindi da stupirsi se la lezione fondamentale sia che la

crittografia si può scardinare con la crittanalisi, come è accaduto nella recente disputa FBI-Apple sullo sblocco dell'iPhone cifrato dell'autore di una strage negli USA. A prevalere sono sempre le tecnologie e chi le possiede o le sa usare meglio. Occorre, pertanto, definire nuovi equilibri: diventiamo sempre tecnologicamente più potenti ma resta difficile stabilire il confine tra il bene e il male, per questo motivo bisogna riscoprire l'arte del limite [26]. E occorre tenere sempre a mente che l'uso di una tecnologia – o scienza – è ambivalente: gli esiti possono essere costruttivi o no, etici o no, buoni o no. Di per sé una tecnologia non è mai neutrale – recita una ben nota legge formulata dallo storico Melvin Krantzberg (1917-1995). In ultima istanza, le conseguenze dipendono esclusivamente dalla specie *Homo sapiens*, cioè da noi stessi.

0

1

0

1

0

Riquadro 1 – L'immagine delle agenzie di intelligence nei media

Why shouldn't I work for the NSA?

(Matt Damon, nel film *Will Hunting* – *Genio ribelle*, 1997, di Gus Van Sant)

L'ossessione per la segretezza e la security delle organizzazioni di intelligence nordamericane – così come quella delle analoghe britanniche – è risaputa. La NSA spende da sola un terzo dell'intero budget dell'intelligence USA (66,8 miliardi di dollari nel 2015) per un'attività di sorveglianza di massa con la raccolta incontrollata di metadati riguardanti politici, imprese, semplici cittadini. I dubbi riguardano la liceità e la compatibilità con la democrazia di questo comportamento, nonché l'efficacia a prevenire atti di terrorismo sempre più minacciosi e diffusi.

La NSA, a differenza del suo corrispettivo britannico, ha generalmente una pessima reputazione presso tutti i media. Colerico, paranoico, disilluso il ventenne genio matematico Will Hunting (l'attore Matt Damon), quando gli si offre un promettente e ben remunerato lavoro come crittografo presso la NSA, risponde – nel film prima citato – con un'invettiva antimilitarista alla proposta, agendo contro il proprio interesse economico. La sua filippica snocciola tutti i principali guai del mondo, con la NSA che sembra esserne la causa prima, se non l'unica.

Un altro esempio è il film *Nemico pubblico* (1998) dove l'innocente protagonista, impersonato dall'attore Will Smith, viene perseguitato dalla NSA per fini non certamente commendevoli. Essa, peraltro, sembra fare di tutto per meritarsi questa nomea: basta pensare alle vicende di Edward Snowden, l'ex analista dell'NSA che, nel maggio del 2013, ha rivelato le pratiche dell'Agenzia di azioni capillari ed estese di intercettazioni e spionaggio rivolte tanto ad alleati quanto a nemici, tramite la sua rete mondiale di satelliti, fibre ottiche, server. Al di là dell'imbarazzo diplomatico, la giustificazione è che gli amici si controllano tra loro da millenni ("così fan tutti"), come dimostra la celebre vicenda Yardley-Stimson sull'apertura della corrispondenza altrui, riportata in [27] e ricordata in [1]. Lo spionaggio – oggi, più elegantemente, chiamato intelligence – non è certamente equiparabile alla diplomazia che André Maurois definiva "l'arte di esporre le ostilità con cortesia".

Tradizionalmente, l'ambiente accademico USA rivendica orgogliosamente autonomia e indipendenza dalle organizzazioni governative di intelligence. Per questa ragione, i risultati delle ricerche crittologiche ottenuti in ambito universitario vengono prontamente pubblicati, suscitando talora aspre reazioni polemiche da parte governativa per "superiori ragioni di sicurezza della nazione". I pur validi crittologi della NSA sono invece soggetti a stringenti vincoli di segretezza.

È bensì corretto osservare che a partire dal 2009, con l'amministrazione Obama, anche il Central Security Service (CSS) della NSA ha cominciato a mettere a disposizione una gran mole di pubblicazioni e documenti inediti, d'interesse storico*.

Infine, un gustoso aneddoto sulla Seconda guerra mondiale, questa volta riguardante l'intelligence britannica e l'insigne giallista Agatha Christie, è ricordato in [1]. Al contrario dell'intelligence statunitense, quella britannica pare avere, in linea di massima, una più favorevole reputazione presso l'opinione pubblica e i media. Stranamente, perché sono gli USA che hanno coniato il patriottico motto "My country, right or wrong" (del commodoro Stephen Decatur, 1779-1820): sembra quasi che i britannici, sempre molto pragmatici, abbiano fatta propria l'icastica espressione di amor patrio.

* Cfr. la sua politica di "Declassification and Transparency" in https://www.nsa.gov/public_info/declass/index.shtml.

Bibliografia

- [1] Luvison, A. (2015). "La crittologia da arte a scienza: l'eredità di Shannon e Turing", *Mondo Digitale – Rassegna critica del settore ICT*, anno XIV, n. 60, 1-31, http://mondodigitale.aicanet.net/2015-5/articoli/03_crittologia_da_arte_a_scienza.pdf (ultimo accesso marzo 2016).
- [2] Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet* (Nuova edizione), Scribner. Prima edizione (1967). Macmillan. Tr. it. parziale della prima edizione (1969). *La guerra dei codici. La storia dei codici segreti*, Mondadori.
- [3] Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Doubleday Books. Tr. it. (1999). *Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet*, Rizzoli.
- [4] Massey, J.L. (2008). "A review of series on Arabic origins of cryptology", *Cryptologia*, vol. 32, n. 3, 280-283.
- [5] VV. AA. (2016). Spotlight on "How Platforms Are Reshaping Business", *Harvard Business Review*, vol. 94, n. 4.

- [6] Shannon, C.E. (1949). "Communications theory of secrecy systems", *Bell System Technical Journal*, vol. 48, n. 4, 656-715.
- [7] Paar C., Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioner*, Springer.
- [8] Simmons, G.J. (a cura di) (1992). *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press-Wiley.
- [9] Peres, E. (2012). *È l'enigmistica, bellezza! Lettere e cifre per allenare la mente*, Ponte alle Grazie.
- [10] Massey, J.L. (2001). "Cryptography – Science or magic?", MIT-EECS Colloquium, http://videolectures.net/mitworld_massey_csom/ (ultimo accesso marzo 2016).
- [11] Massey, J.L. (1992). "Contemporary cryptology: An introduction", in [8], 1-39.
- [12] Hellman, M.E. (1978). "An overview of public-key cryptography", *IEEE Communications Magazine*, vol. 16, n. 6, 24-31. Ristampa Id. (2002). *IEEE Communications Magazine 50th Anniversary Issue: Landmark 10 Papers*, vol. 40, n. 5, 42-49 [con una nuova introduzione che, tuttavia, non cita neppure i lavori del GCHQ].
- [13] Gardner, M. (1977). "Mathematical games: A new kind of cipher that would take millions of years to break", *Scientific American*, vol. 237, n. 2, 120-124.
- [14] Strumia, A. (2003). *Le scienze e la pienezza della razionalità*, Cantagalli.
- [15] Ellis, J.H. (1999). "The history of non-secret encryption" (Prefazione di Cliff Cocks), *Cryptologia*, vol. 23, n. 3, 267-27. [Il documento originale di Ellis è disponibile al link: <https://web.archive.org/web/20030610193721/http://jya.com/ellisdoc.htm> (ultimo accesso marzo 2016)].
- [16] Mezzalama, M., Liroy, A., Metwalley, H. (2013). "Anatomia del malware", *Mondo Digitale – Rassegna critica del settore ICT*, vol. XII, n. 47, pp. 1-20, http://mondodigitale.aicanet.net/2013-3/articoli/02_Anatomiadelmalware.pdf (ultimo accesso marzo 2016).
- [17] Goodman, M. (2015). *Future Crimes: A Journey to the Dark Side of Technology – and How to Survive It*, Bantam Press.
- [18] Winnefeld, J.A., Jr., Kirchoff, C., Upton, D.M. (2015). "Cybersecurity's human factor: Lessons from the Pentagon", *Harvard Business Review*, vol. 93, n. 9, 86-95.
- [19] Mosteller, F. (1987). *Fifty Challenging Problems in Probability with Solutions*, Dover.
- [20] Harbert, T. (2012). "New king of security algorithms crowned", *IEEE Spectrum*, vol. 49, n. 12, 10-11.
- [21] Quisquater, J.J. *et al.* (1990). "How to explain zero-knowledge protocols to your children", in Brassard, G. (a cura di), *Advances in Cryptology – CRYPTO '89: Proceedings (Lecture Notes in Computer Science 435)*, 9th

Annual International Cryptology Conference, Santa Barbara, California, USA, 20-24 August 1989, Springer-Verlag, 628-631.

[22] Kaku, M. (2016). *Il cosmo di Einstein*, Codice Edizioni.

[23] Ratcliff, R.A. (2006). *Delusions of Intelligence. Enigma, Ultra, and the End of Secure Cyphers*, Cambridge University Press.

[24] VV. AA. (2016). Special Issue on “Big Data: Theoretical Aspects”, *Proceedings of the IEEE*, vol. 104, n. 1; Special Issue on “Big Data: Applications”, *ibid.*, in corso di pubblicazione.

[25] Lanier, J. (2014). “Il senso della privacy al tempo di Internet”, *Le Scienze*, n. 546, 50-57.

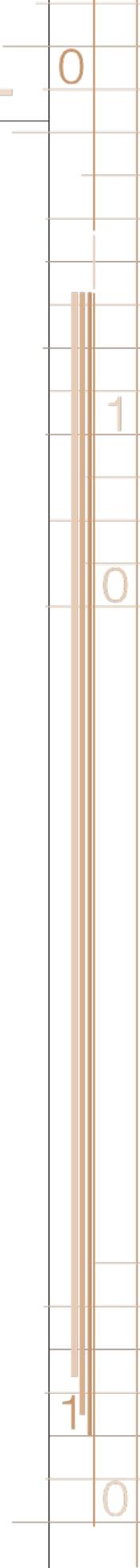
[26] Bodei, R. (2016). *Limite*, il Mulino.

[27] Kahn, D. (2004). *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking*, Yale University Press.

Biografia

Angelo Luvison è ingegnere elettronico dal 1969 (Politecnico di Torino), con successivi perfezionamenti in teoria statistica delle comunicazioni al MIT e in management aziendale all'INSEAD-CEDEP di Fontainebleau. Per oltre trent'anni in CSELT, ha svolto e coordinato ricerche in teoria delle comunicazioni, reti di fibre ottiche ad alta velocità, società dell'informazione, anche nell'ambito di progetti cooperativi internazionali. È stato professore di “Teoria dell'informazione e della trasmissione” all'Università di Torino. Ha ricoperto la posizione di segretario generale dell'AEIT. È stato consulente per la formazione permanente dei dirigenti d'azienda. Detiene sette brevetti ed è autore, o coautore, di quasi 200 lavori, uno dei quali è stato ripubblicato (2007) nel volume celebrativo *The Best of the Best* della IEEE Communications Society. È *Life Member* dell'IEEE e membro del Comitato scientifico di *Mondo Digitale*. Si occupa e scrive di temi di innovazione per le tecnologie informatiche e di telecomunicazioni (ICT).

Email: angelo.luvison@alice.it



Riconoscimento di gesti mediante dispositivi a basso costo:

tecniche, applicazioni, prospettive

Vito Gentile, Salvatore Sorce, Alessio Malizia,
Antonio Gentile

Sommario

Negli ultimi anni abbiamo assistito ad una grande diffusione dei cosiddetti "Kinect-like devices", ovvero dispositivi basati su un insieme di sensori a basso costo, che consentono di ottenere un'immagine di profondità della scena ripresa. L'alta accessibilità di questi dispositivi, principalmente in termini di costi, ne ha facilitato la diffusione nell'ambito del riconoscimento dei gesti in numerose applicazioni, sia commerciali che di ricerca. In questo articolo saranno inizialmente illustrati i principi generali su cui si fondano le principali tecniche utilizzate per riconoscere i gesti, sfruttando i dati ottenibili dai dispositivi "Kinect-like". Successivamente, saranno presentati alcuni ambiti applicativi, spaziando dal settore educativo-ricreativo a quello più scientifico (domotica, robotica ed ingegneria biomedica). In appendice, verranno elencati i principali prodotti disponibili in commercio e ne verrà presentata una sintetica analisi comparativa. Verrà inoltre descritto uno dei più noti e usati algoritmi di skeletal tracking, su cui si fonda la maggior parte delle soluzioni per il riconoscimento dei gesti.

Abstract

In the last decades, we have witnessed to the increase of the so-called Kinect-like devices, which are based on a set of low-cost sensors to acquire RGB and depth data of a scene. The high accessibility of such devices, mainly in terms of costs, has pushed their adoption as fundamental tool for gesture recognition in a large number of applications, both commercial and research-related ones. In this paper, we first discuss some of the general principles adopted by most of the main gesture recognition techniques described in literature. Then we present some application fields in which Kinect-like devices and gesture recognition algorithms have been used, ranging from educational-recreational examples to more complex



and scientific fields (e.g. domotics, robotics and biomedical engineering). In two annexes, we list and shortly compare the main features of the Kinect-like devices available on the market, and we describe one of the most popular algorithm for skeletal tracking, which is the basis for the gesture recognition.

Keywords: Gesture recognition; Kinect-like devices; Human-Computer Interaction; Touchless Interaction

1. Introduzione

Negli ultimi decenni, la ricerca nell'ambito dell'interazione uomo-macchina (o *Human-Computer Interaction, HCI*) ha visto un crescente interesse verso la scoperta di nuove modalità di interazione. L'innovazione e le nuove tecnologie, dalle più comuni (come i dispositivi mobili) a quelle meno diffuse, hanno contribuito in maniera significativa all'introduzione di nuove forme di interazione. Si è passato dall'interazione a riga di comando, al desktop, fino ad arrivare alle interfacce *touch*. Oggi, una delle nuove frontiere in termini di modalità di interazione sembra essere quella dell'interazione *touchless* e, in particolare, a gesti.

Per *interazione touchless* si intende una modalità di interazione che avviene senza che l'utente entri in contatto meccanico con alcun dispositivo o strumento fisico e tangibile del sistema [1]. Questo tipo di funzionalità può essere realizzata tramite l'uso di opportuni strumenti hardware, che forniscono dati utili ad un sistema informatico per "percepire" il comportamento interattivo di uno o più utenti. È importante notare che, secondo la precedente definizione di interazione *touchless*, interagire con un sistema utilizzando un controller, come accade ad esempio nell'interazione con Nintendo Wiimote o altri dispositivi simili (si veda ad esempio [2]), non è considerato una tipologia di interazione *touchless*. Al contrario, dispositivi che riconoscono la direzione dello sguardo (*eye tracker*), o i cosiddetti dispositivi *Kinect-like* [3], sono largamente accettati come validi esempi di dispositivi che permettono l'interazione *touchless*.

In questo articolo discuteremo dell'utilizzo di dispositivi *Kinect-like* al fine di implementare le principali tecniche utilizzate per il riconoscimento dei gesti, sfruttando i dati ottenibili da tali dispositivi. Verranno poi presentati alcuni ambiti applicativi, spaziando dal settore educativo-ricreativo a quello più scientifico (domotica, robotica ed ingegneria biomedica).

2. Riconoscimento di gesti statici

Secondo la definizione proposta da Henze et al. [4], un gesto *statico* è definito dalla *posizione* della mano nello spazio, mentre un gesto *dinamico* è definito dal *movimento* compiuto dalla mano. Ovviamente la definizione può essere estesa a gesti di altre parti o dell'intero corpo. In questa sezione si discuterà lo stato dell'arte relativo al riconoscimento dei gesti statici, con particolare attenzione a quelli della mano, per poi estendere la discussione al caso dei gesti corporali.

Nella sezione successiva verranno trattati gli approcci tipici per il riconoscimento di gesti dinamici.

2.1. Gestii statici della mano

Il processo di riconoscimento della posizione della mano è stato studiato da molti autori, e la letteratura fornisce numerose soluzioni. Spesso, soprattutto nei lavori più recenti, sono stati messi a punto sistemi in grado di funzionare in tempo reale sfruttando dispositivi *Kinect-like*.

In linea di massima, gli algoritmi di riconoscimento dei gesti statici della mano presentano alcuni tratti comuni. La Figura 1 mostra un tipico diagramma di flusso.

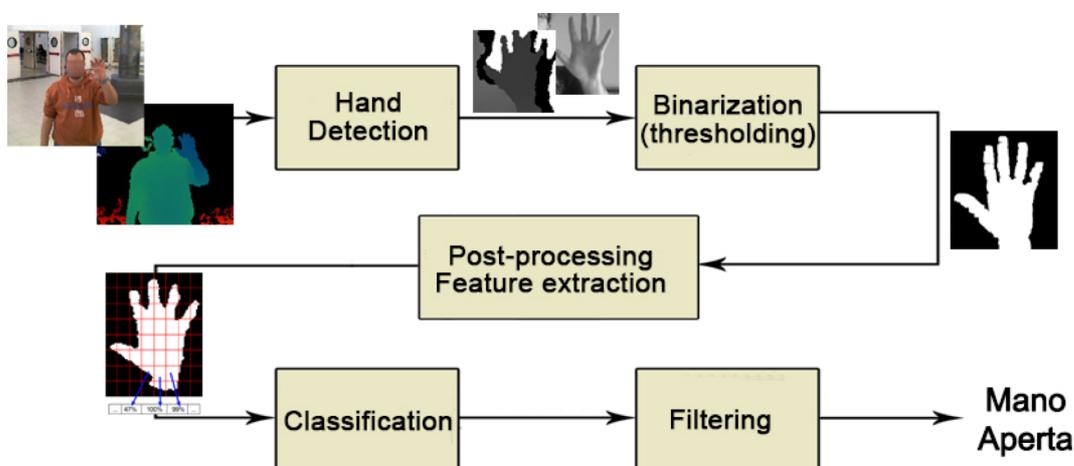


Figura 1.

Tipico diagramma di flusso per un algoritmo di riconoscimento di gesti statici della mano

In alcuni casi il diagramma può non rispecchiare perfettamente gli algoritmi presenti in letteratura, in quanto le operazioni di *feature extraction* (estrazione di caratteristiche) possono essere basate anche su dati diversi dalle maschere binarie (come ad esempio i bordi o qualsiasi altra informazione significativa). La discussione seguente si baserà comunque su questo schema, che è quello seguito da molti dei lavori presi in esame.

2.1.1. Riconoscimento e localizzazione della mano (*hand detection*)

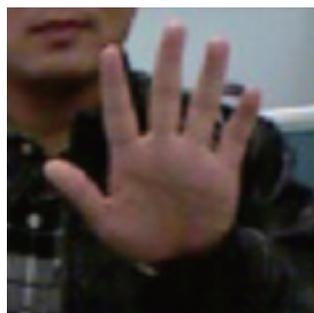
Il processo di *hand detection* consente l'individuazione della mano e della sua posizione all'interno di un'immagine comunque complessa. Il risultato di questo processo è una porzione dell'immagine (detta *region of interest, ROI*), contenente la mano. Sulla *ROI* estratta saranno effettuati tutti i successivi passi per l'estrazione delle caratteristiche ed il filtraggio.

La complessità del processo di localizzazione dipende da fattori quali la complessità della scena ripresa, nonché la disponibilità di dati aggiuntivi relativi

alla posizione della mano. La figura 2a mostra un caso favorevole, in cui la mano si trova in primo piano, su uno sfondo uniforme. In questo caso l'estrazione è semplice, essendo sufficiente procedere con il ritaglio dell'immagine (operazione conosciuta anche come *cropping*) basato sul calcolo del *bounding box* della mano (ovvero il minimo rettangolo contenente il contorno della mano). In casi meno controllati, come quello mostrato in figura 2b, un approccio di questo tipo può risultare più complesso.



(a)



(b)

Figura 2.

Alcuni esempi di frames a livelli di difficoltà crescente per la localizzazione della mano

Talvolta è possibile utilizzare algoritmi di rimozione di uno sfondo statico (*background removal*) da una sequenza di immagini con elementi dinamici in primo piano (come la mano) [5]. In tal modo è successivamente possibile procedere al calcolo della ROI come precedentemente descritto. Tali algoritmi di *background removal* (che, da soli, possono funzionare in real-time) hanno delle limitazioni relative al fatto che, se in primo piano non vi è soltanto la mano, altre porzioni del corpo potrebbero essere erroneamente incluse nella ROI.

Utilizzando i dispositivi *Kinect-like*, l'approccio seguito in [6] si riconduce all'utilizzo dei giunti scheletrici, che possono essere agevolmente estratti tramite un algoritmo molto efficiente di *skeletal tracking* (si veda il relativo riquadro di approfondimento) [7]. Prendendo a riferimento il giunto relativo alla mano, si può centrare su di esso un rettangolo opportunamente dimensionato, che rappresenterà la ROI. Il dimensionamento di esso può essere valutato sulla base di considerazioni antropometriche, fissando euristicamente le sue dimensioni, oppure valutandole sulla base di quelle di altre parti del corpo.

2.1.2. Binarizzazione

Una volta individuata la ROI su cui operare per l'estrazione delle caratteristiche, si può procedere con la successiva fase, che è quella della *binarizzazione* (figura 3): si tratta di un'operazione che ha lo scopo di trasformare l'immagine della mano in una immagine binaria, che utilizza cioè due soli colori (tipicamente bianco e nero). Per questo processo, in generale, si possono utilizzare approcci basati sul colore della pelle, sui dati di profondità, o su entrambi questi tipi di informazioni.

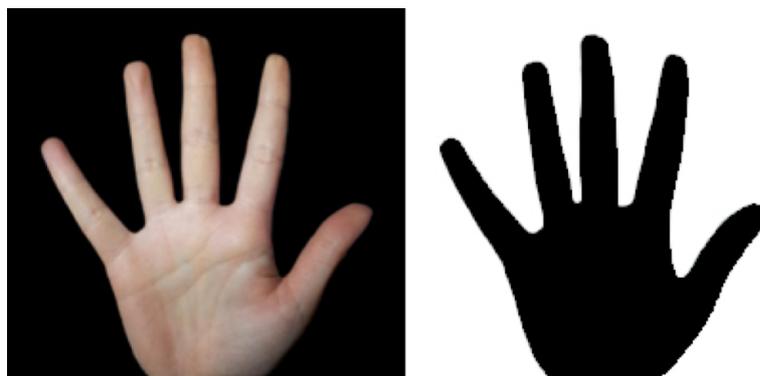


Figura 3.
Un esempio di binarizzazione di una mano

Alcuni autori hanno utilizzato approcci basati sul colore della pelle [8] [9], finalizzati all'estrazione della mano. A tal fine, sono stati proposti metodi che si basano sull'utilizzo di spazi di colore più appropriati di RGB, uniti a modelli probabilistici che assegnano ad ogni pixel una probabilità di appartenere alla pelle, in funzione del colore. In casi come quello di figura 2b, però, ciò può facilmente comportare errori, dal momento che anche altre zone del corpo vengono riconosciute, nonostante non facenti parte della mano.

Altri autori, invece, si basano sulla segmentazione basata unicamente sui dati di profondità [6] [10] [11]. Ciò ha il grande pregio di consentire un funzionamento indipendente dalle condizioni di illuminazione, ed è per questo motivo che è stato largamente utilizzato.

Si può migliorare il processo di binarizzazione, correggendo la maschera di profondità estratta, utilizzando le informazioni di colore fornite dalla videocamera RGB di un dispositivo *Kinect-like*. Approcci ibridi di questo tipo sono stati usati da alcuni ricercatori per ottenere i risultati più accurati da questa fase del processo [12].

La tabella 1 riassume le caratteristiche principali dei metodi di binarizzazione sopra accennati.

Metodo di binarizzazione	Indipendente dalle variazioni di illuminazione	Robusto all'utilizzo di guanti e accessori
Segmentazione basata sul colore della pelle	NO	NO
Segmentazione basata sulla mappa di profondità	SI	SI
Segmentazione ibrida, (colore + profondità)	Solo alcuni metodi	Solo alcuni metodi

Tabella 1.
Caratteristiche dei metodi di binarizzazione

2.1.3. *Post-processing ed estrazione di caratteristiche*

Una volta concluso il processo di binarizzazione (ma quel che segue può essere applicato anche prima di questa fase), si può procedere con la correzione del profilo della forma ottenuta, tramite operazioni di *post-processing* che, ad esempio, ne correggono le imperfezioni. Un semplice esempio, mostrato in figura 4, è l'utilizzo di un filtro mediano per lo smussamento [13], mentre soluzioni più complesse prevedono l'utilizzo di tecniche per la rimozione dell'avambraccio [9] [14] [15], eventualmente incluso nel risultato della segmentazione.



Figura 4.

Esempio di post-processing effettuato applicando un filtro mediano all'immagine binaria di una mano.

Ottenuta, quindi, un'immagine binaria rappresentante la forma della mano, essa deve essere trasformata in una forma che ne evidenzi le caratteristiche essenziali per il riconoscimento, e che possa al tempo stesso essere utilizzata per la classificazione. A tale scopo, sono state adottate molte tecniche. Le più interessanti sono quelle in grado di offrire un elevato grado di invarianza alla scala ed alla rotazione (per motivi che saranno meglio chiariti più avanti).

Alcune tecniche proposte in letteratura codificano il contorno della mano in modo che esso venga rappresentato da una o più funzioni lineari [14]. Esistono poi altre tecniche, più o meno complesse, basate sul calcolo di caratteristiche che possano descrivere un contorno (per esempio la combinazione di grandezze come l'area, il perimetro, il numero di concavità, eccetera). Molte di queste tecniche sono riassunte e descritte in [16].

Approcci alternativi si basano sull'estrazione di caratteristiche locali, calcolate cioè su sottoregioni (eventualmente - ma non necessariamente - organizzate gerarchicamente) delle immagini binarie originariamente utilizzate [15] [10] (figura 5). Altri autori, utilizzando anche le informazioni di profondità e di colore, ricavano lo scheletro della mano e lo adoperano per il riconoscimento [8], oppure estraggono descrittori di forma tridimensionali da un modello 3D ricavato dai dati di profondità [17]. In [6] e [11], vengono estratti dei descrittori *SURF* (*Speeded Up Robust Features*), utilizzando la maschera di profondità per evidenziare la sola ROI all'interno dell'immagine RGB. Van den Bergh e Van Gool [12] utilizzano un sistema di riconoscimento basato sulle *Haarlets*, descritte a loro volta in [18].

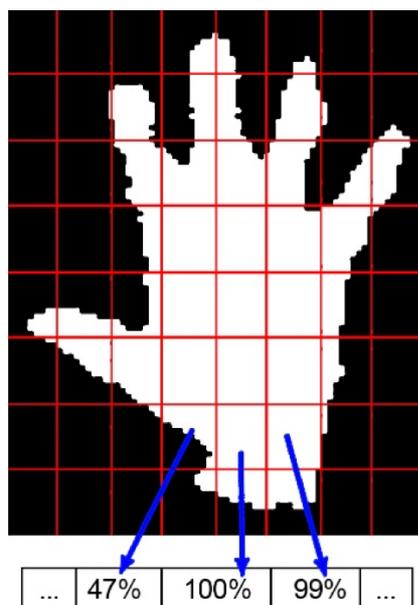


Figura 5.

Esempio di estrazione di caratteristiche locali, in cui si nota la suddivisione dell'immagine in sottoregioni

La tabella 2 mostra un confronto tra pro e contro dei metodi di post-processing presi in considerazione.

METODO	PRO	CONTRO
Descrittori di boundary	Buon livello di compressione Robusto a rotazione e scala	Richiede un alto livello di dettaglio dell'input, soprattutto per la differenziazione delle dita
Features locali	Si presta alla parallelizzazione Efficiente	Generico, non sempre fornisce una buona descrizione della forma della mano
Scheletro della mano	Garantisce un ottimo livello di dettaglio del riconoscimento	Richiede un alto livello di dettaglio dell'input, soprattutto per la differenziazione delle dita
Descrittori di forma 3D	Garantisce un ottimo livello di dettaglio del riconoscimento	Algoritmo di riconoscimento computazionalmente pesante
Descrittori SURF	Efficace per elaborazioni in tempo reale	Poco robusto alle variazioni di luminosità
2D e 3D Haarlets	Efficace per elaborazioni in tempo reale	Poco robusto alle variazioni di luminosità

Tabella 2.

Confronto tra tecniche di post-processing

2.1.4. Classificazione e filtraggio

Le tecniche più adoperate per la classificazione sono quelle basate sull'uso delle reti neurali [6] [19], o in alternativa quelle che utilizzano le macchine a vettore di supporto (*Support Vector Machine, SVM*) [11]. In entrambi i casi si tratta di strumenti matematici in grado di "apprendere" un algoritmo tramite una fase detta di "addestramento": utilizzando un insieme di input e output noti, una serie di algoritmi consente di "configurare" un programma in modo che esso "impari" ad ottenere un output valido anche per nuovi input.

Alcuni autori classificano i gesti statici seguendo anche approcci di tipo diverso. Ren et al. [14] si basano sul calcolo di una opportuna misura di distanza tra una rappresentazione della mano ed alcuni prototipi caratteristici di una classe. La classificazione avviene, quindi, in base alla minore misura di dissimilarità.

Subito dopo il processo di classificazione, talvolta è possibile applicare un filtro che rimuova il rumore dell'uscita. In [6], si utilizza un filtro di media temporale. In alternativa, è possibile modellare il rumore come gaussiano, ed adoperare filtri più complessi, come quello di Kalman [11].

2.2. Gesti statici del corpo

Abbiamo descritto finora alcuni principi su cui si basano le tecniche di riconoscimento di una "posa" della mano. È intuibile come molte delle idee sopra esposte possono essere utilizzate anche per il riconoscimento delle "pose" del corpo (che, secondo la definizione di Henze et al. precedentemente citata, sono anch'esse definite come gesti statici [4]). In letteratura, il processo di riconoscimento posturale si articola generalmente in due fasi:

1. estrazione delle caratteristiche;
2. classificazione vera e propria, per stabilire qual è la configurazione posturale in esame.

Diversi autori seguono lo schema appena descritto, utilizzando un algoritmo di *skeletal tracking* (si veda il relativo riquadro di approfondimento) per estrarre una serie di giunti scheletrici (che rappresentano le *caratteristiche* di cui sopra, in questo caso) da utilizzare per la classificazione [20] [21]. Gli autori utilizzano diverse metriche per valutare la distanza tra le posture esaminate e quelle appartenenti ad un set di riferimento, operando quindi una classificazione. È anche possibile riconoscere alcune nuove classi di posture, ed aggiungerle al set di riferimento (implementando ciò che viene definito un "sistema di apprendimento incrementale").

Altri lavori simili migliorano il riconoscimento tramite tecniche più o meno sofisticate mirate a risolvere i problemi di parziale occlusione del corpo [22].

È comunque possibile effettuare il riconoscimento posturale anche estraendo caratteristiche diverse dai giunti scheletrici (e quindi senza utilizzare alcun algoritmo di *skeletal tracking*). Biswas e Basu [10], ad esempio, utilizzano un approccio basato sulla suddivisione della sagoma del corpo (ricavata dalla binarizzazione dell'immagine di profondità), in sottoregioni organizzate gerarchicamente. Da ognuna di esse sono poi estratte delle caratteristiche locali, utilizzate tutte insieme per la classificazione. Quest'ultima avviene tramite l'uso di una *SVM* opportunamente addestrata.

3. Riconoscimento di gesti dinamici

In questa sezione si discuterà lo stato dell'arte relativo al riconoscimento dei gesti dinamici, costituiti cioè da una sequenza di gesti statici. Nella prima parte ci concentreremo sugli algoritmi utilizzati per il riconoscimento dei gesti dinamici della mano, per poi estendere la discussione al caso più ampio dei gesti del corpo. Il processo di riconoscimento dei gesti dinamici richiede l'analisi di più immagini consecutive, e di conseguenza è generalmente richiesto un carico computazionale più oneroso rispetto al riconoscimento dei gesti statici.

3.1. Panoramica

Per i gesti dinamici, siano essi relativi alla mano o al corpo intero, i lavori presenti in letteratura scientifica prevedono ancora un processo di estrazione di caratteristiche della parte del corpo interessata, utilizzabili poi in una successiva fase di classificazione. Nei casi dei gesti statici, queste caratteristiche sono tipicamente legate alla forma (che, per questo, sono identificate come *shape features*). Nei casi di gesti dinamici, anche grandezze come la velocità del movimento o la traiettoria di alcuni punti salienti diventano parametri di decisione rilevanti, che possono essere utilizzati per la classificazione. Per riuscire ad ottenere questo genere di informazioni occorre, quindi, tenere conto di finestre temporali successive, e dei vettori di caratteristiche relativi ad esse che vengono via via calcolati.

Quindi, un generico processo di riconoscimento dei gesti dinamici può essere schematizzato come mostrato in figura 6:

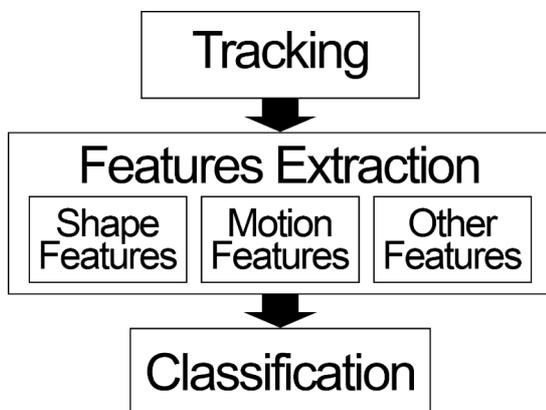


Figura 6.

Schema riepilogativo del processo di riconoscimento dei gesti dinamici.

Mentre per quanto riguarda le fasi di estrazione delle *shape features*, si può fare riferimento alle stesse tecniche viste per i gesti statici, le fasi di estrazione delle *motion features* (caratteristiche legate alle traiettorie dei punti, e quindi al movimento che definisce il gesto) richiedono considerazioni diverse. Per quanto riguarda la classificazione, le tecniche generalmente utilizzate sono quelle in grado di indirizzare dinamicamente il processo decisionale, in funzione dei

vettori di caratteristiche estratti di volta in volta da ogni immagine della sequenza che compone il gesto.

3.2. Gesti dinamici della mano

Nel riconoscere un gesto della mano, vi sono numerosi fattori da tenere in considerazione. In primis, durante il gesto, la postura delle singole dita può variare, e tale variazione può essere parte del gesto. Inoltre, la traiettoria tracciata dalla mano caratterizza anch'essa il gesto. In alcune situazioni, uno di questi due aspetti può essere ritenuto meno importante ai fini del riconoscimento, riducendo anche l'onere computazionale dell'intero processo. Xiao Jang et al. [23], per esempio, effettuano il solo riconoscimento della traiettoria, a patto però che la mano sia aperta: utilizzando un metodo di riconoscimento statico per riconoscere la corretta posa della mano, si può utilizzare la sola traiettoria come input per un classificatore basato su *Hidden Markovian Model (HMM)* (uno strumento matematico molto utilizzato in scenari come il riconoscimento dinamico di gesti).

Per gesti più complessi, in cui la configurazione delle singole dita ha una valenza significativa, è necessario tenere in considerazione anche le variazioni di forma della mano. In questo senso, il lavoro di Kurakin et al. [15] rappresenta una soluzione più completa. Essi, infatti, effettuano una serie di operazioni che estraggono diverse *shape features*. A queste, gli autori aggiungono la velocità del centro della mano (che è una *motion feature*), rappresentata dallo spostamento di essa tra due immagini successive. Queste caratteristiche vengono quindi classificate tramite uno strumento matematico chiamato *action graph* (definito in [24]).

Una delle principali applicazioni del riconoscimento dei gesti dinamici è quella del riconoscimento delle lingue dei segni. A tale scopo, Geetha et al. [25] utilizzano una tecnologia che consente di estrarre una serie di giunti scheletrici di entrambe le mani. Utilizzando sette punti dello scheletro di ogni mano, estratti da ogni frame, si possono tracciare le traiettorie che tali giunti delineano durante il movimento della mano. In questo modo si riassumono sia le informazioni sulla forma (date dai giunti scheletrici) sia quelle relative al moto.

Esistono comunque un gran numero di tecniche alternative a quelle citate, ma quelle citate rendono l'idea del tipo di approccio necessario per implementare il riconoscimento di gesti dinamici della mano.

3.3. Gesti dinamici del corpo

Sebbene, in linea di principio, il riconoscimento dei gesti dinamici del corpo non differisca molto da quello dei gesti dinamici della sola mano, la disponibilità di algoritmi di *skeletal tracking* come quelli già citati ne rende meno complicato lo sviluppo nelle applicazioni pratiche. Molti metodi, infatti, si basano semplicemente sull'uso di sequenze di posture [20] [21] [22], ciascuna delle quali non è altro che un insieme di giunti scheletrici che vanno a comporre il gesto dinamico del corpo. Tali metodi, inoltre, sono in grado di funzionare in tempo reale.

Ciò che differenzia i metodi non è tanto, quindi, l'estrazione delle *shape features* (che sono proprio i giunti scheletrici), quanto piuttosto l'utilizzo di *motion features* e le diverse possibilità di classificazione. Quest'ultimo processo può utilizzare diversi strumenti matematici (*Hidden Markovian Model*, reti neurali, *SVM*, reti bayesiane), la cui descrizione richiederebbe però un approfondimento notevole, ed esula dagli scopi del presente articolo.

4. Applicazioni

Le tecniche di riconoscimento dei gesti sono state utilizzate in svariati ambiti di ricerca, nonché in numerose applicazioni. Esse si prestano innanzitutto alla costruzione di interfacce multimodali, offrendo la possibilità di incrementare il livello di immersività dell'interazione tra l'utente ed il computer. Inoltre, riconoscere i gesti e le posture può rivelarsi molto utile nell'ambito della sicurezza degli utenti all'interno di ambienti domotici, al fine di prevenire incidenti domestici o segnalare malori.

Si possono definire alcune macroaree di interesse, all'interno delle quali trovano applicazione alcune tecniche di riconoscimento dei gesti (siano essi statici o dinamici). Esse sono:

- *area ludico-educativa*, che rappresenta il principale ambito di applicazione di molti dispositivi *Kinect-like*, in particolare Microsoft Kinect (nato per offrire modalità di interazione a gesti e innovative agli utenti di Xbox). La sfera educativa può essere inclusa in questa macroarea, dal momento che utilizzando la multimodalità dell'interfaccia, si può accrescere l'interesse di studenti verso varie discipline, facilitando i compiti degli educatori;
- *area domotica*, in cui si sfruttano le tecniche di riconoscimento dei gesti al fine di garantire una maggiore sicurezza dell'utente, ma anche per aumentare le possibilità di controllo delle componenti *smart* della casa;
- *area divulgativa*, in cui si utilizza il riconoscimento dei gesti per aumentare l'*immersione* dell'utente all'interno di un ambiente, al fine di accrescerne l'interesse. È il caso delle installazioni museali interattive, ma anche di proposte pubblicitarie finalizzate ad aumentare il coinvolgimento dell'utente, o ad accrescerne la curiosità;
- *area robotica*, nella quale i dispositivi *Kinect-like* sono stati ampiamente utilizzati per facilitare il riconoscimento delle azioni degli utenti che interagiscono con i robot (nell'ambito che viene definito di *Human-Robot Interaction, HRI*);
- *area bio-medica*, nella quale si sfruttano le funzionalità dei dispositivi *Kinect-like* sia in ambito riabilitativo (ad esempio per valutare eventuali problemi nei movimenti di un paziente) sia a scopi meno critici (ad esempio per interagire a gesti con immagini medicali proiettate su un display).

Nel seguito saranno analizzate alcune delle soluzioni proposte in letteratura, evidenziandone i pregi e le limitazioni.

4.1. Applicazioni ludico/educative

L'ambito ludico è uno dei principali campi di applicazione di alcuni dispositivi *Kinect-like*. Si pensi, ad esempio, a Microsoft Kinect, sviluppato e commercializzato principalmente per essere utilizzato insieme alla console Microsoft Xbox (figura 7). Per questa piattaforma, infatti, sono stati sviluppati e pubblicati centinaia di giochi basati su interazione a gesti, tuttora in vendita ed in continua evoluzione.



Figura 7.

Due utenti interagiscono a gesti con un gioco per Xbox tramite Microsoft Kinect.

Tuttavia, l'utilizzo di Microsoft Kinect in congiunzione con Xbox non è l'unico caso di applicazione ludico-educativa che sfrutta dispositivi *Kinect-like*. Infatti, è facile immaginare come le possibilità offerte da questa tecnologia possano essere estese ed applicate nelle più svariate piattaforme. Questa idea è esattamente ciò che sta alla base di KinectEDucation [26], una community che ha lo scopo di promuovere l'utilizzo di Microsoft Kinect in ambito educativo, offrendo materiale didattico direttamente a studenti ed educatori, ma anche supporto per gli sviluppatori interessati in questo senso. Molti dei software proposti da KinectEDucation consentono agli studenti di imparare nozioni di base, utilizzando i gesti per creare un'interfaccia innovativa, che ne stimoli l'interesse. Per citare qualche esempio, sono stati sviluppati software per facilitare l'apprendimento della lingua dei segni, per esplorare ed imparare l'anatomia umana osservandola direttamente sul proprio corpo, nonché per ispirare la creatività tramite la possibilità di tracciare disegni o manipolare e muovere oggetti.

Un interessante lavoro mirato, invece, a facilitare il compito di un educatore, è il sistema proposto da Shuai Zhang et al. [27], che prevede l'integrazione dei dispositivi *Kinect-like* con alcune videoproiezioni per creare una lavagna virtuale proiettabile, senza l'utilizzo di alcuno schermo. Utilizzando un controller wireless (basato su tecnologia IR) delle dimensioni di una penna, si può infatti tracciare

un qualsiasi disegno, proiettarlo su una parete e visualizzarlo tramite video proiezione. Il tracciamento può essere realizzato effettuando il tracciamento della mano ripresa, con i metodi già descritti in precedenza.

Infine, alcune applicazioni possono essere quelle relative alla valutazione di particolari attività, legate ad alcuni sport come il golf, in cui la postura ha una rilevanza fondamentale. Lichao Zhang et al. [28] hanno studiato un sistema in grado di valutare la correttezza dei movimenti di un giocatore di golf, tramite l'assegnazione di un punteggio ad ogni prova di lancio della pallina da golf effettuata utilizzando un'apposita mazza.

4.2. Domotica

Negli ambiti della domotica e della home automation, i dispositivi *Kinect-like* sono stati utilizzati (e continuano ad essere studiati) sia per aumentare le possibilità di interazione con la casa ed i suoi componenti, utilizzando direttamente i gesti, sia per garantire un maggiore livello di sicurezza, tramite funzionalità di riconoscimento automatico di incidenti domestici (come descritto in [29]).

Relativamente al controllo domestico, ha particolare rilevanza il progetto chiamato WorldKit [30], che utilizza dispositivi *Kinect-like* congiuntamente ad opportune videoproiezioni per implementare funzionalità di controllo (figura 8). Sostanzialmente, questo sistema consente di trasformare le pareti di una casa in superfici con le quali è possibile interagire tramite gesti. Le possibilità offerte sono moltissime: si va dal controllo di svariati apparecchi (volume dello stereo o della televisione, impianto di climatizzazione, ecc.), fino alla pianificazione delle attività tramite proiezioni interattive.



Figura 8.

Un esempio di interazione supportata da WorldKit [30], in cui è visibile l'integrazione tra dispositivi Kinect-like e videoproiezioni.

In [31] vengono analizzate diverse applicazioni domotiche, sia per il controllo dell'ambiente guidato dai gesti, sia per la sicurezza degli utenti. Tra quelle studiate dagli autori, se ne possono citare alcune abbastanza interessanti.

Hands-Up [32], ad esempio, è un sistema che combina l'uso di un proiettore e di Microsoft Kinect per sfruttare il soffitto al fine di creare uno schermo col quale interfacciarsi tramite i gesti. Lo stesso tipo di funzionalità sono implementate anche in [33].

Un'altra applicazione che sfrutta Microsoft Kinect per l'utilizzo in ambito domestico è *Kinect in the Kitchen* [34], che utilizza il riconoscimento dei gesti in ambienti come la cucina, in cui l'interazione gestuale può consentire l'interazione con uno schermo pur avendo le mani sporche o unte. Gli autori affermano di aver avuto feedback molto positivi dagli utenti che hanno provato questo sistema.

4.3. Servizi Informativi

Le applicazioni in questo campo sfruttano i gesti non solo per l'interazione, ma soprattutto per accrescere l'interesse degli utenti alle informazioni da esse fornite.

Un tipico esempio è *Interactive Wall* [35], un progetto che ha consentito la realizzazione di un intero muro interattivo lungo più di 10 metri, animato in funzione dei gesti e degli spostamenti degli utenti che passavano davanti ad esso. In questo modo, è stato possibile applicare le funzionalità dei dispositivi *Kinect-like*, e le relative tecniche di riconoscimento dei gesti, al fine di stimolare l'interesse dei passanti a scopi pubblicitari. Progetti analoghi sono descritti in [36] e [37].

Anche in molte installazioni museali i dispositivi *Kinect-like* hanno trovato applicazione, risultando strumenti estremamente utili a stimolare l'interesse degli utenti verso la cultura [38] [39].

4.4. Robotica

Il riconoscimento dei gesti si presta non solo all'interazione tra uomo e computer, ma anche a contesti come la *Human-Robot Interaction (HRI)* e la *Robot-Robot Interaction (RRI)*. È per questo che sono state spesso integrate diverse tecniche di riconoscimento dei gesti in sistemi robotici [40], ed anche i dispositivi *Kinect-like* sono stati utilizzati a tale scopo [41]. Un esempio delle recenti applicazioni di più alto livello è *JediBot* [41], un braccio robotico in grado di analizzare i gesti del corpo di un "avversario" dotato di spada (o bastone) per generare una risposta in tempo reale (figura 9). Altro tipo di applicazione, invece, è quella proposta in [42], dove gli autori discutono come sia possibile controllare uno scheletro robotico mediante un dispositivo *Kinect-like*.

4.5. Bio-medicina

Recentemente, i dispositivi *Kinect-like* sono stati utilizzati nel campo dell'ingegneria biomedica come parte di sistemi per il monitoraggio degli esercizi di riabilitazione dei pazienti. È il caso, ad esempio, di *Kinerehab* [43], un sistema per la riabilitazione fisica di giovani e adulti con disabilità motorie. In questo caso, il dispositivo *Kinect-like* è utilizzato per verificare la qualità del movimento, in modo da fornire un supporto al terapeuta sul trattamento da

effettuare. In maniera concettualmente analoga, Lange et al. [44] hanno sviluppato un gioco con interfaccia a gesti, compatibile con Microsoft Kinect, i cui scopi vengono raggiunti solo tramite movimenti finalizzati al trattamento riabilitativo. Alvarez e Grogan [45] hanno utilizzato questo tipo di dispositivi su pazienti affetti da morbo di Parkinson per migliorare anomalie motorie e disfunzioni dell'andatura.



Figura 9.
JediBot in azione.

Altre applicazioni biomediche utilizzano i dispositivi *Kinect-like* per il controllo della respirazione [46], nonché (più semplicemente) per consentire l'interazione a gesti con immagini medicali (molto utile in contesti operatori, in cui il medico è contemporaneamente impegnato nell'operare un paziente) [47].

5. Discussione

Il riconoscimento di gesti del corpo o di sue parti gioca oggi un ruolo chiave nell'ambito dell'interazione uomo-macchina. Infatti, la grande diffusione di sistemi informativi e la crescente richiesta di interattività, pongono nuove sfide circa le modalità di interazione, a causa di vincoli che non consentono l'uso dei consueti dispositivi di input.

Fino ad ora, la necessità di nuove modalità di interazione, e la loro applicazione, si è evidenziata soprattutto in ambiti molto particolari, in cui l'uso di dispositivi classici di input è scomodo o impossibile (telemedicina, controllo remoto di robot in zone ad alto rischio, ecc.), in ambito ludico (console per videogiochi), nell'*home entertainment*. Oggi, grazie alle nuove tecnologie, sono sempre più frequenti i casi in cui nuovi modi di interazione vengono produttivamente e utilmente impiegati.

Quelli descritti in questo articolo sono solo alcuni esempi di contesti in cui la capacità di interagire a distanza, mediante gesti in modalità *touchless*, ha aperto nuove prospettive e possibilità di impiego. Da tale apertura discende una

serie di sfide trasversali, dal punto di vista delle tecnologie, del fattore umano, delle possibili applicazioni.

Per quanto riguarda le tecnologie, l'analisi condotta in questo articolo dimostra come ormai sia economicamente accessibile e tecnicamente fattibile la realizzazione di sistemi di riconoscimento affidabile e veloce di gesti a scopo interattivo.

Nonostante l'accessibilità tecnica ed economica, tale modalità di interazione pone alcuni problemi relativamente al fattore umano, per esempio in termini di:

- *accettabilità sociale*: non è detto che le persone siano disposte a gesticolare (soprattutto in pubblico) davanti a un display per accedere alle informazioni da esso fornite;
- *naturalezza percepita*: i gesti da utilizzare per interagire dovrebbero essere "naturali" [48], nel senso di non necessitare di nessuna forma di addestramento all'uso, e risultare quindi massimamente intuitivi;
- *utilità effettiva*: l'utente deve percepire il vantaggio di tale tipo di interazione, a fronte di un servizio utile e innovativo;
- *efficacia*: i gesti devono condurre all'informazione desiderata in pochi passaggi.

In conclusione, i vincoli posti dall'interazione gestuale in termini di sviluppo, messa in opera e validazione, hanno finora limitato la sua adozione sui sistemi informativi di largo uso. La natura *touchless* di tale interazione, e le sue conseguenti potenzialità applicative, costituiscono però il motore principale della spinta evolutiva in corso, che è dimostrata dal vasto interesse in ambito scientifico. Le soluzioni in fase di studio e la disponibilità di tecnologie abilitanti a costi accessibili, lasciano presagire che, in un futuro non lontano, l'interazione gestuale uomo-macchina verrà sempre più adottata e riconosciuta come "naturale", alla stregua dell'interazione tra umani.

6. Bibliografia

- [1] R. de la Barré, P. Chojecki, U. Leiner, L. Mühlbach e D. Ruschin, «Touchless Interaction-Novel Chances and Challenges,» in *Human-Computer Interaction. Novel Interaction Methods and Techniques*, Jacko, Julie A., 2009, pp. 161-169.
- [2] A. Bellucci, A. Malizia, P. Diaz e I. Aedo, «Don't touch me: multi-user annotations on a map in large display environments,» in *Proceedings of the International Conference on Advanced Visual Interfaces (AVI '10)*, 2010.
- [3] V. Gentile, S. Sorce e A. Gentile, «Continuous Hand Openness Detection Using a Kinect-Like Device,» in *2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, Birmingham, UK, 2014.
- [4] N. Henze, A. Löcken, S. Boll, T. Hesselmann e M. Pielot, «Free-hand gestures for music playback: deriving gestures with a user-centred

process,» in *9th International Conference on Mobile and Ubiquitous Multimedia*, New York, NY, USA, 2010.

[5] J. Sun, W. Zhang, X. Tang e H.-Y. Shum, «Background cut,» in *Proceedings of the 9th European conference on Computer Vision (ECCV'06)*, Graz, Austria, 2006.

[6] S. Sorce, V. Gentile e A. Gentile, «Real-time Hand Pose Recognition Based on a Neural Network Using Microsoft Kinect,» in *Proceedings of the Eighth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA 2013)*, Compiègne, France, 2013.

[7] J. Shotton, A. Fitzgibbon, M. Cook, T. Sharp, M. Finocchio, R. Moore, A. Kipman e A. Blake, «Real-time human pose recognition in parts from single depth images,» in *2011 IEEE Conference on Computer Vision and Pattern Recognition*, Providence, RI, USA, 2011.

[8] H. Matos, H. P. Oliveira e F. Magalhães, «Hand-Geometry Based Recognition System A Non Restricted Acquisition Approach,» in *9th International Conference on Image Analysis and Recognition (ICIAR)*, Aveiro, Portugal, 2012.

[9] M. K. Bhuyan, R. N. Debanga e K. K. Mithun, «Fingertip Detection for Hand Pose Recognition,» *International Journal on Computer Science and Engineering (IJCSE)*, vol. 4, n. 3, 2012.

[10] K. K. Biswas e K. B. Saurav, «Gesture Recognition using Microsoft Kinect®,» in *5th International Conference on Automation, Robotics and Applications (ICARA)*, Wellington, New Zealand, 2011.

[11] A. D. Bagdanov, A. Del Bimbo, L. Seidenari e L. Usai, «Real-time hand status recognition from RGB-D imagery,» in *21st International Conference on Pattern Recognition*, Tsukuba, Japan, 2012.

[12] M. Van den Bergh e L. Van Gool, «Combining RGB and ToF cameras for real-time 3D hand gesture interaction,» in *IEEE Workshop on Applications of Computer Vision (WACV)*, Kona, HI, USA, 2011.

[13] S. Marchand-Maillet e Y. M. Sharaiha, *Binary Digital Image Processing: A Discrete Approach*, Academic Press, 2000.

[14] Z. Ren, J. Yuan e Z. Zhang, «Robust Hand Gesture Recognition Based on Finger-Earth Mover's Distance with a Commodity Depth Camera,» in *Proceedings of the 19th ACM international conference on Multimedia*, New York, NY, USA, 2011.

[15] A. Kurakin, Z. Zhang e Z. Liu, «A real time system for dynamic hand gesture recognition with a depth sensor,» in *20th European Signal Processing Conference (EUSIPCO)*, Bucharest, Romania, 2012.

[16] Y. Mingqiang, K. Kidiyo e R. Joseph, «A survey of shape feature extraction techniques,» *Pattern Recognition*, pp. 43 - 90, November 2008.

[17] S. Poonam, S. Anbumani e M. Dinesh, «Dynamic Hand Pose Recognition using Depth Data,» in *International Conference on Pattern Recognition*, Istanbul, Turkey, 2010.

- [18] M. Van den Bergh, E. Koller-Meier e L. Van Gool, «Real-Time Body Pose Recognition Using 2D or 3D Haarlets,» *International Journal of Computer Vision*, vol. 83, n. 1, pp. 72 - 84, June 2009.
- [19] G. P. Zhang, «Neural Network for Classification: A Survey,» *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 30, n. 4, pp. 451-462, Novembre 2000.
- [20] S. Monir, S. Rubya e H. S. Ferdous, «Rotation and scale invariant posture recognition using Microsoft Kinect skeletal tracking feature,» in *12th International Conference on Intelligent Systems Design and Applications (ISDA)*, Kochi, India, 2012.
- [21] F. D. Zainordin, H. Y. Lee, N. A. Sani, Y. M. Wong e C. S. Chan, «Human pose recognition using Kinect and rule-based system,» in *World Automation Congress (WAC)*, Puerto Vallarta, Mexico, 2012.
- [22] H. P. H. Shum, E. S. L. Ho, Y. Jiang e S. Takagi, «Real-Time Posture Reconstruction for Microsoft Kinect,» *IEEE Transactions on Cybernetics*, vol. 43, n. 5, pp. 1357 - 1369, 2013.
- [23] X. Jiang, X. Lu, L. Chen, L. Zhou e S. Shen, «A Dynamic Gesture Recognition Method Based on Computer Vision,» in *6th International Congress on Image and Signal Processing (CISP 2013)*, Hangzhou, China, 2013.
- [24] W. Li, Z. Zhang e Z. Liu, «Expandable data-driven graphical modeling of human actions based on salient postures,» *IEEE Trans. Circuits Syst. Video Techn.*, vol. 18, n. 11, p. 1499 – 1510, 2008.
- [25] M. Geetha, C. Manjusha, P. Unnikrishnan e R. Harikrishnan, «A vision based dynamic gesture recognition of Indian Sign Language on Kinect based depth images,» in *International Conference on Emerging Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA)*, Bangalore, India, 2013.
- [26] J. Kissko, December 2011. [Online]. Available: <http://www.kinecteducation.com/blog/2011/11/15/what-is-kinecteducation-all-about/>.
- [27] S. Zhang, W. He, Q. Yu e X. Zheng, «Low-cost interactive whiteboard using the Kinect,» in *International Conference on Image Analysis and Signal Processing (IASP)*, Hangzhou, China, 2012.
- [28] L. Zhang, J.-C. Hsieh, T.-T. Ting, Y.-C. Huang, Y.-C. Ho e L.-K. Ku, «A Kinect based Golf Swing Score and Grade System using GMM and SVM,» in *5th International Congress on Image and Signal Processing (CISP)*, Chongqing, Sichuan, China, 2012.
- [29] H. Haggag, M. Hossny, S. Haggag, S. Nahavandi e D. Creighton, «Safety applications using Kinect technology,» in *IEEE International Conference on Systems, Man and Cybernetics (SMC)*, San Diego, CA, USA, 2014.
- [30] R. Xiao, C. Harrison e S. E. Hudson, «WorldKit: Rapid and Easy Creation of Ad-hoc Interactive Applications on Everyday Surfaces,» in *31st Annual SIGCHI Conference on Human Factors in Computing Systems*, Paris, France, 2013.

- [31] A. C. d. C. Correia, L. C. d. Miranda e H. H. Hornung, «Gesture-Based Interaction in Domestic Environments: State of the Art and HCI Framework Inspired by the Diversity,» *INTERACT 2*, vol. 8118, pp. 300-317, 2013.
- [32] J. Oh, Y. Jung, Y. Cho, C. Hahm, H. Sin e J. Lee, «Hands-up: motion recognition using kinect and a ceiling to improve the convenience of human life,» in *CHI'12 Extended Abstracts on Human Factors in Computing Systems*, Austin, Texas, USA, 2012.
- [33] H.-J. Kim, K.-H. Jeong, S.-K. Kim e T.-D. Han, «Ambient Wall: Smart Wall Display interface which can be controlled by simple gesture for smart home,» in *SIGGRAPH Asia 2011 Sketches*, Hong Kong, 2011.
- [34] G. Panger, «Kinect in the Kitchen: Testing Depth Camera Interactions in Practical Home Environments,» in *CHI '12 Extended Abstracts on Human Factors in Computing Systems*, Austin, Texas, USA, 2012.
- [35] Flightphase, May 2014. [Online]. Available: <http://www.flightphase.com/expanded-media/interactive-wall-at-ud>.
- [36] H. Stindl, June 2011. [Online]. Available: <http://www.horizont.at/home/detail/digital-station-branding-premium-inszenierung.html>.
- [37] Kinect Hacks, December 2011. [Online]. Available: <http://www.kinecthacks.com/kinect-used-in-university-campaign/>.
- [38] C.-K. Hsieh, W.-C. Liao, M.-C. Yu e Y.-P. Hung, «Interacting with the past: Creating a time perception journey experience using kinect-based breath detection and deterioration and recovery simulation technologies,» *Journal on Computing and Cultural Heritage (JOCCH)*, vol. 7, n. 1, 2014.
- [39] C.-S. Wang, D.-J. Chiang e Y.-C. Wei, «Intuitional 3D Museum Navigation System Using Kinect,» in *Information Technology Convergence*, Springer Netherlands, 2013, pp. 587-596.
- [40] J. Triesch e C. v. d. Malsburg, «Robotic gesture recognition,» in *Gesture and Sign Language in Human-Computer Interaction*, Springer Berlin Heidelberg, 1998, pp. 233-244.
- [41] T. Kröger, K. Oslund, T. Jenkins, D. Torczynski, N. Hippenmeyer, R. B. Rusu e O. Khatib, «JediBot – Experiments in Human-Robot Sword-Fighting,» *Springer Tracts in Advanced Robotics*, vol. 88, pp. 155-166, 2012.
- [42] J. Ekelmann e B. Butka, «Kinect Controlled Electro-Mechanical Skeleton,» in *Proceedings of IEEE Southeastcon*, Orlando, FL, USA, 2012.
- [43] Y.-J. Chang, S.-F. Chen e J.-D. Huang, «A Kinect-based system for physical rehabilitation: A pilot study for young adults with motor disabilities,» *Research in Developmental Disabilities*, vol. 32, n. 6, pp. 2566-2570, November–December 2011.
- [44] B. Lange, C.-Y. Chang, E. Suma, B. Newman, A. Rizzo e M. Bolas, «Development and evaluation of low cost game-based balance rehabilitation tool using the microsoft kinect sensor,» in *Annual*

International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC, Boston, MA, USA, 2011.

[45] M. Alvarez e P. Grogan, «Connecting with Kinect® To Improve Motor and Gait Function in Parkinson Disease,» *Neurology*, vol. 78, April 2012.

[46] M. Alnowami, B. Alnwaimi, F. Tahavori, M. Copland e K. Wells, «A quantitative assessment of using the Kinect for Xbox360 for respiratory surface motion tracking,» in *SPIE Medical Imaging*, 2012.

[47] G. C. S. Ruppert, L. O. Reis, P. H. J. Amorim, T. F. d. Moraes e J. V. L. d. Silva, «Touchless gesture user interface for interactive image visualization in urological surgery,» *World Journal of Urology*, vol. 30, n. 5, pp. 687-691, 2012.

[48] A. Malizia e A. Bellucci, «The artificiality of natural user interfaces,» *Communications of ACM*, vol. 55, n. 3, pp. 36-38, Marzo 2012.

Biografia

Vito Gentile è studente di dottorato in Ingegneria dell'Innovazione Tecnologica presso il Dipartimento di Ingegneria Chimica, Gestionale, Informatica, Meccanica (DICGIM) dell'Università degli Studi di Palermo. I temi di ricerca di cui si occupa sono quelli dell'interazione uomo-macchina e dell'ubiquitous computing, con particolare interesse verso l'interazione touchless a gesti con i display pubblici.

Ha studiato Ingegneria Informatica presso l'Università degli Studi di Palermo, dove ha ottenuto la laurea magistrale col massimo dei voti e la lode nel 2013.

Email: vito.gentile@unipa.it

twitter: @ViGentile

Salvatore Sorce è ricercatore presso il Computer-Human Interaction Laboratory (CHILab) del Dipartimento di Ingegneria Chimica, Gestionale, Informatica, Meccanica (DICGIM) dell'Università degli Studi di Palermo. È inoltre co-fondatore e project manager di InformAmuse S.r.l., spin-off accademico dell'Università degli Studi di Palermo. Attualmente si occupa di ubiquitous computing e sistemi pervasivi; interazione uomo-macchina; display pubblici; dispositivi indossabili; programmazione mobile. Salvatore è inoltre senior member di ACM.

Ha studiato Ingegneria Informatica all'Università degli Studi di Palermo, dove si è laureato nel 2001 e dove ha ottenuto il dottorato di ricerca in Ingegneria Informatica nel 2006.

Email: salvatore.sorce@unipa.it.

Twitter: @salvosorce

Alessio Malizia è Senior Lecturer in Human-Computer Interaction presso il Dipartimento di Computer Science della Brunel University London (UK) e membro dell'Istituto di Human-Centred Design. Si è trasferito a Brunel dall'Universidad Carlos III de Madrid (Spagna), dove era Professore Associato in interazione uomo-macchina e social computing. Ha lavorato in precedenza all'Università La Sapienza di Roma, nonché presso IBM, SGI e Xerox PARC, presso il gruppo di Human-Document Interaction. Alessio è inoltre distinguished speaker e senior member di ACM e membro di IEEE.

Email: alessio.malizia@brunel.ac.uk

Twitter: @cikay72

Antonio Gentile è professore associato presso l'INovative Computer Architecture Laboratory (INCA Lab) del Dipartimento di Ingegneria Chimica, Gestionale, Informatica, Meccanica (DICGIM) dell'Università degli Studi di Palermo. Appassionato imprenditore, dal 2009 è anche CEO e fondatore di InformAmuse S.r.l., spin-off accademico dell'Università degli Studi di Palermo, nonché presidente e fondatore di Jujo Inc, una startup americana fondata nel 2013. Il prof. Gentile ha conseguito il titolo di Ph.D. in ingegneria elettrica ed informatica presso il Georgia Institute of Technology, Atlanta (USA) nel 2000. Attualmente si occupa di sistemi portabili di elaborazione ad alto rendimento, architetture per l'elaborazione di immagini e video, sistemi ed architetture embedded, riconoscimento del parlato, interfacce uomo-macchina e mobile computing. È inoltre associate editor di *Integration* e dell'*International Journal of Grid and Utility Computing*. Antonio è inoltre senior member di IEEE ed ACM, nonché membro di AEIT.

Email: antonio.gentile@unipa.it

Twitter: @tonneiro

Approfondimento 1: I dispositivi Kinect-like

I dispositivi *Kinect-like* sono costituiti da un insieme di sensori a basso costo, e possono essere riassunti dalle seguenti caratteristiche:

- consentono di acquisire una rappresentazione in 3D della scena ripresa in tempo reale (figura 1a);
- consentono di acquisire una rappresentazione RGB della scena ripresa in tempo reale (figura 1b);
- sono poco costosi (dell'ordine di poche centinaia di euro).

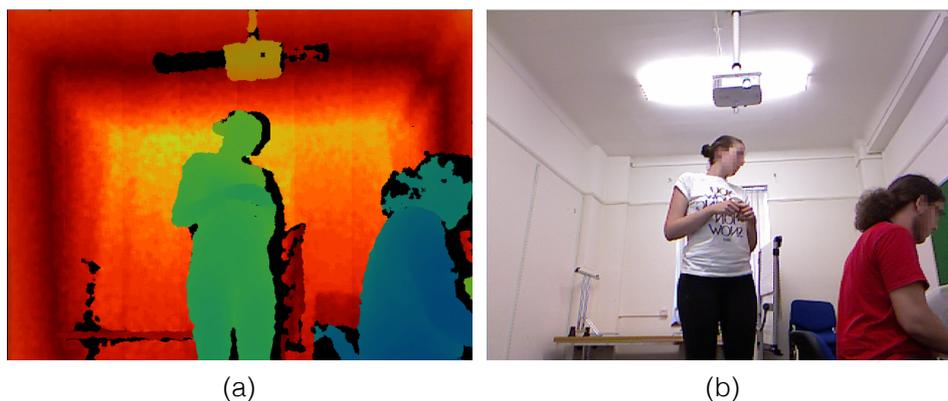


Figura 1.

Un tipico esempio dei dati RGB-D ottenibili tramite un dispositivo Kinect-like

Nella maggior parte dei dispositivi *Kinect-like* disponibili in commercio, la rappresentazione 3D della scena viene realizzata usando un sistema di raggi infrarossi (IR), costituito da un emettitore e da un sensore. L'emettitore proietta nell'ambiente esaminato un pattern ben definito di spot luminosi la cui disposizione è nota. La ricostruzione avviene confrontando la distribuzione dei punti proiettati sulla scena attuale con il pattern di riferimento così come dovrebbe essere visto dal sensore se esso fosse proiettato su una superficie posta ad una distanza ben definita e perfettamente parallela al piano della coppia emettitore-sensore. Come esempio, si può pensare al pattern di riferimento come ad una coperta a pois distesa su un piano e posta ad una distanza ben definita (figura 2a). Se un oggetto entra a contatto con la coperta (figura 2b), questa verrà deformata (figura 2c), e di conseguenza si potrà dedurre la disposizione spaziale dell'oggetto sulla base della nuova disposizione dei pois della coperta.

Un'alternativa al metodo appena descritto, che in genere è più costosa ma che Microsoft ha reso disponibile a basso costo con l'introduzione della versione 2 di Kinect, è il calcolo della profondità misurando il tempo di volo dei raggi infrarossi inviati dall'emettitore. Ciò consente, in genere, di ottenere dati di profondità più accurati.

I dispositivi *Kinect-like* attualmente disponibili sul mercato sono molti. Alcuni produttori hanno rilasciato diverse versioni di uno stesso dispositivo, talvolta anche abbastanza diverse l'una dall'altra in termini di funzionalità, SDK e hardware. Di seguito vedremo un confronto tra alcuni di questi dispositivi.



(a)

(b)

(c)

Figura 2.

Inserendo un oggetto (a) dietro una coperta a pois (b), la disposizione dei pois verrà deformata (c), e tale deformazione può consentire di risalire alla forma dell'oggetto. In maniera analoga, il pattern di raggi infrarossi proiettato e deformato dagli oggetti della scena consente di risalire alle informazioni di profondità.

Microsoft Kinect

Prodotto originariamente destinato all'ambito ludico (insieme alla console Xbox 360), Microsoft Kinect fu messo in vendita nel Novembre 2010, mentre nel 2012 è stata rilasciata un versione leggermente perfezionata, ma destinata ad un utilizzo su Windows. Oggi fuori produzione, si può trovare ancora in vendita a prezzi che variano tra i 20 ed i 200 €.



Figura 3.

Microsoft Kinect, nella versione per Xbox360.

Depth camera					RGB Camera			Altri sensori	microfono	inclinazione variabile
risoluzione	profondità	frame rate	campo visivo	tecnologia	Risoluzione	Frame rate	Campo visivo			
320x240	Default: 0.8 - 4 m Near mode: 0.4 - 3 m	30 fps	58.5° x 45.6°	PrimeSense PS1080-A2	1280x960	30 fps	62.0° x 48.6°	Accelerometro a tre assi	Array di microfoni (stereo mic)	Sì, motorizzata. Campo visivo ± 27°

Tabella 1.
Specifiche tecniche di Microsoft Kinect.

Nel 2014 è stata rilasciata una seconda versione di Microsoft Kinect, compatibile sia con la console Xbox One che (tramite un apposito adattatore) utilizzabile su PC con Microsoft Windows 8. La nuova versione utilizza una depth camera basata sul calcolo del tempo di volo, e risulta molto più precisa della versione precedente. La versione per Xbox One, a Febbraio 2016, è in vendita a circa 150 €, cui va aggiunto il costo dell'adattatore che consente di collegare questo dispositivo alla porta USB di un PC



Figura 4.
Kinect per Xbox One

Depth camera					RGB Camera			Altri sensori	microfono	inclinazione variabile
risoluzione	profondità	frame rate	campo visivo	tecnologia	Risoluzione	Frame rate	Campo visivo			
512x424	0.4 - 4.5 m	30 fps	70.6° x 60.0°	Microsoft X871141-001	1920x1080	30 fps	84.1° x 53.8°	Accelerometro a tre assi	Array di microfoni (stereo mic)	Non presente

Tabella 2.
Specifiche tecniche di Microsoft Kinect v2.

Asus Xtion PRO Live

Un altro dispositivo che ha trovato numerose applicazioni nella ricerca è stato prodotto da Asus, in collaborazione con PrimeSense. Rilasciato nel 2012, Asus Xtion PRO Live è in vendita (a Maggio 2015) per circa 170 €. Asus Xtion PRO Live è stato ispirato da un altro dispositivo, prodotto inizialmente da PrimeSense stessa, chiamato *Carmin*.



Figura 5.
Asus Xtion PRO Live

Depth camera					RGB Camera			Altri sensori	microfono	inclinazione variabile
risoluzione	profondità	frame rate	campo visivo	tecnologia	Risoluzione	Frame rate	Campo visivo			
320x240	0.8 – 3.5 m	30 fps	58° x 45°	PrimeSense PS1080-A2	1280x1024	30 fps	58° x 45°	N.D.	N.D.	Sì, manuale

Tabella 3.
Specifiche tecniche di Asus Xtion.

Altri dispositivi simili

Oltre ai dispositivi *Kinect-like* appena citati, vi sono altre soluzioni degne di nota ma meno diffuse delle precedenti.

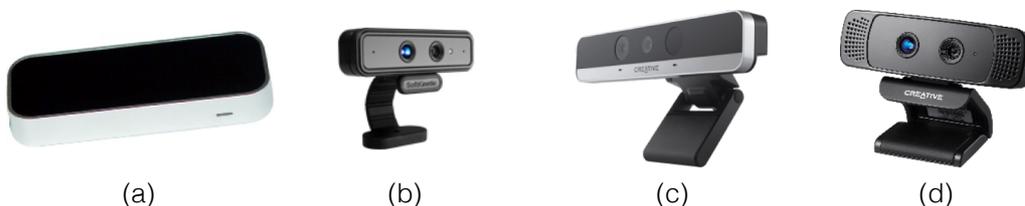


Figura 6.
Leap Motion Controller (a), SoftKinetic DS325 (b), Intel RealSense 3D camera (c), Creative Senz3D(d).

Il *Leap Motion Controller* (LMC), sviluppato dalla Leap Motion Inc. (figura 6a), ha avuto una discreta fortuna nell'ambito della ricerca. Lo scopo principale di questo dispositivo è il riconoscimento e tracciamento di mani e dita, con un grado di precisione di circa 2 mm. Il LMC è in grado di funzionare a 200 fps, e di riconoscere un range di profondità che varia tra 25.4 mm e 1.2 m, sfruttando due camere a infrarossi e tre LED. LMC viene generalmente utilizzato in modo diverso dai dispositivi fin qui descritti, in quanto viene poggiato su un piano orizzontale ed il suo campo visivo si estende verticalmente. Sebbene questo dispositivo abbia molte analogie con le tecnologie descritte fin qui, esso non rientra nella categoria dei dispositivi *Kinect-like* in quanto non include una

camera RGB. Esso è comunque disponibile a basso costo (il prezzo di lancio, nel 2013, era di circa 80 dollari USA).

Un'alternativa ai dispositivi *Kinect-like* più diffusi è stata prodotta dalla compagnia belga *SoftKinetic*, al fine di offrire una tecnologia di visione 3D per i PC, l'elettronica portatile, le auto e le macchine in genere. Tale compagnia produce un sensore di profondità a tempo di volo, basato su una tecnologia brevettata. Questo tipo di sensore è utilizzato in due dispositivi prodotti da *SoftKinetic*, ovvero *DepthSense 325* (DS325 – figura 6b) e *DepthSense 311* (DS311), che includono quindi anche una camera RGB e sono disponibili a prezzi relativamente accessibili (il costo di DS311 è di 299 dollari USA; DS325 può essere invece acquistato per 250 dollari USA). *SoftKinetic* fornisce anche un SDK compatibile con Windows e Visual Basic, ma anche questo tipo di prodotti non hanno avuto il successo di Microsoft Kinect o Asus Xtion, probabilmente per via del minore potere di marketing di *SoftKinetic*.

Anche Intel ha recentemente iniziato a sviluppare una tecnologia che consente l'interazione a gesti basata sui dati di profondità della scena, chiamata *RealSense*. Tale tecnologia è stata integrata in molti prodotti commerciali, tra cui i dispositivi *Intel RealSense 3D Camera* (figura 6c) e *Creative Sens3D* (figura 6d). Quest'ultimo include una camera RGB con risoluzione di 1280x768 ed un sensore di profondità in grado di funzionare a 30 fps, con un campo visivo di 74° ed un range di profondità tra i 15.24 ed i 99.05 centimetri. Dal momento che si tratta di una tecnologia relativamente giovane, Intel *RealSense* non è stata molto applicata nella ricerca, soprattutto se paragonata con Asus Xtion o Microsoft Kinect.

Approfondimento 2: Skeletal tracking

Una delle funzionalità più utilizzate quando si ha a che fare con i dispositivi *Kinect-like*, è la possibilità di ottenere una serie di giunti scheletrici a partire dall'immagine di profondità di un utente. Ciò è reso possibile tramite una classe di algoritmi nota con il nome di *skeletal tracking*. In particolare, uno dei più noti algoritmi di questo tipo (ed integrato in Microsoft Kinect SDK) è stato sviluppato da Microsoft Research.

L'algoritmo in esame è conosciuto come *pose recognition in parts* (riconoscimento della postura in parti), nome dovuto al modo in cui i giunti scheletrici vengono ottenuti. A partire da una singola immagine di profondità, infatti, la sagoma del corpo umano (ricavata dall'immagine di profondità) è suddivisa in sezioni, ciascuna rappresentante diverse parti del corpo (mani, testa, braccia, gambe, ecc.).

Dopo aver provveduto ad eliminare qualsiasi elemento di sfondo, estraendo la fisionomia dell'utente, viene operata un'etichettatura probabilistica sull'immagine, che assegna ad ogni punto del corpo dell'utente le probabilità che tale punto appartenga ad ogni porzione del corpo. In tal modo, verranno generate tante distribuzioni di probabilità quante sono le parti del corpo prese in esame. A questo punto, i giunti scheletrici altro non sono che le mode statistiche di ciascuna distribuzione di probabilità (figura 1).



Figura 1.

Processo di etichettatura dell'immagine di profondità, seguito dall'ottenimento dei giunti scheletrici del corpo umano ripreso.

L'etichettatura probabilistica di cui sopra viene effettuata tramite un processo di classificazione, che utilizza a sua volta un algoritmo basato sull'addestramento di alberi decisionali. Senza scendere nei dettagli, si precisa che tale algoritmo ha richiesto una fase di addestramento, in cui l'insieme di dati utilizzati per l'apprendimento è stato generato artificialmente con alcuni modelli 3D. Da tali modelli, infatti, può essere ricavata sia un'immagine di profondità (input), sia la corrispondente etichettatura probabilistica (output atteso), in situazioni tipiche e particolarmente significative per garantire un apprendimento quanto più

soddisfacente. In particolare, Microsoft ha ricavato un database di 500.000 immagini, dalle quali è stato ottenuto un insieme di addestramento composto da 10.000 posture.

Una volta ottenuta l'etichettatura (che può essere pensata come una *texture* da applicare ai modelli 3D, in cui ogni colore identifica una parte del corpo), si ricavano i singoli punti che rappresentano i giunti scheletrici. Essi vengono calcolati tramite un algoritmo di ricerca della moda di ciascuna distribuzione di probabilità (ognuna corrispondente ad una parte del corpo).

I ricercatori Microsoft che si sono occupati dello sviluppo dell'intero algoritmo di *skeletal tracking*, affermano che un'implementazione ottimizzata di questo algoritmo permette l'analisi di un'immagine e l'estrazione dei giunti scheletrici in circa 5 ms (utilizzando la GPU integrata in Xbox 360), sufficiente a garantire un funzionamento in tempo reale.

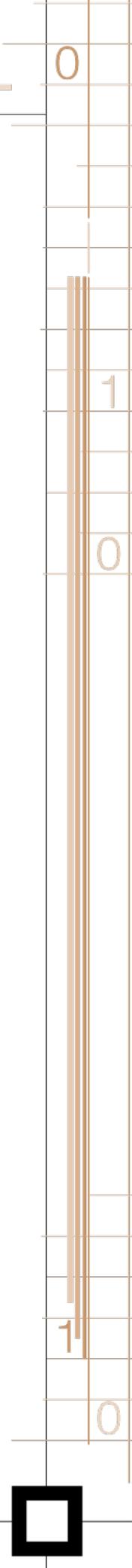
0

1

0

1

0



L'uomo artificiale e il perturbante

Giuseppe O. Longo

Sommario

Nel 1970 Masahiro Mori avanzò un'interessante ipotesi sulla reazione emotiva degli esseri umani di fronte a un robot. Secondo Mori, via via che la somiglianza del robot con l'uomo cresce, esso ci appare sempre più familiare, ma a un certo livello di perfezione il suo aspetto diviene perturbante. Nell'articolo si rintracciano le origini letterarie e storiche del perturbante. Si riportano due studi psicologici su questo tema e si indica il legame che esso presenta con la roboetica. Infine si accenna ad alcune forme contemporanee di perturbante.

Abstract

In 1970 Masahiro Mori suggested an interesting hypothesis about the emotional reaction of human beings when facing a robot. According to Mori, as the similarity of the robot with man increases, it appears to us more and more familiar, but beyond a certain level of resemblance its appearance becomes uncanny. In the article the literary and historical origins of the uncanny are traced. Two psychological studies on this subject are described and its connections with roboethics are hinted at. Finally, some contemporary forms of the uncanny are indicated.

Keywords: Uncanny, uncanny valley, robot, automaton, animism, psychology

1. Introduzione

Per manifestarsi, il perturbante non aspetta certo i robot: già in passato le figure ospitate nei musei delle cere e gli automi, letterari e reali, offrono esempi di artefatti capaci di suscitare un'impressione, a volte sinistra, di disagio. Ed è un disagio che, più o meno evidente, percorre tutto il filone delle ricerche e delle attuazioni dell'intelligenza artificiale, che si colloca nel solco di una millenaria ambizione dell'uomo: quella di imitare l'atto divino della creazione. Più o meno dichiarata, quest'ambizione risale all'antichità biblica e classica, e la leggenda del Golem ne è forse l'esempio mitologico e letterario più noto. In quest'impresa



s'intrecciano la vertigine della creazione e il timore della creatura, che talora minaccia di soverchiare e distruggere l'inesperto demiurgo. Il controllo del Golem passa attraverso la parola: per dargli vita gli si scrive in fronte *emet* (verità), ma basta cancellare la prima lettera perché *emet* divenga *met* (morte) e il Golem cessi di vivere. Anche nel caso del mostro di Frankenstein la creatura trascende il progetto e si ribella, suscitando negli uomini angoscia e terrore. Talvolta gli esseri umani subiscono invece il fascino degli esseri artificiali, come nei racconti di Hoffmann, su cui torneremo

Passando dal mito e dalla letteratura al versante costruttivo, i tentativi di fabbricare l'uomo artificiale sono altrettanto se non più numerosi, anche se i risultati, per la pesantezza della materia e per le difficoltà di lavorazione, assumono forme più modeste rispetto ai prodotti della fantasia, ma forse più ammirevoli per la loro concretezza: nascono così gli automi. Questi prodotti dell'ingegno umano oggi non si costruiscono più e si trovano solo nei musei e nei teatri della nostalgia. Eppure gli automi continuano a popolare di inquiete proiezioni e torbidi sogni la dimensione immaginaria del nostro tempo e da qui travalicano nelle creazioni artistiche e nelle attuazioni tecniche. Anche se forme e strumenti sono mutati, esiste tuttora un campo di ricerca contrassegnato dalla dubitosa e mutevole linea di separazione tra ciò che l'uomo può attuare e ciò che può solo sognare. In questo senso gli automi incarnano da sempre - anche nelle nuove vesti informatiche, protesiche e robotiche - l'aspirazione dell'uomo a superare i limiti della propria contingenza e colorano di perturbante la storia della tecnica, fino a travasarsi nei loro eredi, i *robot umanoidi* [1,2,3].

2. Masahiro Mori e l'avvallamento del perturbante

Il perturbante appartiene alla sfera dello spaventoso, di ciò che genera angoscia e orrore, e questo termine non viene sempre usato in un senso nettamente definibile, tanto che quasi sempre coincide con ciò che è genericamente angoscioso.
Sigmund Freud

Nel 1970 lo studioso giapponese di robotica Masahiro Mori, allora quarantatreenne, pubblicò un articolo dal titolo *Bukimi No Tani (L'avvallamento del perturbante)*, in cui avanzava un'interessante ipotesi sulla reazione emotiva degli esseri umani di fronte ad artefatti aventi un grado maggiore o minore di somiglianza con l'uomo [4]. Un pezzo di legno non suscita reazioni emotive particolari, ma se lo si scolpisce dandogli una forma antropomorfa, la cosa è diversa, come insegna la fiaba di Pinocchio. Mori era interessato soprattutto alla nostra reazione di fronte ai robot al crescere del loro grado di similarità con noi. In prima approssimazione, si può ritenere che al crescere della somiglianza cresca anche il senso di familiarità e di simpatia e cresca la nostra inclinazione a concedere al robot un certo grado di parentela con noi, insomma di "umanità". Questo è vero, ma fino a un certo punto: secondo Mori, quando la somiglianza supera un certo livello, l'aspetto e i movimenti del robot lo rendono sinistro e inquietante. Si ha la sensazione di avere a che fare non con un robot che somiglia a un uomo, ma con un uomo non del tutto umano. Se ne scorgono le discrepanze rispetto all'essere umano e certi difetti, anche minimi, che prima

non si notavano o si accettavano senza problemi: il nostro atteggiamento positivo subisce un brusco calo e si rovescia in una reazione negativa. L'artefatto, che prima era chiaramente tale e al quale per simpatia eravamo disposti a concedere un certo grado di umanità, ci appare ora come una evidente imitazione, non del tutto riuscita, e ciò provoca un sentimento di repulsione, appunto di perturbante, perché ci pone in uno stato di incertezza riguardo alla sua natura.

Se si rappresenta il fenomeno su un piano cartesiano con un grafico che abbia in ascissa la somiglianza delle entità considerate con l'uomo (da 0% a 100%) e in ordinata la sensazione positiva di familiarità o empatia, secondo Mori si ottengono le curve della Fig. 1.

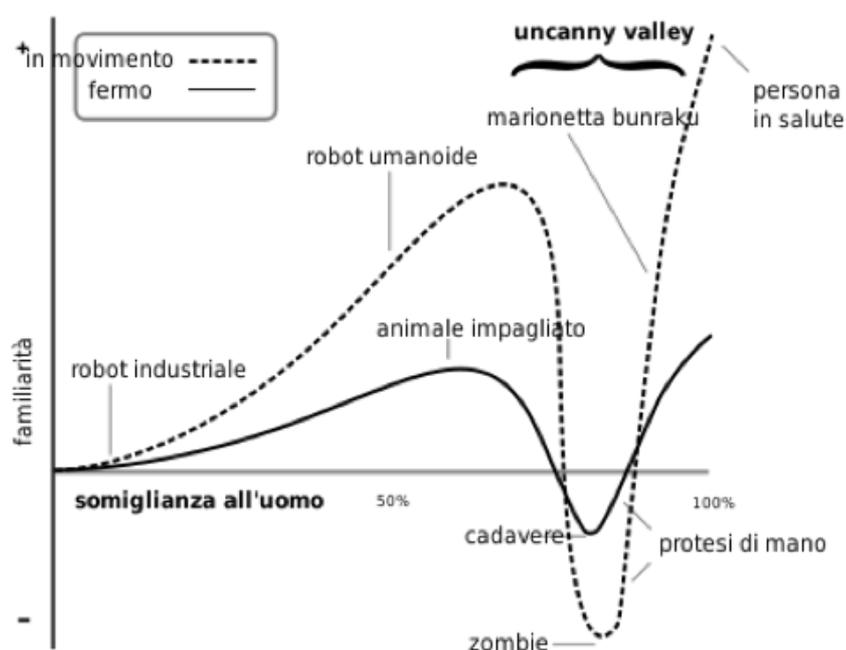


Figura 1

Il grafico dell'avvallamento del perturbante di Masahiro Mori (1970)

La linea tratteggiata si riferisce a robot umanoidi dotati di movimento: la nostra simpatia cresce fino al 70% circa di somiglianza per poi subire un brusco abbassamento, corrispondente allo spaesamento provato dall'osservatore umano. Il valore minimo si ha in corrispondenza di uno *zombie*, la cui somiglianza con gli umani è grandissima ma non completa¹. Tuttavia al crescere

¹ *Zombie* è un termine di origine haitiana e prima ancora bantu, legato ai riti vudù, che indica un morto vivente. Per i filosofi lo *zombie* è un essere che ha tutta l'apparenza e il comportamento di un umano, ma è privo di mente, di coscienza e di emozioni. Il Golem della leggenda ebraica si può considerare uno zombie. La cinematografia si è impadronita degli zombie, presentandoci come creature dementi, animate da una violenza fine a sé stessa e dedite al cannibalismo.

ulteriore della somiglianza la curva risale, per esempio quando ci si confronta con arti artificiali o con marionette, come nel caso dei burattini giapponesi *bunraku*², e raggiunge il massimo quando gli osservatori si trovano di fronte a esseri umani veri. La cunetta presentata dalla curva fu chiamata da Mori "avvallamento del perturbante" (in inglese *uncanny valley*). Un andamento analogo, ma meno spiccato, si osserva nel caso di oggetti privi di movimento, come animali impagliati o bambole: in questo caso l'avvallamento del perturbante raggiunge il minimo quando ci si trova davanti a un cadavere, cioè a un corpo umano inanimato (Fig. 1).

È interessante notare che nel 1970 non esistevano robot umanoidi, anzi la ricerca sui robot umanoidi non era presa sul serio neppure nell'accademia, che li considerava giocattoli. Quella di Mori fu dunque un'intuizione presaga, che affondava le radici nel fascino orrorifico che sullo studioso avevano esercitato da bambino le figure di cera e, in seguito, anche le mani artificiali elettroniche. Mori stesso ammette che a quel tempo non immaginava che la sua idea sarebbe stata oggetto di interesse crescente: secondo lui l'esistenza dell'avvallamento doveva essere una sorta di monito a non costruire artefatti troppo simili all'uomo nell'aspetto e nei movimenti³. Fu solo nel 2005, grazie a un convegno sui robot umanoidi organizzato dall'IEEE a Tsukuba, in Giappone, che l'idea di Mori cominciò a circolare in ambito internazionale [5]. Oggi, studiando le onde cerebrali, i neurologi hanno dimostrato sperimentalmente l'esistenza dell'avvallamento, anche se non è chiarissimo perché esista, cioè perché a un certo punto il soggetto avverta la sensazione di perturbante⁴.

È forse possibile spiegare questo effetto come il risultato di due spinte opposte: da una parte l'osservatore è incline a simpatizzare con l'oggetto che ha di fronte (per esempio un robot umanoide semovente, *androide* o *gineide*) e ad attribuirgli alcune caratteristiche umane che il robot non possiede; dall'altra ha la consapevolezza che si tratta pur sempre di un artefatto e non di un essere umano. Se la somiglianza non è eccessiva, la concessione dell'umanità, accompagnata dalla simpatia e da un certo qual divertito stupore, non presenta problemi. Ma oltre una certa soglia la consapevolezza che si tratta di un artefatto si attenua, mentre il processo di umanizzazione continua a crescere e diventa così intenso che la presenza degli inevitabili difetti diventa insostenibile: non più un robot che somiglia a un umano, ma un umano difettoso: quindi ci si trova in una situazione perturbante. In altre parole ci si trova nel *dubbio* se

² Il *Bunraku* è un tipo di teatro giapponese, i cui personaggi sono rappresentati da burattini di grandi dimensioni, manovrati a vista ciascuno da tre uomini. È stato dichiarato patrimonio dell'umanità.

³ Forse perché una somiglianza eccessiva minaccia la nostra identità? In realtà alcuni robot hanno più o meno superato l'avvallamento, per esempio la replicante giapponese Q2, costruita dalla Kokoro Company, o la gineide a grandezza naturale HRP-4C, costruita dall'Istituto Nazionale Giapponese per la Scienza e la Tecnologia (per questi e altri esempi si veda la sezione 10).

⁴ Si veda Ayse Pinar Saygin et al. (2012). "The thing that should not be: predictive coding and the uncanny valley in perceiving human and humanoid robot actions", *Social Cognitive and Affective Neuroscience*, 7 (4), pp. 413-422.

l'oggetto sia o no umano. Soltanto quando la somiglianza cresce ancora e i difetti scompaiono si ha un'accettazione imperturbata.

3. I racconti di Hoffmann

Come accade spesso, anche nel caso del perturbante e delle sue radici psicologiche gli scrittori e i registi hanno fornito e forniscono un abbondante materiale di indagine per gli scienziati, in particolare per gli psicologi. A proposito dell'inconscio, Italo Calvino, riferendosi ai racconti di quel singolare personaggio che fu E. T. A. Hoffmann, scrisse: «La scoperta dell'inconscio avviene qui, nella letteratura romantica fantastica, quasi cent'anni prima che ne venga data una definizione teorica» [6].

Ernesto Teodoro Amedeo Hoffmann (1776-1822) nacque a Königsberg, nella Prussia orientale. Ereditò dal padre giurista una forte attitudine artistica e dalla madre, ipersensibile e soggetta a depressioni, un carattere incline al fantastico e al visionario. Dopo la separazione dei genitori, Hoffmann visse con la soffocante famiglia materna. Conseguita la laurea in legge, seguì una carriera di funzionario in Germania e a Varsavia. Irrequieto e sognatore, fervido lettore, s'interessò di disegno e di medicina, e, in modo professionale, di musica. Nel 1809 pubblicò il suo primo racconto fantastico (*Il cavalier Gluck*), cui ne seguirono molti altri, che presero le mosse dai traumi psichici della sua infanzia (*Racconti fantastici alla maniera di Callot*) e dal suo interesse per l'occultismo e l'ipnotismo (*Gli elisir del diavolo*). Sempre sull'orlo dello squilibrio, in lui si dissolveva la distinzione tra sogno e realtà: tipico in questo senso *L'uomo della sabbia*, che fa parte dei *Racconti notturni* del 1816. Perseguitato dal timore di diventare pazzo, Hoffmann approfondì l'argomento della follia studiando i ricoverati nel manicomio di Bamberg e le persone che incontrava grazie al suo lavoro di consigliere giudiziario a Berlino. Qui ci interessa in particolare la presenza, nei racconti di Hoffmann, di automi talmente simili agli umani da trarre in inganno gli osservatori più acuti.

Nell'*Uomo della sabbia* (Fig. 2), Nataniele s'innamora perdutamente di Olimpia, una bambola meccanica di cui non riesce a scorgere la vera natura, nonostante le tante prove che agli occhi degli altri sono evidenti. Quando scopre la verità, si ammala e poi, in una crisi di follia, si precipita da una torre [7]. Un altro racconto, emblematico fin dal titolo, è *L'automa* (che appartiene alla raccolta *I fedeli di san Serapione*, 1819-21), epitome di quella meccanica misteriosa e allucinata tanto cara allo scrittore tedesco. L'automa si presenta nell'aspetto e nelle vesti esotiche di un Turco ed è in grado di fornire risposte a chi l'interroga sussurrandogli la domanda nell'orecchio destro. A volte, alzando il braccio, l'automa minaccia l'interrogante o si rifiuta di rispondere. In ogni caso, dopo un certo numero di risposte il mago che lo manovra «infilava la chiave nel fianco sinistro della figura, caricando con gran fracasso una macchina ad orologeria» [8].

**Figura 2**

Un'illustrazione per il racconto L'uomo della sabbia di Hoffmann

4. Automi perturbanti: i Turchi

Passando dal versante letterario a quello costruttivo, ci si imbatte nella figura del Turco, che concentra in sé sortilegi, magie e meraviglie tipiche dell'Oriente. Il Turco è piuttosto popolare nel mondo degli automi: basti ricordare le macchine teatrali del mago, ciarlatano, prestigiatore, fisico e matematico toscano Joseph Pinetti (1750-1800), il cui pezzo forte era il Piccolo Turco sapiente o Gran Sultano, capace di indovinare una carta scelta da uno spettatore e di varie altre prestazioni. Ma il Turco più famoso è l'automa scacchista costruito nel 1769 dal barone e ingegnere ungherese Wolfgang von Kempelen, che lo esibì in Russia, a Parigi e a Londra, suscitando stupore ed entusiasmo (Fig. 3).

Nel 1783 il Turco giocò contro Benjamin Franklin e nel 1809 contro Napoleone, battendoli entrambi. Acquistato dopo la morte del barone da Johann Maelzel, continuò la sua tournée in tutta Europa e, nel 1825, sbarcò negli Stati Uniti. Il Turco stava seduto dietro una specie di canterano che lo nascondeva dalla vita in giù. Prima dell'esibizione, Maelzel apriva e chiudeva in successione gli sportelli anteriori e posteriori del canterano per dissipare il dubbio che vi si celasse una persona [2]. Il celebre scrittore Edgar Allan Poe, dopo aver assistito ad alcune esibizioni del Turco, analizzò il susseguirsi delle aperture e chiusure delle ante, e nell'aprile 1836 pubblicò un lungo articolo in cui concludeva che di fatto nel canterano doveva celarsi uno scacchista provetto (Fig. 4).

Naturalmente, viste le dimensioni del canterano, lo scacchista poteva solo essere un nano e così era davvero: è il primo esempio di... nanotecnologia che la storia ricordi [2,9].



Figura 3

Il Turco scacchista di von Kempelen

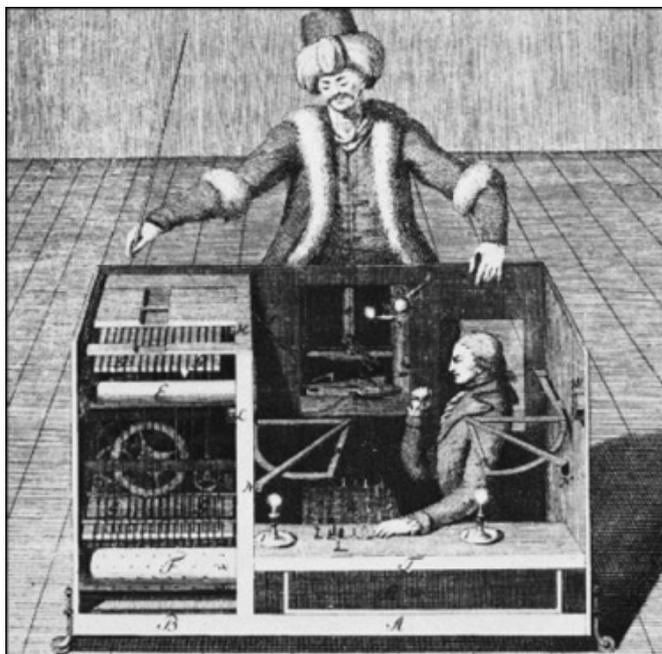


Figura 4

L'interno del Turco di von Kempelen con il nano scacchista

5. I problemi etici

In questo territorio della creazione imitata, o creazione del second'ordine, ci si muove dunque tra diversità palese, suscitatrice di stupore o di orrore, e inquietante somiglianza, generatrice di equivoci e di non facili problemi etici, che ci richiamano alla responsabilità del creatore: di fronte alla complessità della creatura, presupposto della sua somiglianza (quasi) perfetta al modello, ci si può infatti interrogare sui suoi possibili sentimenti, sulle sue frustrazioni e sulle sue reazioni. La psicologia degli automi, degli androidi e dei ciborg è uno dei temi più interessanti della moderna fantascienza e forse uno dei problemi più complessi di un futuro già a portata di mano. Perché suscitare dal nulla creature tanto simili a noi da essere capaci di soffrire? La loro sofferenza, che nasce spesso dalla coscienza di non essere del tutto assimilabili agli uomini, sarebbe un triste corollario della nostra abilità creatrice [2].

6. L'avvento del computer

È evidente che l'abilità creatrice dell'uomo raggiunge i suoi vertici nella letteratura, poiché le tecniche costruttive immaginarie (che non è necessario attuare) sono ben superiori a quelle dei più abili meccanici. I prodotti reali, gli automi, pur nella loro stupefacente precisione, restavano sempre lontanissimi dal modello, cui li avvicinava, più o meno, soltanto la forma esteriore ma non una puntuale somiglianza strutturale e funzionale. Le cose cambiarono radicalmente quando si venne palesando e materiando una corrente di pensiero e di ricerca legata all'informazione, che per secoli era stata quasi del tutto celata dalle più clamorose conquiste della materia e dell'energia. Del mondo dell'informazione, che è dotato di leggi piuttosto diverse da quelle della fisica, si cominciò ad avere piena consapevolezza soprattutto grazie alle ricerche stimolate dalla seconda guerra mondiale nel campo dei calcolatori e delle telecomunicazioni. Si vide che energia e informazione, pur non essendo riconducibili l'una all'altra, interagiscono in modi vari e talora sorprendenti [10]. Si capì che il calcolatore, lungi dall'essere una semplice macchina per far di conto, possedeva capacità enormi e tutte da esplorare proprio nell'ambito del mondo dell'informazione e della mente. Intorno al 1956 nasceva una nuova disciplina, cui fu dato il nome, un po' infelice per la verità, e fonte di equivoci durevoli, di intelligenza artificiale e il calcolatore divenne il modello di elezione della mente umana. Non di tutto l'uomo, si badi, ma di quella che era considerata e ancora è considerata, la parte più nobile e caratteristica degli umani: l'intelligenza. Così, a meno di futili nostalgie corporali, si era convinti di aver raggiunto il traguardo: la costruzione dell'uomo artificiale. Sui conseguimenti e sulle limitazioni di questa prima intelligenza artificiale esiste una bibliografia sterminata, e quindi non mi ci soffermo.

7. Le cose acquistano vita

Da sempre l'uomo tende a dotare di vita cose inanimate e di umanità entità non umane. Così la mitologia greca era gremita di ninfe, creature immaginarie associate a luoghi particolari di cui erano la trasfigurazione: dalle oreadi alle driadi, dalle naiadi alle esperidi e via enumerando. Questo atteggiamento, che

possiamo chiamare *animismo*, non è sparito del tutto con l'avanzata della civiltà e il progressivo affermarsi della razionalità, forse perché si tratta di un'esigenza profonda dell'essere umano. Anche oggi siamo inclini a largheggiare: basta che un ente presenti qualche caratteristica (che ci ricordi qualche caratteristica) umana, ecco che siamo portati ad attribuirgli altri tratti umani, al limite tutti, quindi ad concedergli l'umanità. Tra le caratteristiche che più ci spingono a questa attribuzione sono in primo luogo l'aspetto, poi la capacità di comunicare e di esprimere sentimenti ed emozioni, per esempio il piacere e il dolore. Per quanto riguarda l'aspetto, basti pensare alla forza di suggestione che esercita su un bambino un giocattolo antropomorfo come una semplice bambola di pezza, con la quale egli intesse un dialogo come con un compagno di giochi. Per quanto riguarda le capacità comunicative, si pensi alla suggestione esercitata sugli adulti da certi programmi anche molto elementari (come *Eliza* di Weizenbaum)⁵, che ci inducono ad esprimerci e a confidarci, da cui si accettano consigli e ammonimenti e in cui si crede di percepire un profondo interesse per la nostra persona [11].

È interessante a questo proposito un esperimento condotto dal sociologo americano Clifford Nass: tramite terminale, due computer con caratteristiche comunicative diverse ponevano domande di carattere personale a due gruppi di soggetti. Il primo computer andava subito al sodo, mentre il secondo agiva con più delicatezza, ponendo la stessa domanda dopo qualche preliminare. I soggetti interrogati dalla prima macchina erano molto più riluttanti a fornire le risposte di quelli interrogati dalla seconda macchina, alla quale i soggetti erano propensi ad attribuire caratteristiche comunicative 'umane'⁶. Altri esperimenti di Nass hanno confermato questa tendenza ad attribuire proprietà umane alle macchine in base non al loro aspetto bensì alle loro capacità linguistiche⁷. Per quanto riguarda invece l'aspetto, è interessante un esperimento condotto da

⁵ Il programma *Eliza*, allestito nel 1964 da Joseph Weizenbaum (allora ricercatore del MIT), consente alle persone di conversare in linguaggio naturale con un computer. Il dialogo avviene tramite telescrivente: l'utente batte una frase e passa la parola a *Eliza*, che analizza la frase e risponde battendo una frase. In *Eliza* non c'è nessun barlume d'intelligenza: il programma va semplicemente in cerca di parole chiave come "madre" o "depresso" e poi pesca una domanda appropriata da un repertorio; se questa tattica non funziona, produce una frase generica tentando di riavviare la conversazione. Il programma dà all'interlocutore l'impressione di essere uno psicoterapeuta comprensivo benché piuttosto inerte: pone domande vaghe, parla poco e per un po' risulta piuttosto convincente. In realtà quello che sembra un dialogo è un monologo dell'interlocutore umano, il quale dà senso a domande e risposte solo sue, comportandosi da animista. *Eliza* ebbe un enorme successo: chi conversava con "lei" spesso provava sollievo dopo le sedute. Weizenbaum, tuttavia, molto turbato da questo successo, ritirò il programma e decise di schierarsi contro l'intelligenza artificiale, che riteneva pericolosa per gli umani.

⁶ Si veda Fogg H.J., Nass C. (1997). "Silicon sycophants: the effects of computers that flatter", *International Journal of Human-Computer Studies*, 46 (5): 551-561.

⁷ Si veda Nass C. et al. (1994). "Machines, social attributions, and ethopoeia: performance assessments of computers subsequent to «self-» or «other-» evaluations", *International Journal of Human-Computer Studies*, 40 (3): 543-559. Nass C. et al. (1995). "Can computer personalities be human personalities?", *International Journal of Human-Computer Studies*, 43 (2): 223-239.

Sören Krach e colleghi ad Aachen, in Germania. I soggetti erano invitati a giocare contro entità diverse che di volta in volta vedevano di fronte a sé: un computer, un robot dinamico non antropomorfo, un robot antropomorfo, un essere umano. Quello che i soggetti non sapevano era che tutti gli avversari, qualunque fosse il loro aspetto, erano guidati dallo stesso programma di intelligenza artificiale. L'impegno dei soggetti e il loro piacere nel partecipare al gioco era massimo quando giocavano contro un essere umano, mentre il piacere diminuiva via via che l'aspetto dell'avversario si allontanava dall'umano: giocare contro il computer era piuttosto noioso⁸. Quando è evidente che abbiamo di fronte un manufatto, la nostra disposizione ad attribuirgli proprietà umane è molto bassa, mentre quanto più l'aspetto dell'oggetto è simile al nostro tanto più siamo disposti a concedergli l'umanità e di conseguenza tanto più volentieri ci impegniamo in una sfida [12].

Per destare sentimenti di affinità, non è necessario che la comunicazione con le entità artificiali sia verbale. Può bastare una manifestazione affettiva, un impulso di compassione, una muta invocazione di assistenza, tratti e atteggiamenti che appartengono solo a noi e che noi crediamo di scorgere nell'altro. Si spiegano così non solo i comportamenti di accudimento verso gli animali domestici, dei quali peraltro è ormai accertata la capacità empatica e affettiva, ma anche verso certi artefatti la cui unica dote di innesco sentimentale è l'aspetto esteriore o una richiesta più o meno esplicita di assistenza. Si pensi al giocattolo Tamagotchi, un 'cucciolo' virtuale bisognoso di attenzione costante e di cure assidue, e al 'cucciolo' robot di foca Paro, che hanno vissuto un periodo di grande popolarità⁹.

Può darsi che la nostra insopprimibile tendenza all'animismo, cioè a umanizzare le entità che per l'aspetto o le capacità comunicative ci ricordano gli umani, sia alla base dei secolari tentativi di costruire l'uomo artificiale: in passato automi sempre più simili a noi e oggi robot umanoidi, magari capaci di esprimere emozioni (e in futuro di provarle? [2]). Questa propensione a estendere agli artefatti le caratteristiche della vita, dell'intelligenza e della comunicazione

⁸ Krach S. et al. (2008), Can machines think? Interaction and perspective taking with robots investigated via fMRI, *PLoS ONE*, 3 (7). Questi risultati sono stati confermati dall'analisi dell'attività cerebrale, che era tanto più intensa quanto più l'avversario somigliava a un uomo.

⁹ Tamagotchi è un piccolo giocattolo elettronico giapponese, inventato nel 1996 da Aki Maita. Il gioco consiste nel prendersi cura sin dalla nascita di questo essere, dargli il necessario per farlo crescere ed essere suo amico; inoltre bisogna farlo vivere il più a lungo possibile e curarlo in caso di malattia. Mediante tre tasti, il giocatore interagisce con il Tamagotchi, per esempio dandogli da mangiare, giocando con lui, curandolo se si ammala, nettandone le deiezioni. Bisogna poi controllarne l'età, il comportamento, la fame, il peso, la felicità e altre caratteristiche, tutte segnalate con un punteggio; sgridarlo se si rifiuta di obbedire, per esempio quando non vuol mangiare o giocare. Paro è un peluche robotico, anch'esso giapponese, che risponde al suo nome, reagisce alle carezze, muove corpo e testa, sbatte gli occhi, emette suoni, fa le fusa, mostra fastidio o stanchezza, e riesce perfino a imparare alcune parole. Paro è un potente catalizzatore di comunicazione emotiva, in grado di stimolare sentimenti di affetto, tenerezza, mansuetudine e accudimento, specie in anziani affetti da demenza.

umane è probabilmente anche alla base della roboetica, per quella parte di essa che concerne il nostro comportamento nei confronti dei robot [2]. La proiezione sugli artefatti di caratteristiche umane conferisce loro una certa aura di sacro, di intangibile¹⁰.

8. Jentsch: un'indagine psicologica sul perturbante

Nel 1906 lo psichiatra tedesco Ernst Jentsch¹¹ (1867-1919) pubblicò un saggio, *Zur Psychologie des Unheimlichen (Sulla psicologia del perturbante)* [13], in cui affermava che il perturbante (di cui non s'impegnava a dare una definizione) scaturisce dall'incertezza che si prova di fronte a certe entità o in certe situazioni, benché non tutti i soggetti avvertano il perturbante nelle stesse circostanze e nella stessa misura. L'impressione del perturbante è dunque molto soggettiva, dipende dalla sensibilità individuale, dall'abitudine a certi stimoli, dalla cultura e dallo sviluppo mentale. Secondo Jentsch, «tra tutte le incertezze psichiche che possono generare un senso di perturbante, ve n'è una in particolare capace di produrre un effetto piuttosto regolare, potente e generale, cioè il dubbio se un essere apparentemente vivo sia davvero animato e, viceversa, il dubbio se un oggetto che sembra privo di vita possa in realtà essere animato». Per esempio, aggiunge Jentsch, una situazione di indecisione si presenta a chi visita un museo delle cere: nella semioscurità è difficile distinguere una cera a grandezza d'uomo da una persona. Gli individui più sensibili continuano ad avvertire una sensazione sgradevole anche quando hanno deciso che si tratta di un'entità animata (o inanimata). Se esaminiamo la teoria di Masahiro Mori alla luce di questa interpretazione, vediamo che c'è perfetta consonanza. Il dubbio comincia infatti a presentarsi quando l'attribuzione all'entità di caratteristiche umane diventa problematica; non si presenta invece quando l'entità è chiaramente un artefatto (prima dell'avvallamento) oppure quando è chiaramente un essere umano (dopo l'avvallamento). Nella categoria del perturbante Jentsch annovera anche gli attacchi epilettici e le manifestazioni della pazzia, fenomeni che suscitano nell'osservatore il sospetto che dietro l'immagine consueta degli esseri umani possa celarsi qualche processo automatico e meccanico che ne mette in forse la natura umana.

Anche in letteratura l'effetto perturbante scaturisce dall'incertezza in cui viene lasciato il lettore quanto alla natura di un personaggio, se sia un essere umano o un automa. Jentsch indica in Hoffmann un narratore che ha impiegato questo artificio psicologico con notevole successo. Si veda in particolare *L'uomo della sabbia*, racconto nel quale, come si è visto, il protagonista s'innamora perdutamente dell'automa Olimpia non riuscendo a distinguerlo da una donna:

¹⁰ La cautela con cui ci si deve avvicinare al sacro è così espressa da Alexander Pope nella sua poesia *An Essay on Criticism* (1709): *For fools rush in where angels fear to tread* (Perché gli stolti si precipitano dove gli angeli temono di posare il piede), un verso spesso citato da Gregory Bateson.

¹¹ Jentsch coltivò una vasta gamma di interessi, che comprendevano anche la musica (scrisse il trattato *Musik und Nerven*), e tradusse in tedesco opere di Havelock Ellis e di Cesare Lombroso.

in questo racconto il lettore viene tenuto sapientemente in uno stato di incertezza sulla vera natura dell'automa. Altre figure letterarie che lasciano in dubbio il lettore quanto alla loro natura, animata o inanimata, o meglio umana o non umana, sono il Golem (si veda il romanzo di Gustav Meyrink [14]), il mostro di Frankenstein, dovuto alla penna di Mary Shelley, e Dracula, il vampiro creato dalla fantasia di Bram Stoker: tutti personaggi portati sullo schermo¹². Come si è visto, nello schema del perturbante proposto da Mori compare anche, in fondo all'avvallamento relativo alle entità immobili, il cadavere, e proprio ai cadaveri, agli scheletri e simili Jentsch dedica le conclusioni del suo scritto, affermando che l'orrore che queste entità ci ispirano può essere spiegato in quanto esse portano sempre con sé il pensiero di uno stato animato latente e quindi danno luogo al conflitto psichico descritto, che si oppone al desiderio umano di dominare intellettualmente l'ambiente circostante. Poiché la certezza intellettuale, conclude Jentsch, fornisce una difesa psichica nella lotta per l'esistenza, quando tale certezza viene a mancare viene meno la protezione contro le forze ostili che ci minacciano da ogni parte e siamo preda del perturbamento [13].

9. Sigmund Freud: *Das Unheimliche*

Si dice unheimlich tutto ciò che dovrebbe restare segreto, nascosto, e che invece è affiorato.

Friedrich Schelling

Nel 1919 Sigmund Freud (Fig. 5) riprende in mano un vecchio manoscritto, lo riscrive e lo intitola *Das Unheimliche* [14]. Come nota lo stesso autore, l'aggettivo tedesco *unheimlich* non ha in italiano (né in altre lingue) un corrispondente preciso e si potrebbe tradurre di volta in volta con inquietante, pauroso, sinistro, lugubre, sospetto; per qualche motivo, alla lunga si è affermato *perturbante*. Nel saggio Freud si richiama esplicitamente al lavoro di Jentsch, in parte tuttavia per criticarne l'interpretazione del perturbante fondata sull'incertezza, che trova limitata.

Per Freud infatti il perturbante è «quella sorta di spaventoso che risale a ciò che ci è noto da lungo tempo, a ciò che ci è familiare», e basa questa definizione sulla lunga e articolata voce *heimlich* del vocabolario della lingua tedesca di Daniel Sanders [16] e sulla definizione che si trova nel vocabolario dei fratelli Jacob e Wilhelm Grimm [17]. L'aggettivo *heimlich* ha due significati, entrambi risalenti alla radice *heim* (casa): in primo luogo domestico, familiare, fidato, grato; in secondo luogo nascosto, segreto, celato (e mantenuto celato senza far conoscere agli altri il motivo del nascondimento). Il contrario, *unheimlich*,

¹² Un caso paradigmatico di attribuzione incerta presentano i replicanti del film *Blade Runner* (Ridley Scott, 1982), tratto da un racconto di Philip K. Dick, che potrebbero situarsi in qualche punto della parete ascendente dell'avvallamento, visto che le loro discrepanze rispetto al modello umano sono lievissime. Massimo Bontempelli, nel dramma teatrale *Minnie la candida*, (1928, ristampato da Liberilibri, Macerata 2005), ci presenta la giovane e ingenua Minnie, alla quale vien fatto credere che sono stati fabbricati esseri umani artificiali, che non si distinguono dagli originali e che per di più *non sanno* di essere imitazioni. Minnie comincia a sospettare di essere uno di questi manichini e, sconvolta, si uccide.

significa quindi disagiata, infido, che suscita orrore; ma è *unheimlich* anche tutto ciò che dovrebbe restare nascosto (*heimlich*) e che invece è affiorato. Si osservi che questa seconda definizione di *unheimlich* era stata già proposta dal filosofo Friedrich Schelling (1775-1854). E, nota Freud, dalla lunga voce del vocabolario di Sanders emerge che *heimlich* (nella sua prima accezione, di familiare, palese) tra i suoi significati ne ha anche uno in cui coincide con il suo contrario, *unheimlich* (emerso, palese, cioè il contrario del secondo significato). Insomma *unheimlich* è in qualche modo una variante di *heimlich*. Se qualcosa suscita spavento è proprio perché non è familiare, anche se non tutto ciò che è ignoto suscita spavento. Ma, continua Freud, per capire meglio bisogna seguire la definizione di Schelling, che ha a che fare, secondo il fondatore della psicoanalisi, con la rimozione.

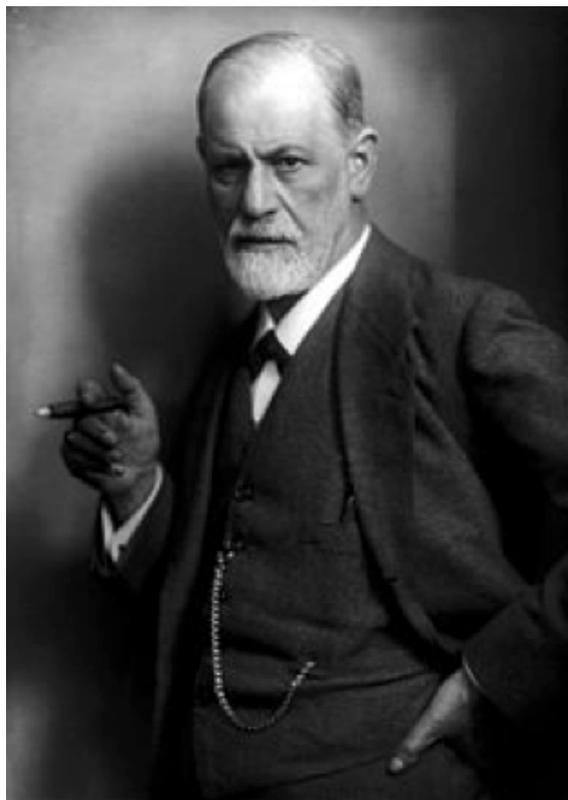


Figura 5
Sigmund Freud (1856-1939)

Per dimostrarlo, seguendo Jentsch, Freud volge poi la sua attenzione ancora una volta all'analisi dell'*Uomo della sabbia* di Hoffmann, ma in opposizione a Jentsch afferma che nel racconto il perturbante non nasce tanto dall'incertezza che il lettore prova nei confronti della natura di Olimpia quanto dalla figura dell'uomo della sabbia, che strappa gli occhi ai bambini [7]. E, sempre confutando Jentsch, afferma che l'effetto perturbante del racconto non ha nulla a che fare con l'incertezza intellettuale: «Oseremo dunque ricondurre l'elemento perturbante rappresentato dall'uomo della sabbia all'angoscia propria del complesso di evirazione infantile». Di qui in avanti, Freud approfondisce la sua interpretazione psicoanalitica, nella quale non intendo addentrarmi se non per accennare che tra i tanti motivi che s'intrecciano nel saggio vi sono quello del sosia, cioè del doppio, e quello della coazione a ripetere, entrambi fonte di perturbante. Freud elenca alcuni esempi di perturbante, che cataloga all'interno di un principio da lui chiamato col nome suggestivo di "onnipotenza dei pensieri", che corrisponde all'antica concezione del mondo propria dell'animismo: una concezione «caratterizzata dagli spiriti umani che popolavano il mondo, dalla sopravvalutazione narcisistica dei propri processi psichici, dall'onnipotenza dei pensieri e dalla tecnica della magia [...] nonché da tutte le creazioni con le quali il narcisismo illimitato di quella fase dell'evoluzione

si opponeva alle esigenze irrecusabili della realtà». E ciascuno di noi ha attraversato una fase di animismo che si è lasciata dietro residui capaci di manifestarsi: ciò che oggi ci appare perturbante risponde «alla condizione di sfiorare tali residui di attività psichica animistica e di spingerli ad estrinsecarsi». Ecco allora perché ciò che è *heimlich* (familiare-nascosto) può trapassare in *unheimlich*, che non è niente di estraneo, ma è qualcosa di familiare alla vita psichica «fin da tempi antichissimi e a essa estraniatosi soltanto a causa del processo di rimozione».

Secondo Freud, dunque, i fattori che trasformano l'angoscioso in perturbante sono l'animismo, la magia, l'onnipotenza dei pensieri, la relazione con la morte, la ripetizione involontaria e il complesso di evirazione. Anche l'epilessia e la follia hanno effetti perturbanti (come già aveva affermato Jentsch), poiché rivelano la presenza di forze insospettate, ma di cui si percepisce oscuramente la presenza in angoli remoti della propria personalità. Il perturbante si manifesta quando il confine tra fantasia e realtà si intorbida e quando ciò che era considerato fantastico si rivela reale: ciò accade anche nelle pratiche magiche, che si ricollegano all'onnipotenza dei pensieri. Infine l'autore distingue il perturbante legato agli accadimenti della vita reale dagli effetti perturbanti, solo immaginati, appartenenti al mondo della finzione letteraria. Il perturbante letterario è molto più ampio e non si limita a ciò che si sperimenta nella vita reale; inoltre il regno della fantasia è esonerato da quello che Freud chiama "l'esame di realtà". Da una parte molte cose che, se accadessero nella vita sarebbero perturbanti, non lo sono in letteratura, e viceversa la letteratura possiede molti mezzi di cui la vita non dispone per suscitare il perturbante. Per esempio lo scrittore può tenerci nascoste le premesse che stanno alla base della vicenda narrata, evitando di chiarirle fino alla fine [15].

10. I robot umanoidi: sono perturbanti?

Nel giugno 2008 il Centro Giapponese per la Scienza e la Tecnologia ha presentato il bambino robot CB2, un umanoide alto un metro e trenta per 33 chili di peso (Fig. 6).



Figura 6

Il robot bambino giapponese CB2

(si veda <https://www.youtube.com/watch?v=rYLM8iMY5io> e <http://www.dailymail.co.uk/sciencetech/article-460015/Baby-robot-walk-talk-feel.html>)

Dotato di oltre 200 sensori ottici, acustici e tattili e di una cinquantina di articolazioni di precisione mosse da muscoli all'aria compressa, CB2 reagisce agli stimoli ambientali imitando il comportamento di un bambino di 18 mesi. Il suo viso manifesta una grande varietà di espressioni, fino a un'astuta e grottesca imitazione dell'occholino. A quell'epoca, per molti, CB2 era la macchina più inquietante mai costruita. Un video impressionante mostra questo grosso e sgraziato burattino che, rivestito di una morta epidermide grigiastra, metà pelle, metà tuta, fa gli occhi dolci a un ricercatore, suo "padre putativo", oppure si contorce sul pavimento invocando l'aiuto dei grandi per rialzarsi.

Non c'è dubbio che CB2 metta bene alla prova la teoria di Mori, che può essere verificata anche sugli umanoidi della Hanson Robotics di Dallas, Texas, in particolare sul robot che ha le sembianze di Einstein da vecchio, l'icona più significativa e abusata della scienza del Novecento (Fig. 7). La somiglianza è impressionante: il personaggio si riconosce come lo si riconoscerebbe in una caricatura, ma là avrebbe un che di distorto ed esagerato, quindi di rassicurante, qui ha un che di liscio, ammiccante e ambiguo. Il robot Einstein non è e non vuol essere una caricatura, vuol essere *proprio* Einstein: di qui la sensazione di perturbante. Si veda anche il robot Philip K. Dick, della stessa Hanson Robotics (Fig. 8), impressionante per la sua somiglianza con l'originale umano.



Figura 7
Il robot Einstein della Hanson Robotics
(si veda: http://inventorspot.com/articles/einstein_lives_and_smiles_animated_life_relative_23682)

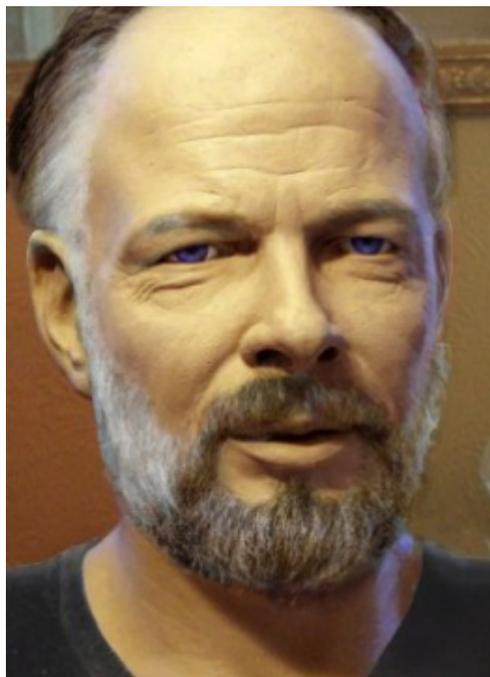


Figura 8

*Il robot Philip K. Dick della Hanson Robotics
(si veda: <http://www.hansonrobotics.com/robot/philip-k-dick/>)*

A quanto pare i ricercatori del Sol Levante non percepiscono appieno il contenuto potenzialmente destabilizzante sotto il profilo psicologico di questi robot umanoidi. Destabilizzante, o meglio *perturbante*. Di fronte a questi artefatti, noi Europei ci sentiamo a disagio: nella nostra tradizione, la storia degli automi antropomorfi è gravida di superstizione, di magia, di occultismo, tocca la religione, l'etica, la metafisica, l'essenza dell'uomo. Ridesta echi di lontani castighi legati al mito di Prometeo: superare certi limiti è una colpa che merita la punizione. La progressiva confusione tra naturale e artificiale riguarda tanto l'aspetto esteriore dei robot quanto le loro caratteristiche intellettuali (e domani forse anche emotive) e mette in crisi la radicata convinzione che l'uomo rappresenti qualcosa di speciale, inimitabile e assoluto. Questi scrupoli e questi timori sono legati alla nostra tradizione culturale e religiosa. In un contesto diverso per storia e sensibilità (penso al Giappone e, anche, agli Stati Uniti, sempre più disincantati e avulsi dalla tradizione europea), l'atteggiamento di fronte alla tecnica in generale e in particolare alla robotica umanoide è molto più disinvolto e spregiudicato.

Se al tempo dell'articolo di Mori non si costruivano ancora robot umanoidi, nel frattempo la situazione è molto cambiata, specie in Giappone: nonostante l'ammonimento di Mori, che invitava a non fabbricare robot antropomorfi troppo simili agli umani, dopo CB2 molti altri ne sono stati costruiti. Qui di seguito riporto le immagini di alcuni umanoidi che potrebbero rientrare nella categoria

del perturbante. Alcune gineidi, come HRP-4C (Fig. 9), Valerie (Fig. 10) e Q2 (Fig. 11), sono dotate di una spiccata sensualità¹³.



Figura 9

La gineide giapponese HRP-4C

*(si veda HRP-4C che canta: <https://www.youtube.com/watch?v=H0fgdUALpSU>
e HRP-4C che balla : <https://www.youtube.com/watch?v=xcZJqiUrbnl>)*

¹³ Può essere interessante indagare il rapporto tra tecnologia, erotismo e perturbante. Nel romanzo *Crash* (1973) lo scrittore inglese James G. Ballard (1930-2009) esplora la possibilità, al limite della psicopatologia, di un rapporto tra sessualità e tecnologia, in particolare tra la sessualità e la devastazione dei corpi causata dagli incidenti automobilistici. Nel saggio *Il sex appeal dell'inorganico*, Mario Perniola (1941) sostiene che oggi la sessualità organica è sostituita da una sessualità inorganica, neutra e artificiale, che non si cura della bellezza e dell'età, ed esplora il ruolo dell'eros in un'epoca, la nostra, condizionata dalla tecnologia. Entrambi gli autori si possono considerare esploratori del perturbante tecnologico-sessuale. Per una gineide molto sensuale si veda il filmato <https://www.youtube.com/watch?v=biBHJvGx3s8>

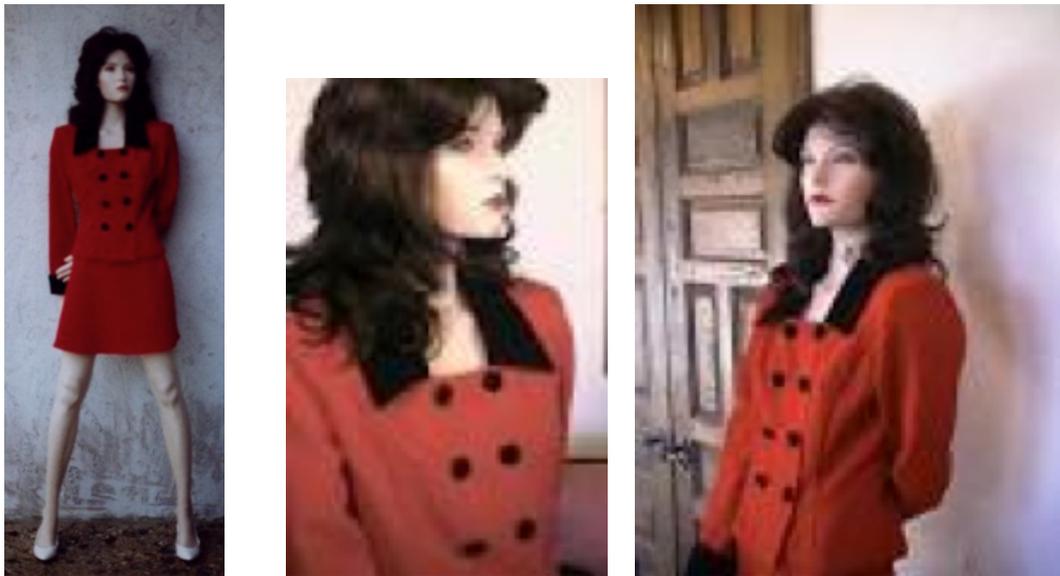


Figura 10
La gineide giapponese Valerie
(si veda: <http://www.androidworld.com/valerie.jpg>)



Figura 11
La replicante giapponese Q2
(si veda: https://en.wikipedia.org/wiki/Actroid#/media/File:Repliee_Q2.jpg)

11. Conclusioni

I robot sono ormai dappertutto ed eseguono molte attività al pari degli umani e talora meglio: dirigono orchestre, scrivono articoli, compongono poesie, giocano a golf, a calcio, a scacchi e a go, parlano, cantano, sbrigano le faccende domestiche, accudiscono infermi e anziani, eseguono interventi chirurgici, compiono salvataggi, disinnescano ordigni esplosivi ed esplorano luoghi impervi, inaccessibili o pericolosi. Forse avvertiamo una forma nuova di perturbante, che ha a che fare con il nostro timore di essere sostituiti, forse spodestati, da questi artefatti sempre più invadenti e sempre più simili a noi per aspetto e funzioni. Un perturbante legato a ciò che di inquietante, estraneo, o addirittura pericoloso, può nascondersi nel cuore stesso della nostra identità. Di conseguenza perturbante è il doppio, il sosia, l'ambiguo, l'ammiccante: ciò che suscita diffidenza per la sua somiglianza *quasi* perfetta, che allude all'Altro ma anche a noi stessi [18]. È il perturbante secondo la definizione di Schelling (il rimosso che doveva restare nascosto e che invece riemerge), ripresa poi da Freud, oppure è il perturbante descritto da Jentsch, collegato al dubbio e all'incertezza (incertezza se si tratti ancora di macchine o già di altro)?

Posti di fronte a questi nostri collaboratori, e un domani concorrenti, li riconosciamo come degni del nostro rispetto e della nostra simpatia perché ci somigliano tanto, oppure li rifiutiamo come sinistre incarnazioni di tratti rimossi che affiorano per toglierci la serenità e il buon umore? In fondo, per tornare al tema del sosia o del doppio caro a Freud, l'uomo artificiale rappresenta una nostra immagine più o meno deformata, che ci mostra ciò che potremmo essere o che potremmo essere stati. Ma, come nota Caronia, mentre l'automa del Settecento rassicura «riguardo all'eccellenza del corpo dell'uomo (così complesso da meritare di essere imitato) e della sua mente (così acuta da essere capace di realizzare quell'imitazione), il robot, l'androide, il cyborg della fantascienza annunciano invece il declino dell'uomo quale noi lo conosciamo [...] e la nascita di un uomo nuovo, simbiote della creatura che egli stesso ha costruito ma ormai in qualche modo autonomizzata». [18]

Si ripropone qui un interrogativo che negli ultimi tempi è diventato sempre più pressante: come si distingue un uomo da un uomo artificiale? Ovvero un uomo da un post-uomo? [19] La fantascienza ha ipotizzato un passaggio dall'uomo alla macchina passando per il ciborg e per il robot androide; e viceversa dalla macchina all'uomo passando per il robot e per il simbiote¹⁴. Tutti questi esseri, scaglionati lungo il percorso che va dall'uomo alla macchina, reclamano una definizione della loro identità: finché l'uomo era il solo rappresentante dell'umanità ed era nettamente distinto dalle macchine elementari di un tempo, il problema dell'identità non si poneva; ma oggi, con la comparsa di congegni e apparecchi sempre più complessi, il confine tra uomo e macchina tende a

¹⁴ Questo duplice passaggio non è più soltanto tema di racconti o film fantascientifici o di speculazioni filosofiche, ma è ormai oggetto anche di ricerche scientifiche e attuazioni tecniche. Si veda l'ampia bibliografia sul post-umano, per esempio [19], e, per quanto attiene alla genetica e alla biologia, anche [20]. Un vasto repertorio di abitatori delle zone intermedie tra scienza, tecnica e fantascienza si trova in [21].

sfumare, o meglio la zona di transizione si amplia ad ospitare una famiglia di creature "intermedie", che si distribuiscono secondo una tassonomia non necessariamente lineare, che tende al continuo ed è animata da spunti evolutivi, da intrecci e interfecondazioni ibridative. E tutti questi esseri intermedi sembrano esigere non solo la qualifica di sosia o doppi più o meno legittimi dell'uomo, ma pretendono anche una considerazione del loro statuto etico: non più solo le leggi di Asimov e neppure solo la roboetica, ma anche una "simbioetica", dove il termine simbiote tende a moltiplicarsi e a differenziarsi per indicare una famiglia proliferante di mostri speranzosi e di enti informi o quasi perfetti (rispetto al modello che, per il nostro vizio antropocentrico, è sempre l'uomo), i quali si affacciano al teatro dell'esistenza: un'esistenza forse transitoria, addirittura effimera, che può trapassare facilmente nella non esistenza per far posto ad altri enti. E questa provvisorietà potrebbe un giorno coinvolgere anche l'uomo come lo conosciamo oggi: forse questo pensiero, riportando alla luce ciò che avevamo rimosso, la nostra transitorietà, è ciò che desta in noi il perturbante quando ci specchiamo nelle creature che abbiamo costruito.

Bibliografia

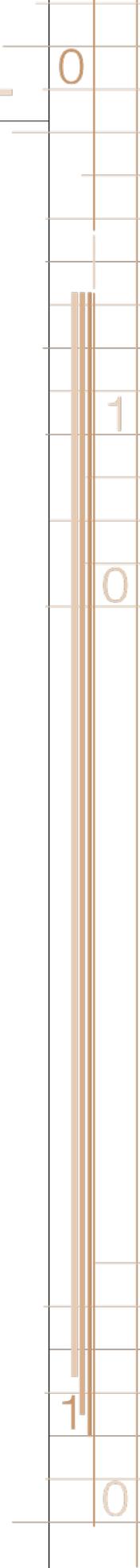
- [1] Longo, G. O. (2006). "Dal golem al robot", *Prometeo*, 95, , 14-21.
- [2] Longo, G. O. (2007). "L'etica al tempo dei robot", *Mondo Digitale*, 21, 3-20.
- [3] Losano, M. G. (1990). *Storie di automi*, Einaudi.
- [4] Mori, M. (1970). "Bukimi no tani", *Energy*, 7, 33-35.
- [5] Kageki, N. (2012). "An Uncanny Mind: Masahiro Mori on the Uncanny Valley and Beyond", intervista, *IEEE Spectrum*:
<http://spectrum.ieee.org/automaton/robotics/humanoids/an-uncanny-mind-masahiro-mori-on-the-uncanny-valley> (ultimo accesso febbraio 2016).
- [6] Calvino, I., a cura di, (2015). *Racconti fantastici dell'Ottocento*, Mondadori.
- [7] Hoffmann, E. T. A. (1950). *L'uomo della sabbia e altri racconti*, Rizzoli.
- [8] Hoffmann, E. T. A. (1957). *I Fedeli di San Serapione*, Gherardo Casini.
- [9] http://www.federscacchi.it/doc/art/d20050115041248_racconto8.pdf (ultimo accesso febbraio 2016)
- [10] Longo, G. O. (2006). "Il poliedrico mondo dell'informazione", *Mondo Digitale*, 18, 3-17.
- [11] Longo, G. O. (2009). "Il test di Turing: storia e significato", *Mondo Digitale*, 29, 11-24.
- [12] Gallina, P. (2015). *L'anima delle macchine*, Dedalo.
- [13] http://www.art3idea.psu.edu/locus/Jentsch_uncanny.pdf (ultimo accesso febbraio 2016)
- [14] Meyrink, G. (2000). *Il Golem*, Bompiani.

- [15] Freud, S. (1969). "Il perturbante", in *Saggi sull'arte, la letteratura e il linguaggio*, I, Boringhieri, 267-307.
- [16] Sanders, D. (1876). *Wörterbuch der deutschen Sprache*, Otto Wigand.
- [17] Grimm, J., Grimm, W. (1877). *Deutsches Wörterbuch*, Hirzel.
- [18] Caronia, A. (2001). *Il cyborg*, Shake.
- [19] Longo, G. O. (2013). "Paesaggi del post-umano", *Mondo Digitale*, 45, 1-15.
- [20] Nowotny, H., Testa, G. (2012). *Geni a Nudo*, Codice.
- [21] Tagliasco, V., (1999). *Dizionario degli esseri umani fantastici e artificiali*, Mondadori.

Biografia

Giuseppe O. Longo, ingegnere e matematico, è professore emerito di Teoria dell'informazione all'Università di Trieste. Romanziere, drammaturgo, traduttore, divulgatore scientifico e attore, è interessato alla comunicazione in tutte le sue forme.

Email: giuseppe.longo41@gmail.com



Calcolo distribuito volontario: l'esperienza Boinc

Stefano Bologna

Sommario

Negli ultimi decenni l'home computing e internet hanno modificato la nostra vita quotidiana, ma hanno anche cambiato radicalmente il modo di fare ricerca. Questa doppia rivoluzione, recentemente, ha permesso un avvicinamento tra il mondo della scienza e il cittadino, anche attraverso il calcolo distribuito. La piattaforma Boinc, la più usata per il calcolo distribuito volontario, viene descritta nella sua storia, nel suo funzionamento e nei risultati conseguiti.

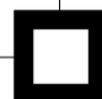
Abstract

In last decades, the home computing and the Internet have changed our daily life, but also changed the way of doing research. This double revolution, recently, allowed an approach between the world of science and the citizen, through the distributed computing. Boinc platform, the most widely used for voluntary computing, is described in its history, its operation and results.

Keywords: Volunteer computing, citizen science, boinc, middleware, in silico

1. Introduzione: cos'è il calcolo distribuito?

Cos'è il calcolo distribuito? Lo dice, in maniera sintetica, il nome stesso, ovvero distribuire un carico di lavoro tra più computer in modo da poterlo velocizzare. Le simulazioni in silico, nate all'inizio degli anni 80 grazie alla lungimiranza di alcuni ricercatori come Martin Klarplus, sono diventate uno strumento quotidiano per moltissimi scienziati delle più diverse branche. Ricercatori di tutto il mondo spesso necessitano di incredibili potenze di calcolo (con server molto costosi) dell'ordine dei vari multipli di Tflops (floating point operation per second), per i loro studi e spesso queste richieste non sono accolte nell'immediato. Con l'avvento di internet e dell'home computing, alcuni scienziati hanno ritenuto che un computer di casa o dell'ufficio usato mediamente al 10-15% delle proprie potenzialità, potesse divenire parte di una rete (grid) e che questo portasse ad indubbi vantaggi computazionali. In tal senso erano state create alcune piattaforme già nei primi anni 90, come ad esempio Condor, che permettevano di chiedere aiuto via internet a volontari, i quali mettevano a disposizione la



potenza inutilizzata dei propri pc. Ai loro computer venivano quindi “spedite” delle minuscole porzioni in cui era stato suddiviso il lavoro (in gergo wu, ovvero working unit), che venivano elaborate. I risultati ottenuti, infine, erano rispediti ai ricercatori che provvedevano ad analizzarli e a trarne conclusioni.

2. Boinc: le caratteristiche e un po' di storia

La piattaforma più nota ed importante è BOINC (Berkley Open Infrastructure for Network Computing) [1], un sistema non commerciale su cui vengono eseguiti una vastità di progetti che vanno dalle simulazioni proteiche all'astrofisica, dalla ricerca climatologica a quella matematica, ecc, ecc. Il suo funzionamento è molto simile alle piattaforme precedenti, quindi un sistema middleware client/server, ma con un occhio particolare alla sicurezza e alla semplicità d'uso. BOINC è stato sviluppato presso lo Space Sciences Laboratory della University of California Berkeley, da un team diretto dal ricercatore David Anderson. Nel 2002, dietro richiesta di altri ricercatori, lo scienziato pensò ad una piattaforma “eterogenea”, che potesse contenere tutta una serie di diverse simulazioni.

Un esempio tra i molti è legato al progetto “*Help Fight Childhood Cancer*” (aiutaci a sconfiggere il cancro infantile), supportato dall'università giapponese di Chiba e dalla IBM. I suoi ricercatori hanno calcolato, per la prima fase della ricerca, che con i server a loro disposizione, impegnati 24 ore su 24, 365 giorni l'anno, avrebbero impiegato circa 8000 anni per finirla. Grazie a BOINC e ai suoi volontari, i ricercatori l'hanno completata in meno di 2 anni. [2]

Alla stregua di una piattaforma HPC (High Performance Computing, ovvero grandi server dedicati alla ricerca), BOINC conta circa 433.000 computer attivi (hosts) in tutto il mondo che elaborano una media di 8,6 petaFLOPS (a Febbraio 2015), posizionandosi - come capacità di calcolo - al sesto posto tra i supercomputer più potenti al mondo[3]. Il software client è supportato da tutti i più diffusi sistemi operativi, come Microsoft Windows, Mac OS X e sistemi Unix-like tra cui Linux e FreeBSD. La licenza di rilascio è LGPL, i sorgenti possono quindi essere scaricati liberamente e modificati per integrare le necessità di ogni struttura.

I 13 anni che sono trascorsi dalla nascita della piattaforma sono costellati da una costante evoluzione hardware che, anche grazie all'evoluzione software, ha reso possibile l'utilizzo delle nuove tecnologie: il passaggio delle cpu (central processing unit) single-core a quelle multi-core, l'utilizzo delle gpu (graphic processor unit, le schede video che si trovano comunemente nei nostri pc) (**RIQUADRO GPGPU – General Purpose on Gpu**), per finire con l'avvento del calcolo distribuito anche su piattaforme smart come Raspberry Pi.

3. Boinc Manager (Client)

Il funzionamento del client di gestione dei progetti è molto semplice: è sufficiente scaricare dal sito www.boincitaly.org, tradotto in italiano dal nostro team, ed installarlo. Una volta avviato il client Boinc bisogna scegliere il progetto a cui si vuole partecipare, iscriversi ad esso (basta una email ed una password) e lanciare l'elaborazione. La fase successiva viene fatta automaticamente, e non

sono richieste particolari conoscenze tecniche da parte degli utenti (figura 1): sarà il client stesso, infatti, ad analizzare la configurazione hardware dell'host (per esempio, rilevare la presenza di cpu in grado di supportare istruzioni SIMD, come le SSEx o le AVX) e richiedere al server il carico di lavoro adeguato.

The screenshot shows the Boinc Manager Italian interface. The main window displays a table of projects with columns for Project, Progress, Status, Time, Time remaining, Deadline, Application, and Name. The 'rosetta@home' project is highlighted in blue and shows 73,239% progress. Other projects listed include 'World Communi...' with 0.000% progress and 'Mapping Cancer Markers 7.36'.

Progetto	Avanzamento	Stato	Tempo	Tempo manca...	Scadenza	Applicazione	Nome
rosetta@home	73,239%	In elaborazione	01:38:16	00:31:16	06/05/2016 18:29:35	Rosetta Mini 3.73	psh_1012_1
World Communi...	35,416%	In elaborazione	01:15:19	02:04:56	04/05/2016 18:23:59	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012
World Communi...	0,000%	Pronto per l'elaborazione	---	03:13:27	05/05/2016 09:46:01	Mapping Cancer Markers 7.36	MCM1_012

Figura 1
Boinc Manager italiano

Il client Boinc è ampiamente configurabile: è possibile, per esempio decidere quanti core cpu dedicare, oppure gli orari in cui elaborare i dati, ecc, ecc. Con l'avvento delle tecnologie mobili (**vedere riquadro dispositivi mobili**), è stato creato anche un manager facilitato che possa essere facilmente fruibile da dispositivi mobili quali gli smartphone o i tablet. E' un sistema facile e sicuro, che non danneggia il pc e soprattutto non mette a rischio la privacy degli utenti, dal momento che crea un ambiente protetto che non va ad influenzare eventuali altre applicazioni.

4. Boinc Server

Il server Boinc è quel server collocato presso il centro di ricerca/università che si occupa di creare e distribuire le porzioni di lavoro, oltre che a riceverne i risultati già calcolati e successivamente a convalidarli (figura 2). Dal momento che il lavoro è fatto "esternamente" dai client, questi server non hanno la necessità di essere potenti: anche un giovane ricercatore con una buona idea o una facoltà con pochi fondi hanno la possibilità di accedere a potenze di calcolo ingenti (**vedere riquadro virtual campus**). Il team di amministratori di Boinc ha pensato, per facilitare l'adozione di questo sistema, di creare una macchina server virtuale già pronta all'uso[4], così che i ricercatori possano concentrarsi maggiormente sulla parte scientifica che sulla creazione dell'infrastruttura.

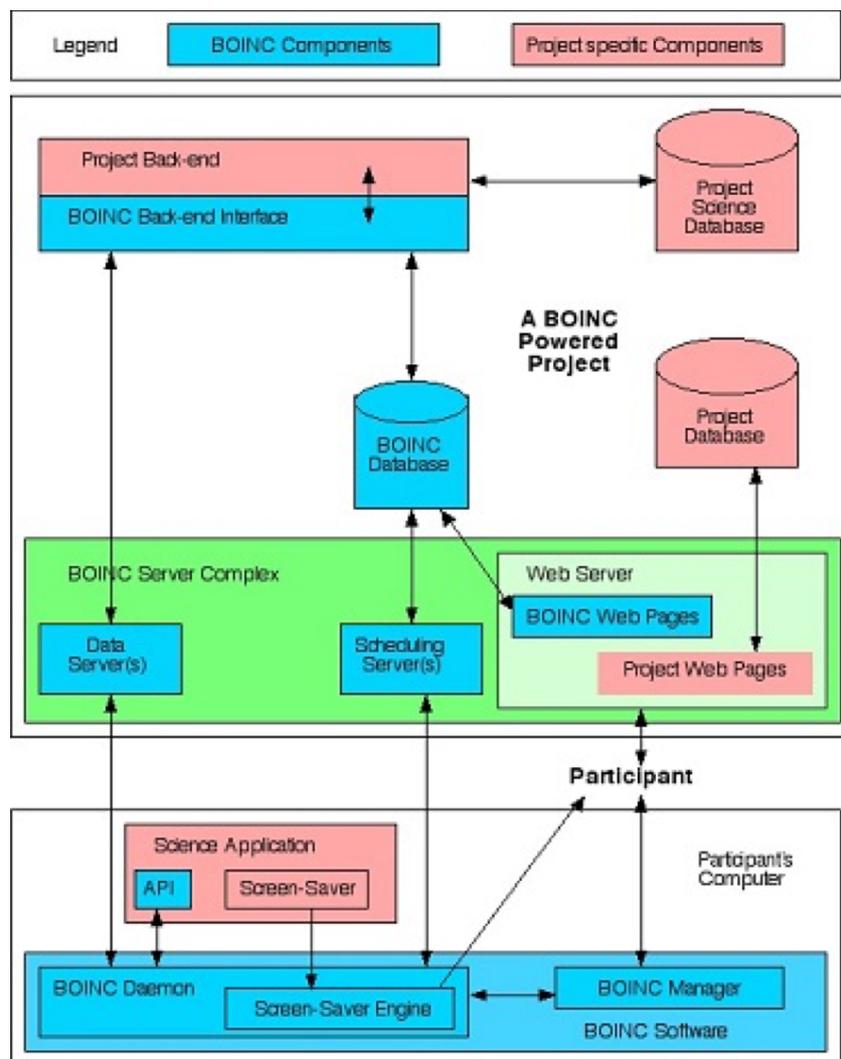


Figura 2
Lo schema di funzionamento della piattaforma

5. I Progetti

Ogni progetto ha un proprio applicativo che viene fatto elaborare nell'ambiente boinc e che permette di utilizzare i pc dei volontari, sfruttando sia i processori, sia le schede video che i dispositivi mobili. I progetti riguardano i più svariati campi della scienza e al momento sono circa una cinquantina. Di seguito alcuni esempi:

Seti@Home[5]: il primo e più famoso progetto di calcolo distribuito, nato per la ricerca di segnali di vita extraterrestre, negli anni ha portato anche ad ottimi risultati scientifici (come lo studio del rumore di fondo dell'universo).

Rosetta@Home[6] (figura 3): è uno dei progetti più "vecchi" del panorama Boinc e si occupa di simulazioni proteiche (folding, docking, ab initio, ecc) con risultati spesso pubblicati su riviste importanti come Science o Nature [7].



Figura 3
screensaver di Rosetta@Home

LHC@Home[8]: Il CERN di Ginevra è particolarmente sensibile al calcolo distribuito e ha creato un progetto, con vari sottoprogetti, con profondi legami scientifici con l'acceleratore LHC.

Einstein@Home[9]: un importante progetto di ricerca nel campo dell'astrofisica, specializzato nello studio delle pulsar, che si prefigge di vedere se, come previsto dalla teoria di Einstein, le pulsar sono in grado di generare onde gravitazionali.

World Community Grid[10]: è un multi-progetto finanziato dall'IBM. Al suo interno comprende molti progetti che vanno dallo studio di migliori pannelli fotovoltaici a metodi che usano le nanotecnologie per filtrare l'acqua, alla ricerca sul cancro. Qualsiasi ricercatore può partecipare, presentando il proprio progetto alla IBM, la quale metterà a disposizione server ed expertise.

6. Il progetto Italiano

In Italia, purtroppo, questo tipo di ricerca scientifica è ancora poco noto anche se, grazie al progetto supportato dall'Università di Trento e dal CNR, ci auguriamo possa divenire sempre più popolare.

Il progetto in questione, Tn-Grid, si occupa di ricerche legate alle reti geniche e delle loro relazioni di causa. [11](figura 4). Al momento attuale i ricercatori stanno processando dati riguardanti le LGN (local gene network) dell'*Escherichia Coli*, noto organismo modello.

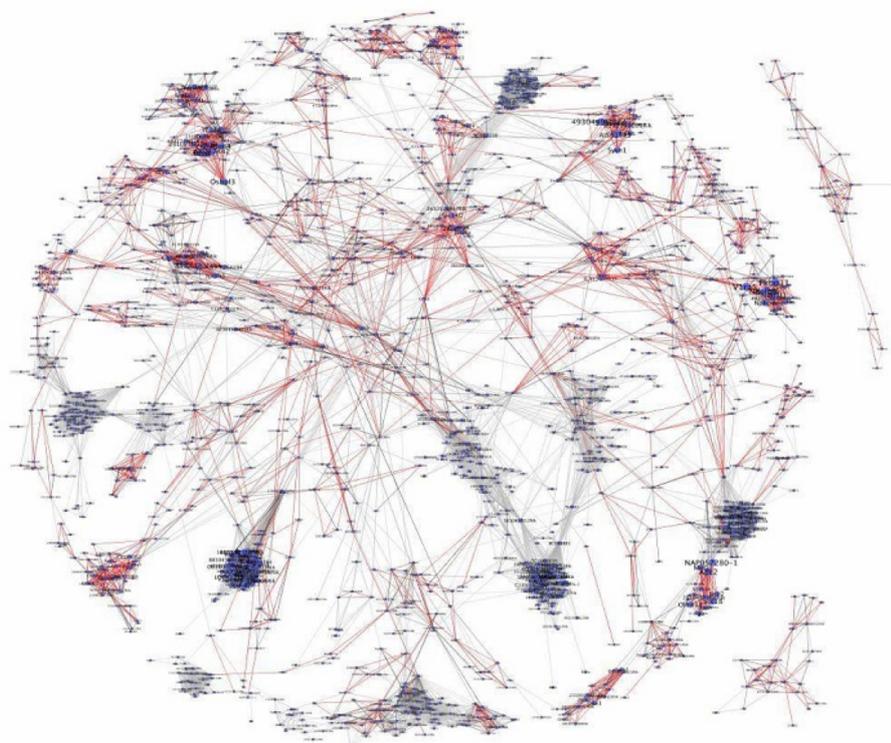


Figura 4
mappa genica Tn-Grid

7. I risultati

I progetti sono senza scopo di lucro e i risultati sono pubblici [12]. Il calcolo distribuito volontario, d'altro canto, non vuole sostituirsi al lavoro che si fa in laboratorio, ma anzi vuole anzi sostenerlo e accelerarne le tempistiche e la precisione.

8. I volontari

Chi aderisce ad un progetto di ricerca (o a più progetti) non lo fa per ricevere ricompense, ma per poter aiutare la scienza senza il vincolo di risultati minimi da raggiungere: vi potrà contribuire in maniera spontanea per il tempo che vorrà e con quanti computer vorrà. Il calcolo distribuito, in questo senso, va interpretato come una nuova forma di beneficenza o di volontariato. Oltre a questa forma di partecipazione "passiva", è possibile partecipare anche attivamente: sui forum dei progetti è possibile, per esempio, dialogare direttamente con i ricercatori stessi; oppure, aiutarli a migliorare il software stesso, dal momento che i sorgenti degli applicativi sono, per la quasi totalità, opensource (oppure con accesso riservato alle università).

E' questo lo spirito che anima quello che viene definito il movimento della "Citizen Science", ovvero di una scienza aperta alla gente e a cui è possibile contribuire fattivamente[13].

9. I crediti

Nonostante i progetti non assegnino ricompense a chi vi partecipa, per ogni unità di lavoro completata e riconsegnata correttamente viene assegnato un punteggio. Questo permette ai volontari di creare classifiche personali o per team, e di partecipare a sfide simboliche i cui unici beneficiari sono i progetti stessi.

10. Boinc Italy

Il gruppo Boinc Italy [14], composto da oltre 5000 volontari, si è aggregato attorno all'idea di poter concretamente aiutare i ricercatori e, negli anni, si è imposto come una realtà (per potenza di calcolo e partecipazione) a livello internazionale. La partecipazione al gruppo è aperta a tutti e tutti possono, nel portale, trovare risposta ai propri dubbi/curiosità e approfondimenti sui singoli progetti. Si occupano, inoltre, della traduzione di tutte le news dei progetti e dell'organizzazione delle "sfide" nazionali ed internazionali sui progetti quali, ad esempio, quelle dedicate a Rita Levi Montalcini o quella dedicata a Margherita Hack.

11. Le criticità

A fronte degli indubbi vantaggi derivanti dall'uso della piattaforma boinc, ci sono alcune criticità che devono essere considerate al momento della creazione di un progetto:

1. Boinc non è adatto ad eseguire calcoli real-time (come i sistemi cluster), ovvero quelle simulazioni che necessitano di elevato parallelismo per poter ottenere una risposta soddisfacente. Un esempio di cluster italiano dedicato alla ricerca scientifica è il sistema GALILEO, presente presso il Cineca, con i suoi 8000 core che lavorano in simultanea.
2. La volatilità del lavoro (un client può anche non restituire i risultati, per i più disparati motivi). Questo problema viene attenuato con l'utilizzo del quorum, ovvero con l'invio di una o più copie dello stesso lavoro a diversi pc, così da ottenere almeno un risultato utile.
3. Una presenza non stabile della potenza di calcolo erogata dai client, con picchi e momenti di "stanca".

Il futuro è qui

Le difficoltà che vengono incontrate più spesso dagli amministratori di Boinc Italy nel divulgare questa risorsa sono principalmente due: primariamente la paura degli istituti di ricerca di vedere "rubato" il proprio lavoro, derivante in genere dalla scarsa comprensione che la frammentazione del lavoro da svolgere introdotta da Boinc, impedisce la divulgazione delle informazioni all'esterno dell'ambiente di ricerca. Secondariamente un certo timore, da parte dei nuovi volontari, di non capire appieno i progetti (dal momento che tutte le home page sono in lingua inglese), nonostante il continuo lavoro di traduzione del gruppo.

La continua evoluzione (e l'abbattimento dei costi) dell'home computing, rendono il calcolo distribuito su base volontaria una alternativa veramente valida per chi vuol fare ricerca attraverso la scienza computazionale.

Riquadro GPGPU (“general purpose computing on graphic processor unit – calcolo a scopo generale su unità di elaborazione grafiche”. Wikipedia).

L'utilizzo di schede video per attività “general purpose” è stato sicuramente uno dei punti di svolta dell'informatica moderna, grazie ai costi relativamente bassi e alla potenza di calcolo messa a disposizione. Il primo settore a rendersi conto delle possibilità insite nelle schede grafiche, è stato ovviamente quello dei videogiochi: non a caso due dei maggiori vendor di schede per uso gpgpu sono AMD e Nvidia, leader nel settore dei videogames. I principali linguaggi di programmazione ad alto livello utilizzati sono due: Cuda ed OpenCl. Il primo è un linguaggio proprietario della casa produttrice Nvidia e funziona solo sulle loro gpu, mentre OpenCl è uno standard aperto supportato da AMD che può girare, dopo le ovvie modifiche, su un variegato parco hw (cpu, gpu, fpga, Xeon Phi, ecc). Gli incrementi, con codice adeguato, vanno dal raddoppio della potenza rispetto ad una cpu fino a fattori 100x.

Riquadro Virtual Campus

Gli amministratori di Boinc propongono, tra le varie opzioni, la creazione di “Virtual Campus Supercomputer”, ovvero progetti ospitati totalmente all'interno delle università, ricercando la potenza di calcolo nei vari pc presenti (per esempio negli uffici amministrativi), utilizzati per poche ore al giorno e con compiti poco onerosi dal punto di vista dell'utilizzo delle risorse. Per esempio in un campus con 5.000 pc in funzione al 50% delle risorse, la potenza di calcolo corrisponderebbe ad un cluster del costo di circa 2 milioni di dollari (con 500 mila dollari di mantenimento annuale). Utilizzando Boinc, il costo sarebbe di poco più di 10.000 dollari.

Riquadro Dispositivi Mobili

Negli ultimi anni sono nati molti progetti Boinc che utilizzano la piattaforma Android per eseguire le proprie simulazioni (semplicemente scaricando l'app dallo store). Il client Boinc sviluppato per l'utilizzo su dispositivi mobili è stato creato per permettere il completo controllo, da parte dell'utente, dei progetti scelti. Il client, infatti, si avvierà solo alla connessione della ricarica elettrica (non andando ad intaccare, così, la batteria) e solo in presenza di rete wireless (non utilizzando il traffico della Sim) e sarà possibile, inoltre, controllare anche altri parametri: quanti core utilizzare, l'uso dello spazio, ecc, ecc. La relativa potenza di calcolo di smartphone e tablet (ancora molto inferiore a quella di un pc) viene, però, compensata dalla loro massiccia adozione e dalla facilità d'uso degli stessi.

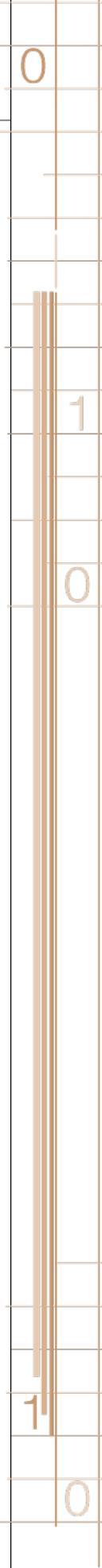
Bibliografia

- [1] <http://boinc.berkeley.edu/> (Settembre 2015)
- [2] <https://secure.worldcommunitygrid.org/research/hfcc/overview.do> (Settembre 2015)
- [3] https://it.wikipedia.org/wiki/Berkeley_Open_Infrastructure_for_Network_Computing (Settembre 2015)
- [4] <https://boinc.berkeley.edu/trac/wiki/VmServer> (Settembre 2015)
- [5] <http://setiathome.ssl.berkeley.edu/> (Settembre 2015)
- [6] <https://boinc.bakerlab.org/> (Settembre 2015)
- [7] Pearson A.D., Mills J.H., Baker D. et al. "Transition states. Trapping a transition state in a computationally designed protein bottle" *Science* 347(6224), pp 863-867, 2015.
- King N.P., Bale J.B, Sheffler W., Baker D. et al. - "Accurate design of co-assembling multi-component protein nanomaterials". *Nature* 510 (103-108), 2014.
- [8] <http://lhathome.web.cern.ch/> (Settembre 2015). Un esempio di pubblicazione è:
- Karneyeu A., Mijovic L., Prestel S., Skands P.Z. "MCPLOTS: a particle physics resource based on volunteer computing". *European Physical Journal C* 74, pp. 1-22, 2014.
- [9] <http://www.einsteinathome.org/> (Settembre 2015)
- [10] <https://secure.worldcommunitygrid.org/> (Settembre 2015)
- [11] <http://gene.disi.unitn.it/test/> (Settembre 2015). Nonostante il progetto sia ancora in fase di test e l'accesso non sia completamente pubblico, ma su invito, ha già raggiunto alcuni risultati, presentati in conferenze scientifiche internazionali, come:
- Erculiani L., Asnicar F., Sella N., Cavecchia V. et al. - "Discovering Candidates for Gene Network Expansion by Variable Subsetting and Ranking Aggregation". *Network Biology in SIG Poster*, 2015.
- [12] <http://www.boincitaly.org/progetti/pubblicazioni-scientifiche.html> (Settembre 2015)
- [13] <https://www.whitehouse.gov/blog/2015/09/09/open-science-and-innovation-people-people-people> (Settembre 2015)
- [14] www.boincitaly.org (Settembre 2015)

Biografia

Stefano Bologna informatico con laurea in filosofia, è uno degli amministratori del gruppo Boinc Italy, nonché referente italiano dei progetti Correlizer e Citizen Science Grid. Mi occupo, inoltre, di tenere aggiornata la lista delle pubblicazioni scientifiche legate a Boinc e che risulta essere la più completa a livello internazionale.

Email: stefano.bologna@boincitaly.org



Il paradigma didattico: osservazioni alla luce dell'esperienza “FabLab Ivrea - OPEN”

Ugo Avalle, Giovanni Leccisotti

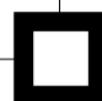
Sommario

L'automazione dei processi lavorativi basata su algoritmi sempre più “intelligenti” pretende competenze prioritariamente decisionali. L'idea di fondo, che queste note percorrono, fa leva sull'attuale situazione formativa ed educativa (talvolta distante da quanto il mondo lavorativo richiede) che le realtà scolastiche attuano, riferendosi in particolare al ciclo di studi che accompagna i nostri ragazzi fino alla maggiore età. In tal senso l'articolo pone dei quesiti, discutendone osservazioni e suggerimenti. Significativa per gli autori l'esperienza didattica tracciata. Come descritto questa è realizzata con ragazzi di età e provenienza scolastica eterogenee, internamente ad un FabLab che usa esclusivamente tecnologie open.

Abstract

The automation of work processes based on more and more “ intelligent ” algorithms claims priority decision-making skills . The basic idea , that these notes cover, insists on the current training and educational context (sometimes far from what the working world requires) that the school actually carries out, referring in particular to the study cycle that follows our children through up to full age . In this sense, the article raises questions , discussing observations and suggestions . The traced educational experience is significant for authors. As described, this is achieved with children of different age and educational background , within a FabLab that uses exclusively open technologies.

Keywords: FabLab, know-how, didactis, opensource, collaborative learning, skill, automation, connectivism, abilities, learning by doing, flipped classroom



1. Introduzione

Gli attuali processi lavorativi mostrano come algoritmi sempre più sofisticati sono in grado di sostituire il lavoro dell'uomo. Le capacità più attese diventano quindi la creatività, l'immaginazione, l'intuito risolutivo ovvero quelle da sempre ritenute come innate dell'individuo. C'è bisogno di modelli didattici che favoriscano lo sviluppo concreto di queste attitudini. Il mercato del lavoro muta velocemente mentre molti schemi didattici sono ancora legati a sollecitazioni del secolo passato.

Negli ultimi anni molte esperienze didattiche innovative hanno portato suggerimenti e stimoli sempre più interessanti. Una delle frasi più attuali negli ambiti formativi è "capovolgere il paradigma".

A Ivrea è nato nell'ultimo anno, in seno all'Accademia A.Olivetti, un piccolo ma ben strutturato FabLab.

Non è il primo né l'unico: esperienze simili si trovano un po' ovunque. Molte di queste hanno sollecitato vari autori a fornire la loro opinione, a suggerire qualcosa di nuovo alle consolidate esperienze e metodologie didattiche. Così anche noi ci siamo posti delle domande dalle quali sono scaturite alcune riflessioni e, forse, suggerimenti: queste note ne tracciano una sintesi.

Essere riusciti ad interessare e coinvolgere ragazzi, a partire dalle loro scuole, ci ha indotti a riflettere quanto e come si possa mutuare un approccio didattico di questo tipo all'interno delle istituzioni scolastiche più classiche. In altri termini un modello come quello che stiamo sperimentando può essere pensato per favorire nuovi approcci alla costruzione della conoscenza e delle competenze dei nostri allievi?

2. Le domande

Proviamo a scomporre la domanda in item più facilmente discutibili.

Perché pensare a nuovi paradigmi?

I curricula ministeriali possono essere "adattati"?

La classica esperienza "laboratoriale" delle nostre scuole favorisce lo sviluppo di quali capacità intrinseche¹?

E' possibile inserire nei curricula tecnologie innovative e open (e quindi sostenibili) anche se, a prima vista, poco attinenti con il contesto di inserimento?

E, spingendoci oltre, può essere pensabile un ambiente scolastico non più suddiviso per classi, bensì per tematiche di interesse coinvolgendo interi bienni piuttosto che trienni?

Per inciso gli allievi che partecipano al FabLab hanno età comprese fra gli 11 e i 21 anni, provengono perlopiù da istituti tecnici e licei e, cosa interessante, si "raggruppano" in modo eterogeneo a partire da interessi e curiosità comuni.

In queste riflessioni non vorremmo approfondire temi ben noti, ma provare ad avvicinare loro e a contestualizzare con loro un modello del "fare" che diventi

¹ Creatività, immaginazione, volontà ...

perno e volano per la costruzione della conoscenza, delle capacità e delle competenze. Un modello che acceleri considerevolmente l'attitudine dell'imparare ad imparare [1].

Questa idea è corretta, a nostro modo di vedere, se letta come la capacità di potenziare e sviluppare le competenze intrinseche che ogni nostro allievo possiede e che, tuttavia, rischiano di rimanere inespresse. Sono competenze che in natura fanno già parte del bagaglio umano. Si pensi alla capacità di immaginazione, di creatività, di ingegno puro, di volontà di sfida.

Il mercato del lavoro che le odierne generazioni di studenti dovranno affrontare sarà sempre più permeato da soluzioni automatiche. E non solo. Algoritmi in grado di suggerire soluzioni sulla base dell'elaborazione "velocissima" di enormi quantità di dati [2] saranno, e già lo sono, in grado di supportare e, in molti casi, di sostituire l'operato umano. L'operato, non il talento.

Allora il punto è proprio questo, dobbiamo sperimentare e usare modelli che favoriscano lo sviluppo delle competenze intrinseche. Tutto ciò che favorisce la sfera empatica, la creatività, la collaborazione e la condivisione [3]. Gli strumenti per stimolare un processo simile esistono e, a nostro parere, sono quelli che equipaggiano e accomunano molti FabLab.

Sono perlopiù tecnologie open che fanno leva sull'elettronica e l'informatica ma che non disdegnano alcuna teoria o logica operativa basata su qualsiasi altra disciplina. Anzi l'indice di integrazione e contaminazione tra le varie discipline è molto elevato.

Lo strumento basilare (può sembrare banale ricordarlo) resta il web, con la sua enorme potenzialità informativa, in grado di fornire supporto in ogni occasione. Tuttavia un approccio corretto va suggerito. Lo spirito critico va affinato, le fonti selezionate con cura. Il web, se ben usato, può restituire le indicazioni teoriche per affrontare la soluzione di problemi: le nozioni da acquisire, a casa, per poter affrontare, con l'aiuto di pari ed esperti, la realizzazione del progetto condiviso ed attuato nel FabLab.

Queste idee trovano riscontro rispettivamente in una teoria pedagogica, relativamente giovane, ed in una altrettanto giovane metodologia didattica.

Il connettivismo [4], introdotto da George Siemens nel 2005, fonda i suoi dettami sulle suggestioni di un sapere distribuito e in continua evoluzione, che trova la sua naturale dimora in internet. Il connettivismo, probabilmente ancora alla ricerca di solide e diffuse conferme, focalizza le sue indicazioni sulla pluralità di prospettive richieste nell'osservare e comprendere un sapere, sul doverlo, quanto poterlo confrontare con altri, sulla necessità di mantenerlo aggiornato e, non ultimo, sul bisogno di mantenere connesse le fonti di costruzione del sapere stesso.

La flipped classroom[5] è invece una metodologia che invita il docente a selezionare e proporre contenuti multimediali presenti perlopiù sul web (possibilmente di libera fruizione N.d.A.) per favorire la preparazione teorica degli allievi, che non sarà affrontata in aula, ma dove, e quando, l'allievo ritiene più opportuno. L'aula può divenire così il luogo per poter discutere i temi

affrontati ma, soprattutto, dove mettere in pratica esperienze basate sulla teoria appresa[6].

Il web² diventa allora, se non banalizzato, lo "scaffolding" naturale per lo sviluppo di progetti in FabLab.

Sarà quindi possibile immaginare una scuola senza classi, una scuola senza banchi e cattedre, allineati, messi in cerchio o a zig zag, ma con spazi per "fare" ?

Forse no ! Tuttavia una scuola dove i docenti formino una "rete" di competenze da fornire agli allievi e gli allievi sono da subito pronti a condividere la loro conoscenza con i loro pari, sì.

Una scuola in grado di cercare trame didattiche capaci di mescolare differenti discipline tra di loro a favore del talento, della creatività, della capacità di risolvere problemi. Bisognerà lavorare ai limiti imposti dalle propedeuticità. L'apprendimento più classico è basato, come è giusto che sia, su una serie di conoscenze graduali (verticali) e, tra di loro, propedeutiche. Tuttavia bisognerà dare spazio a modelli più orizzontali, capaci di mescolare l'esperienza e lo studio teorico orientandoli al risultato e alla capacità creativa. In questo caso il connettivismo suggerisce trame e strutture interessanti.

Una considerevole fetta di letteratura di dominio consiglia di "mutare" il paradigma classico dell'istruzione, di sicuro quella di base: primaria e secondaria. La necessità è palese, il sistema scolastico attuale presenta enormi legami strutturali, non più accettabili, con l'era storica in cui si è andato formando e consolidando: gli inizi del XX secolo.

La realtà lavorativa muta con velocità impressionante e questa accelerazione è data dalle tecnologie e dalle possibilità comunicative. L'automazione, gli algoritmi smart, l'analisi dei big data [7], le intelligenze artificiali assumono ruoli sempre più importanti nel processo lavorativo e produttivo in genere, togliendo di fatto molte opportunità all'uomo. Se la prima rivoluzione industriale ha trasferito, tra uomo e automa, gran parte del lavoro fisico, oggi assistiamo ad un graduale, quanto veloce passaggio delle attività cognitive [8] . Questi aspetti cruciali inducono a riflettere sull'attuale architettura del sistema educativo per renderla più idonea ai nuovi scenari sociali del XXI secolo. E' evidente quanto sia importante ripensare agli attuali modelli didattici e ai sistemi per trasferire e formare competenze da fare agire nel modo migliore ai nostri allievi. Questo è un punto d'attenzione netto e indistinguibile che, se ignorato, presenterà ben presto conti salati in svariati ambiti dell'attuale sistema sociale e lavorativo.

3 . L'esperienza FabLab

L'esperienza che vi presentiamo è un tentativo di risposta, se non a tutti, a molti degli interrogativi posti.

² Relativamente all'uso del web si pensi anche al fenomeno MOOC (massive open online course), alle OER (Open educational resource), agli attuali servizi di ricerca e navigazione e ai social network (più o meno caratterizzati da scopi didattici), che offrono strumenti idonei per costruire "personal learning environmet" adeguati.

L'attuale modello didattico nella scuola superiore è strutturato, come sappiamo, perlopiù in lezioni frontali che seguono (o dovrebbero seguire) un preciso percorso pianificato, per ciascun anno, da un programma ministeriale. Insegnanti che alternano lezione frontale a verifiche e interrogazioni³.

A questo modello dobbiamo aggiungere due osservazioni di dominio pubblico:

- gli insegnanti di ogni ordine e grado sono alla ricerca continua di elementi o metodi in grado di coinvolgere e interessare un target di discenti che, negli ultimi anni, è spesso disinteressato ad acquisire le competenze perché è profondamente mutato ed è in continua evoluzione⁴. Tutto sembra funzionale al voto e nulla più.
- Spesso il mondo del lavoro (particolarmente dopo la scuola dell'obbligo o dopo la maturità) richiede skill differenti da quelli "prodotti" dai tredici anni di percorso scolastico. Il mondo del lavoro richiede figure con competenze ampie, autonome, che siano in grado di orientarsi e diventare produttive in tempi brevissimi.

Si parla spesso di learning by doing, ma cosa significa o, ancor più, come si può applicare nel nostro modello scolastico / formativo ?

La nostra, seppur breve, esperienza con il FabLab di Ivrea ha tentato di dare una risposta agli interrogativi posti sopra ribaltando in toto il paradigma formativo descritto.

Cosa significa ?

In breve abbiamo chiesto ad alcuni ragazzi di partecipare (in orario prescolare extrascolastico) ad un "laboratorio" esterno alla struttura scolastica ed alcuni di loro (circa una ventina) hanno aderito al progetto (Il laboratorio ha sede nei locali del polo formativo OfficinaH di Ivrea).

Già dal primo incontro abbiamo concordato e condiviso le regole di un ambiente per loro nuovo: il FabLab.

³ Ovviamente si tratta di una triste semplificazione: sappiamo bene che esistono eccellenze neppure così rare, ma che purtroppo non fanno numero perché non supportate dal "sistema"

⁴ Le nuove generazioni sono bombardate di informazioni dalla rete, dalla scuola, dai canali informali e non formali. "Overload" informativo in contrapposizione alla necessità di "cercare" l'informazione che ha caratterizzato la nostra generazione. Cambia così il modello mentale che richiede rapide e continue operazioni di "filtro", di selezione per individuare ciò che realmente ci serve e che dobbiamo interiorizzare e legare agli schemi mentali. Da qui potrebbe derivare, a nostro avviso, un disinteresse diffuso nei confronti delle varie materie. Un secondo elemento è caratterizzato dal sistema che richiede di "monetizzare" le energie spese: voti, crediti formativi e poi CFU nell'università inducono il giovane a ragionare per "miglior profitto e non migliore competenza creando circoli viziosi pericolosi. Quanti studenti all'università frequentano un laboratorio o un seminario perché "dà più crediti di un altro".

Intendiamoci, non stiamo sminuendo il valore della valutazione, giammai, ma oggi il significato originale "premiante" è stato via via sostituito dalla ricerca del voto o del credito predominante anche sul sapere stesso.

4. Le regole

Regole semplici, immediate, chiare :

- è un luogo nel quale si "porta" il proprio contributo nella consapevolezza che la ricchezza (anche culturale) deriva da ciò che si porta e non da ciò che si prende;
- è un luogo nel quale la parola chiave è "condivisione" perché i migliori risultati sono il frutto di molte competenze e di molte "teste"⁵;
- non esistono gruppi precostituiti e attività pianificate;
- non esiste un voto o un "premio" per il migliore perché l'obiettivo non è primeggiare, ma arrivare insieme all'obiettivo;
- e' un luogo nel quale il discente deve essere proattivo;
- e' un luogo nel quale si fa, si costruisce, si crea e le competenze si acquisiscono perché "servono" per raggiungere l'obiettivo.

Negli ultimi tre punti, in modo particolare, sta il ribaltamento del paradigma.

Al primo incontro, intorno al tavolo, i tutor pongono senza indugio la seguente domanda: "bene, ora che facciamo ? "

Una domanda che crea dapprima un po' di smarrimento fra i presenti che in genere si guardano come a domandarsi "ora che succede?". Dopo poco però qualcuno prende coraggio e vuole capire meglio il senso della domanda che, chiaramente richiede una spiegazione di rinforzo.

La domanda ha una sola risposta ed è la seguente: all'interno del FabLab sono i ragazzi che devono proporre (proattivamente) un obiettivo da raggiungere che, insieme, dovranno raggiungere: indispensabile un idoneo brainstorming nel quale escono, via via, le proposte più inattese. Proposte talvolta molto fantasiose che, considerato che andranno realizzate, tendono sempre più ad orientarsi verso il concreto, pratico e utile: più proposte, più gruppi!

I gruppi devono avere, al loro interno, le competenze necessarie e quindi si torna al dialogo, alla collaborazione, a valorizzare le peculiarità e i contributi di ciascuno.

E' fondamentale che tutti i componenti del gruppo condividano l'obiettivo scelto perché è il processo che garantisce la costruzione della motivazione.

Bastano pochi minuti di entusiasmo dopo la scelta dell'obiettivo per arrivare alle fasi successive che, con semplicità, sono "ed ora che facciamo?" oppure "da dove si comincia?".

⁵ Spesso i ragazzi non conoscono il "lavoro cooperativo" come modalità di costruzione del sapere, ma, frequentemente, come scorciatoia per lavorare meno. La loro attività scolastica è prevalentemente individuale e, pur vivendo in un gruppo, il rapporto è fra il singolo e il docente. Raramente il risultato è frutto della sinergia.

Ovviamente i ragazzi non sanno come affrontare un progetto, come muoversi, quali passaggi servono, ecc. Ma sono motivati a raggiungere, quantomeno per spirito di competizione fra loro e fra i gruppi, l'obiettivo nel migliore dei modi.

E qui nasce un forte bisogno di competenza.

In questo contesto le competenze non sono più viste come "l'ennesimo contributo teorico" ma il tassello per portare avanti il lavoro.

Imparare a lavorare insieme, conoscere gli strumenti corretti, strutturare un progetto,

individuare i materiali, il benchmarking e quant'altro possa servire diventano competenze che loro chiedono, perché effettivamente servono e, combinazione, i docenti illustrano tali contenuti.

Può sembrare strano, ma questo passaggio cambia realmente la dinamica del rapporto fra discente e docente.

Il discente, anzi il gruppo coeso, ha bisogno di competenze e si fa proattivo per chiedere tali competenze ai docenti. E' sempre il gruppo a decidere i tempi.

Il percorso di apprendimento non è certo lineare perché dipende dalle soluzioni adottate, dai tempi di ciascun gruppo, dai leader naturali che spingono il gruppo e il progetto.

Un ultimo aspetto che, dall'osservazione, riteniamo importante sottolineare è il formidabile risultato ottenuto nella formazione tra pari.

Il linguaggio, il ritmo, la modalità di affrontare il problema e anche le soluzioni adottate sono differenti e più efficaci (a parità di tempo impiegato).

Le dinamiche che si sviluppano sono diverse, curiose e, talvolta, a noi anche incomprensibili, ma ugualmente efficaci per il target a cui sono rivolte.

Tali dinamiche però rafforzano la coesione del gruppo e la fiducia reciproca.

5. L'Open

La scelta rigorosamente "open"⁶ (strumenti e contenuti) della nostra offerta didattica ha inoltre dimostrato una valenza ulteriore nel contesto di apprendimento.

I nostri ragazzi sono abituati a fare la "lista della spesa" sul web prima ancora di iniziare qualsiasi cosa. La fase di "acquisto" è prerequisito per qualsiasi progetto e, di conseguenza presuppone una adeguato budget.

Per utilizzare una metafora di un collega dell'Accademia: i nostri ragazzi sono spesso abituati ad avere a disposizione 48 colori senza i quali neppure iniziano il lavoro.

E se cambiano le regole del gioco?

⁶ Il FABLAB Ivrea è un progetto di Accademia dell'hardware e software libero "Adriano Olivetti". Chiaramente abbiamo mutuato i principi dell'Associazione anche alle attività del fablab. Così ai ragazzi viene proposto sempre hardware libero (ad esempio Arduino) e software libero (programmi di modellazione Open, Linux, LibreOffice, ecc). Tutti gli strumenti da noi proposti sono sempre di provenienza Open Source per insegnare loro che spesso esiste una alternativa valida, sostenibile e etica.

Abbiamo fornito loro il colore rosso e il colore blu e abbiamo spiegato che si può costruire un intero mondo solo con il rosso e con il blu. E così è stato.

Costruire con ciò che si ha a disposizione non si ridurrà mai ad uno sterile montaggio, ma una acuta ricerca di soluzioni che richiedono la partecipazione attiva di ogni individuo, le competenze di tutti, le buone idee e la motivazione per "riuscire".

Il gruppo raggiunge il risultato e non il singolo.

Mutuando dagli insegnamenti di McLuhan [9] possiamo dire che avere due colori richiede un "riscaldamento" personale, una partecipazione attiva di grande coinvolgimento e, di conseguenza, sicura soddisfazione.

Questo esercizio stimola la creatività, la fantasia, l'arte di "arrangiarsi" lasciando il sapore d'avercela fatta con le proprie forze.

I due colori non vanno visti come un limite, ma come una ricchezza, un'opportunità di crescita e il superamento di barriere (virtuali o meno) che, spesso, siamo noi stessi ad autocostruire.

L'utilizzo delle risorse open garantisce inoltre illimitata disponibilità di informazione, di risorse aperte, condivise, libere.

6. Conclusione

L'esperienza di questi primi anni di attività è sicuramente troppo limitata per poter trarre conclusioni certe, tuttavia è più che sufficiente per esprimere alcune considerazioni e consigli. Il rapporto tra docente e studente, come già accennato, è estremamente delicato quanto importante: chi guida è il gruppo e non il programma. Al tempo stesso però il ruolo del docente-tutor è strategico per il buon funzionamento dell'intero impianto. La scelta dei progetti e percorsi è importantissima perché i ragazzi, talvolta, perdono di vista il giusto equilibrio: fattibilità del progetto in base alle risorse e ai tempi a disposizione per arrivare alla giusta soddisfazione e così via.

Ma ogni gruppo è una storia a sé e va studiato, occorre individuare leader naturali e distribuzione delle rispettive competenze.

Il resto si acquisisce sul campo.

La motivazione che, fra le innegabili fatiche, ci esorta a continuare e migliorare l'impianto è certamente l'entusiasmo che alcuni ragazzi (non certo tutti) manifestano nel "chiedere" (e proprio in questo sta la rivoluzione) di poter partecipare a più corsi perché ne hanno "bisogno", chiedono di venire in laboratorio giorni non previsti per il FabLab, arrivano con tre ore di anticipo, portano i loro amici e compagni di scuola.

Insomma: piccoli segnali importanti che testimoniano un "felice" cambiamento che, ci auguriamo, possano, esportati, produrre analoga soddisfazione.

Punti di forza di questo modello:

- lavoro in sinergia di gruppo
- apprendere per obiettivi
- alta motivazione in quanto "scelta" da ciascun discente
- acquisizione di competenze pratiche
- competenze su tutta la filiera del progetto
- soddisfazione d'aver realizzato un progetto con le proprie mani
- necessità di far convergere competenze teoriche con abilità pratiche
- Abituare i ragazzi a trovare soluzioni nuove a problemi nuovi nel contesto scelto
- Conoscere le nuove tecnologie attraverso il loro utilizzo effettivo

Punti di possibile criticità

- non esiste un programma didattico predefinito e predefinibile e questo richiede elasticità da parte della dirigenza e dei docenti
- competenze non "calendarizzabili"
- organizzazione dinamica dei docenti
- Applicabile a piccoli gruppi
- Elasticità nel sottoporre soluzioni nuove alle sollecitazioni ricevute.
- Disponibilità di laboratorio
- Alcune attività necessarie al progetto non possono essere svolte dai ragazzi e serve un "sistema" di consulenti che le prepari all'esterno: ad esempio lavori di falegnameria, metalli, lavorazioni pericolose o difficili.

Il FabLab è un servizio per la comunità, un luogo dove chi ha un'idea trova macchine, persone, processi, competenze, modalità per realizzare questa idea. Il movimento dei Maker è stato poi codificato e divulgato da alcune esperienze editoriali, come Make Magazine, una rivista americana che ha contribuito a dare "visibilità" a progetti di "fai-da-te creativo", frutto di competenze trasversali artistiche, tecniche, collaborative orientate a creare competenze, imparare a lavorare in team, imparare a "portare" per arrivare all'obiettivo sempre con la massima soddisfazione.

Il FABLAB Ivrea nasce nel 2014 come progetto sperimentale dell'Accademia. Oggi ha numerosi, quanto ambiziosi, progetti in itinere (alcuni in autonomia, altri in collaborazione con aziende del territorio e con l'Università), due partecipazioni alla Maker Faire di Roma e oltre 30 studenti che partecipano con regolarità alle attività. E' dotata di quattro stampanti 3D, due postazioni per modellazione, attrezzature di laboratorio elettronico e una vastissima gamma di schede e dispositivi Arduino (azienda del territorio con la quale è nata una spontanea quanto efficace collaborazione reciproca). www.facebook.com/fablabivreaanavese

7 - Bibliografia

(per tutti i siti indicati l'ultimo accesso è a marzo 2016)

- [1] http://archivio.pubblica.istruzione.it/normativa/2007/allegati/all2_dm139new.pdf
- [2] http://www.mckinsey.com/insights/strategy/artificial_intelligence_meets_the_c-suite
- [3] Brynjolfsson E., McAfee A.- 2014 The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies - W. W. Norton & Company, New York
- [4] Siemens G. – 2005 - *Connectivism: A learning theory for the digital age* - International Journal of Instructional Technology and Distance, DonEl Learning Inc, Thousand Oaks California
https://er.dut.ac.za/bitstream/handle/123456789/69/Siemens_2005_Connectivism_A_learning_theory_for_the_digital_age.pdf?sequence=1&isAllowed=y
- [5] https://it.wikipedia.org/wiki/Insegnamento_capovolto
- [6] Bonaiuti G., 2012 – *Flipping the classroom* - Università di Cagliari <http://people.unica.it/gbonaiuti/flipping-the-classroom/>
- [7] https://it.wikipedia.org/wiki/Big_data
- [8] Osborne M, Frey B., 2013 - *The future of employment: how susceptible are jobs to computerization* - Oxford University http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf
- [9] McLuhan M., 1964 - *Gli strumenti del comunicare*- Il Saggiatore, Milano

Biografie

Ugo Jacopo Avalle è nato a Torino e si laurea in Scienze della Comunicazione presso Università degli studi di Torino con il massimo dei voti. Si specializza in Informatica presso il Centro Studi Honeywell di Milano e consegue il master in E-learning presso l'Università di Firenze con 110 e lode. Appassionato di robotica e progettazione elettronica segue numerosi filoni di ricerca fra il mondo degli elettromedicali e l'elettronica industriale fino all'attività di sistemista informatico presso l'ASLTO4 di Ivrea. Dalla nascita (2011) è responsabile aziendale del progetto "elearning" con oltre 80 corsi e oltre 14000 presenze/anno.

Docente di sistemi, Informatica generale, applicata presso l'università di Torino (Scienze della Comunicazione, Infermieristica al POLO OfficinaH e ad Aosta) e Milano oltre a numerosi istituti di formazione superiore. Co-fondatore e presidente dell'Accademia dell'hardware e software libero "Adriano Olivetti" da cui nasce il progetto PADDI (2012) e, nel 2014, il progetto FabLab che coinvolge molte scuole del territorio eporediese.

Email: uavalle@gmail.com

Giovanni Aristodemo Leccisotti è nato a Foggia. E' laureato in Scienze dell'Informazione (Università degli Studi di Torino) ed ha conseguito un master in Metodi e Tecnologie per l'Elearning (Università degli studi di Firenze) con il massimo dei voti. Progettista di corsi definisce, in seno alla Regione Piemonte, profili professionali in ambito informatico. Partecipa alla realizzazione di diversi progetti tra cui "Fit-for Ecommerce" (EU 2001-2003) e "Paddi" (la patente per la didattica digitale, 2012). Svolge docenza in ambito universitario, aziendale e professionale, occupandosi perlopiù di informatica e didattica digitale. Svolge docenza e progettazione continuativa presso la Fondazione Casa di Carità Arti e Mestieri di Torino. Nel 2011 partecipa alla fondazione dell'Accademia dell'Hardware e del Software Libero Adriano Olivetti di Ivrea, di cui è membro del consiglio direttivo. Attualmente gli interessi maggiori sono rivolti all'open education e alle tecnologie open per la didattica.

Email: leccisotti@gmail.com



Il Software parla anche italiano

Damian A. Tamburri - Luca Guarini

Sommario

La tecnologia dell'informazione è costantemente in rapida evoluzione. Tenersi aggiornati e seguire tale evoluzione costituisce una vera e propria sfida, persino per gli addetti ai lavori di questa disciplina. Sono senz'altro numerose le riviste di settore specializzate nella divulgazione di tematiche informatiche cosiddette "scottanti": IEEE Software rappresenta la più autorevole di queste. Da anni riferimento imprescindibile per tutto ciò che riguarda l'attualità informatica proveniente dalle "trincee", là dove l'informatica prende vita, crea innovazione ed energia industriale. Nel presente articolo vi parleremo proprio di IEEE Software Italia e degli spunti "hot" contenuti nella sua edizione più recente.

Abstract

Information technology is constantly in rapid change - keeping up with the times can be a real problem, even for direct practitioners of the discipline. There are several magazines that specialize in providing clear and concise information about "hot" topics in the business - IEEE Software is among the top of such magazines, dealing for years with practitioners from the trenches, gathering and reporting their insights and experiences threading where computing comes to life, creating innovation and industrial creative energy. In this piece, we report on the Italian edition for IEEE Software, outlining some "hot" ideas and contents therein.

Keywords: IEEE Software; Software Magazine; Italian IEEE Software Translation; Software Engineering Insights; Industry and Academy

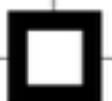
0

1

0

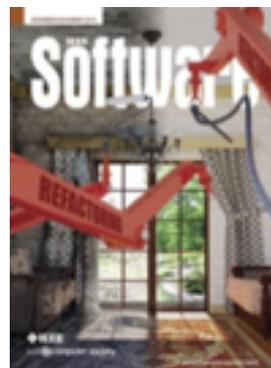
1

0



1. Introduzione

Come restare costantemente aggiornati sulle tematiche connesse alla ricerca e pratica software industriale? La risposta a tale quesito è *IEEE Software* [1]. IEEE Software è una rivista bimestrale edita da IEEE [4], una delle maggiori organizzazioni mondiali per l'ingegneria e l'automazione industriale, ivi compresa l'ingegneria del software. La rivista ha recentemente rinnovato la sua missione dotandosi di una nuova redazione, diretta al momento dal Prof. Diomidis Spinellis dell'Università di Atene, nome noto negli ambienti dell'ingegneria del software automatica e sociale. La nuova missione di IEEE Software è costruire la comunità leader di professionisti del software per il terzo millennio.



La rivista offre idee pionieristiche, analisi di esperti dalle suddette “trincee”, sia accademiche che industriali, oltre a suggerimenti e riflessioni destinate a sviluppatori e manager del settore. Tradurre la ricerca software in pratica è un altro degli orizzonti perseguiti.

Da qualche tempo la rivista si è preposta l'obiettivo di accrescere la propria visibilità attraverso numerose iniziative atte a raggiungere un pubblico prima non contemplato: piccoli imprenditori, istruttori, assistenti informatici secondari. Fra queste iniziative spicca la volontà di aumentare la propria tiratura attraverso edizioni “nazionali”, mirate cioè a rendere fruibili localmente, ovvero a livello nazionale, idee e concetti emersi dalle varie edizioni della rivista madre in lingua inglese [2]. Con questa nuova edizione IEEE Software intende essere un vero e proprio volano, atto a connettere sempre più la comunità dei praticanti software; allo stesso tempo, come detto, intende aumentare la propria visibilità e l'impatto dei propri contributi. Inoltre, un contributo fattivo di questa riedizione nazionale è la sua contestualizzazione con alcuni dei temi più sentiti dall'IT italiano, e.g., le esigenze crescenti di digitalizzazione nel nostro apparato governativo.

2. Un assaggio dei contenuti

Cosa troverete in IEEE Software? E in che termini? Lo standard dei contenuti e lo stile con cui gli stessi vengono trattati risultano essere incalzanti ed accessibili, tuttavia non mancano tecnicismi, corredati sempre da opportuni chiarimenti. Nell'ultimo numero reso disponibile (l'edizione Novembre / Dicembre), ad esempio, il caporedattore Diomidis Spinellis discute le tecniche ed i processi che gli ingegneri software hanno perfezionato per manipolare la complessità dei progetti software, il loro versioning, la collaborazione sottesa ai loro progetti di ingegneria del software per molteplici campi della ricerca e della tecnica. Al contempo il guru Grady Booch di IBM, esprime opinioni forti in merito al crescente interesse per l'intelligenza artificiale complessa: “molti sembrano spaventati dalle intelligenze artificiali superiori di questi giorni. Tali paure sono infondate e malriposte per via del controllo capillare che possiamo esercitare”, sottolinea l'eminente scienziato.

Oltre a trafiletti ed opinioni di grande interesse, troverete anche ricerche su tematiche solitamente considerate inaccessibili in molte riviste di settore: un esempio lampante è il cloud. Le automobili nella nube, o “la macchina connessa alla nube”. Cosa significa? IEEE Software fornisce in questa edizione un’introduzione accessibile e interessante ad una piattaforma di prototipazione per networking e inter-operazione/collaborazione di automobili connesse che fornisce una infrastruttura completa per tutte le applicazioni che vogliono interagire con macchine interconnesse. Siete degli ingegneri automatici o meccanici? Siete interessati al tema “security” delle vostre automobili? La piattaforma di cui sopra fornisce anche servizi comuni, come la manipolazione delle identità e la pervasività dei dati. La piattaforma è stata ideata per lo studio e l’ideazione di prototipi, con lo scopo ultimo di ridurre il time-to-market e accelerarne il successo industriale.

IEEE Software Italia è altro ancora. Siete degli avvocati interessati agli aspetti “legali” del codice o ai brevetti? In questa edizione la rivista offre spunti chiave relativi al tema del possesso intellettuale del codice [3]. Nel suo saggio “Code Ownership — a Quality Issue,” Sigrid Eldh insiste sulla necessità di adattare l’ownership ed il possesso del codice sorgente in situazioni specifiche, come la valutazione della qualità o il possesso sul corrispettivo codice di test. In un saggio simile, “Code Ownership — More Complex to Understand Than Research Implies”, Brendan Murphy presenta un’analisi più dettagliata e profonda del possesso del codice. Nella rivista troverete riassunti, interazioni ed opinioni su entrambi i saggi. Allo stesso modo potreste trovare articoli estremamente tecnici come lo “scrivere codice affidabile” del Turing Award Gerard J. Holzman. Holzman ricorda che scrivere codice affidabile significa essenzialmente comprendere e combinare limiti. Solo un numero finito di memoria è disponibile per la computazione, solo un ammontare finito di tempo esiste per completare la computazione, e ogni oggetto che catturiamo e manipoliamo deve essere finito e ben confinato. Gli stack hanno limiti, le code hanno limiti, il file-system e la sua capacità sono finite e persino i numeri-macchina sono finiti. Questi sono i confini del mondo dei computer, estremamente diverso dal mondo della matematica, tuttavia il numero di persone che considerano questi confini quando scrivono codice è troppo esiguo. Allo stesso modo, i colleghi Emerson Murphy-Hill, Don Roberts et Al. ricordano che, spesso, il refactoring si traduce essenzialmente nel cambiare il codice sorgente senza cambiarne il comportamento generale, tipicamente per migliorare il design del software - la vera arte nel farlo, è mantenere la qualità del comportamento originario pur alterando il sorgente utilizzato per ottenere tale comportamento. Gli articoli selezionati in questa edizione comprendono una vasta gamma di registri, dal racconto storico (i.e. “La Nascita Del Refactoring” di Griswold et Al.), ad un ritorno alle origini, alle esperienze più pratiche (i.e. “I Miti del Refactoring” di Hafiz) nel refactoring industriale, fino alla teoria pura che esplora nuove frontiere del refactoring e delle tecniche che ancora non sono apparse o state applicate.

3. Le rubriche periodiche

Gli spunti descritti in precedenza rappresentano solamente un assaggio di ciò che serba IEEE Software nel suo paniere. Ogni periodico contiene:

- *Editor's choice* - Un'introduzione ad un articolo scelto dall'editore capo, il quale generalmente tocca argomenti di particolare interesse per un pubblico prettamente industriale. Questa sezione tratta solitamente argomenti di immenso impatto innovativo o idee dirompenti su come introdurre innovazione nelle organizzazioni.
- *Riflessioni* - Argomenti "hot" accompagnati da riflessioni "d'autore", siano esse provenienti da scettici del settore o da professionisti che hanno confermato il valore di tali trend e argomenti con delle storie di successo industriale degne di nota.
- *Contributi su invito* - Contributi, su invito per l'appunto, ad opera di luminari dell'ingegneria del software o dell'innovazione industriale guidata dal software.
- *La voce dell'evidenza* - Argomenti che toccano la vera ricerca basata sull'applicazione rigorosa del metodo scientifico, applicazione tesa ad osservare e sperimentare fenomeni di interesse scientifico in merito alla disciplina dell'ingegneria del software. Questo mese, ad esempio, IEEE Software investiga l'evoluzione dei team di sviluppo software agili. Tramite l'analisi di nove team di sviluppo, i vari autori elaborano le idiosincrasie del processo sotteso. Ogni team adotta pratiche sulla base delle circostanze e adatta tali pratiche in base alle sfide incontrate in itinere. Basandosi su questa ricerca, gli autori propongono un questionario che agisce come una sorta di bussola, fornendo valori, decisioni e principi applicati in precedenza nella pratica industriale.,
- *Focus* - Una serie di articoli dedicati ad un particolare topic di impatto estremamente rilevante per la pratica industriale dell'ingegneria del software. I temi di questa sezione sono scelti accuratamente dall'intero board editoriale di IEEE Software e trasformati in validi campionamenti di interi settori di ricerca e del relativo stato dell'arte.
- *Punto/Contrappunto* - Che succede quando due ricercatori di fama mondiale, ma con punti di vista antitetici, vengono chiusi in una stanza virtuale a discutere dello stesso tema? La cronaca la troverete raccontata con uno stile libero e pacato proprio all'interno di questa sezione: di solito se ne vedono delle belle!

4. Conclusioni

In un mondo che si evolve sempre più velocemente e soggetto a pressanti ritmi e regole del mercato, IEEE Software si propone come una fonte inesauribile (purchè riusciate ad aspettare due mesi fra una rivista e l'altra!) di consigli, spunti, idee, prospettive e tecniche estremamente innovative, provenienti dalla pratica industriale e accademica dell'ingegneria del software. E' con questo che concludiamo la nostra introduzione, confidando di avervi convinti a dare uno

sguardo là dove i giganti dell'informatica raccontano dei loro esperimenti e prototipi di frontiera. Se abbiamo suscitato il vostro interesse non mancate di seguire i link che trovate in bibliografia, di rimanere in contatto con noi o addirittura di abbonarvi ad IEEE Software.

Bibliografia

- [1]<https://www.computer.org/web/computingnow/software>
- [2]<https://www.computer.org/cms/Computer.org/ComputingNow/docs/ieee-software-november-december-2015-table-of-contents-in-italian.pdf>
- [3]<https://www.computer.org/csdl/mags/so/2015/06/mso2015060018.pdf>
- [4]<https://www.ieee.org/index.html>

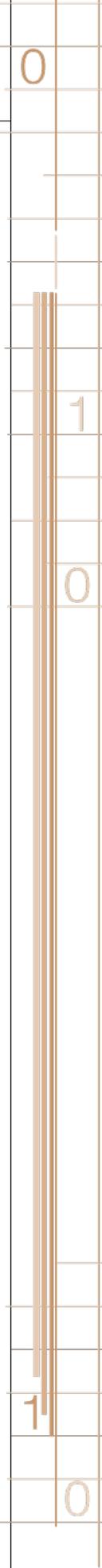
Biografia

Damian A. Tamburri è Research Fellow presso il Politecnico di Milano, in Italia. Damian ha completato il suo dottorato di ricerca presso la VU University Amsterdam, Paesi Bassi nel marzo 2014. Ancora agli inizi della sua carriera, ha pubblicato più di 30 volte sia in riviste che in conferenze top nell'ingegneria del software. I suoi attuali interessi di ricerca risiedono principalmente in ingegneria del software sociale e le architetture software avanzate.

Email: damianandrew.tamburri@polimi.it

Luca Guarini si è laureato col massimo dei voti in Teorie della comunicazione presso l'Università degli Studi di Firenze con una tesi su media e processi di legittimazione, prima di perfezionare le sue doti di comunicatore, editor e public relator in varie esperienze lavorative nell'ambito della comunicazione e della pubblica amministrazione in diversi paesi, quali il Regno Unito e l'Olanda. Luca è adesso permanent associate presso Amazon Ireland.

Email: luca@guarini.it



Le competenze digitali nella formazione.

Un progetto di didattica multimediale

Francesca Palareti

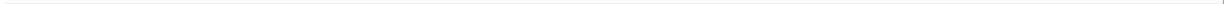
Sommario

Il contributo illustra il percorso formativo affrontato durante lo svolgimento della prima edizione del master sulle competenze digitali istituito presso l'Università degli Studi di Firenze, che ha portato alla realizzazione di un learning object sulla vita e le opere di Italo Svevo. Pubblicato sulla piattaforma "DidaSfera", l'e-book affronta la sfida di trattare un argomento "classico" sfruttando tutte le potenzialità offerte dalle nuove tecnologie. L'analisi della struttura del prodotto offre lo spunto per esporre alcune problematiche relative alla progettazione didattica e alle nuove competenze digitali richieste in ambito educativo.

Abstract

The paper illustrates the training process carried out within the first edition of digital skills master established at the University of Florence, which has led to the creation of a learning object on the life and works of Italo Svevo. The e-book was published on the platform "DidaSfera" and addresses the challenge of dealing with a classic subject by exploiting the potential offered by new technologies. The product analysis provides an opportunity to deal with some issues about instructional design and new digital skills required in education field.

Keywords: ePub, e-book, e-book tools, multimedia learning, digital skills, learning object, educational technology, digital divide, open educational resources



1. Introduzione

L'articolo rende conto del percorso formativo avviato nell'a.a. 2012-2013 e conclusosi l'anno successivo nell'ambito del master di primo livello "Le nuove competenze digitali: open education, social e mobile learning"¹, istituito presso il Dipartimento di Scienze della Formazione e Psicologia dell'Università degli Studi di Firenze.

In considerazione delle tematiche affrontate e del taglio operativo che ha caratterizzato il corso di studi il Comitato scientifico si è avvalso della collaborazione del Laboratorio di Tecnologie dell'Educazione [1] per la sua esperienza di ricerca nel campo del web e dell'*Instructional design*².

La tesi finale per il conseguimento del titolo del master ha previsto l'elaborazione progettuale e la conseguente realizzazione di un prodotto ad uso didattico, che si è proposto l'obiettivo di mettere a frutto le competenze digitali acquisite durante le attività online.

2. Organizzazione e struttura del master

2.1. Obiettivi

Collocandosi nella strategia Europe 2020 [2], il master ha cercato di fornire una risposta alla richiesta avanzata dall'OCSE al nostro Paese di sviluppare competenze digitali [cfr. riquadro 1] relative a progettazione, realizzazione ed erogazione di interventi formativi sostenuti dalle nuove tecnologie³. A tale riguardo il recente rapporto OCSE 2015 "Students, Computers and Learning. Making the connection" [3] evidenzia, però, come l'uso della tecnologia non comporti necessariamente un miglioramento nel rendimento, costituendo talvolta un fattore di distrazione per le carenze della pedagogia, incapace di sfruttare il potenziale offerto dalle nuove tecnologie. Ad oggi, infatti, non si riscontrano risultati apprezzabili conseguenti all'introduzione nelle aule scolastiche del digitale, da utilizzare invece in chiave di didattica innovativa. Elemento decisivo diventa, quindi, il ruolo degli insegnanti, volto non solo all'implementazione delle innovazioni tecnologiche, ma anche alla loro progettazione. In linea con questo contesto di riferimento l'obiettivo del percorso formativo è stato quello di sviluppare abilità relative all'utilizzo di *new social media* ed al loro rapporto con la formazione, dando particolare rilievo al

¹ Il master è stato coordinato dal Prof. Antonio Calvani, docente di Didattica e Pedagogia speciale presso l'Università degli Studi di Firenze.

² Processo volto ad individuare principi, metodi, contenuti e tempi relativi alla progettazione didattica per migliorare l'efficienza dell'apprendimento e di conseguenza la qualità didattica degli interventi educativi.

³ A livello nazionale nell'ambito delle strategie adottate per promuovere le competenze digitali è stato varato il Piano Nazionale Scuola Digitale (PNSD) a cura del MIUR a valenza pluriennale e contestualmente si è attivata la Coalizione italiana per le competenze digitali coordinata da AgID (Agenzia per l'Italia Digitale) che costituisce la declinazione del nostro Paese dell'Agenda Digitale Europea – una delle iniziative strategiche del piano di sviluppo dell'Unione Europea per la crescita e l'impiego – allo scopo di programmare interventi organici a favore dell'innovazione digitale.

momento della progettazione didattica e privilegiando contenuti e risorse educative aperte⁴.

2.2. Percorso formativo

Il master si è strutturato intorno a tre profili emergenti per la formazione: *Open Education Manager*, *Network and Mobile Learning Manager*, Esperto di *Media Education*⁵ e di Competenza digitale.

Le attività didattiche si sono svolte completamente a distanza in modalità *e-learning* attraverso *web conference*, con interazioni sincrone e asincrone via chat e forum.

A scopo propedeutico sono stati organizzati alcuni *webinar*, attivati in collaborazione con associazioni e case editrici interessate all'uso di *new media* e alla produzione di e-book – MED⁶ media education [4], Bibienne editrice [5], ePubEditor [6] – e con piattaforme di *social learning* come Insegnalo.it [7], ambienti web nati per gestire attività didattiche in modo condiviso.

Il percorso, articolato in sei moduli didattici⁷, si è completato con uno stage formativo e con lo sviluppo e la realizzazione di un *project work*.

3. Project work: genesi e struttura

La prova finale sostenuta a conclusione del corso di studi ha previsto lo svolgimento progettuale di un prodotto tecnologico costituito da un e-book, parte integrante della tesi. Nello specifico, dopo l'elaborazione di un progetto dettagliato, è stato realizzato un *learning object* multimediale per la didattica sulla vita e le opere di Italo Svevo [Fig. 1], che affronta la sfida di trattare un argomento "classico" con un percorso inconsueto, sfruttando tutte le potenzialità offerte dalle nuove tecnologie ed attingendo a risorse educative *open*.

3.1. Finalità, obiettivi e strategie didattiche

Sulla base delle competenze maturate in materia di *Instructional design*, è stata prestata particolare attenzione alla fase progettuale, definendo finalità, obiettivi e

⁴ OER (Open Educational Resources), materiali didattici in formato digitale resi disponibili con licenze che ne permettono il riutilizzo, la modifica e la distribuzione.

⁵ L'educazione ai media è un'espressione entrata in uso con lo sviluppo tecnologico dei mezzi di comunicazione di massa e si riferisce alla formazione delle capacità di utilizzarli opportunamente. Indica il processo di insegnamento e apprendimento centrato sui media, il cui risultato è la *media literacy*, intesa come capacità di saper "leggere" e "scrivere" i media. La *media education* si propone, quindi, di sviluppare sia una comprensione critica sia una partecipazione attiva.

⁶ Associazione italiana per l'educazione ai media e alla comunicazione, promuove lo studio dei media attraverso una prospettiva educativa, proponendosi come laboratorio di idee e di sperimentazioni.

⁷ 1. *Instructional Design* e progettazione didattica 2. *Open education* 3. *Social computing* e formazione 4. *Mobile e tablet based learning* 5. *Digital e media literacy* 6. Percorsi di *media education*.

strategie didattiche⁸ modellate sul target di utenza di riferimento; contestualmente è stato elaborato uno *storyboard* dettagliato della struttura dell'opera, schematizzato anche sotto forma di mappa concettuale realizzata con Mindomo, ed utilizzati strumenti *free* come aggregatori di risorse – Diigo, Google Drive, Blog – ai fini dell'organizzazione preliminare dei contenuti.

La finalità dell'e-book è quella di fornire strumenti per la costruzione di modelli funzionali di intervento all'interno di contesti educativi scolastici, proponendo un prodotto innovativo sia per l'argomento scelto sia per la struttura dei contenuti, che intende valorizzare la componente interattiva, ipertestuale e multimediale, mentre attualmente i libri di testo elettronici rappresentano per lo più la riproposizione digitalizzata della versione cartacea. L'utilità primaria, quindi, consiste nella possibilità di influire positivamente sulla motivazione ed il coinvolgimento degli studenti nello studio di uno scrittore classico, offrendo nuovi percorsi di conoscenza dell'autore.

Quanto agli obiettivi, ai fini della razionalizzazione del lavoro è stato definito un obiettivo didattico specifico⁹ per ognuno dei cinque capitoli¹⁰ in cui è articolata l'opera ed allestite adeguate prove di verifica dell'apprendimento. L'e-book, infatti, prevede l'utilizzo di diverse tipologie di strumenti di valutazione¹¹ per sequenzializzare le varie fasi dell'apprendimento ed accertare il livello di conoscenze e competenze raggiunto.

In relazione alle strategie didattiche volte a favorire il conseguimento degli obiettivi, è necessario premettere che comunicare un contenuto didattico non implica semplicemente trasmettere informazioni, ma attivare processi cognitivi complessi.

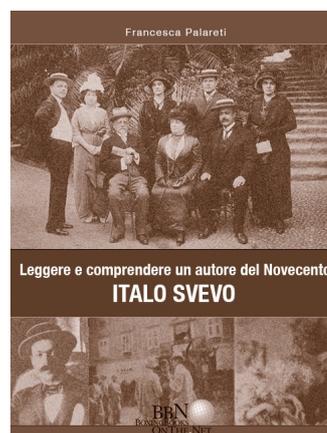


Figura 1.
Copertina dell'e-book

⁸ Per una trattazione sistematica delle strategie didattiche cfr. Bonaiuti G. [8].

⁹ Sono stati individuati i seguenti obiettivi: conoscere gli elementi rilevanti del contesto storico, sociale, filosofico e letterario legati alla figura di Svevo; conoscere la biografia dell'autore; conoscere le date di pubblicazione, la trama e i protagonisti dei tre romanzi principali di Svevo; conoscere le tematiche poetiche ricorrenti nei tre romanzi dell'autore: salute e malattia, psicoanalisi come strumento conoscitivo, inettitudine, vizio del fumo; comprendere i motivi del tardivo successo di Svevo e del cosiddetto "caso Svevo": il ruolo decisivo svolto da James Joyce ed Eugenio Montale.

¹⁰ 1. Contesto (storico, sociale, filosofico, letterario) 2. Biografia di Italo Svevo 3. Opere 4. Tematiche poetiche e stile 5. Fortuna dell'autore ed origini del "caso Svevo".

¹¹ La valutazione formativa, da intendersi come azione motivante oltre che funzionale al miglioramento, è requisito essenziale nel processo di apprendimento, che deve necessariamente essere rendicontabile.

La multimedialità e l'utilizzo delle ICT¹², come abbiamo visto, in assenza di un'attenta progettualità non mostrano di per sé potenzialità pedagogiche apprezzabili nelle performance scolastiche. La didattica non appare attualmente matura, ma ancora saldamente ancorata ai metodi tradizionali, orientata ad un approccio principalmente tecnologico privo di modelli teorici. Per rispondere a questa esigenza di implementare nuovi standard metodologici, nella realizzazione dell'e-book sono stati utilizzati strumenti volti a collegare nuovi saperi a quelli pregressi in un'ottica costruttivistica attivando preconcoscenze¹³, con l'intento di trasformare l'ambiente di comunicazione in ambiente di apprendimento. Sono stati privilegiati approcci *problem based* dal taglio non meramente erogativo e strategie mirate all'ibridazione tra percorsi mirati in presenza e spazi di apertura in remoto, con alternanza di momenti guidati in aula ed altri più aperti a distanza in fase di autoapprendimento in funzione dell'*expertise* degli studenti. Sono state adottate strategie di apprendimento prevalentemente di tipo meta-cognitivo strutturate sull'alternanza tra esperienza e riflessione e sullo sforzo di aumentare la consapevolezza – individuale e del gruppo-classe – non solo di *cosa* si stia imparando, ma anche di *come* sia necessario imparare. L'apertura intesa come autogeneratività porta ad autoregolazione, consapevolezza critica, sviluppo di autonomia.

A tal fine sono stati valorizzati gli elementi ipertestuali, multimediali ed infografici, utilizzando mappe concettuali, *timeline*¹⁴ e *slideshow*. L'*evidence based learning*, infatti, ha dimostrato da tempo il valore nel processo di apprendimento di infografiche e mappe interattive¹⁵, assai efficaci grazie alla loro capacità di tradurre graficamente relazioni tra i concetti avvalendosi del potenziale comunicativo delle immagini.

3.2. Caratteristiche e struttura dell'e-book

L'e-book, consultabile integralmente online, è stato concepito come un percorso in autoapprendimento rivolto agli studenti dell'ultimo anno della Scuola secondaria di II grado.

Intende costituire una guida introduttiva allo studio di Italo Svevo, illustrando il contesto storico-letterario, la vita, le opere ed il pensiero dell'autore triestino. La trattazione, che in prospettiva futura potrà essere integrata con l'inserimento di schede di approfondimento su singole tematiche, si focalizza sull'inquadramento interdisciplinare dell'autore, al centro di una nuova cultura mitteleuropea fervida di impulsi culturali e di innovazioni che coinvolgono ancor

¹² Il termine, acronimo di *Information and Communications Technology*, indica l'insieme delle tecnologie che consentono il trattamento e lo scambio delle informazioni in formato digitale.

¹³ La capacità del soggetto di stabilire un collegamento tra quanto già sa e le nuove conoscenze costituisce un elemento basilare di ogni processo di apprendimento. A tale riguardo è più in generale in relazione alle *guideline* da seguire per una didattica efficace cfr. Calvani A. [9].

¹⁴ Sull'utilizzo della *timeline* nella didattica cfr. Palareti F. [10].

¹⁵ Per un'analisi sistematica sull'utilizzo delle mappe nella didattica cfr. Fogarolo F., Guastavigna M. [11]

prima del campo letterario quello storico, sociale, filosofico ed artistico dell'epoca, privilegiando la narrazione per tematiche ed esperienze significative.

Viene, in tal modo, incoraggiato un nuovo metodo di studio letterario dei classici, sottolineando l'incidenza del contesto nella formazione e negli esiti letterari di un autore, con l'intento di favorire negli studenti la capacità critica ed agevolare l'apprendimento, antepoendo le capacità fruibili a quelle produttive, facendo leva ancor prima che sull'analisi di testi esemplificativi sulla visione e sull'ascolto, attivo e consapevole, propedeutici alla produzione testuale.

Il percorso formativo aggrega al suo interno diverse OER disponibili in rete, distribuite con licenze libere di tipo *Creative Commons*¹⁶, ed include l'utilizzo di strumenti tecnologici liberamente accessibili online – Mindomo, Dipity, Prezi – allo scopo di integrare le fonti reperite in un percorso didattico organico nell'ottica di una condivisione aperta del sapere. Per altre risorse inserite nell'e-book coperte da copyright è stata ottenuta la liberatoria da autori ed enti che ne detengono i diritti.

È suddiviso in cinque capitoli, ciascuno dei quali presenta una parte teorica integrata con elementi multimediali ed una di esercitazione. Chiudono l'e-book tre appendici: la prima dedicata alla "Cronologia" della vita e delle opere di Italo Svevo sotto forma di *timeline* [Fig. 2] realizzata con Dipity, la seconda al "Glossario" dei termini chiave ricorrenti e la terza ai "Materiali di approfondimento" – bibliografia, sitografia, corsi online su Italo Svevo.

L'opera è navigabile sia in modo guidato tramite l'indice, che mostra la sequenza dei vari capitoli in cui è suddivisa la trattazione, sia liberamente selezionando gli argomenti di proprio interesse, dal momento che ogni capitolo è strutturato in modo tale da godere di una propria autonomia argomentativa. Viene, quindi, suggerito un procedimento sequenziale per nuclei tematici fondamentali, ciascuno dei quali corrispondente ad un preciso capitolo in cui è articolato il progetto. Segmentare le unità didattiche, infatti, risulta una tecnica efficace nel processo di apprendimento, alleggerendo il

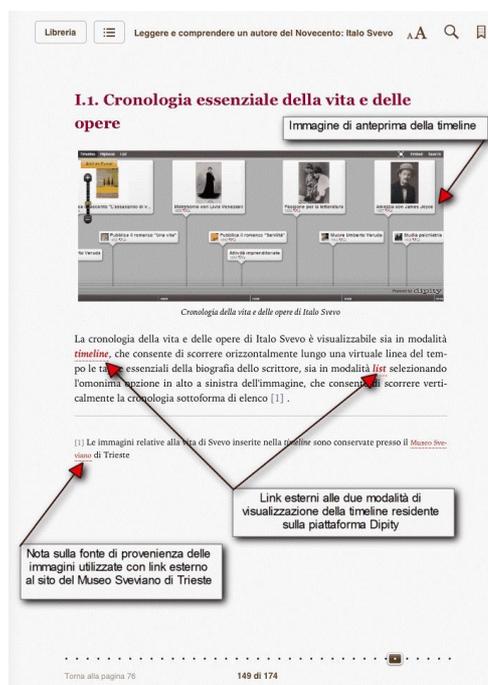


Figura 2.
Pagina illustrativa della timeline

¹⁶ Licenze di tipo copyleft che permettono agli autori di scegliere e comunicare quali diritti riservarsi e a quali diritti rinunciare a beneficio dei destinatari. Forniscono un modo semplice e standardizzato per concedere pubblicamente il permesso di condividere ed utilizzare il lavoro creativo in base alle condizioni stabilite dagli autori.

carico cognitivo. In alcuni casi glosse, caratteri diversificati, schemi, integrazioni audio/video possono offrire un supporto specifico per lievi disturbi dell'apprendimento.

Accanto all'approccio lineare viene proposta un'apertura ipertestuale controllata con spazi per approfondimenti guidati su web; inoltre a partire dal testo base vengono indicati successivi livelli di analisi con note contestuali [Fig. 3], appendici, sitografia, bibliografia.

Libreria Leggere e comprendere un autore del Novecento: Italo Svevo

5.3. James Joyce, Lettera a Italo Svevo

Victoria Palace Hotel, 6 rue Blaise Desgoffe, Parigi, rue de Rennes 30 gennaio 1924 [1]

Caro amico,
[...] Grazie del romanzo con la dedica. Ne ho due esemplari anzi, avendo già ordinato uno a Trieste. Sto leggendolo con molto piacere. Perché si disperse? Deve sapere ch'è di gran lunga il suo migliore libro. Quanto alla critica italiana non so. Ma faccia mandare degli esemplari a stampa a M. Valéry Larbaud... Mr. Benjamin Crémieux... Mr. T.S. Eliot, Editor... Mr E.M. Ford... Parlo-
ter-
nito.
ma:
esse
app-
ver-
la.

[2] Livia Veneziani nella già citata Vita di mio marito aveva parlato dell'apprezzamento di Joyce espresso anche per i primi due romanzi di Svevo con queste parole: "Mio marito gli presentò a sua volta i due volumi dimenticati, prima *Una vita*, per il quale aveva una particolare tenerezza, e poi *Semilità*, come per dirgli: *Anch'io fui uno scrittore*. Joyce li lesse subito e durante la lezione successiva dichiarò che secondo la sua opinione Svevo era stato ingiustamente negletto. Aggiunse con calore che certe pagine di *Semilità* non avrebbero potuto scriverle meglio i più grandi maestri del romanzo francese"

Nota contestuale di approfondimento

Torna alla pagina 76 141 di 174

Figura 3.
Utilizzo della nota contestuale

dotazione ai singoli studenti. Un prodotto, quindi, fruibile a scopo dimostrativo, volto a promuovere un nuovo impianto metodologico, capace di integrare la conoscenza teorica di base con le nuove tecnologie dell'informazione, coniugando in tal modo tradizione ed innovazione senza rinunciare al dovuto rigore dei contenuti.

Il modello proposto per coerenza ed organizzazione strutturale risulta replicabile in un'ottica sistematica per lo studio di altri classici della letteratura, di conseguenza potrebbe costituire la prima unità didattica all'interno di un

¹⁷ Sono state privilegiate le attività *problem based* allo scopo di ottimizzare la capacità di studio ed acquisire una competenza fondamentale, il *digital reading*, la capacità cioè non solo di saper leggere testi su internet, ma anche di orientarsi tra le fonti e filtrare le notizie rilevanti e autorevoli dal web.

progetto più strutturato, il primo *item* di una collana *Leggere e comprendere un autore del Novecento*.

3.3. Realizzazione tecnica e distribuzione

Il *project work* è stato sviluppato utilizzando ePubEditor, software che permette di realizzare, anche in modo condiviso e collaborativo, e-book multimediali ed interattivi. È stato esportato in formato ePub3¹⁸ ed HTML5 allo scopo di renderlo *multidevice* e *multiplatforma*, quindi accessibile da qualunque dispositivo e browser indipendentemente dall'utilizzo di hardware o software specifici.

Il suo valore aggiunto risiede nella spendibilità immediata grazie all'inserimento nella piattaforma "DidaSfera" [12], ambiente digitale all'interno del quale risiede tra i supporti per la didattica, collocazione che lo rende fruibile da qualunque *device* di lettura.

Il testo originale integrale è consultabile dalla pagina di "Introduzione" dell'e-book sia online in modalità streaming nella versione web utilizzando un qualunque browser sia offline in modalità download in versione ePub3¹⁹.

Ai fini dell'accessibilità e dell'usabilità sono stati adottati criteri di alta leggibilità, testo alternativo delle immagini, indici navigabili, approccio top-down e mappa interattiva dei contenuti, medesimo layout ed immagine di immediata associazione con i contenuti testuali per identificare contenuti affini, rispettando il criterio della coerenza comunicativa²⁰.



Figura 4.
Inserimento di una video lezione

¹⁸ La versione 3 del formato ePub – standard aperto ufficiale per la pubblicazione di libri elettronici – è basata sulla tecnologia HTML5, che consente di rendere interattivo e multimediale un libro digitale grazie alla possibilità di inserire documentazione audio e video.

¹⁹ In quest'ultimo caso è necessario installare Radium – estensione di Google Chrome – su PC, mentre per la fruizione da dispositivi mobili sono disponibili applicazioni dedicate, diversificate a seconda dell'hardware e del sistema operativo utilizzato. Tali software consentono non solo di riproporre su digitale le funzionalità proprie del cartaceo – note, sottolineature, segnalibri – ma anche di integrarne altre proprie del formato elettronico, come la possibilità di selezionare tipologia, colore e dimensione del carattere, di regolare la luminosità dello schermo, di ricercare termini chiave all'interno dell'e-book e di sincronizzare lo stato di lettura con altri dispositivi.

²⁰ Per una trattazione sistematica dei principi di comunicazione visiva e multimediale nella didattica cfr. Calvani A. [13].

La distribuzione dell'opera via web – *rilasciata* con licenza *Creative Commons BY-NC-ND 4.0*²¹ – che si affianca a quella di consultazione offline fa dell'e-book un *learning object* condivisibile sui *social network*, ambienti informali di apprendimento collaborativo che negli ultimi anni hanno dato un impulso decisivo alla diffusione del *social learning* [cfr. riquadro 2]. Il loro impiego, crescente in contesti formativi, fa emergere una nuova dimensione sociale della cultura ed esercita un impatto pervasivo non solo sulle pratiche di socializzazione, ma anche sulle modalità di fruizione e produzione del sapere²².

4. Conclusioni

Abbiamo visto come la rivoluzione digitale abbia modificato radicalmente gli scenari della didattica e dell'apprendimento e come di conseguenza i prodotti destinati alla formazione debbano necessariamente adeguarsi ai processi in atto, in particolare allo scopo di promuovere quelle competenze digitali che da alcuni anni sono al centro del dibattito internazionale.

Accanto alla necessità di un'accurata progettazione didattica, infatti, problematica prioritaria è proprio quella del *digital divide*²³ e delle competenze digitali, fattori che richiedono da una parte investimenti infrastrutturali con spendibilità di lunga durata, dall'altra progetti sostenibili mirati al *lifelong learning*. La capacità di utilizzare in modo efficace gli strumenti digitali dipende ancora in modo significativo dalle diverse competenze di alfabetizzazione di base, che richiedono l'acquisizione di abilità trasversali in una nuova organizzazione del sapere sempre più "collettivo".

A tale riguardo, nonostante alcuni segnali positivi, i dati ISTAT ed Eurostat relativi alle competenze digitali mostrano un'Italia ancora in grave ritardo rispetto ai maggiori Paesi europei, con un analfabetismo digitale imputabile alla disaffezione politica verso il valore del sapere, oltre ad una incapacità di fondo nel gestire il cambiamento e la progettazione a medio-lungo termine²⁴.

È prioritario delineare azioni di sviluppo delle competenze digitali come elementi centrali del piano di diffusione di programmi infrastrutturali di crescita, definendo obiettivi annuali ed enfatizzando la misurazione dei risultati.

Attualmente, comunque, a fronte delle numerose criticità ancora da arginare, si riscontra una certa sensibilizzazione ai temi delle competenze e dell'inclusione, che di recente ha portato a prevedere nel Piano Nazionale Scuola Digitale la

²¹ BY (Attribuzione) – NC (Non commerciale) – ND (Non opere derivate).

²² Sulle potenzialità educative dei social network cfr. Ranieri M., Manca S. [14].

²³ Le linee di intervento definite nell'ambito delle competenze digitali di base si fondano su quanto previsto dal pilastro 6 dell'Agenda Digitale Europea *Enhancing digital literacy, skills and inclusion*, i cui obiettivi sono la realizzazione della cittadinanza digitale – accesso e partecipazione alla società della conoscenza, con una piena consapevolezza digitale – e dell'inclusione digitale – uguaglianza delle opportunità nell'utilizzo della rete e per lo sviluppo di una cultura dell'innovazione e della creatività – per prevenire il digital divide.

²⁴ Sui ritardi del nostro Paese in campo digitale cfr. Iacono N. [15].

figura dell'animatore digitale. Individuato tra gli insegnanti come esperto del settore, ha il compito di gestire le attività di formazione interna del personale docente, di proporre metodologie e soluzioni innovative per la didattica e di monitorare il processo di informatizzazione della scuola di appartenenza.

In tale contesto potrebbe configurarsi come valore aggiunto la possibilità per i docenti di avvalersi di testi didattici interattivi completi come quello illustrato, realizzati con media differenti e consultabili da qualunque dispositivo di lettura anche in modalità remota. L'ulteriore vantaggio della redazione condivisa, strumento avanzato offerto da diverse piattaforme per la creazione di e-book, è in grado di promuovere le capacità collaborative e la costituzione di gruppi di studio, in una dimensione sempre più etica e partecipativa dell'apprendimento.

RIQUADRO 1 - La competenza digitale

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet²⁵.

Sulla base delle Raccomandazioni europee la competenza digitale consiste nel saper esplorare ed affrontare in modo flessibile situazioni tecnologiche nuove, nel saper analizzare, selezionare e valutare criticamente dati e informazioni, un'attitudine critica e riflessiva nei confronti delle informazioni ed un uso responsabile dei mezzi di comunicazione interattivi. Implica, quindi, la capacità di avvalersi del potenziale delle tecnologie per la rappresentazione e soluzione di problemi e per la costruzione condivisa e collaborativa della conoscenza, mantenendo la consapevolezza della responsabilità personale, del confine tra sé e gli altri e del rispetto dei diritti/doveri reciproci. Il dato di fatto che ad oggi sembra emergere è che tali competenze vengano acquisite sempre più spesso in maniera informale al di fuori dell'ambito scolastico.

²⁵ Cfr. Unione Europea, *Raccomandazione del Parlamento Europeo e del Consiglio relativa a competenze chiave per l'apprendimento permanente, 2006/962/CE* [16].

RIQUADRO 2 - Social learning

Il valore educativo del *social learning* per la costruzione di conoscenza, sottolineato da tempo in ambito didattico, affonda le proprie radici nella teoria dell'apprendimento sociale sistematizzata da Albert Bandura [17], psicologo canadese di fondamentale importanza nel passaggio dall'approccio comportamentista alla nascita della teoria sociale cognitiva. Si soffermò sulle strutture cognitive alla base dei comportamenti ed evidenziò come l'apprendimento non implicasse esclusivamente il contatto diretto con gli oggetti, ma avvenisse anche attraverso esperienze indirette, sviluppate attraverso l'osservazione di altri. Il comportamento sarebbe, quindi, il risultato di un processo di acquisizione graduale delle informazioni, sottolineandone l'impatto sul processo cognitivo.

Il *social learning* facilita il docente nel compito di formare gli studenti attraverso un percorso dinamico di scoperta consapevole dei contenuti, degli ambienti e degli strumenti. La produzione collaborativa e la possibilità di condivisione consente di consolidare le competenze digitali relative all'area della comunicazione, della creazione dei contenuti e del *problem solving*.

Lo spazio fisico della classe si apre, quindi, alla partecipazione di nuovi membri e alla fruizione in autonomia libera da vincoli spazio-temporali, diventando laboratorio di competenze e di cittadinanza digitale²⁶.

Bibliografia

Ultimo accesso ai siti web: 30 aprile 2016

- [1] <http://www.lte.unifi.it/>
- [2] http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/index_it.htm
- [3] http://www.keepeek.com/Digital-Asset-Management/oeecd/education/students-computers-and-learning_9789264239555-en#page1
- [4] <http://www.mediaeducationmed.it/>
- [5] <http://www.bibienne.com/>
- [6] <http://www.epubeditor.it>
- [7] <http://www.insegnalo.it/>
- [8] Bonaiuti, G. (2014). *Le strategie didattiche*, Carocci Faber
- [9] Calvani, A. (2011). *Principi dell'istruzione e strategie per insegnare. Criteri per una didattica efficace*, Carocci
- [10] Palareti, F. (2014). "L'uso della timeline nella didattica: ambiti di applicazione, caratteristiche e funzionalità", *Bricks*, 1, 162-173

²⁶ Cfr. Troia S. [18].

- [11] Fogarolo, F., Guastavigna, M. (2013). *Insegnare e imparare con le mappe. Strategie logico-visive per l'organizzazione delle conoscenze*, Erickson
- [12] <http://didasfera.it/didattica/s2-supporti-didattici>
- [13] Calvani, A. (a cura di) (2011). *Principi di comunicazione visiva e multimediale. Fare didattica con le immagini*, Carocci
- [14] Ranieri, M., Manca, S. (2013). *I social network nell'educazione. Basi teoriche, modelli applicativi e linee guida*, Erickson
- [15] Iacono, N. (2015). "Competenze digitali: come recuperare i ritardi nel 2016", *Agenda Digitale*, 30 dicembre
- [16] <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32006H0962>
- [17] Bandura, A. (1977). *Social learning theory*, Prentice Hall
- [18] Troia S. (2015). "Educare alle competenze digitali: costruire esperienze d'apprendimento in Edmodo", *Bricks*, 4, 9-18

Biografia

Francesca Palareti, laureata in Lettere classiche, lavora presso la Biblioteca di Scienze sociali dell'Università di Firenze. Si occupa di formazione, redazione web, risorse digitali ed in particolare di e-book. Ha conseguito il master di I livello "Le nuove competenze digitali", nell'ambito del quale ha realizzato un e-book pubblicato sulla piattaforma "DidaSfera". Collabora con i periodici TD: Tecnologie didattiche, Bricks, AIB Notizie, DigItalia ed ha curato un contributo relativo a Percorsi di Media Education contro la discriminazione – Attivismo online e networking su e-EAV e-Engagement against violence. È coautrice del volume "Architettura della biblioteca e identità universitaria" (S. Bonnard, 2007).

Email: francesca.palareti@unifi.it