

CORSI DI STORIA DELL'INFORMATICA NELLE UNIVERSITÀ ITALIANE

In coerenza con il costante impegno nel preservare la memoria storica dell'Informatica, AICA ha varato un'iniziativa di durata triennale grazie alla quale dodici università propongono per la prima volta un corso di storia dell'informatica. Dopo aver discusso la rilevanza culturale, le motivazioni e le finalità del progetto, si espongono i risultati conseguiti e le esperienze maturate nei primi due anni di attività. Si conclude con una riflessione su come, al termine del triennio, si potrà valorizzare il lavoro svolto dando all'iniziativa un seguito visibile e duraturo.

1. INTRODUZIONE

La missione di un'associazione con le caratteristiche di AICA non può prescindere dall'impegno a coltivare, promuovere e diffondere la memoria storica dell'informatica.

Un impegno che si affianca ai molti altri che l'Associazione si è assunta e dai quali possono trarre beneficio i suoi soci, i professionisti del settore e il pubblico in generale.

Un impegno che si è tradotto in azione concreta nell'ormai lontano 1984, quando un apposito gruppo di lavoro fu istituito per iniziativa di Giorgio Sacerdoti, allora presidente AICA¹.

Ma, col tempo, la partecipazione attiva al gruppo di lavoro si è rivelata assai problematica in quanto le sue finalità non trovavano riscontro nelle attività professionali

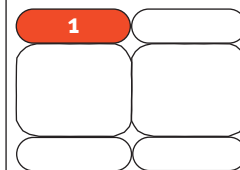
correnti – accademiche o aziendali che fossero – dei pur numerosi interessati all'argomento.

Si è quindi passati alla formula del “Progetto storia dell'Informatica” inteso come linea di attenzione continua entro la quale intraprendere singole iniziative focalizzate su obiettivi precisi e attorno alle quali coagulare di volta in volta le competenze professionali più appropriate oltretutto, beninteso, risorse economiche ed eventuali *partnership* con aziende, enti e istituzioni culturali.

Diverse manifestazioni di notevole rilievo hanno confermato l'efficacia di tale approccio che è risultato estremamente flessibile e che è tuttora in atto.

Tra quelle di maggior impegno e successo si ricordano: la mostra storica in occasione del con-

Corrado Bonfanti



¹ In alcuni congressi annuali AICA di quel periodo, è stata inserita una sessione “storica”, curata per l'appunto dal Gruppo di lavoro; i relativi contributi sono pubblicati negli atti.



gresso AICA di Trento (1987), il convegno internazionale sulla storia e preistoria del calcolo automatico (Siena, 1991 – Figura 1) che, accanto a quelli italiani, ha visto la partecipazione di relatori provenienti da sei Paesi stranieri, e la grande rassegna dal titolo “Per fili e per segni – Ingegno italiano e società dell’informazione” (Genova, 2004 – Figura 2). Ad esse si è aggiunta di recente un’inedita iniziativa rivolta al mondo accademico – docenti e studenti – con cui AICA promuove

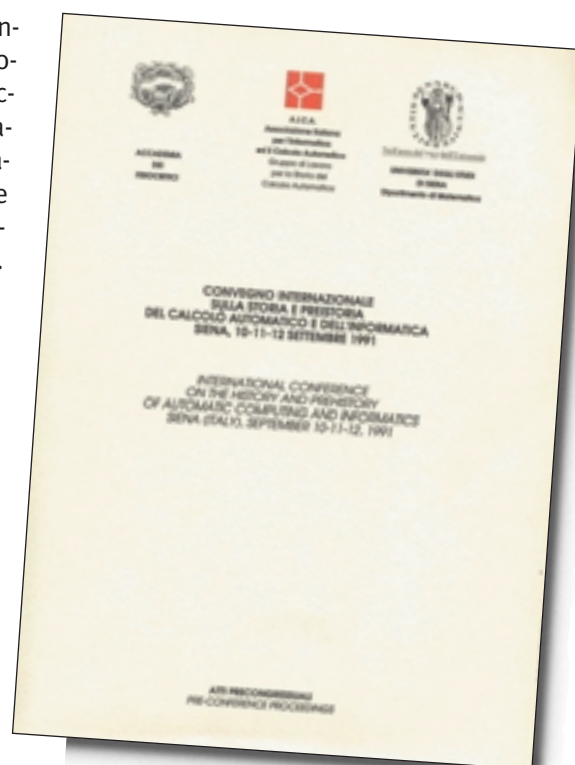


FIGURA 1

Atti del Convegno internazionale sulla storia e preistoria dell'informatica organizzato da AICA a Siena nel 1991, nel 750° anno dell'Università



FIGURA 2

Alcuni padiglioni della mostra Per fili e per segni organizzata da AICA nel 2004 a Genova '04, in occasione di Genova Capitale Europea della Cultura. La mostra, che si estendeva su un'area di 3.000 m², raccontava l'evoluzione storica e le prospettive delle Tecnologie ICT



ve e sostiene l'insegnamento della storia dell'informatica nelle università italiane; iniziava che ha preso il nome convenzionale di "Corsi AICA per la storia dell'informatica" ovvero, in breve, "Corsi AICA".

Il progetto coinvolge dodici atenei che sono stati a suo tempo individuati di concerto con i presidenti dei gruppi GRIN e GII, rispettivamente per le facoltà di scienze e di ingegneria (riquadro).

Il contributo di AICA consiste in primo luogo

SEDI E DOCENTI DEI CORSI AICA SULLA STORIA DELL'INFORMATICA

Univ. di Palermo¹ – *Filippo Sorbello*

Univ. del Sannio, Benevento¹ – *Michele Di Santo*

Univ. di Roma La Sapienza¹ – *Giorgio Ausiello*

Univ. di Pisa² – *Fabrizio Luccio*

Univ. di Bologna e Polo di Cesenaz – *Giorgio Casadei*

Univ. di Venezia Ca' Foscari² – *Marcello Pelillo*

Univ. di Udine² – *Corrado Bonfanti, Paolo Giangrandi*

Univ. di Verona² – *Alfio Andronico, Vincenzo Manca*

Univ. di Genova¹ – *Gerardo Costa, Arrigo L. Frisiani*

Univ. di Milano "Statale"² – *Mario Italiani, Gianfranco Prini*

Univ. di Milano Bicocca² – *Mauro Pezzè*

Politecnico di Torino¹ – *Alfredo Benso, Angelo R. Meo*

¹ Facoltà d'Ingegneria (GII)

² Facoltà di Scienze (GRIN)

nell'assumere a proprio diretto carico, per tre anni accademici a partire dal 2005-2006, la retribuzione dei docenti ai quali le rispettive università, in piena autonomia, hanno affidato il corso a titolo gratuito.

Obiettivo di fondo dell'iniziativa è quello di favorire lo stabilirsi nella comunità accademica di un'attenzione durevole nei confronti di questa materia; attenzione che possa in

seguito consolidarsi in forma "istituzionale", almeno presso alcune sedi. In questo senso il supporto offerto da AICA va considerato come un periodo di sperimentazione e di avviamento la cui durata dovrebbe risultare commisurata allo scopo.

La storia dell'informatica è infatti già da parecchi anni – e specialmente nei Paesi anglofoni – una materia largamente praticata a livello di singoli specialisti, di un'autorevole e ormai corposa letteratura² e di stabile inserimento nei *curricula* universitari.

L'iniziativa AICA aderisce a questa tendenza generale e inoltre contribuisce a portare all'attenzione della comunità nazionale e, si spera, di quella internazionale, la finora alquanto negletta storia dell'informatica italiana e i non trascurabili contributi che il nostro Paese ha dato in campo teorico, tecnologico e industriale³.

2. CULTURA (NON SOLO) INFORMATICA

È del tutto naturale porsi almeno un paio di domande faticose e pregiudiziali. Ha senso parlare di una storia dell'informatica? A che scopo coltivarla e insegnarla? Sono questioni su cui si potrebbe – e si dovrebbe – dibattere a lungo; azzardo qualche cenno di risposta, a titolo personale ma non senza il conforto di altre numerose voci.

Alla prima domanda risponde il fatto che l'informatica – pur nell'articolarsi in filoni specialistici e nel condividere ampie zone di confine con le discipline contigue – ha da tempo conseguito lo *status* di disciplina autonoma e globalmente riconoscibile. Ne è prova la semplice esistenza dei corsi di laurea ad essa pur

² Quanto alla letteratura, l'estensione e la profondità del fenomeno si possono percepire considerando che l'autorevole *quarterly* "IEEE Annals of the History of Computing" è giunto alla sua ventinovesima annata e che la mia biblioteca personale – un campione quindi largamente incompleto – comprende non meno di duecento titoli sull'argomento, tra storie generali, monografie, atti di convegni, memorialistica e opere "classiche". Se poi si preferisce navigare nel *mare magnum* di internet, non c'è che l'imbarazzo – e la difficoltà – della scelta.

³ Sulla scia del citatissimo "Informatica: un'occasione perduta" (L. Soria; Einaudi, 1979), negli ultimi anni sono comparsi diversi libri di buon livello – memorialistica e saggistica – comprensibilmente incentrati sulle vicende dell'Olivetti. Si tratta però di lavori scritti "da italiani per italiani" dei quali non risulta infatti alcuna traduzione in altre lingue. Cade a proposito il commento fatto per iscritto, in margine a uno dei "corsi AICA", da una studentessa di madrelingua inglese: "*La storia italiana dell'informatica, spesso non racconta, mi ha fatto comprendere lo stile dell'informatica in Italia, altrimenti incomprensibile*".

variamente intitolati⁴. Dal momento che una disciplina esiste, coltivarne la storia è un “atto dovuto” in termini di dignità scientifica e di consapevolezza professionale, al pari di quanto avviene per esempio per la matematica, la fisica e la medicina, per non parlare delle materie umanistiche e delle arti figurative.

Quanto alle finalità, vorrei ricondurle al tentativo di mitigare quella sorta di inaridimento culturale indotto dalla pur necessaria impostazione specialistica dei corsi universitari oltraché, a beneficio dei discenti, all’opportunità di rendere meno evanescenti le tracce di cosiddetta “cultura generale” acquisite ma spesso non digerite sui banchi di scuola. Si tratta infatti di rivisitare i principi fondanti e i passi tecnologici cruciali – compresi quelli attinenti a tecnologie ormai superate ma facenti parte di un filo rosso non interrompibile – per esaminarli nel loro contesto culturale, sociale e geopolitico, ovvero storico *tout court*. Si tratta, ancora, di valutare criticamente i disparati modi in cui la priorità cronologica o l’eccellenza qualitativa si sono tradotte – o non si sono tradotte – in impatto sul mondo reale della scienza e dell’industria: i “casi” di Atanasoff e di Zuse sono emblematici in tal senso ma anche le vicende Olivetti-Concorrenza e IBM-Concorrenza si prestano egregiamente ad essere lette in questa chiave.

3. L’ESPERIENZA DEI “CORSI AICA”⁵

Va rimarcata innanzitutto la quantità e il livello delle risorse professionali che si stanno impegnando in questa impresa culturale la cui estensione e coesione interna, per

quanto a mia conoscenza, non hanno precedenti neppure all’estero.

Volendo quantificare le dimensioni che il progetto ha assunto nei primi due anni di attività, si rileva per prima cosa che i docenti titolari dei corsi sono stati ben diciassette. Il numero va poi più che raddoppiato ove si tenga conto degli esperti – provenienti dalle aziende e dalle professioni del settore ICT oltre che dalla stessa accademia – i quali, su invito dei docenti, hanno arricchito i corsi con seminari monografici⁶.

Da una stima approssimativa risulta inoltre che, negli stessi due anni, sono stati non meno di cinquecento gli studenti che hanno fruito dei corsi sponsorizzati da AICA e alla conclusione del triennio il loro numero aumenterà in proporzione. In effetti, i docenti hanno concordemente testimoniato la risposta positiva da parte degli studenti che si è concretizzata nel soddisfacente numero di frequentanti: 25 in media, con punte di 40 a Verona e di 75 a Palermo. Circa altrettante sono state le prove d’esame, svoltesi peraltro con modalità diverse da sede a sede. Il corso di Udine – che ho condiviso con il collega Paolo Giangrandi – è venuto però a costituire una notevole eccezione. Infatti, a fronte di un numero di frequentanti allineato alla media suddetta, il numero di studenti che hanno sostenuto l’esame è risultato sorprendentemente elevato: 158 (con 260 prove d’esame)⁷ nel 2005-2006 e 123 (con 165 prove) nel 2006-2007, non ancora concluso⁸.

Ancora riguardo all’atteggiamento degli studenti, non è privo d’interesse l’esito di un sondaggio cui hanno finora aderito cinquanta degli studenti udinesi del corso 2006-2007 che hanno già superato l’esame⁹. Uno dei quesiti

⁴ Se oggi è naturale parlare di “semplice esistenza”, non si possono dimenticare le annose difficoltà che Sandro Faedo ha dovuto a suo tempo superare per varare, nel 1969, il corso di laurea in Scienze dell’Informazione. È illuminante anche il seguente “amarcord”, riferito al 1971, narrato da Luigi Dadda il quale conduceva la stessa battaglia sul fronte delle facoltà d’ingegneria: “[...] egli [un suo autorevole interlocutore nell’ambito di una tavola rotonda] affermò a un certo punto di non ritenere che l’informatica fosse una vera e propria disciplina scientifica, in quanto, pur realizzando macchine di indubbio interesse, non ne aveva ancora delineato i principi teorici”.

⁵ Per quanto si espone in questo paragrafo, attingo liberamente alle notizie che i colleghi titolari dei corsi hanno avuto la cortesia di fornire sulla falsariga di un apposito questionario.

⁶ A La Sapienza e a Pisa, in particolare, i seminari dei relatori invitati hanno coperto la maggior parte del corso.

⁷ Nel numero delle prove d’esame sono comprese quelle ripetute.

⁸ Questa singolarità quantitativa deve pur essere ascrivibile a una serie di concause; decifrarle e attribuire loro un peso è però tutt’altro che agevole. Comunque, a prescindere dalle cause, il gran numero delle prove d’esame ha offerto occasione e materiale per l’analisi che Mirolo e Giangrandi descrivono e commentano nell’articolo che appare in questo stesso numero di Mondo Digitale.

⁹ Il sondaggio, ben distinto dalla valutazione didattica istituzionale, è stato ideato dai colleghi Mirolo e Giangrandi.

recitava *“Quali sono le principali motivazioni che ti hanno portato a scegliere il corso di Storia dell’Informatica?”*. Un piccolo numero di risposte del tipo *“mi servono i crediti!”* sono state sinceramente pragmatiche oppure espressive ma laconiche del tipo *“curiosità/cultura personale/cultura generale”*; la maggior parte degli studenti ha invece risposto, in maniera più o meno articolata, con espressioni che possono ricondursi al seguente paradigma: *“interesse/curiosità verso una materia che studiamo esclusivamente sotto il profilo tecnico”*. Una risposta atipica, per completare il florilegio, merita la citazione testuale: *“Perché una materia ‘letteraria’ è piacevole da studiare”*. Non può sfuggire la sostanziale concordanza tra le finalità esposte nel paragrafo precedente e l’opinione prevalente tra gli studenti, sia pure desunta da un campione non distribuito sull’intera popolazione dei fruitori dei corsi.

Nel progettare il corso, il problema cruciale che i docenti hanno affrontato è stato quello di definire i contenuti. Problema che ciascun docente ha risolto ovviamente in completa autonomia e in base alla propria sensibilità; in tutti i casi è stato peraltro necessario tenere conto di alcuni vincoli oggettivi che hanno pesato in misura diversa da caso a caso.

La durata del corso ha oscillato tra le 16 h del “corso breve” di Verona (2 CFU) e le 46 h di Genova (6 CFU) e Torino (4 CFU) con una media, riferita a nove corsi, di circa 35 h e 4 Crediti.

Seppure in misura diversa, tutti i corsi hanno fatto risentito del vincolo della brevità; vincolo che peraltro, date le quasi illimitate possibilità di estendere e di approfondire qualsiasi discorso storico, sarebbe rimasto tale anche raddoppiando la durata. Ci si è quindi orientati verso l’unica scelta ragionevole: quella di imporsi una drastica selezione degli argomenti da includere nel programma onde evitare di mettere troppa carne al fuoco col rischio di ridurre il tutto a un mero scheletro cronologico.

Va da sé che la scura del silenzio, o del quasi silenzio, è caduta su capitoli diversi in base al ponderato discernimento di ciascun docente. Tra le vittime più ricorrenti si sono annoverati quegli argomenti che presentano il minor numero di connessioni con la traccia principale – anche se, come si è già detto, la storia dell’informatica è un insieme connesso che non ammette zone del tutto isolate dal resto – quali il calcolo analogi-

co, il software (talvolta ristretto ai linguaggi di programmazione), l’intelligenza artificiale e la robotica, il calcolo meccanico numerico (riservando comunque un occhio di riguardo per Babbage), i sistemi meccanografici a schede perforate, le reti. Sono state rinunce sofferte in compensazione delle quali si sono potuti talvolta mettere in programma anche temi meno consueti ma forse più stimolanti come la storia della crittografia oppure l’esplorazione del futuro prevedibile o possibile.

In pochissimi casi si è invece rinunciato a prendere le mosse dagli albori dei concetti numerici, dei sistemi di numerazione *et similia*. Ciò che, tra l’altro, testimonia il consolidarsi della comoda convenzione secondo la quale la storia dell’informatica s’intende estesa a ritroso fino a quel remoto passato, con buona pace del purista che arriccia il naso di fronte all’uso retroattivo del neologismo *informatique* coniato appena nel 1962.

È stato poi indispensabile tenere in considerazione il contesto disciplinare e il bagaglio delle conoscenze pregresse degli studenti – vale a dire: tipo del corso di laurea e anno di corso – di estrazione quasi sempre eterogenea. Il divario tra lauree (triennali) e lauree specialistiche ha pesato specialmente per calibrare il tono dell’esposizione in presenza di argomenti, sia concettuali che tecnologici, che avessero stretta attinenza con l’attuale stato dell’arte e con cui gli “specialisti” hanno una familiarità superiore rispetto ai colleghi “triennali”. Divario che scompare invece del tutto quando si affrontano tematiche decisamente obsolete, ma non per questo meno rilevanti per la storia. In tali situazioni il problema didattico, nei confronti dell’intero uditorio, diventa quello di decidere se e fino a che punto entrare nel merito del cos’è e del come funziona: a fare la storia degli oggetti misteriosi si rischia di costruire sulla sabbia. E se si parla del regolo logaritmico la cosa si può liquidare in poche battute; il compito si fa più impegnativo nel caso dei sistemi meccanografici a schede perforate – è solo un esempio – in cui una descrizione puramente cronologica e tecnologica avulsa dal concetto di “procedura meccanografica”, magari illustrato in termini euristici, non può rendere conto dell’impatto applicativo e delle fortune industriali legati a quei sistemi né, tanto meno, del loro ruolo di precursori degli elabo-

ratori elettronici “commerciali” con memorie di massa sequenziali.

L’eterogeneità dell’uditorio è stata particolarmente pronunciata a Ca’ Foscari e all’Università di Udine: nella prima sede il *mix* era costituito da studenti di Informatica (triennale) e di Informatica per le Discipline Umanistiche (specialistica) mentre in quel di Udine si sono incrociati ben quattro corsi di laurea dei quali due triennali (Informatica e Tecnologie Web e Multimediali) e due specialistici (Informatica e Tecnologie dell’Informazione)¹⁰.

Al Politecnico di Torino la situazione è risultata piuttosto atipica per un motivo diverso: il corso era infatti offerto praticamente a tutte le specialità d’ingegneria tranne a quelle d’indirizzo informatico col risultato che il corso – peraltro uno dei più robusti, come si è visto – è risultato una sorta di “informatica per non addetti” mimetizzata tra le pieghe della storia.

A Verona si è realizzata un’ulteriore variante nella composizione dell’uditorio grazie al fatto che gli organizzatori del corso l’hanno pubblicizzato come un vero e proprio evento culturale aperto al pubblico. Due comunicati stampa, emessi come annuncio e come commento alla conclusione del corso, sono stati recepiti dai *media* locali con il duplice effetto di lanciare il messaggio che la storia dell’informatica è una faccenda seria e non una fantasia, e di far conoscere il ruolo di AICA a sostegno dell’iniziativa. Nel breve spazio di questo resoconto non può infine mancare un cenno al problema dei supporti didattici, da servire sia come traccia durante le lezioni e sia come ausilio agli studenti in fase di studio/ripasso. Problema che è nato dall’oggettiva impossibilità di fare riferimento a un unico testo – il fatidico manuale – che aderisse ai contenuti prescelti dal docente e che lo facesse in modo conforme al suo peculiare stile espositivo.

I docenti si sono quindi sobbarcati l’onere di approntare il materiale di supporto che, in quasi tutte le sedi, è stato realizzato in formato elet-

tronico e reso disponibile in rete¹¹; da notare che per il popolo degli studenti non frequentanti si è trattato dell’unico punto di appoggio.

Onere assolto con impegno tanto più apprezzabile in quanto i docenti, per la quasi totalità, erano digiuni di precedenti esperienze nell’insegnamento di una materia così nuova e sono quindi partiti da zero sviluppando con tratti di non comune originalità una nutrita serie di moduli di comprovata efficacia didattica; ogni cosa, d’altra parte, è perfezionabile e a maggior ragione possono esserlo questi contributi che scaturiscono da uno sforzo di natura genuinamente diletantistica nel senso che la qualifica/professione di storico dell’informatica non è stata ancora inventata.

4. PROSPETTIVE

Sulla base dei risultati fin qui conseguiti non sembrano esserci dubbi che l’iniziativa AICA e l’attività degli atenei e dei docenti che vi partecipano giunga felicemente al compimento del triennio. Ma, come detto in apertura, l’obiettivo più qualificante rimane quello che il progetto lasci un’eredità stabile e visibile in modo che la storia dell’informatica continui ad essere coltivata e insegnata come un componente non secondario della cultura informatica e dell’offerta formativa.

Dato per scontato che i docenti si faranno parte attiva affinché ciò avvenga, è pure evidente che, concluso l’a.a. 2007-2008, l’esaurirsi del sostegno finanziario da parte di AICA avrà pure un certo peso. Inoltre la recente riforma comporterà un aumento del carico didattico tale che, in molte sedi, sarà problematico mantenere attivo il corso; come soluzione di ripiego, alcuni suggeriscono di erogarlo ad anni alterni.

Non sembra irrealistico che la ristrutturazione dell’offerta formativa, conseguente anch’essa dalla riforma, porti a sacrificare proprio questo insegnamento, l’ultimo arrivato; c’è da augurarsi che ciò non avvenga almeno in quelle sedi nelle quali il gradimento da parte degli studenti si è manifestato in termini quantitativamente rilevanti.

Considerando la questione da un diverso punto di vista, un segnale positivo viene dalle tesi di laurea – una decina in complesso, con esito talvolta eccellente – che sono state

¹⁰ Segnalo anche la “incursione” di una studentessa del corso di laurea in Biotecnologie.

¹¹ In aggiunta alla ricca iconografia che correda i materiali in rete, le lezioni sono state talvolta vivacizzate dalla proiezione di filmati e dall’esibizione di reperti storici.



assegnate su argomenti attinenti alla storia dell'informatica, i cui autori hanno pertanto manifestato un interesse che va ben oltre la fruizione del corso. È quindi possibile che siano proprio questi giovani laureati, o almeno alcuni di loro, a raccogliere il testimone decidendo di dedicare stabilmente alla storia dell'informatica una parte della loro futura attività professionale, specialmente nei casi in cui tale attività si svolga all'interno dell'università.

Nell'ambito della collaborazione AICA-CILEA per il "Museo dell'Informatica" è peraltro allo studio un'ulteriore iniziativa intesa a dare continuità al progetto qui presentato e a non

disperdere, anzi a valorizzare, i frutti dei suoi tre anni di attività.

Si tratta di allestire, a coronamento del triennio, un corso multimediale di ampio respiro, strutturato e fruibile in maniera aperta con metodologia e-learning e di assicurarne poi la "manutenzione" con un costante lavoro di aggiornamento e di incremento. L'esperienza del CILEA in materia di e-learning e la collaborazione degli attuali docenti costituiranno altrettanti punti di forza per questo nuovo progetto il cui primo passo consisterà nel raccogliere in un sito unitario, con il consenso dei docenti che ne sono gli autori, i materiali didattici già disponibili (riquadro).

REPERTORIO

Corsi AICA: i siti dei docenti

Link ai materiali didattici che risultano accessibili alla data di queste note.

Univ. di Genova:	http://www.disi.unige.it/person/CostaG/Storia_o6/
Univ. di Milano "Statale":	http://homes.dico.unimi.it/~gfp/StIn/2005-06/index.html
"	http://homes.dico.unimi.it/~gfp/StIn/2006-07/index.html (da completare)
Univ. di Roma La Sapienza:	http://www.dis.uniroma1.it/~storia/
Univ. del Sannio:	http://www.ing.unisannio.it/disanto/Teaching/Storia DellaInformatica/2007/info.htm
Univ. di Udine:	http://users.dimi.uniud.it/nid/history//history.html
Univ. di Venezia Ca' Foscari:	http://www.dsi.unive.it/~pelillo/Didattica/Storia%20dell'informatica/
Univ. di Verona:	http://www.profs.sci.univr.it/~manca/

Lectture consigliate: le più gettonate

Opere che i docenti hanno suggerito a chi volesse approfondire.

Il numero di  indica il rispettivo score.

-    M.R. Williams: *A History of Computing Technology*. Prentice-Hall, 1985.
Trad.it. [possibilmente da evitare!] *Storia dei computer. Dall'abaco ai calcolatori elettronici*. Franco Muzzio, 1989.
-  W. Aspray (editor): *Computing Before Computers*. Iowa State University Press, 1990.
-  P.E. Ceruzzi: *A History of Modern Computing*. The MIT Press, 2003 (2nd ed.).
Trad.it. *Storia dell'informatica: dai primi computer digitali all'era di internet*. Apogeo, 2006.
-  M. Davis: *The Universal Computer – The road from Leibniz to Turing*; 2000.
Trad.it. *Il calcolatore universale: da Leibniz a Turing*. Adelphi, 2004.
-  M. Calvo, F. Ciotti, G. Roncaglia, M.A. Zela: *Internet 2004*. Laterza, 2003.
-  M. Campbell-Kelly, W. Aspray: *Computer: A History of the Information Machine*. Basic Books - HarperCollins Publishers, 1996.
-  A.D. Chandler: *Inventing the Electronic Century*. The Free Press, 2001.
Trad.it. *La rivoluzione elettronica*. Egea - Università Bocconi editore, 2003.
-  G. Ifrah: *Histoire universelle des Chiffres*. Éditions Seghers, 1981.
Trad.it. *Storia universale dei numeri*. Arnoldo Mondadori, 1983.
-  M. Morelli: *Dalle calcolatrici ai computer degli anni cinquanta*. Franco Angeli, 2001.
-  R.W. Sebesta: *Concepts of Programming Languages*. Addison-Wesley, 2006 (7th ed.).

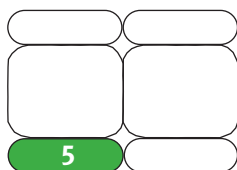
CORRADO BONFANTI (1940) è responsabile del progetto AICA "Storia dell'informatica" e docente a contratto per tale materia nelle università di Udine e Trieste-SSIS. Laureato in fisica a La Sapienza, ha lavorato con IBM Italia e poi nel gruppo Finsiel: con l'Italsiel a Roma, con l'Insiel a Trieste – dove risiede – e infine a Bucarest come direttore generale di Finsiel-România. Ha ricoperto altri incarichi universitari a Roma, Trieste, Bari e Milano. Da vent'anni si occupa di storia del calcolo automatico e dell'informatica, pubblicando articoli e tenendo conferenze su invito di numerose istituzioni culturali. È socio onorario della Mathesis, sezione di Udine, e socio ordinario dell'AICA.

E-mail: corradoBonfanti@hotmail.com



LA CERTIFICAZIONE ECDL NEGLI ATENEI ITALIANI

Cristiana Rita Alfonsi
Elena Breno
Maria Carla Calzarossa
Paolo Ciancarini
Paolo Maresca
Luisa Mich
Fulvia Sala
Nello Scarabottolo



L'articolo presenta lo stato dei progetti di certificazione delle abilità nell'uso delle tecnologie informatiche svolti dagli Atenei Italiani, evidenziandone gli aspetti salienti, l'evoluzione e le principali linee di tendenza. L'articolo presenta anche il punto di vista di un campione di studenti che hanno ottenuto la certificazione ECDL nel corso della loro carriera universitaria.

1. INTRODUZIONE

Le politiche per lo sviluppo della Società della Conoscenza danno un grosso rilievo ai giovani, in quanto rappresentano le generazioni future, destinate a confrontarsi quotidianamente con le moderne tecnologie dell'informazione e della comunicazione.

Le nuove generazioni si presentano sempre più composte da persone "native digitali", cioè abituate a un utilizzo ubiquo e continuo degli strumenti informatici. Occorre però garantire che la conoscenza e l'utilizzo di queste tecnologie non rimangano solo superficiali e con una valenza sostanzialmente ludica. Anche la cultura digitale necessita di opportuni approfondimenti, esercizi, verifiche e valutazioni.

AICA (*Associazione Italiana per l'Informatica ed il Calcolo Automatico*) nel suo impegno a sviluppare, diffondere e promuovere la cultura informatica e le relative certificazioni, ha sempre posto particolare attenzione al mondo della Scuola e dell'Università. In questo ambito sono molteplici i progetti che vedono AICA collaborare con la Fondazione

CRUI (*Conferenza dei Rettori delle Università Italiane*) e con il CINI (*Consorzio Interuniversitario Nazionale per l'Informatica*).

Per esempio, proprio da una collaborazione tra AICA, CINI e Fondazione CRUI è nato nel 2001 l'Osservatorio sulle Certificazioni Informatiche negli Atenei Italiani [1], il cui obiettivo è quello di analizzare l'introduzione e la diffusione nel mondo universitario di progetti di certificazione di abilità e competenze informatiche. A questo scopo l'Osservatorio promuove indagini a periodicità annuale rivolte ai referenti della formazione informatica nei vari Atenei [2, 3, 11]. L'indagine è arrivata alla sua sesta edizione: l'edizione 2007 è stata arricchita con una nuova rilevazione mirata ad analizzare – oltre al punto di vista istituzionale degli Atenei – anche il punto di vista di un campione di studenti che avevano ottenuto una certificazione informatica durante la carriera universitaria.

Il presente articolo illustra i principali risultati di entrambe le rilevazioni, focalizzandosi dapprima sulle attività di certificazione delle abilità informatiche di base intraprese dagli

Atenei nel corso dell'anno solare 2006 e successivamente sulle opinioni degli studenti nei confronti della certificazione ECDL. L'articolo presenta anche un'analisi dettagliata dell'evoluzione e delle principali linee di tendenza della diffusione della certificazione ECDL negli Atenei.

2. I PROGETTI DI CERTIFICAZIONE DELLE ABILITÀ INFORMATICHE NEGLI ATENEI

In questa sezione si riassumono gli aspetti salienti emersi dall'indagine 2007 dell'Osservatorio in relazione all'accREDITAMENTO delle abilità informatiche di base possedute dagli studenti e alle scelte organizzative e gestionali degli Atenei nell'ambito dei progetti di certificazione ECDL nell'anno solare 2006. Per maggiori dettagli si rimanda al documento completo dell'indagine [9] disponibile online sul sito dell'Osservatorio (<http://osservatorio.consortio-cini.it>).

All'indagine 2007 ha aderito la quasi totalità degli Atenei, più precisamente 64 dei 69 Atenei a cui era stato inviato il questionario utilizzato per l'indagine.

Un primo interessante aspetto emerso dall'indagine riguarda le modalità utilizzate dagli Atenei per accreditare le abilità informatiche di base degli studenti. Come mostrato nella figura 1, le modalità prevalenti sono l'esame tradizionale e la certificazione ECDL. Al contrario, risulta poco diffuso il test senza certificazione e ancora meno diffusi sono gli altri tipi di certificazione. A questo riguardo, è importante puntualizzare come di norma gli Atenei non utilizzino le diverse modalità di accREDITAMENTO in maniera esclusiva. Per esempio, dei 40 Atenei che fanno ricorso all'esame tradizionale, circa la metà lo affianca alla certificazione ECDL, mentre circa un quarto lo affianca al test senza certificazione. Va notato però che l'analisi non ha evidenziato alcun comportamento tipico che caratterizzi gli Atenei, a testimonianza di come l'autonomia adottata nella stesura degli ordinamenti didattici porti a far prevalere le esigenze locali, talvolta anche a scapito di un coordinamento più cogente a livello nazionale. Al contrario, si è rilevata una buona propensione di tutti gli Atenei ad accreditare una

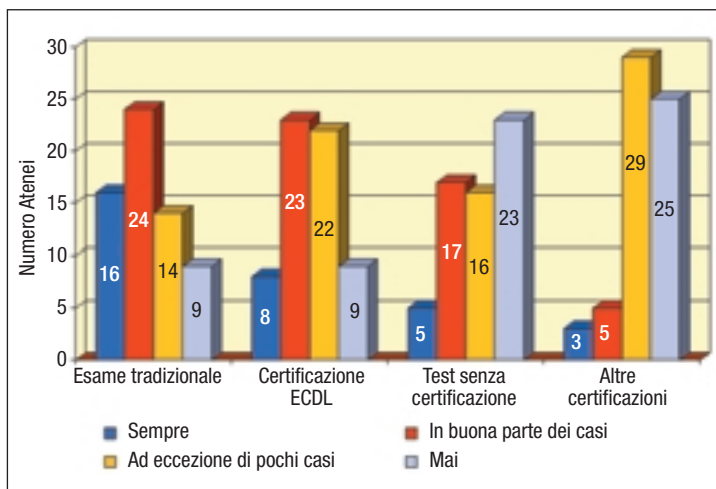


FIGURA 1

Diffusione delle modalità di accREDITAMENTO delle abilità informatiche di base degli studenti

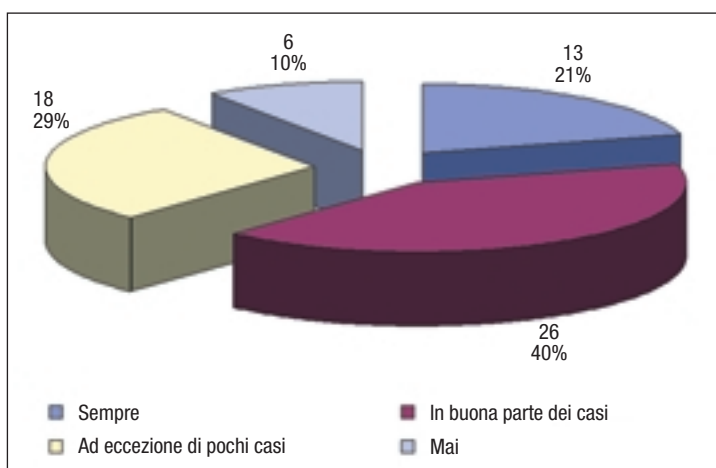


FIGURA 2

Diffusione del riconoscimento di una certificazione precedentemente acquisita

certificazione acquisita dallo studente prima della sua immatricolazione (Figura 2). È importante sottolineare come oltre un terzo di questi 39 Atenei preveda il riconoscimento di una certificazione nonostante non utilizzi la certificazione ECDL come modalità di accREDITAMENTO. I pochi Atenei che non riconoscono in alcun modo una certificazione precedentemente acquisita basano l'accREDITAMENTO in prevalenza sull'esame tradizionale. Questi risultati sono in linea, come sarà evidenziato più dettagliatamente in seguito, con la progressiva diffusione della certificazione ECDL a livello di scuole secondarie superiori. Decisamente buono è stato nell'anno solare 2006 il livello di diffusione dei progetti ECDL negli Atenei: ben 55 dei 64 Atenei che hanno partecipato all'indagine (pari all'85,9%) avevano

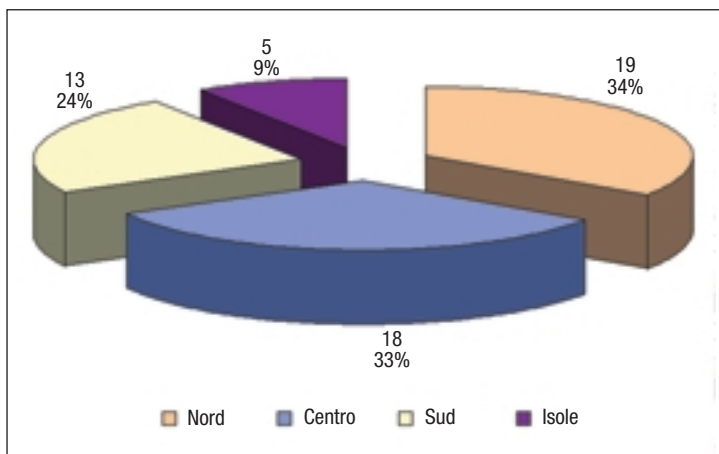


FIGURA 3

Distribuzione geografica degli Atenei con attivi progetti ECDL

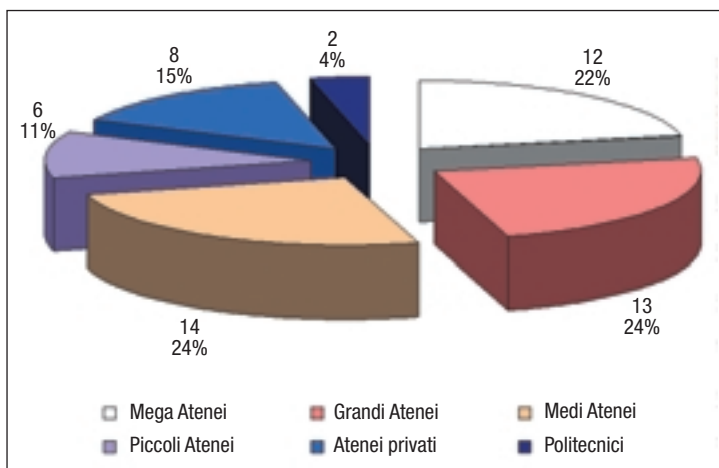


FIGURA 4

Distribuzione dimensionale degli Atenei con attivi progetti ECDL

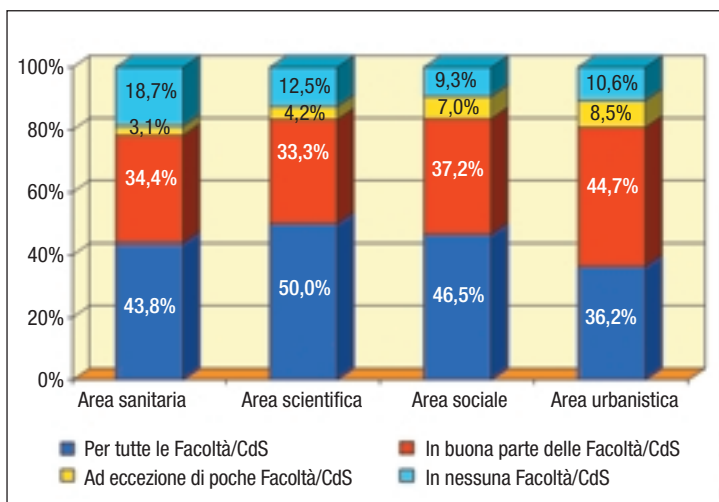


FIGURA 5

Obbligatorietà di insegnamenti di abilità informatiche rispetto alle quattro macro-aree ministeriali

attivi progetti ECDL. Per una caratterizzazione più precisa di questi 55 Atenei, nella figura 3 e nella figura 4 sono riportate, rispettivamente, la loro distribuzione geografica e dimensionale. La classificazione dimensionale degli Atenei fa riferimento all'indagine 2006 Censis – La Repubblica sulle Università Italiane [12], nella quale gli Atenei sono distinti in Piccoli, Medi, Grandi e Mega, Università Private e Politecnici. Nonostante l'elevato numero di progetti ECDL attivi presso gli Atenei, si è riscontrato che un numero alquanto limitato di Corsi di Studio considera la certificazione ECDL come un requisito obbligatorio per gli studenti. In ogni caso, si è rilevata una particolare attenzione degli Atenei nei confronti della formazione informatica, anche laddove la certificazione ECDL non è obbligatoria; come mostra la figura 5, gli Atenei di norma prevedono come obbligatori insegnamenti di abilità informatiche di base. Si nota, ad esempio, che per le Facoltà dell'area Sanitaria questo accade presso il 78,2% degli Atenei con Facoltà afferenti a tale area, mentre per le Facoltà delle aree Scientifica, Sociale e Umanistica, le percentuali si attestano su valori anche superiori all'80%. Si sottolinea che la suddivisione delle Facoltà in aree fa riferimento alle quattro macro-aree ministeriali utilizzate nella banca dati dell'offerta formativa universitaria (<http://off.miur.it>).

La novità della certificazione ECDL ha portato gli Atenei a sperimentare varie modalità di formazione per il conseguimento della certificazione stessa. Nell'anno solare 2006 si è assistito ad una netta crescita della formazione tramite autoapprendimento (adottata da 39 Atenei, pari al 70,9%); in particolare, un terzo di questi Atenei vi fa ricorso in maniera esclusiva. Di contro, è diminuito in maniera significativa il numero di Atenei che utilizza unicamente la formazione di tipo frontale (adottata solo da tre Atenei). Questi risultati mostrano come gli Atenei si stiano sempre più orientando verso un tipo di formazione che non richieda l'impegno di risorse umane ed infrastrutturali da parte degli Atenei stessi. Si è infatti rilevato che, a seguito della conclusione del progetto CampusOne e dei relativi incentivi economici, la maggioranza degli Atenei fa ricorso a fondi propri (di Ateneo) per la copertura finanziaria delle attività di formazione ECDL.

Un altro risultato interessante riguarda l'am-

biente operativo utilizzato per la formazione ECDL nell'anno solare 2006: si è registrata una leggera crescita dell'uso di ambienti *open source*, anche se la loro diffusione rimane ancora alquanto modesta.

L'indagine ha poi evidenziato, come mostrato nella figura 6, una polarizzazione sempre più marcata degli Atenei verso la certificazione completa ECDL FULL (che prevede il superamento degli esami di tutti i sette moduli ECDL). Questo tipo di certificazione è adottata dal 71,7% degli Atenei in modo esclusivo o prevalente, mentre è decisamente in calo il numero di Atenei (solo due) che utilizzano in maniera esclusiva la certificazione ECDL START (che prevede il superamento degli esami di quattro dei sette moduli ECDL). È infine interessante sottolineare una maggiore propensione degli Atenei che hanno attivato i progetti ECDL in tempi più recenti ad orientarsi verso una certificazione completa come quella di tipo FULL.

Per quanto riguarda la copertura finanziaria della certificazione ECDL, nell'anno solare 2006 si è notato un forte incremento del numero degli Atenei che mettono a carico degli studenti il pagamento della Skills Card e degli esami. Come si osserva dalla figura 7, la grande maggioranza degli Atenei (43 Atenei, pari al 78,2%) utilizza questo tipo di modalità, mentre decisamente più basse sono le percentuali di Atenei che fanno ricorso a fondi propri (di Ateneo) o di altri Enti. L'analisi ha poi evidenziato che la grande maggioranza degli Atenei che traggono la copertura finanziaria per la certificazione ECDL da un'unica fonte richiede agli studenti il pagamento di Skills Card ed esami. Poco diffusa è la pratica di conglobare i costi della certificazione ECDL nelle tasse universitarie.

Si è rilevata, infine, un'associazione tra il tipo di certificazione richiesta e la fonte di finanziamento; in particolare, la certificazione ECDL FULL è di norma associata alla richiesta di pagamento diretto da parte degli studenti.

3. EVOLUZIONE E TENDENZE DEI PROGETTI DI CERTIFICAZIONE DELLE ABILITÀ INFORMATICHE NEGLI ATENEI

Come è noto, AICA ha iniziato a diffondere il programma ECDL in Italia nel 1997 e già nel 1998 un primo Ateneo lo aveva introdotto all'interno della sua offerta formativa. Due so-

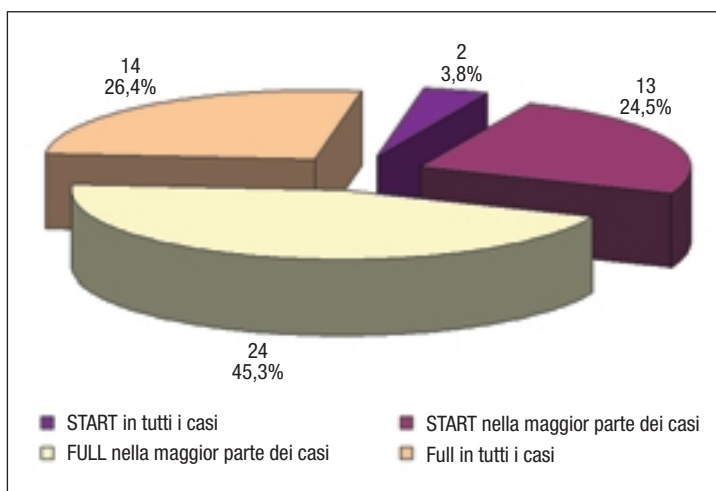


FIGURA 6

Distribuzione del tipo di certificazione ECDL adottata dagli Atenei

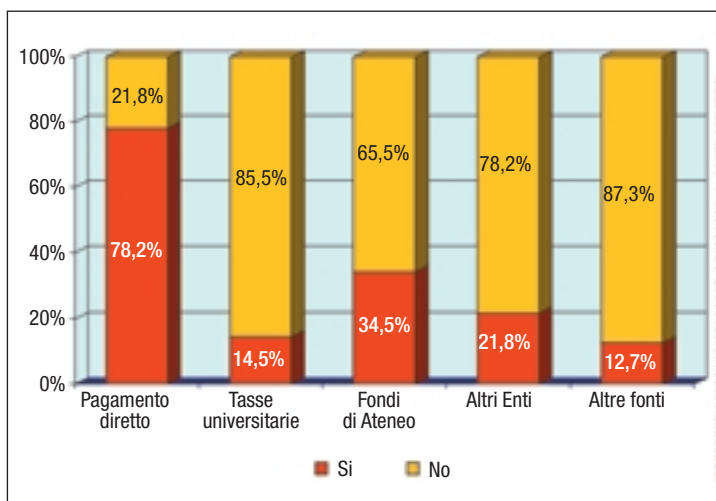


FIGURA 7

Fonti di finanziamento per la certificazione ECDL

no gli eventi fondamentali che hanno avuto un ruolo determinante per la penetrazione della certificazione ECDL negli Atenei italiani: la riforma dei percorsi di studio universitari e il progetto CampusOne.

La riforma ha articolato le lauree in due livelli e introdotto i *Crediti Formativi Universitari* (CFU) per misurare l'impegno associato a un determinato Corso di Studio. In sintonia con gli obiettivi del summit dell'Unione Europea di Lisbona del 2000, nel marzo 2001 un accordo tra il Ministero della Pubblica Istruzione e la CRUI stabiliva le basi per il riconoscimento di crediti associati alla certificazione ECDL per tutte le classi di Laurea (eccetto la classe di Scienze e Tecnologie Informatiche). Dall'altro lato, il progetto CampusOne ha permesso di concretizzare uno scenario in

Anno	Numero Atenei con progetti ECDL attivi	Numero Atenei partecipanti all'indagine
2001-02	17	20 (campione)
2002	33	65
2003	46	54
2004	50	54
2005	48	53
2006	55	64

TABELLA 1

Evoluzione dei progetti ECDL

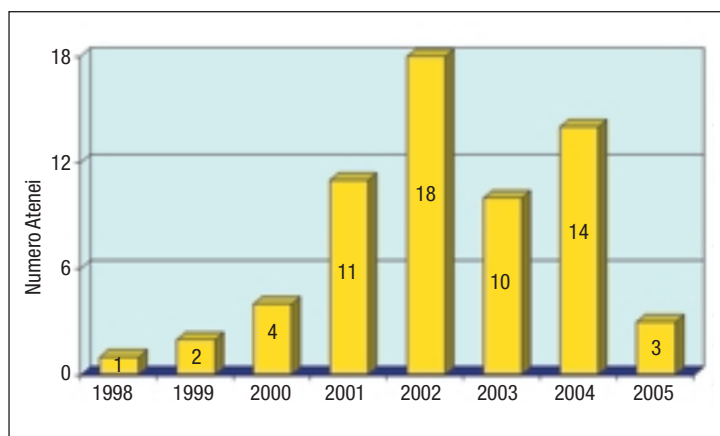


FIGURA 8

Distribuzione degli anni di attivazione dei progetti ECDL

cui la quasi totalità degli Atenei Italiani ha attivato progetti ECDL.

L'evoluzione dei progetti di certificazione ECDL nel mondo universitario è riassunta nella tabella 1, da cui si può notare come la percentuale di Atenei che hanno adottato la certificazione ECDL abbia raggiunto rapidamente livelli molto elevati.

La situazione complessiva delle attivazioni dei progetti ECDL è illustrata nella figura 8, dove si evidenzia una forte concentrazione di attivazioni (42 Atenei) tra gli anni 2002 e 2004 in corrispondenza dell'avvio del progetto CampusOne: 18 Atenei hanno infatti risposto immediatamente alle sollecitazioni ministeriali e dunque ai requisiti di CampusOne, attivando i progetti ECDL nel 2002. 14 Atenei hanno invece attivato i progetti ECDL solo nel 2004, cioè "in coda" al progetto CampusOne (che si è concluso nel settembre 2004). A testimonianza dell'interesse che comunque ha suscitato la certificazione ECDL in ambito accademico, si segnala il numero rilevante di Atenei (18) con progetti ECDL attivi prima che CampusOne ne raccomandasse l'adozione. Per quanto riguarda le conseguenze e i cambiamenti intervenuti nei progetti ECDL a seguito della conclusione del progetto CampusOne, la figura 9 mostra come, nonostante la mancanza degli stimoli e degli incentivi

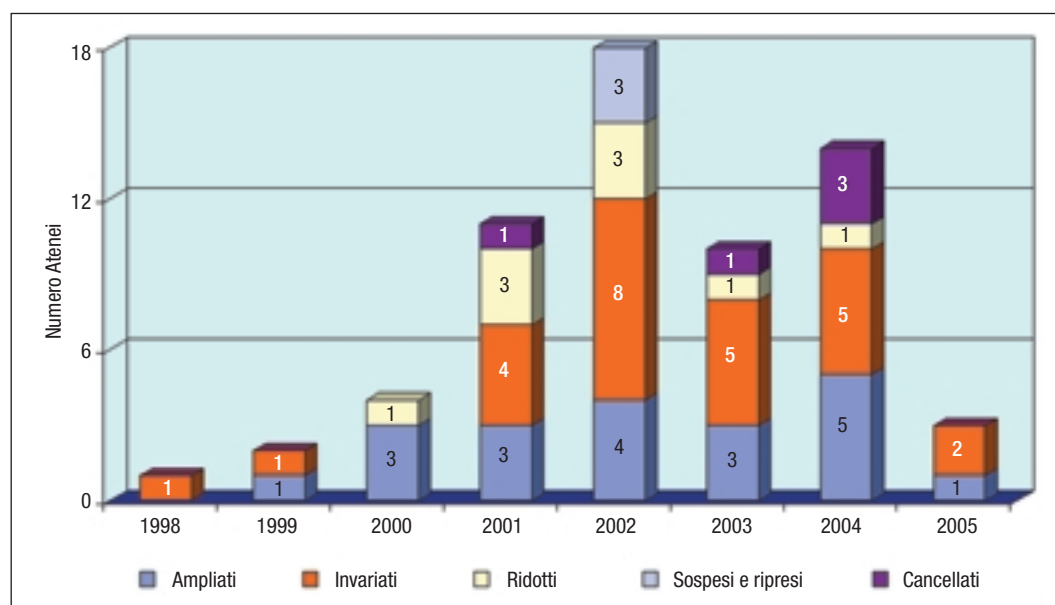


FIGURA 9

Cambiamenti intervenuti nei progetti ECDL dopo la conclusione del progetto CampusOne in funzione dell'anno di attivazione del progetto

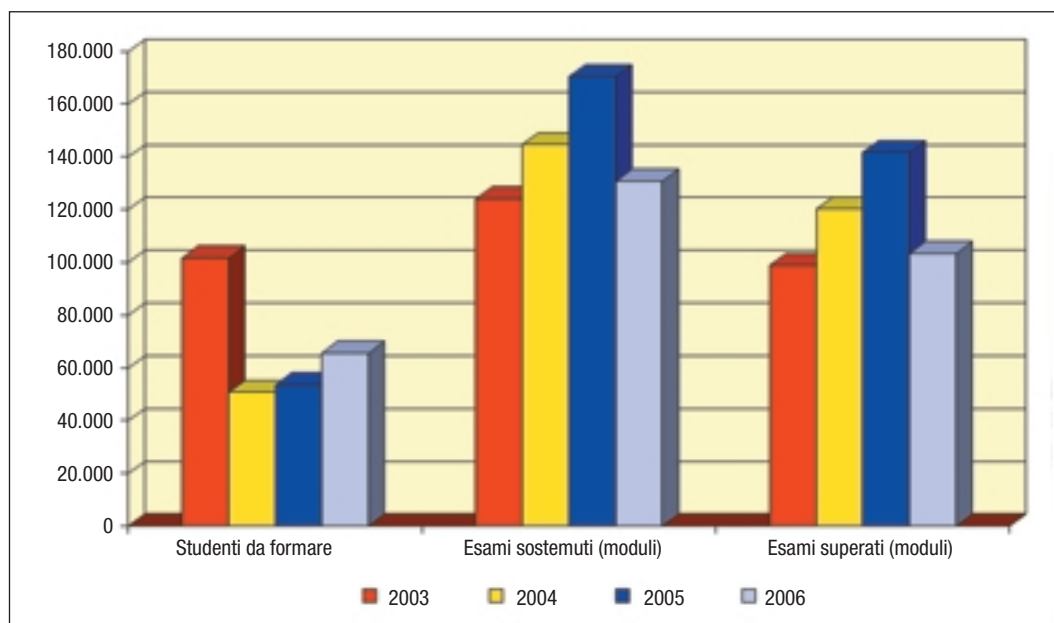


FIGURA 10

Andamento del numero di studenti da formare e del numero di esami ECDL negli anni 2003-2006

finanziari di CampusOne, la cultura della certificazione, ampiamente promossa da questo progetto, sia un fatto riconosciuto e consolidato presso gli Atenei. In particolare, l'indagine 2007 ha rilevato che 46 Atenei (pari al 73%) hanno ampliato o proseguito in maniera invariata i progetti ECDL, mentre solo 5 Atenei (pari al 7,9%) li hanno cancellati dai loro programmi formativi.

I dati forse più significativi per illustrare le dimensioni del fenomeno ECDL in ambito accademico riguardano il numero di studenti da formare e gli esami sostenuti e superati dagli studenti. I dati raccolti nelle indagini degli ultimi quattro anni sono riassunti in figura 10.

Estrapolando da questi dati la produttività degli studenti, definita come rapporto tra il numero di esami sostenuti per i singoli moduli ECDL ed esami superati, si notano valori sostanzialmente stabili intorno all'80%; in particolare, la produttività più bassa (78,9%) si è registrata nell'anno solare 2006, mentre quella più elevata (83,1%) negli anni solari 2004 e 2005. Il motivo principale di questo risultato è da ascrivere all'introduzione – avvenuta proprio a cavallo tra gli anni 2005 e 2006 – del nuovo sistema di gestione automatica degli esami ECDL (Atlas) che, avendo sensibilmente modificato il modo di porre le domande, ha creato maggiori difficoltà nel superamento degli

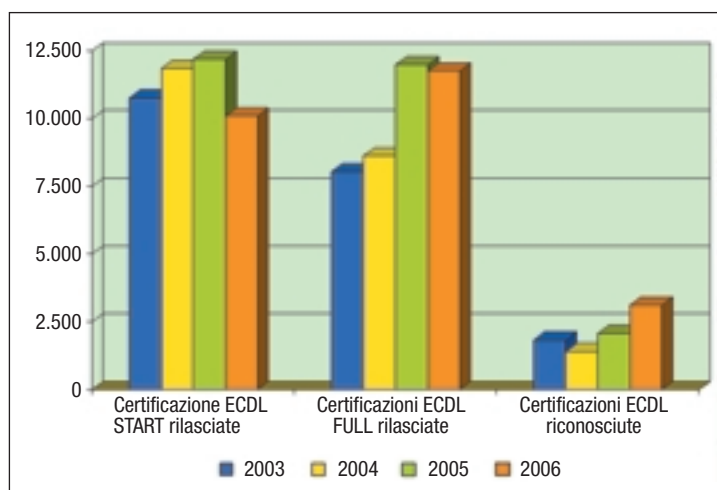


FIGURA 11

Andamento del numero di certificazioni ECDL negli anni 2003-2006

esami da parte degli studenti rispetto all'ormai noto e assestato sistema Alice.

Come già sottolineato, uno degli aspetti che caratterizza l'introduzione dei progetti ECDL negli Atenei Italiani riguarda la scelta sul tipo di certificazione, ECDL START o ECDL FULL. A questo riguardo, la situazione emersa dalle indagini è illustrata nella figura 11, dove si nota un aumento delle certificazioni ECDL FULL rilasciate nell'ultimo anno rispetto a quelle START, oltre che del numero di certificazioni riconosciute a studenti che l'avevano conseguita precedentemente alla loro immatricolazione ad un Corso di Studio universitario.

La tabella 2 riassume i dati quantitativi dei

progetti ECDL negli ultimi quattro anni ed evidenza le relative variazioni percentuali. Dalla tabella si nota una certa contrazione del numero di certificazioni ECDL rilasciate a studenti universitari.

La contrazione nell'anno solare 2006 del fenomeno ECDL negli Atenei è confermata dall'analisi dei dati di AICA relativi alle Skills Card rilasciate a studenti universitari (Figura 12).

Per quanto riguarda le certificazioni ECDL precedentemente acquisite dagli studenti e riconosciute dagli Atenei, l'indagine ha mostrato un forte incremento (pari al 50,3%) del numero di certificazioni ECDL riconosciute agli studenti, che passano da 2.077 nel 2005 a 3.121 nel 2006. Questo incremento è anco-

ra più marcato (pari al 71%) se si confrontano i dati dell'anno solare 2006 con quelli dell'anno solare 2003. È interessante notare che nell'anno solare 2006 i riconoscimenti hanno coinvolto ben 33 Atenei rispetto ai 28 del 2005. Inoltre, oltre un quarto di questi 33 Atenei ha riconosciuto 100 o più certificazioni ECDL ciascuno, per un totale di 2.337 certificazioni (pari al 75%).

L'incremento delle certificazioni ECDL riconosciute dagli Atenei riflette la crescente diffusione di questo tipo di certificazione presso la scuola media superiore e giustifica in parte la diminuzione sia di esami svolti che di certificazioni rilasciate dagli Atenei. Per esempio, il numero di Skills Card rilasciate agli studen-

	Anno 2003	Anno 2004	Variazione 2003-2004	Anno 2005	Variazione 2004-2005	Anno 2006	Variazione 2005-2006
Studenti da formare	101.635	50.755	-50,1%	53.527	5,5%	65.545	22,5%
Esami sostenuti (moduli)	124.159	144.649	16,5%	170.423	17,8%	130.863	-23,2%
Esami superati (moduli)	98.849	120.266	21,7%	141.682	17,8%	103.277	-27,1%
Certificazioni ECDL START rilasciate	10.759	11.842	10,1%	12.191	2,9%	10.097	-17,2%
Certificazioni ECDL FULL rilasciate	8.029	8.612	7,3%	11.981	39,1%	11.757	-1,9%
Certificazioni ECDL riconosciute	1.826	1.402	-23,2%	2.077	48,1%	3.121	50,3%

TABELLA 2

Sintesi del numero di esami svolti e superati dagli studenti e del numero di certificazioni rilasciate negli anni 2003-2006

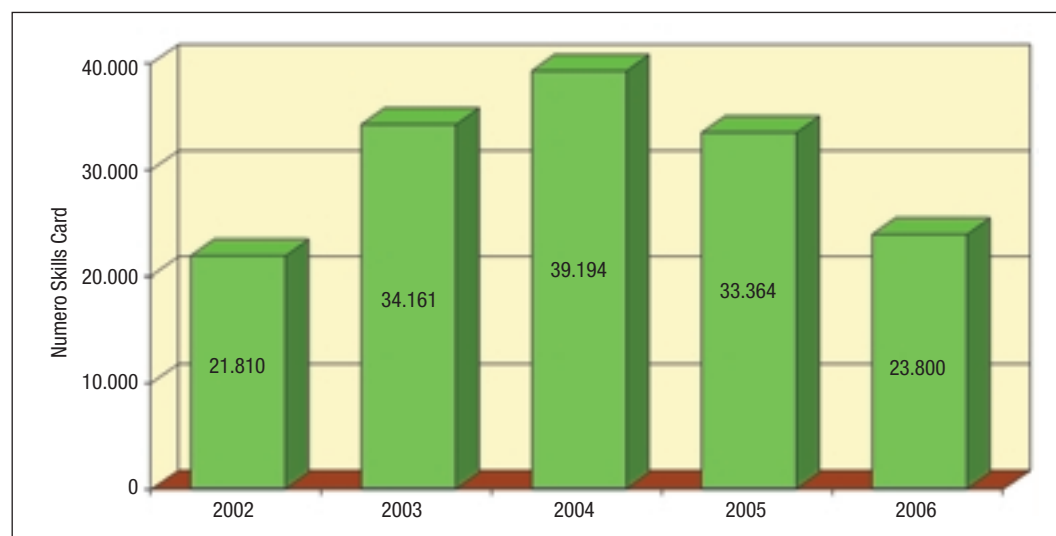


FIGURA 12
Andamento delle Skills Card rilasciate a studenti universitari

ti di scuola media superiore è aumentato, nel periodo 2003-2006, del 70%, una percentuale paragonabile a quella registrata in termini di aumento delle certificazioni riconosciute dagli Atenei.

Sarà interessante nelle prossime indagini dell'Osservatorio approfondire la portata di questo fenomeno e analizzare il suo potenziale impatto a livello universitario. Indubbiamente il progressivo allargamento di un'acquisizione qualificata di abilità informatiche presso una popolazione più giovane può aver contribuito a ridurre la richiesta della certificazione ECDL in ambito universitario. Va comunque sottolineato come il bacino di utenza sia talmente ampio da consentire opportunità ancora molto significative a questo tipo di certificazione.

4. IL PUNTO DI VISTA DEI DESTINATARI DELLE CERTIFICAZIONI INFORMATICHE

La progressiva riduzione di attività relative alla certificazione ECDL negli Atenei – evidenti dai risultati dell'indagine 2007 e in parte emersa nell'indagine 2006 – ha suggerito di rilevare il punto di vista degli studenti che avevano acquisito tale certificazione, al fine di meglio discriminare tra una situazione contingente (legata in particolare alla conclusione del progetto CampusOne e dei relativi finanziamenti) e un effettivo disinteresse verso l'acquisizione certificata di competenze operative di base nell'uso degli strumenti informatici.

Per effettuare questa rilevazione, si è proceduto a selezionare in modo casuale un campione estratto dall'insieme degli studenti universitari che avevano ottenuto la certificazione ECDL negli anni 2004, 2005 e 2006, e a contattare telefonicamente tali studenti fino ad ottenere un numero di interviste pari a circa 70 per ogni anno (più precisamente, 68 interviste a studenti certificati nel 2004, 70 a studenti certificati nel 2005 e 70 a studenti certificati nel 2006).

La distribuzione geografica degli studenti intervistati è riportata nella figura 13, mentre la figura 14 riporta la distribuzione geografica degli Atenei a cui erano iscritti gli studenti intervistati. Come si può notare, l'indagine –

mirata a raggiungere una distribuzione omogenea di studenti sul territorio nazionale – ha di fatto selezionato solo 29 Atenei, con una rappresentatività decisamente significativa al Nord (12 Atenei) e al Sud (7 Atenei) e decisamente inferiore nelle Isole e soprattutto al Centro (solo 5 Atenei).

Il documento completo dell'indagine 2007 dell'Osservatorio [9] presenta in modo approfondito i risultati dell'indagine telefonica. In questo articolo si sintetizzano gli aspetti salienti, inquadrandoli nel contesto più generale delle certificazioni informatiche nel mondo universitario.

Il primo aspetto fondamentale riguarda il livello di gradimento degli studenti nei confronti della certificazione ECDL. Che tale livello di

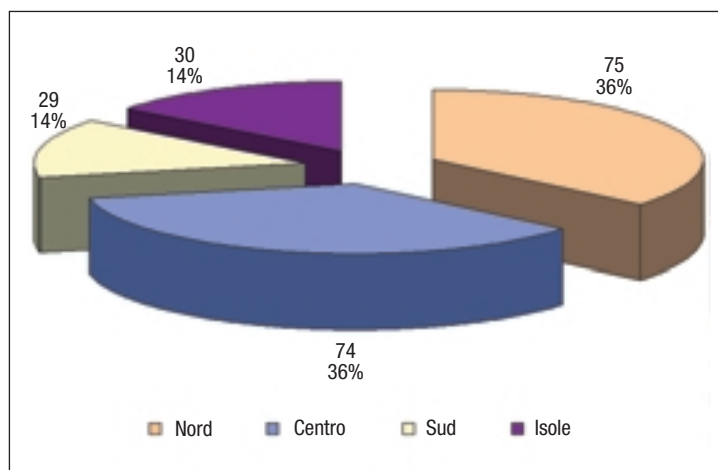


FIGURA 13

Distribuzione geografica degli studenti universitari oggetto dell'indagine telefonica

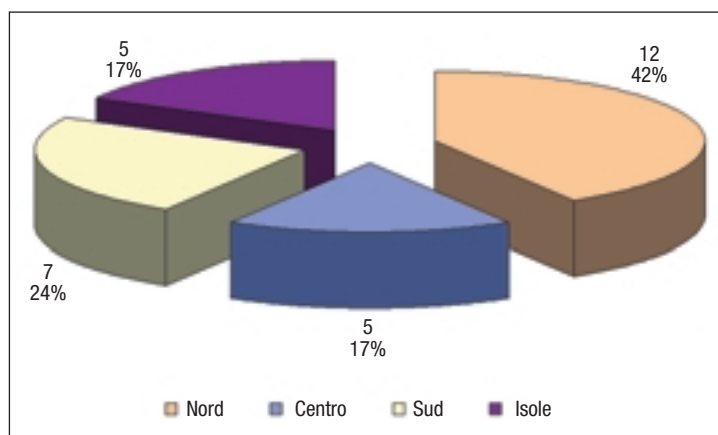


FIGURA 14

Distribuzione geografica degli Atenei a cui erano iscritti gli studenti universitari intervistati

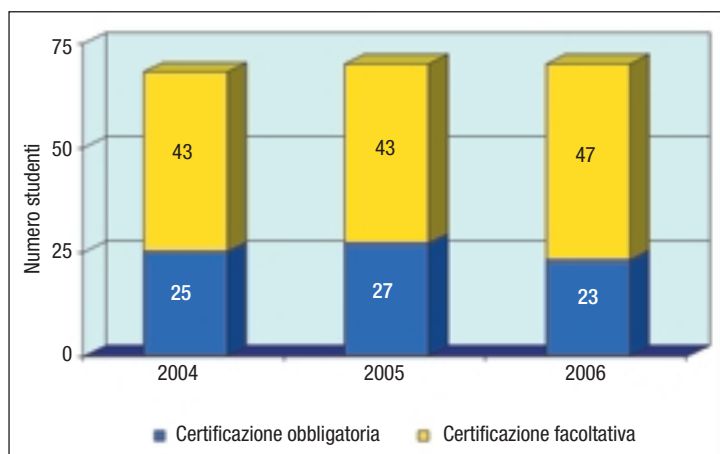


FIGURA 15
Obbligatorietà della certificazione ECDL in funzione dell'anno di conseguimento

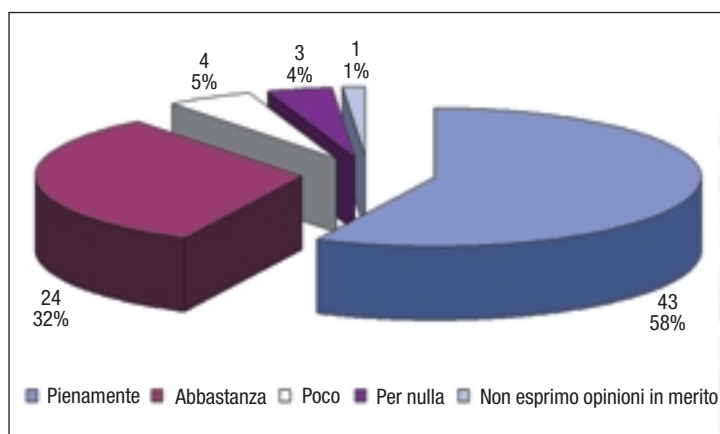


FIGURA 16
Parere degli studenti sulla decisione dei Corsi di Studio di rendere obbligatoria la certificazione ECDL

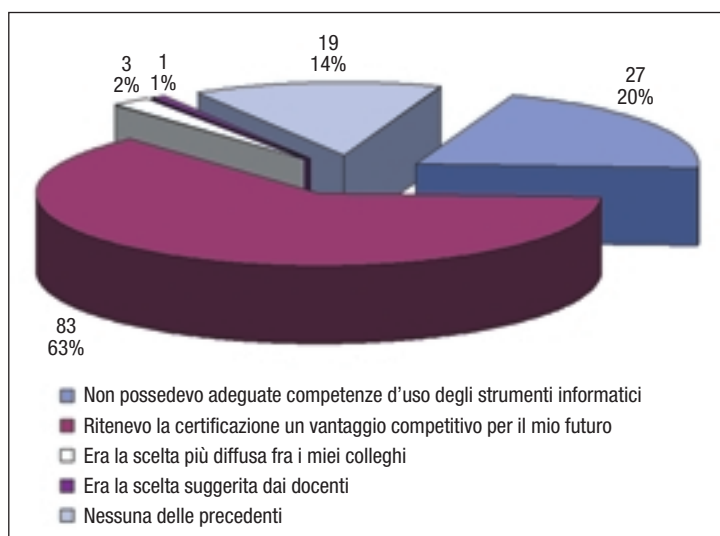


FIGURA 17
Motivazioni al conseguimento della certificazione ECDL facoltativa

gradimento sia in generale buono emerge già dalla distribuzione – riportata nella figura 15 – che mostra come la maggioranza degli studenti abbia ottenuto la certificazione ECDL **senza** che questa fosse considerata obbligatoria nel Corso di Studio a cui erano iscritti. L'elevato livello di gradimento della certificazione ECDL emerge in modo ancora più evidente dalle opinioni dei 75 studenti iscritti a Corsi di Studio per i quali la certificazione ECDL era obbligatoria. Il 58% degli intervistati si dichiara pienamente d'accordo con la decisione del proprio Corso di Studi di rendere obbligatoria la certificazione ECDL, e un altro 32% si dichiara abbastanza d'accordo, portando il totale delle risposte positive al 90%, come indicato nella figura 16.

Da queste considerazioni appare chiaramente come il conseguimento di una certificazione di competenze operative informatiche, sia pure di base, sia stato vissuto non come un'imposizione ma come un valore aggiunto dagli studenti, sia che essi l'abbiano conseguita perché vincolante per proseguire gli studi, sia che siano stati invitati a farlo su base volontaria.

Una conferma ancora più chiara di quanto appena affermato viene dall'analisi delle motivazioni che hanno spinto gli studenti che si sono certificati su base volontaria. Come risulta dalla figura 17, dei 133 studenti per i quali la certificazione ECDL non era obbligatoria, quasi due terzi ritenevano tale certificazione un vantaggio competitivo per l'inserimento nel mercato del lavoro.

Il secondo aspetto emerso dall'indagine telefonica – sul quale vale la pena soffermarsi – riguarda il livello delle competenze raggiunte con il conseguimento della certificazione ECDL. Ben 101 dei 208 studenti intervistati (48,6%) hanno sentito l'esigenza di approfondire le competenze d'uso degli strumenti informatici acquisite con la certificazione, rivelando così come la preparazione necessaria per conseguire la certificazione ECDL non possa essere considerata completamente adeguata per le esigenze di studio e di lavoro degli attuali studenti universitari.

Le opinioni degli studenti circa gli argomenti oggetto di approfondimento sono sintetizzate nella figura 18: emerge chiaramente l'esigenza di approfondire i due strumenti di utilizzo più complesso (*Foglio elettronico* e *Basi di dati*,

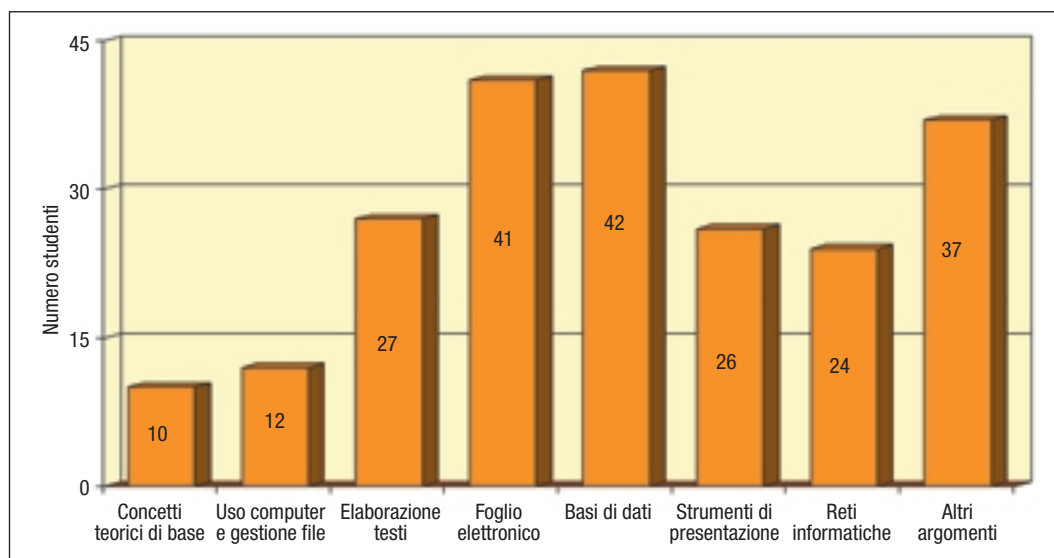


FIGURA 18

Approfondimenti richiesti dagli studenti dopo il conseguimento della certificazione ECDL

segnalati da 41 e 42 studenti, rispettivamente) ma anche l'opportunità di estendere la preparazione strumentale informatica al di fuori delle sette tematiche oggetto del syllabus ECDL (37 studenti dichiarano infatti interesse ad argomenti non trattati nel syllabus ECDL).

Da un'analisi del numero di argomenti oggetto di eventuali approfondimenti (Figura 19), emerge che la maggior parte degli studenti ne indica uno (il 49%) o due soltanto (il 28%). La motivazione più probabile per questo tipo di risultato è legata all'effettivo utilizzo – nella propria carriera universitaria o professionale – degli strumenti oggetto della certificazione: solo gli strumenti effettivamente utilizzati fanno rapidamente comprendere agli studenti che sarebbe auspicabile una loro migliore padronanza.

D'altro canto la certificazione ECDL *Advanced* – da alcuni anni disponibile sul mercato europeo e organizzata in modo modulare per permettere di approfondire solo gli strumenti più appropriati – non sembra essere particolarmente nota: solo 98 dei 208 studenti intervistati ne conoscono l'esistenza, e di questi 98 solo 55 fanno parte del gruppo di studenti che avevano avvertito l'esigenza di approfondimenti.

Inoltre, come evidenziato nella figura 20, si conferma una scarsa propensione degli studenti a conseguire una certificazione ECDL *Advanced*: più della metà degli studenti dichiara di non essere interessato, mentre meno di un quinto ha già conseguito o intende conseguire tale certificazione.

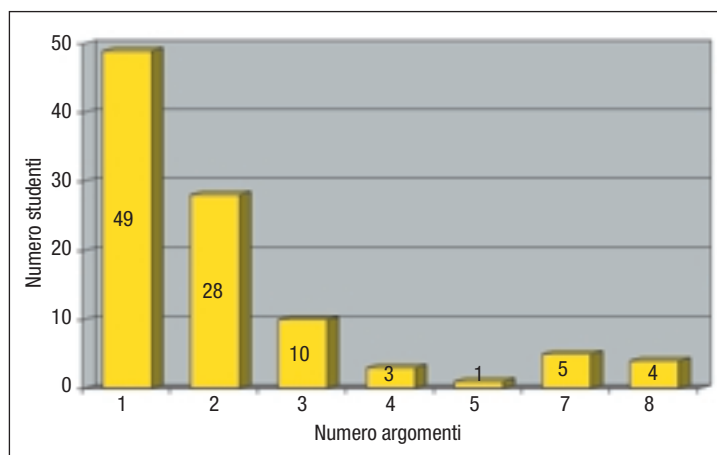


FIGURA 19

Andamento del numero di argomenti da approfondire da parte degli studenti

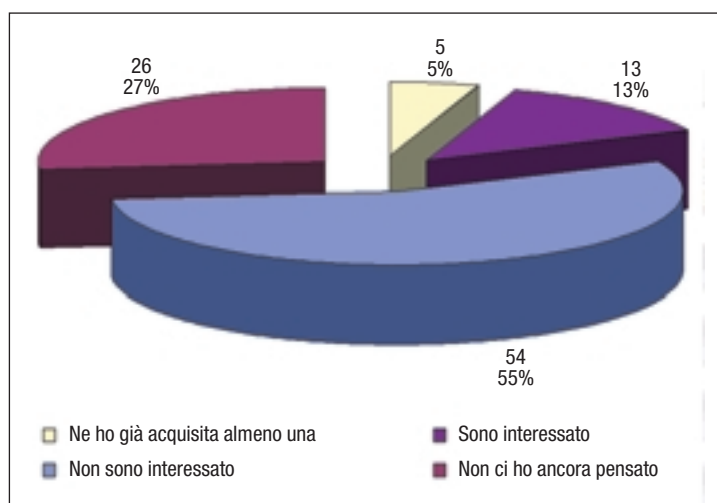


FIGURA 20

Posizione degli studenti rispetto alla certificazione ECDL Advanced

5. IL PROGETTO IT4PS

Dall'indagine telefonica sugli studenti certificati ECDL, emergono in estrema sintesi i seguenti punti:

- la certificazione è considerata un valore aggiunto e viene percepita in modo positivo;
- in molti casi, un uso più costante degli strumenti informatici rivela l'esigenza di acquisire maggiori competenze;
- una certificazione simile all'ECDL ma più approfondita – come l'ECDL *Advanced* – che si concentra sulle caratteristiche avanzate del singolo strumento informatico non viene considerata una strada particolarmente interessante.

Proprio per rispondere a questi punti, è stato lanciato qualche anno fa da parte di AICA e della Fondazione CRUI il progetto IT4PS (*Information Technologies for Problem Solving*).

Il progetto [4] si concentra sui due principali strumenti informatici (*Foglio elettronico* e *Basi di dati*, non a caso indicati dagli studenti come argomenti maggiormente “bisognosi” di approfondimenti) e si propone di arricchire la formazione alle abilità informatiche proposta dalla certificazione ECDL:

- garantendo la preparazione per un utilizzo professionale degli strumenti informatici, quale quello che ci si può aspettare dagli studenti universitari;
- contestualizzando la formazione a specifici ambienti applicativi.

Infatti, alla base del progetto IT4PS c'è l'impostazione di una formazione di livello universitario all'uso dei suddetti strumenti informatici – quindi orientata anche alle funzioni avanzate degli strumenti stessi – strutturata però in modo tale da adottare un approccio didattico mirato al *problem solving* e contestualizzato all'ambito disciplinare di specifiche famiglie di Corsi di Studio, ovvero un approccio didattico che parta da problemi tipici del singolo ambito disciplinare dimostrando come tali problemi possano essere risolti grazie ad un uso avanzato degli strumenti informatici.

Il progetto ha prodotto – nella sua prima fase – sei moduli formativi all'uso contestualizzato del *Foglio elettronico* e delle *Basi di dati* in tre diversi contesti curriculari: Economia, Medicina e Farmacia, Statistica nelle Scienze Sociali. I moduli formativi sono stati pubblicati in altrettanti volumi [5, 6, 7, 8, 10, 14] e sono stati inoltre realizzati due sistemi autore per consentire

la predisposizione di esercizi di autovalutazione a soluzione guidata dal docente [13].

Una prima sperimentazione si è svolta nel 2004 ed ha coinvolto una decina di Atenei e qualche centinaio di studenti, permettendo così di verificare l'efficacia dell'approccio e il suo gradimento da parte di docenti e studenti. D'altro canto, la certificazione delle competenze conseguite non è stata possibile a causa della mancanza di uno strumento di valutazione che mettesse al centro del momento di verifica la risoluzione dei problemi, piuttosto che la conoscenza approfondita dello strumento informatico utilizzato (come avviene tipicamente per la certificazione ECDL *Advanced*).

Proprio per superare tale difficoltà, il progetto IT4PS ha affrontato nella sua fase finale la definizione di un metodo di verifica delle competenze per attestare il possesso di una competenza e di una comprensione delle potenzialità dello strumento per la soluzione concreta di problemi curriculari.

Nel corso del 2006 tale metodo di verifica è stato messo a punto, sono stati progettati i test di verifica e si sono definite le linee-guida per la valutazione degli elaborati dei candidati. Nel primo semestre 2007, alcuni Atenei hanno accettato di somministrare a qualche centinaio di studenti corsi di formazione basati sui materiali didattici prodotti da IT4PS e di sottoporre tali studenti ai suddetti test.

Alla luce dei risultati dei test (svolti intorno all'estate 2007) la metodologia di valutazione sarà definitivamente assestata e utilizzata da AICA per proporre al mercato italiano – soprattutto universitario – questa nuova tipologia di certificazione delle competenze informatiche, centrata appunto sulla capacità di risolvere problemi concreti mediante lo strumento informatico.

Il passo finale, previsto per il 2008, consisterà nella “esportazione” a livello europeo dell'approccio IT4PS, per consentire a studenti di tutta Europa di ottenere una certificazione contestualizzata e per garantire un riconoscimento transnazionale alla certificazione stessa.

6. CONCLUSIONI

Le indagini promosse dall'Osservatorio AICA-CINI-Fondazione CRUI al fine di analizzare l'introduzione e la diffusione delle certificazioni informatiche negli Atenei Italiani hanno

portato ad evidenziare molti aspetti interessanti che riguardano la certificazione ECDL, sia dal punto di vista istituzionale degli Atenei sia dal punto di vista dei suoi utenti finali, cioè degli studenti.

Anche nell'anno solare 2006 la certificazione ECDL si è rivelata uno strumento consolidato e ampiamente utilizzato da molti Atenei per accreditare le abilità informatiche di base degli studenti; ciò nonostante si comincia a notare un suo certo ridimensionamento, legato sia alla conclusione del progetto CampusOne e alla conseguente mancanza del relativo supporto finanziario, sia al lento ma progressivo spostamento della certificazione ECDL a livello di scuole secondarie superiori.

Va tuttavia notato come il ridimensionamento operato dagli Atenei nei confronti della certificazione ECDL contrasti con il punto di vista di un campione di studenti universitari che hanno ottenuto negli ultimi tre anni questo tipo di certificazione. La percezione di questi studenti della certificazione ECDL e della sua valenza di vantaggio competitivo per l'inserimento professionale è pienamente positiva. Gli studenti mostrano un generale apprezzamento della scelta degli Atenei di inserire la certificazione ECDL nella loro offerta formativa e si avvicinano a questo tipo di certificazione anche

laddove non è considerata un requisito per il proseguimento della carriera universitaria.

In prospettiva, è certamente auspicabile un rapido spostamento degli Atenei verso certificazioni più specifiche per il contesto universitario, quali, per esempio, la certificazione IT4PS, destinata ad utenti evoluti degli strumenti informatici, e le certificazioni EUCIP, destinate ai professionisti dell'ICT. Questo spostamento dovrà però essere accompagnato e sostenuto da una sempre più capillare diffusione della certificazione ECDL nelle scuole secondarie. Se, infatti, è vero che gli studenti che accedono oggi alla formazione universitaria sono abituati a una familiarità quotidiana con gli strumenti informatici, è altrettanto vero che la conoscenza e l'utilizzo di questi strumenti rischiano spesso di essere generici; un loro uso adeguato richiede pertanto una specifica formazione approfondita. Occorre evitare che una generazione destinata a confrontarsi sempre di più con le tecnologie dell'informazione e della comunicazione si ritrovi con una diffusa carenza di alfabetizzazione informatica. Questo è un problema non solo italiano [15]; è dunque opportuno che AICA continui con grande energia la sua opera di aggiornamento e diffusione delle certificazioni informatiche nel mondo universitario e non solo.

Il punto di vista dell'intervistatrice



di Ilaria Scarabottolo

Era la prima volta che mi trovavo davanti a un telefono per chiamare uno sconosciuto e fargli delle domande e in effetti all'inizio ero piuttosto impacciata. Poi, man mano che collezionavo dati, anche la lingua si scioglieva e imparavo a porre le domande in modo che fossero più facili da capire e non troppo lunghe.

Una delle primissime cose che ho notato è la varietà di modi di rispondere da parte degli intervistati: c'è chi risponde un po' irritato, chi impiega anni a decidere cosa dire, chi risponde a monosillabi e di corsa, chi dice molto più di quello che hai chiesto, chi ti racconta tutta la sua carriera universitaria e dopo dieci minuti finalmente parla della certificazione e poi ci sono i più simpatici che rispondono contenti e alla fine dell'intervista, quando dici "grazie per l'aiuto", rispondono "ma grazie a te!". Questi sono i migliori, e mi sono accorta che ce n'è una concentrazione sorprendente in Toscana e nelle Marche.

Al nord di solito trovavo parecchia disponibilità, mentre al sud era molto più difficile ottenere un'intervista perché tantissimi studenti avevano fornito il numero di casa ma vivevano da un'altra parte e non sempre i genitori erano disposti a darmi il numero di cellulare.

Una cosa che mi divertiva un sacco era quando qualche genitore un po' diffidente pensava che si trattasse di una pubblicità e stessi cercando di vendere qualcosa, quindi mi rispondevano che il figlio aveva già ottenuto la certificazione o che non gli interessava. Pochi mi hanno chiesto per conto di chi stessi facendo l'intervista, e nessuno mi ha chiesto il numero di riferimento per accertarsi che non fosse uno scherzo. La maggior parte mi ha risposto senza fare domande, evidentemente gli studenti italiani si fidano degli intervistatori telefonici. In generale è stata un'esperienza davvero interessante e in molti casi anche divertente. C'erano sere in cui ero un po' stanca o avevo poca voglia di telefonare, ma mi capitava un intervistato simpaticissimo che mi ringraziava e mi tirava su di morale, oppure la serata era fortunata e mi rispondevano parecchi numeri di fila. Però ci sono state sere piuttosto infruttuose in cui non riuscivo a intervistare quasi nessuno. Nonostante qualche piccolo problema, è un lavoro che ripeterei molto volentieri e mi sono ripromessa che d'ora in poi risponderò a tutte le interviste telefoniche che mi capiteranno!

Ringraziamenti

Gli autori desiderano ringraziare i Referenti degli Atenei che hanno partecipato con costanza e disponibilità alle indagini promosse dall'Osservatorio. Un particolare ringraziamento va anche a Marcello Beccaria, Pietro Marzani e Ilaria Scarabottolo per la preziosa collaborazione alle attività dell'Osservatorio. Gli autori sono infine molto riconoscenti ad AICA, CINI e Fondazione CRUI per il costante incoraggiamento.

Bibliografia

- [1] Sito Osservatorio AICA-CINI-Fondazione CRUI sulle Certificazioni ICT negli Atenei Italiani, <http://osservatorio.consortio-cini.it>.
- [2] Alfonsi C.R., Calzarossa M., Ciancarini P., Maresca P., Mich L., Sala F., Scarabottolo N.: Il Progetto CampusOne e la Certificazione ECDL nelle Università Italiane. In: A. Andronico e G. Casadei (Ed.), *Didamatica 2007 - Informatica per la Didattica*, Cesena, 10-12 Maggio 2007, p. 634-643.
- [3] Alfonsi C.R., Calzarossa M., Ciancarini P., Maresca P., Mich L., Sala F., Scarabottolo N.: Certificazioni delle conoscenze informatiche nelle Università Italiane. *Mondo Digitale*, anno V, n. 4, Dicembre 2006, p. 47-59.
- [4] Alfonsi C.R., Pedreschi D., Scarabottolo N., Simi M.: Il progetto IT4PS: il computer per la soluzione di problemi. *Mondo Digitale*, anno V, n. 3, Settembre 2006, p. 3-15.
- [5] Atzeni P., De Checchi A., Sindoni G., Tirelli M., Fiorentino G., Pala A.P.: *Le basi di dati per Economia*. McGraw-Hill, 2006.
- [6] Atzeni P., De Checchi A., Sindoni G., Tirelli M., Fabrizio A., Pacini G.: *Il foglio elettronico per Economia*. McGraw-Hill, 2005.
- [7] Bagnati D., Nicolini G., Salini S., Viscusi N., Fiorentino G., Pala A.P.: *Le basi di dati per la Statistica nelle Scienze sociali*. McGraw-Hill, 2006.
- [8] Bagnati D., Nicolini G., Viscusi N., Salini S., Fabrizio A., Pacini G.: *Il foglio elettronico per la Statistica nelle Scienze sociali*. McGraw-Hill, 2005.
- [9] Breno E., Calzarossa M., Ciancarini P., Maresca P., Mich L., Sala F., Scarabottolo N.: Le Certificazioni Informatiche nelle Università Italiane – Indagine 2007. Disponibile on-line all'indirizzo: <http://osservatorio.consortio-cini.it/publicazioni.htm>.
- [10] Brogi A., Martinelli A., Gervasi V., Manghi P., Fabrizio A., Pacini G.: *Il foglio elettronico per Medicina e Farmacia*. McGraw-Hill, 2005.
- [11] Calzarossa M., Ciancarini P., Maresca P., Mich L., Scarabottolo N.: The ECDL Programme in Italian Universities. *Computers & Education*, Vol. 49, n. 2, Elsevier, 2007, p. 514-529.

- [12] Censis - *La Repubblica: La Grande Guida all'Università*, 2006. Disponibile on-line all'indirizzo: <http://download.repubblica.it/pdf/2006/censis/11072006.pdf>
- [13] Fabrizio A., Fiorentino G., Pacini G.: *I sistemi autore PSWelcome e Access Test Manager*. McGraw-Hill, 2006.
- [14] Manghi P., Brogi A., Gervasi V., Martinelli A., Fiorentino G., Pala A.P.: *Le basi di dati per Medicina e Farmacia*. McGraw-Hill, 2006.
- [15] Stone J.A., Madigan E.: Inconsistencies and disconnects. *Communications of the ACM*, Vol. 50, n. 4, Aprile 2007, p. 76-79.

CRISTIANA RITA ALFONSI, dal 1996 è Responsabile dell'Unità Progetti, Servizi e Formazione della Fondazione CRUI, occupandosi in particolare della progettazione, della gestione e del coordinamento, del monitoraggio e della valutazione, della formazione del personale universitario non docente, dell'orientamento. I progetti più importanti di cui si è occupata in questo periodo sono: Campus (1996-2000); Credits (1998-2000); Apollo (1999-2000); CampusOne (2000-2003); IT4PS (2003-2004); EUCIP4U (2005-2007); B1-on-line (2005-2007). Ha diretto e coordinato la ricerca sul tutorato universitario e il management didattico. Ha progettato l'Osservatorio sull'e-learning universitario in Italia ed è Responsabile del Progetto ELUE (E-Learning and University Education) co-finanziato dall'Unione Europea. E-mail: alfonsi@fondazionecru.it

ELENA BRENO, esperta nella gestione di banche dati, dal 1995 ha partecipato a numerose attività di ricerca del Centro Studi della Fondazione CRUI, curando la progettazione e la gestione delle banche dati di riferimento. In particolare, fa parte del gruppo di ricerca CRUI che svolge attività di analisi sulla banca dati americana Thomson-ISI; tale attività ha permesso di individuare e sviluppare indicatori bibliometrici standard per la valutazione della produzione scientifica italiana. E-mail: breno@fondazionecru.it

MARIA CARLA CALZAROSSA, Professore ordinario di Impianti di Elaborazione presso la Facoltà di Ingegneria dell'Università di Pavia. Dal 2002 coordina il Gruppo di Lavoro che ha realizzato l'Osservatorio Permanente delle Certificazioni Informatiche negli Atenei Italiani (<http://osservatorio.consortio-cini.it>). Collabora con la Commissione Europea per varie attività di monitoraggio dei Programmi Quadro. E-mail: mcc@unipv.it

PAOLO CIANCARINI, Professore ordinario di Informatica all'Università di Bologna, dove insegna Ingegneria del Software. È socio e consigliere di AICA, nonché membro del Comitato Scientifico di Mondo Digitale. Fa parte del Gruppo di Lavoro che ha realizzato l'Osservatorio Permanente delle Certificazioni

Informatiche negli Atenei Italiani. Dal 2007 è Direttore del Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

E-mail: ciancarini@cs.unibo.it

PAOLO MARESCA, Professore associato di Sistemi per l'Elaborazione delle Informazioni presso il Dipartimento di Informatica e Sistemistica dell'Università di Napoli Federico II. Fa parte del Gruppo di Lavoro che ha realizzato l'Osservatorio Permanente delle Certificazioni Informatiche negli Atenei Italiani. È membro dell'AICA ed è *valued member* dell'IEEE. Autore di circa 100 lavori in congressi, e riviste nazionali ed internazionali su tematiche ICT, è *referee* e *associated editor* di riviste internazionali nel settore informatico e coordinatore della comunità Italiana di Eclipse.

E-mail: paomares@unina.it

LUISA MICH, Professore associato di Ingegneria Informatica presso l'Università di Trento. Fa parte del Gruppo di Lavoro che ha realizzato l'Osservatorio Permanente delle Certificazioni Informatiche negli Atenei Italiani. È promotore dell'ECDL (European Computer Driving License) nell'Università di Trento,

prima Università Italiana ad avviare tale iniziativa.

E-mail: luisa.mich@economia.unitn.it

FULVIA SALA, dopo aver conseguito un Master in Statistica presso l'Università della California - Berkeley, ha ricoperto ruoli direttivi nell'area del marketing e della pianificazione nel settore informatico. Collabora con AICA dove svolge attività di consulenza nelle stesse aree.

E-mail: fulvia.sala@aicanet.it

NELLO SCARABOTTOLO, Professore ordinario di Informatica presso il Dipartimento di Tecnologie dell'Informazione dell'Università di Milano, collabora da tempo con la Fondazione CRUI e con AICA su progetti di definizione, diffusione e monitoraggio delle certificazioni ICT nelle università italiane. Fa parte del Gruppo di Lavoro che ha realizzato l'Osservatorio Permanente delle Certificazioni Informatiche negli Atenei Italiani. È Honorary Secretary del CEPIS (il Council of European Professional Informatics Societies) l'ente che riunisce le Associazioni europee di informatica, di cui AICA è la rappresentante per l'Italia.

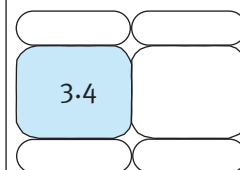
E-mail: nello.scarabottolo@unimi.it



WEB MART: UN PARADIGMA INNOVATIVO PER L'ACCESSIBILITÀ DEI SITI WEB

Nonostante le numerose iniziative per l'accessibilità delle applicazioni web, i metodi e le linee guida sino ad ora proposti risultano spesso insufficienti a garantire la produzione di applicazioni realmente accessibili da parte di ogni categoria di utenti. Molti metodi si concentrano sull'accessibilità della presentazione, trascurando l'accessibilità dei contenuti. Questo articolo presenta un metodo per l'accessibilità dei contenuti, che fa uso di un modello concettuale per guidare la progettazione delle applicazioni web tramite astrazioni di alto livello.

Stefano Ceri
Maristella Matera



1. INTRODUZIONE

L'accessibilità, nella sua accezione più comune, si riferisce a quell'insieme di proprietà che rendono un sito web fruibile da parte di utenti disabili. Sotto questa specifica connotazione, tale termine si fa sempre più varco nel mondo dell'*Information Technology*, ma anche nell'opinione pubblica. Numerose sono le iniziative nazionali e internazionali volte a regolamentare la produzione di siti web accessibili. In particolare, l'iniziativa WAI (*Web Accessibility Initiative*) del consorzio W3C (*World Wide Web Consortium*), definisce l'accessibilità come il bisogno di creare contenuti per il web facilmente *individuabili, comprensibili e utilizzabili* da parte di un vasto insieme di utenti [19]. Tale iniziativa promuove la definizione di linee guida per lo sviluppo di applicazioni web che siano accessibili da utenti con ogni tipo di disabilità, ma anche, più in generale, da individui non affetti da patologie. Essa si colloca infatti nel contesto di un più ampio progetto, la "Progettazione Universale" [16, 18], il cui scopo è permettere l'accesso alle informazioni pubblica-

te sul web a un vasto spettro di utenti, con caratteristiche e bisogni diversi e in una grande varietà di contesti d'uso.

Nonostante le numerose iniziative, e in particolare l'iniziativa promossa dal WAI, costituiscono un valido contributo per la diffusione dei metodi per l'accessibilità, l'utilizzo delle linee guida proposte risulta spesso insufficiente a garantire la produzione di applicazioni web accessibili. Alcuni studi, condotti su mille siti web inglesi per conto della UK Disability Rights Commission [11], hanno dimostrato che nella maggior parte dei casi i siti web sono difficili da accedere e navigare, ma anche che il 45% dei problemi riscontrati non è riconducibile a violazioni delle linee guida del WAI, quanto piuttosto a fattori come la confusa o non evidente organizzazione dei contenuti, o l'utilizzo di intricati meccanismi di navigazione. Infatti, l'accezione più comune di accessibilità si concentra principalmente sulle proprietà della codifica HTML delle pagine web e garantisce che i contenuti di ogni singola pagina siano "leggibili" per mezzo delle tecnologie a supporto degli utenti disabili (per esem-

pio gli screen readers). La conseguenza è che tali linee guida tendono in particolare a garantire l'accessibilità della presentazione. Sebbene tale proprietà sia per molti versi fondamentale, non si può non considerare che, prima ancora di garantire la "leggibilità" dei contenuti, le applicazioni web dovrebbero fornire informazioni ben organizzate e supportare gli utenti, a qualsiasi categoria essi appartengano, a ritrovare e navigare tali informazioni [12, 16], garantendo così un'ulteriore proprietà, che nel corso di questo articolo chiameremo "l'accessibilità dei contenuti".

L'accessibilità dei contenuti è essenziale: quando questa è carente, anche i più ricercati meccanismi di presentazione, pur compatibili con le diverse tecnologie di accesso e di lettura dei siti, non sono in grado di supportare appieno gli utenti nell'accesso e nella navigazione dei contenuti. Tale proprietà è tanto più rilevante quanto più l'applicazione web è chiamata a gestire e pubblicare vaste collezioni di dati; assume quindi un ruolo decisivo nel caso di applicazioni web "centrate sui dati", come le biblioteche digitali, i cataloghi elettronici, o anche i siti istituzionali, il cui obiettivo principale è rendere disponibili agli utenti grandi quantità di dati e servizi.

Al fine di garantire l'accessibilità dei contenuti, la modellazione dei dati rappresenta uno degli aspetti più rilevanti nello sviluppo di un'applicazione web. L'accessibilità dei contenuti richiede, infatti, una chiara individuazione di alcuni contenuti centrali, che sinteticamente convogliano l'informazione dell'intera applicazione e quindi l'uso, nell'interfaccia ipertestuale, di alcune configurazioni di accesso ben organizzate, tali da permettere all'utente di controllare il processo di ricerca e di navigazione dei contenuti.

In questo articolo, discuteremo metodi ed euristiche per ottenere l'accessibilità dei contenuti, che derivano da due principi chiave: l'*adozione di modelli concettuali*, per guidare la modellazione di un'applicazione web tramite l'uso di astrazioni di alto livello, e l'*uso di strategie "top-down"*, per giungere alla specifica dettagliata dell'applicazione partendo da alcune decisioni iniziali sull'organizzazione dei dati e procedendo attraverso passi incrementali di raffinamento. L'articolo propone in particolare i **Web Mart**, una nuova astrazione concettuale

che, in modo simile ai *Data Mart* per le *Data Warehouse*, aiuta a definire l'organizzazione dell'informazione pubblicata da un'applicazione Web centrata sui dati e l'interfaccia ipertestuale che ne permette l'accesso. Per il loro ruolo nella modellazione di applicazioni web, i Web Mart possono essere considerati blocchi fondamentali per la costruzione di applicazioni web dai contenuti accessibili.

2. I WEB MART

La modellazione dei contenuti è forse l'aspetto più importante nello sviluppo delle applicazioni web centrate sui dati. Quando, in un'applicazione, il contenuto informativo è utilizzato per supportare compiti ben precisi, è possibile riconoscere delle configurazioni specifiche per l'organizzazione dei dati. Per esempio, in passato gli esperti di *Data Warehouse* hanno proposto i Data Mart come un particolare schema concettuale che enfatizza la facilità di accesso dei dati, sulla base di scopi particolari riconosciuti in fase di progettazione [13]. I Data Mart sono costituiti da un'entità che descrive "fatti" rilevanti, circondata da diverse entità che descrivono "dimensioni" per l'accesso e l'analisi di tali fatti. Per la loro particolare topologia, i Data Mart sono anche conosciuti come schemi a stella (*star schemas*). Secondo tale organizzazione, gli utenti interessati a ritrovare i dati relativi a certi fatti usano le dimensioni di accesso; alcuni strumenti di aggregazione permettono poi di estrarre dai fatti alcune proprietà di analisi. La topologia fissa permette inoltre la definizione di operazioni specifiche per la gestione dei dati, come "*slicing*" e "*dicing*", cioè la progressiva aggiunta o eliminazione di dimensioni di accesso, al fine di ottenere diverse prospettive di analisi.

In analogia con i Data Mart, per le applicazioni web centrate sui dati abbiamo individuato i Web Mart, una nuova astrazione per la modellazione concettuale dei dati, che aiuta a individuare i concetti principali di un'applicazione web e a organizzare i contenuti relativi a tali concetti in modo da migliorare la loro accessibilità attraverso l'interfaccia ipertestuale.

I Web Mart sono costituiti da un'entità principale, chiamata *concetto centrale*, e da diverse entità accessorie di due tipi: le *entità di accesso* e le *entità di dettaglio*.

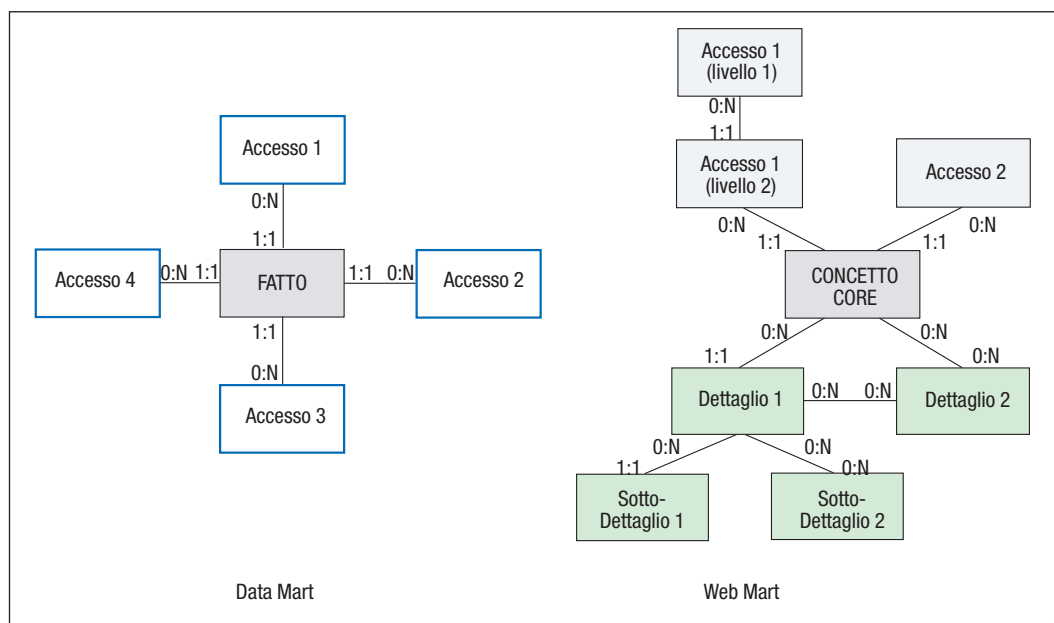


FIGURA 1
Data Mart e Web Mart, rappresentati secondo la notazione del modello Entità-Relazione (ER)

La figura 1 illustra le differenze principali tra un Data Mart e un Web Mart¹:

□ mentre nei Data Mart tutte le dimensioni hanno un ruolo equivalente, cioè quello di facilitare l'accesso dei fatti centrali, nei Web Mart le entità di accesso e le entità di dettaglio hanno ruoli distinti. Le prime sono pensate per facilitare la definizione di meccanismi di accesso nell'interfaccia ipertestuale; esse infatti memorizzano categorie, per la classificazione di concetti centrali, sulla cui base è possibile definire "indici" per ritrovare i concetti centrali. Le seconde favoriscono invece la definizione di schemi strutturati per la navigazione delle informazioni relative ai concetti centrali, secondo i quali, in seguito all'accesso dei dati principali rappresentati dall'entità centrale, è possibile poi ritrovare dati aggiuntivi di dettaglio, eventualmente contenuti in pagine distinte, accessibili a partire dalla pagina dedicata al concetto centrale. In pratica, la struttura dei Web Mart a livello dei dati riflette due diverse modalità d'uso dei dati, rispettivamente la ricerca e l'approfondimento delle informazioni su web;

□ mentre in un Data Mart tutte le informazioni relative ad una certa dimensione di accesso sono accorpate in un'entità singola, in un

Web Mart sia le dimensioni di accesso sia le informazioni di dettaglio possono essere organizzate gerarchicamente su più livelli. Possono inoltre sussistere interconnessioni tra le entità di dettaglio. È possibile quindi giungere alla definizione di schemi dei dati più articolati di una semplice stella.

L'organizzazione di un'applicazione web deve essere tale da favorire la navigazione tra i diversi concetti centrali che la caratterizzano, quindi tra i suoi diversi Web Mart. Al fine di rendere possibile tale navigazione, è necessario introdurre uno *schema di interconnessione*, per poter esplicitare eventuali associazioni semantiche esistenti tra i vari concetti centrali e poter quindi arricchire l'interfaccia ipertestuale con un insieme di link che rappresentino le associazioni individuate. Con l'aggiunta di tale ingrediente, lo schema dei dati di un'applicazione web può essere quindi descritto individuando e rappresentando:

□ gli *schemi dei singoli Web Mart*, ognuno caratterizzato da un *sottoschema centrale*, costituito dall'entità centrale e dalle sue entità di dettaglio, e da un *sottoschema di accesso*, costituito dalle entità di accesso;

□ lo *schema di interconnessione*, relativo alle associazioni esistenti tra i vari Web Mart.

¹ Le composizioni di dati che caratterizzano i Data Mart e i Web Mart sono rappresentate per mezzo della notazione Entità-Relazione [3]: i nodi rettangolari denotano classi di oggetti informativi, le *entità*; gli archi denotano le *relazioni* che sussistono tra oggetti informativi appartenenti alle varie entità.

I Web Mart non si basano su teorie astratte, ma al contrario derivano dall'analisi di pattern di modellazione ricorrenti e di successo, riconosciuti in diversi modelli di applicazioni web [7]. La presenza nel web di strutture regolari, del tutto simili ai Web Mart, è stata inoltre riconosciuta da uno studio sulla topologia del web [9], secondo cui è possibile individuare diverse collezioni coese di pagine, associate tra loro da alcuni collegamenti, tali da formare una "dorsale di navigazione" che è raggiungibile da diverse altre pagine e che a sua volta offre collegamenti verso altre pagine. Tale struttura è frattale per natura e quindi si ripete a vari livelli: l'intero web presenta cioè un'organizzazione simile a quella di ogni sua parte. I risultati sperimentali di tale studio suggeriscono quindi che, per progettare servizi web efficaci ed efficienti, è sufficiente comprendere e riproporre la struttura che emerge da un semplice modello stocastico [9].

Tali risultati sono sorprendentemente coerenti con la nostra ipotesi sull'organizzazione delle applicazioni web: la dorsale di navigazione rappresenta lo schema di interconnessione, che raggruppa sia i concetti centrali, sia le interconnessioni esistenti tra essi. Le pagine da cui è possibile raggiungere la dorsale si basano sul sottoschema di accesso. Le pagine raggiungibili dalla dorsale si riferiscono invece alle entità di dettaglio associate ai vari concetti centrali. Lo studio conferma quindi in gran parte la nostra ipotesi, per la quale i Web Mart possono essere considerati ingredienti fondamentali per la progettazione di applicazioni web orientate all'accessibilità dei contenuti. Tuttavia, mentre da un lato il modello stocastico definito in [9] fonda la sua validità sulla vastità del campione di pagine web osservate (circa 60.000.000), dall'altro lo studio non fornisce alcuna classificazione semantica delle strutture web emerse, che invece sarebbe estremamente utile per comprendere appieno come tali strutture possano essere utilizzate nella progettazione di applicazioni web. Così come descritto nel seguito di questo articolo, il metodo di progettazione da noi proposto si pone invece l'obiettivo di suggerire linee guida per l'utilizzo dei Web Mart nella modellazione di applicazioni web dai contenuti accessibili.

3. UN METODO PER L'ACCESSIBILITÀ DEI CONTENUTI NEL WEB

A partire dall'individuazione dei Web Mart, è possibile definire un metodo per la progettazione di applicazioni web. Il metodo da noi proposto richiede che i progettisti facciano uso di *un modello dei dati*, per esprimere l'organizzazione del contenuto informativo dell'applicazione, e di *un modello di ipertesto*, per specificare l'organizzazione delle pagine e della navigazione nell'interfaccia ipertestuale. Il modello dei dati può essere un modello classico, per esempio il modello E-R o il diagramma delle classi UML, in grado di rappresentare classi di informazioni e le associazioni che tra esse sussistono. Il modello dell'ipertesto deve garantire le seguenti proprietà:

1. lo schema di navigazione dell'applicazione web deve essere espresso come un ipertesto costituito da *pagine* e da *link*, con l'ovvia interpretazione che la selezione di un link da parte dell'utente durante l'interazione con l'interfaccia ipertestuale può attivare:

i) la *navigazione* verso un'altra pagina, oppure;
ii) l'attivazione di alcune *operazioni*, come per esempio l'acquisto di un prodotto in un sito di commercio elettronico.

2. Deve essere possibile modellare molteplici *viste di sito*, in altre parole uno o più ipertesti, da presentare agli utenti a seconda della loro identità o del loro ruolo. Ogni vista avrà un singolo punto di ingresso (la home page), il cui accesso può in alcuni casi essere protetto attraverso una procedura di autenticazione. Ogni vista può poi essere suddivisa in *aree*; ogni area contiene un insieme di *pagine*, che costituiscono gli elementi di interfaccia con cui l'utente finale interagisce. Ogni pagina è infine composta da *unità di contenuto*, che concettualmente rappresentano porzioni di contenuto pubblicabili in diversi formati (per esempio, come istanze di dati singole, come insiemi di istanze di dati, come indici, ecc.), o da unità preposte a raccogliere l'input dell'utente (le cosiddette *form*). La connessione tra pagine, ma anche tra unità all'interno di pagine, è realizzata tramite la definizione di *link* che, oltre a rappresentare associazioni navigabili dagli utenti, hanno anche il ruolo di trasportare informazione, sotto forma di parametri che permettono la computazione delle



unità di contenuto; a seguito della navigazione sui link è anche possibile invocare l'esecuzione di operazioni e servizi.

Diverse metodologie per la modellazione concettuale di applicazioni web soddisfano i requisiti sopra enunciati (si confronti [10] per una rassegna). Nel seguito di questo articolo, faremo in particolare riferimento alla metodologia basata su WebML (*Web Modeling Language*) [6] (riquadro a p. 8 e 9, un modello concettuale per la progettazione di applicazioni web centrate sui dati, che integra ingredienti tradizionali ben noti agli sviluppatori, come la modellazione dei dati per mezzo del modello E-R, con concetti e metodi innovativi specifici per la progettazione degli ipertesti.

WebML incorpora tutte le proprietà sopra enunciate. Il valore aggiunto che tale modello offre non consta tuttavia dei singoli ingredienti, quanto della definizione di un processo di sviluppo sistematico, nel quale le varie attività sono fondate su concetti, notazioni e tecniche, ivi inclusa la trasformazione automatica della specifica concettuale di alto livello in codice applicativo, per mezzo di uno strumento CASE (*Computer Aided Software Engineering*) [20].

Nel seguito descriveremo alcune attività previste dalla metodologia WebML per la progettazione dei dati e dell'ipertesto nelle applicazioni web centrate sui dati, con l'intento specifico di evidenziare la rilevanza dei Web Mart per migliorare l'accessibilità dei contenuti. Il lettore interessato a maggiori dettagli sul metodo può far riferimento al riquadro su WebML incluso in questo articolo e al sito web <http://webml.org>.

3.1. La modellazione dei dati

Il processo di sviluppo di un'applicazione web si apre con la modellazione dei dati, con l'obiettivo di selezionare ed organizzare il contenuto informativo che l'applicazione dovrà pubblicare. Il metodo da noi proposto è in particolare "guidato dai dati", intendendo con ciò che l'intero ciclo di sviluppo dell'applicazione è fortemente influenzato dalle scelte operate durante la modellazione dei dati e quindi dagli schemi definiti per i Web Mart. Al fine di migliorare l'accessibilità dei contenuti, la progettazione dei dati deve quindi concentrarsi sulla scoperta e sulla de-

finizione accurata dei Web Mart, seguendo il flusso di attività di seguito descritto.

3.1.1. INDIVIDUAZIONE DEI CONCETTI CENTRALI

Ogni applicazione web centrata sui dati si basa su un numero limitato di contenuti fondamentali. Si pensi per esempio ai siti web aziendali, i cui concetti principali da presentare all'utente possono riguardare i prodotti, i casi di successo, la rete di distributori, le eventuali "comunità" che possono crearsi attorno agli utilizzatori dei prodotti. È importante sottolineare che i concetti centrali devono essere "centrati sui dati"; essi devono cioè rappresentare classi di dati con molteplici istanze; i concetti con una o poche istanze sono infatti più propriamente descritti da contenuti "statici", e cioè da descrizioni testuali, prive di struttura, non facenti parte dello schema dei dati. Per esempio, la descrizione generale dell'azienda, generalmente pubblicata nella pagina Home, non può essere considerata un concetto centrale; lo stesso vale per la missione e la storia dell'azienda, e per tutti quei contenuti mono-istanza, rappresentabili tramite brevi testi statici.

3.1.2. COSTRUZIONE DEI WEB MART

Ogni concetto centrale individuato in precedenza deve essere modellato come un'entità dello schema dei dati caratterizzata da una ricca collezione di attributi. Si può quindi procedere con l'aggiunta delle entità di accesso e di dettaglio.

Le fonti primarie cui ispirarsi per definire le entità di accesso sono tutte quelle proprietà del dominio di interesse che possono aiutare a classificare i concetti centrali dell'applicazione. Si pensi per esempio alle città dei distributori di prodotti in un sito web aziendale: tale proprietà costituisce una ovvia entità di accesso per il concetto centrale "distributore di prodotti", in quanto offre un valido meccanismo di classificazione sulla cui base è possibile definire degli indici di accesso nelle pagine web. Come rappresentato nella figura 2, l'ulteriore raggruppamento di città in regioni, utile nel caso in cui le città dei distributori siano in numero elevato, porta poi ad una gerarchia di accesso, "regione/città/distributore". La profondità dei cammini di accesso e il numero di istanze da mostrare nell'ipertesto in ogni nodo dei cammini possono essere selezionati in base a criteri largamente riconosciuti in letteratura [17].

Web Modeling Language (WebML)

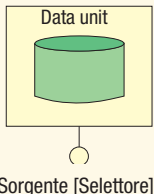
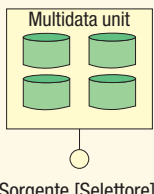
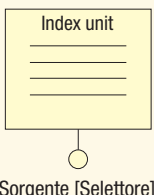
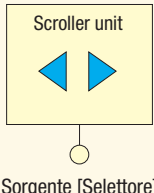
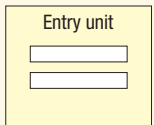
WebML (*Web Modeling Language*) è un modello per la progettazione di applicazioni web, ideato nel 1998, sulla scia dei primi modelli concettuali proposti per le applicazioni ipermediali. L'origine riferimento non è stata trovata..

L'obiettivo principale di WebML è progettare applicazioni web centrate sui dati. Una scelta iniziale è stata quella di riusare modelli dei dati già noti, e di proporre invece una notazione originale e innovativa per specificare la navigazione e la composizione delle interfacce ipertestuali che caratterizzano le applicazioni web. Il modello di ipertesto proposto da WebML si basa su un approccio abbastanza diverso rispetto alle precedenti proposte: il suo intento principale è infatti quello di utilizzare un insieme minimale di concetti, componibili in un certo numero di configurazioni per ottenere un numero arbitrario di strutture di applicazioni. Questa scelta ha influenzato profondamente la definizione del linguaggio e la sua evoluzione verso la modellazione di classi di applicazioni complesse.

La versione iniziale del modello comprendeva un insieme fisso e limitato di primitive per specificare l'organizzazione di siti web "in sola lettura". Tale versione del modello si concentrava, infatti, sull'organizzazione modulare dell'interfaccia ipertestuale per mezzo di alcune *unità di contenuto*, capaci di estrarre dati (tramite opportune interrogazioni) e presentarli sul web organizzati in pagine.

La tabella illustra le cinque unità di contenuto facenti parte del nucleo iniziale di WebML. Esse permettono di rappresentare la pubblicazione di una o più istanze di entità dei dati, selezionate per mezzo di interrogazioni. Le unità di contenuto prevedono infatti la speci-

LE CINQUE UNITÀ DI CONTENUTO CHE FANNO PARTE DEL NUCLEO DI WEBML

Nome	Notazione Visuale	Descrizione
Data unit		Rappresenta la pubblicazione di alcuni attributi di una singola istanza, selezionata da un'entità sorgente per mezzo delle condizioni specificate nel selettore.
Multidata unit		Rappresenta la pubblicazione di alcuni attributi di un insieme di istanze, selezionate da un'entità sorgente per mezzo delle condizioni specificate nel selettore.
Index unit		Rappresenta la pubblicazione di una lista di chiavi che descrivono un insieme di istanze dell'entità sorgente, selezionate per mezzo di condizioni specificate dal selettore. Rispetto alla multidata unit, la index unit permette la selezione da parte dell'utente di una delle chiavi, la cui conseguenza è la navigazione verso nuovi contenuti.
Scroller unit		Permette di navigare in un insieme di istanze selezionate dall'entità sorgente sulla base del selettore. In particolare, tale unit gestisce un insieme di comandi per muoversi in una sequenza ordinata di istanze, selezionando per esempio la prima istanza, l'ultima, la precedente, o la successiva.
Entry unit		Rappresenta form per la raccolta di input dell'utente. A differenza delle altre unit, la entry unit non estrae contenuti da elementi dello schema dei dati.

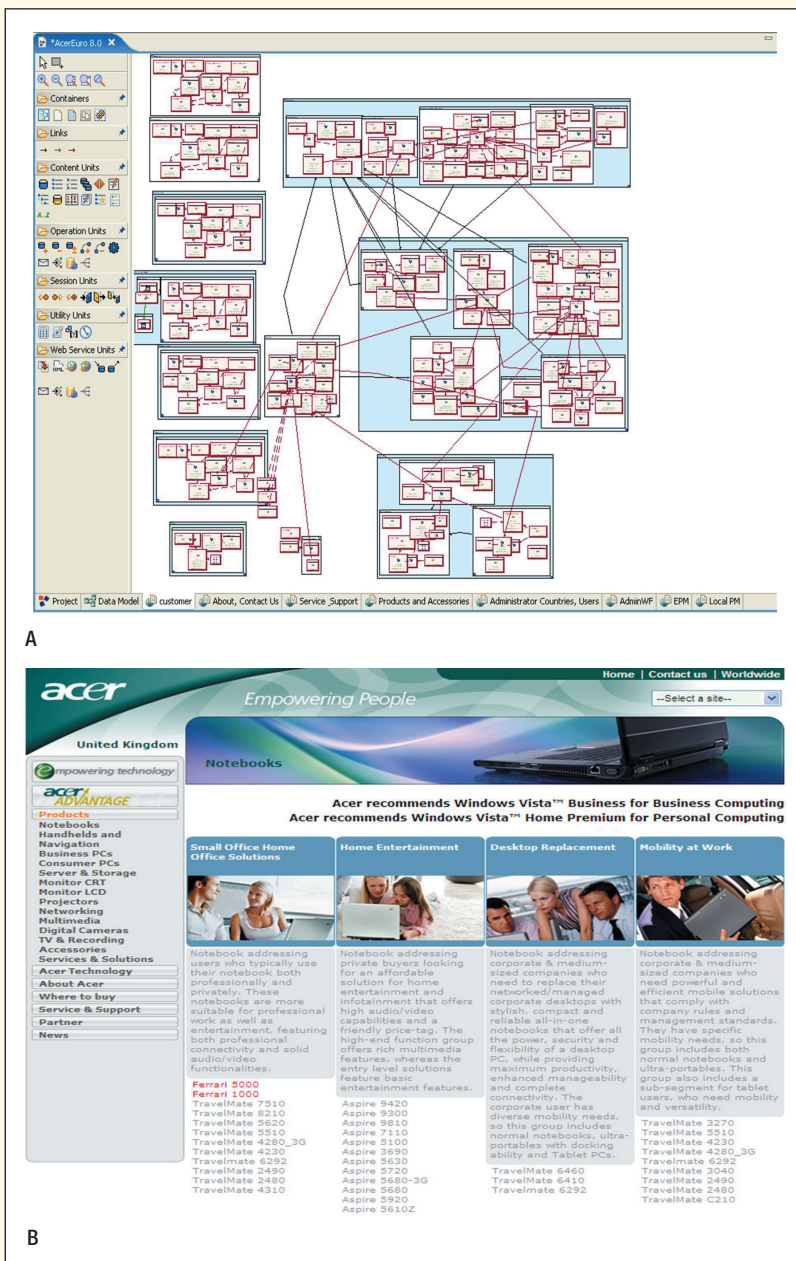
fica di una *sorgente* (l'entità da cui estrarre il contenuto pubblicato dalla unità) e di un *selettore* (un predicato usato per selezionare le istanze dell'entità sorgente). Unica eccezione è la *entry unit*, il cui scopo è rappresentare le *form* tramite cui agli utenti è permesso di inserire dei dati; essa non prevede quindi l'estrazione di contenuti dalla sorgente dei dati.

Versioni successive di WebML hanno introdotto nuove primitive per la specifica di operazioni attivabili dalla navigazione dell'utente. Il potere espressivo del modello è stato così esteso per supportare funzionalità per la gestione dei contenuti (*creazione, cancellazione e modifica* di istanze di entità e di relazioni), e per l'autenticazione e l'autorizzazione degli utenti. L'introduzione della nozione di *plug-in* ha poi reso

WebML un linguaggio aperto, estendibile dai progettisti con primitive concettuali *ad hoc*, per poter far fronte a caratteristiche e funzionalità aggiuntive, eventualmente richieste da nuovi domini applicativi. Questa transizione ha posto le basi per le numerose estensioni operate sul modello. La nozione di *plug-in* è stata infatti utilizzata per definire estensioni ortogonali al nucleo di WebML, coprendo così settori applicativi mai esplorati sotto la prospettiva della modellazione concettuale. Per esempio, sono stati definiti nuovi *plug-in* per specificare l'interazione con i *web service* [14] e l'organizzazione dei *workflow* [3], rendendo possibile la modellazione e lo sviluppo di applicazioni di *workflow* distribuite e multi-attore. Altre estensioni hanno riguardato la modellazione di applicazioni Web multi-canale e context-aware [5], andando così incontro alle recenti esigenze di ubiquità, adattività e personalizzazione manifestatesi nell'ambito del web. Le estensioni più recenti riguardano la realizzazione di applicazioni per il Web semantico [2]. Per maggiori dettagli su WebML il lettore può far riferimento al sito Web <http://webml.org>.

L'evoluzione di WebML è accompagnata dalla presenza di una linea industriale di sviluppo, che corre in parallelo alla ricerca accademica. Il sistema WebRatio (<http://www.webratio.com>), realizzato da Web Models, *spin-off* del Politecnico di Milano, consente di sviluppare applicazioni industriali complesse e innovative basate su WebML.

Il sistema accompagna il progettista dalla raccolta dei requisiti fino alla generazione di codice, che copre la maggior parte dei database relazionali e degli ambienti di esecuzione per il web basati su Java. L'uso di WebRatio porta alla realizzazione evolutiva dell'applicazione, di cui è disponibile una versione iniziale fin dalla prima sessione di design. La figura illustra un'applicazione complessa realizzata con WebML (<http://www.acer-euro.com>) mostrando l'ipertesto completo e la presentazione su web della home page. La versione 5.0 di WebRatio, disponibile da settembre 2007, è sviluppata in ambiente Eclipse.



Ipertesto completo (A) e pagina Home (B) dell'applicazione Acer-Euro (<http://www.acer-euro.com>)

Infine, i concetti centrali devono essere ulteriormente estesi tramite l'introduzione di entità di dettaglio. Per esempio, come illustrato nella figura 2, ogni prodotto sarà dotato di un insieme di specifiche tecniche, modellabili

tramite un'entità aggiuntiva rispetto all'entità centrale, poiché la relazione tra prodotti e specifiche tecniche è uno-a-molti (ogni prodotto può essere infatti caratterizzato da diverse tipologie di specifiche tecniche).

3.1.3. COSTRUZIONE DELLO SCHEMA DI INTERCONNESSIONE

Una volta completata la definizione dei singoli Web Mart, il progettista dei dati deve definire delle interconnessioni per facilitare la navigazione tra i diversi concetti centrali. Per esempio, tra i concetti “prodotto” e “distributore di prodotti” in un sito web aziendale, è possibile definire un’associazione, appartenente allo schema di interconnessione, che può essere usata per la definizione di link nell’ipertesto, così da poter accedere a tutti i distributori che vendono un cer-

to prodotto, e viceversa a tutti i prodotti trattati da un rivenditore.

3.2. La modellazione preliminare dell’ipertesto

Terminata la modellazione dei dati, la fase successiva consiste di un insieme di attività mirate alla definizione della struttura globale dell’interfaccia ipertestuale. Un’applicazione web può offrire agli utenti diversi ipertesti, ognuno dei quali fornisce una vista diversa sugli stessi dati che soddisfa i requisiti di utenti o di ruoli diversi. Per ogni vista, il metodo prevede una progettazione top-down [1]; durante i primi passi si operano alcune scelte preliminari sull’organizzazione dell’ipertesto, che saranno poi esplose e raffinate nei passi successivi. Il risultato è la definizione dell’organizzazione globale di ogni vista di sito, che prescinde ancora dal preciso posizionamento dei contenuti nelle pagine e dalla loro presentazione. Dopo questa attività iniziale, si procederà poi alla specifica sempre più dettagliata dell’organizzazione delle aree e delle pagine.

3.2.1. SELEZIONE DELLE AREE E DELLE PAGINE CENTRALI

Il processo di progettazione inizia associando ad ogni Web Mart un’area, le cui pagine pubblicheranno i contenuti relativi al Web Mart stesso. La selezione delle aree all’interno di una vista di sito può essere abbastanza immediata; l’individuazione delle pagine principali all’interno delle aree richiede invece che si identifichi un sottoinsieme delle pagine che costituiranno l’area, anche se tale decisione potrebbe essere soggetta a diverse riconsiderazioni nei passi successivi di sviluppo nel momento in cui altre scelte di progettazione, relative per esempio alla distribuzione dei contenuti nelle varie pagine dell’ipertesto, saranno valutate. È importante tenere presente che:

- all’interno di ogni area deve essere presente almeno una *pagina centrale*, per la pubblicazione dei dati fondamentali del concetto centrale. La pagina centrale è la pagina con visibilità più alta nell’area; è in altre parole la prima pagina presentata all’utente all’ingresso dell’area. Nella terminologia WebML, la pagina principale è detta *pagina di default*, come indicato dall’etichetta “D” con cui è contrassegnata (si confronti la Figura 3);

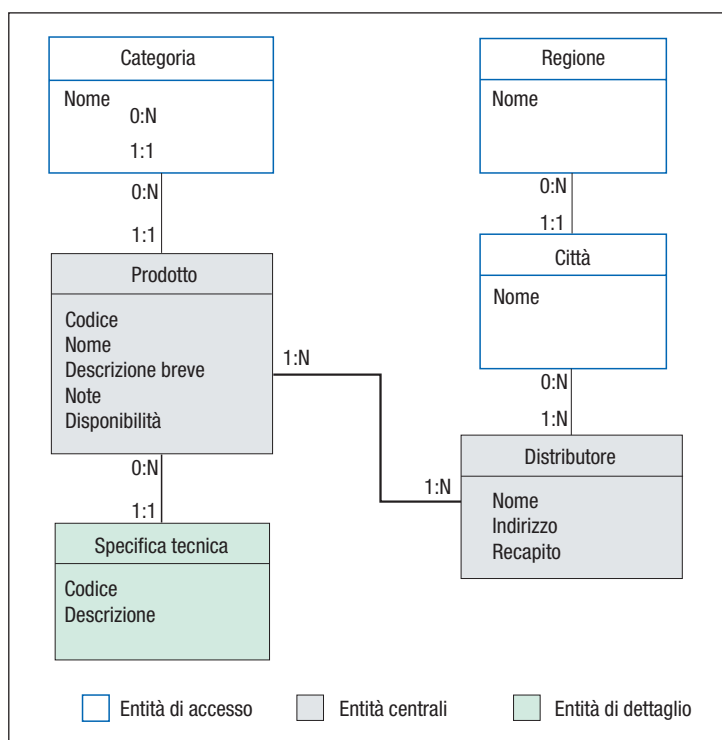


FIGURA 2

Entità centrali, di accesso e di dettaglio in un sito Web aziendale

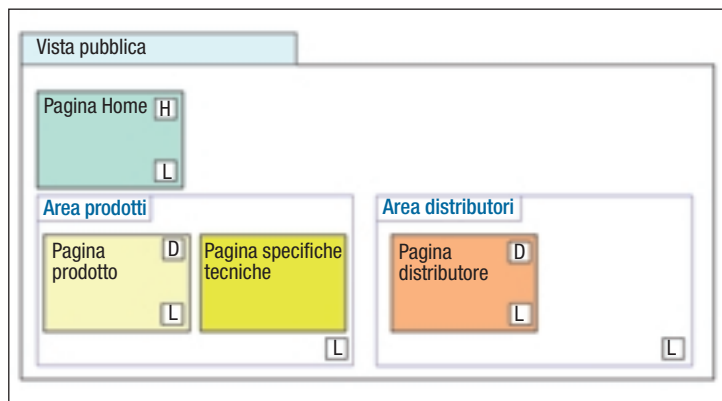


FIGURA 3

Una possibile organizzazione preliminare per la vista pubblica in un sito aziendale



□ per ogni pagina centrale, possono poi essere richieste una o più *pagine ausiliarie* per la pubblicazione delle informazioni memorizzate dalle entità di dettaglio. In caso di schemi complessi, le pagine ausiliarie possono a loro volta essere raggruppate in sotto-aree annidate rispetto all'area principale del Web Mart.

La figura 3 illustra un esempio di organizzazione preliminare per la vista di sito pubblica (destinata cioè a ogni utente senza restrizioni di accesso) in un sito web aziendale. L'organizzazione della vista è rappresentata con la notazione WebML: i vari contenitori, ai vari livelli di annidamento, rappresentano la vista di sito, due aree dedicate ai due concetti centrali "prodotto" e "distributore", e alcune pagine ritenute fondamentali per la pubblicazione dei contenuti dei due concetti centrali. I contenuti di tali pagine riflettono una distribuzione (preliminare) dei contenuti, ma comunque coerente con lo schema dei due Web Mart illustrati nella figura 2.

3.2.2. SELEZIONE DEI LANDMARKS

In un ipertesto, i cosiddetti *landmark* denotano pagine che devono essere visibili e raggiungibili in ogni parte dell'interfaccia ipertestuale, tipicamente per mezzo di link raggruppati in barre di navigazione persistenti. Per facilitare l'accesso ai concetti centrali dell'applicazione, è possibile associare la proprietà di landmark alle pagine centrali delle varie aree, così che queste abbiano buona visibilità in tutta la vista di sito. In aggiunta, è raccomandabile definire come landmark alcune pagine "notevoli", per esempio la pagina *Home*, la pagina di *login*, o le pagine contenenti le form per la *ricerca* per parole chiave. Queste costituiscono, infatti, punti di partenza per la navigazione dei contenuti, e devono quindi risultare di facile accesso agli utenti. Per esempio, nella figura 3 sono rappresentate come pagine landmark (denotate dall'etichetta "L") la pagina *Home* e le due pagine di *default* (denotate dall'etichetta "D") delle due aree. A seconda dell'importanza delle pagine, è possibile definire più livelli di visibilità per i landmark: da una visibilità globale, che si estende a tutta la vista di sito, a una visibi-

lità locale, limitata all'interno di un'area. La definizione delle pagine landmark può quindi dar luogo a una gerarchia di barre di navigazione: per esempio, è possibile definire una *barra di navigazione globale*, visibile in modo persistente in ogni pagina della vista, per raggruppare i link alle pagine di *default* di aree a loro volta marcate come landmark e/o a pagine landmark esterne a qualsiasi area. Per esempio, lo schema di vista della figura 3 induce alla definizione di una barra di navigazione globale con link verso la pagina *Home* e verso le due pagine di *default* delle due aree.

All'interno di ogni area, è possibile poi definire una *barra di navigazione locale*, visibile solo nelle pagine interne all'area, per raggruppare link di accesso alle pagine più importanti dell'area. Per esempio, la specifica illustrata nella figura 3 porta alla definizione di una barra di navigazione locale in ciascuna delle due aree, contenente un link alla pagina landmark dell'area.

3.3. La modellazione dettagliata dell'ipertesto

La modellazione dettagliata dell'ipertesto richiede di determinare il modo in cui le pagine pubblicheranno i contenuti per mezzo di *unità di contenuto*, o in che modo i link all'interno delle pagine permetteranno di richiamare alcune *operazioni* (per esempio l'acquisto di un prodotto, la registrazione di un utente a un sito, o il download di un file), eventualmente dopo aver inserito alcuni dati nei campi di una *form*.

Oltre a pubblicare contenuti, o a permettere l'invocazione di operazioni, ogni pagina deve inoltre contenere *meccanismi di navigazione* per accedere ai vari contenuti del sito. Se articolati, tali meccanismi possono portare all'introduzione di ulteriori pagine dette *pagine di accesso*. In generale, essi possono essere di due tipi:

- *basati sulla navigazione*: all'interno delle pagine si introducono indici, definiti sulle entità di accesso, che permettono la selezione progressiva di categorie di concetti, per esempio le "regioni" o le "città" di un distributore di prodotti, fino al raggiungimento del concetto di interesse;
- *basati sulla ricerca diretta*: all'interno delle pagine si aggiungono *form*, per l'inseri-

mento da parte dell'utente di chiavi di ricerca, e quindi link per invocare l'esecuzione di interrogazioni sulla sorgente dei dati dell'applicazione, per esempio "ritrovare tutti i prodotti di tipo *notebook*". Il risultato della ricerca è poi presentato all'utente sotto forma di lista ordinata di oggetti.

Le due modalità di accesso sono comunque complementari.

Oltre ai meccanismi di accesso, nelle pagine principali è necessario definire meccanismi di navigazione per l'accesso ai contenuti di dettaglio e per la navigazione verso altri concetti centrali. Un esempio di modellazione dettagliata di pagina, che include gli elementi sopra descritti, sarà mostrato nella sezione 4.

3.4. La modellazione della presentazione

Il progetto della presentazione ha lo scopo di definire il modo in cui i contenuti e i meccanismi di accesso e interconnessione devono essere posizionati e presentati all'interno delle pagine. Questa è la fase in cui l'accessibilità dei contenuti diventa meno rilevante, mentre acquisisce maggiore importanza l'accessibilità della presentazione. Questa attività consta dei passi di seguito illustrati.

3.4.1. SPECIFICA DEL LAYOUT DELLA PAGINA

Questo passo richiede la definizione della *griglia di pagina*, cioè di una tabella nelle cui celle è possibile posizionare le unità di contenuto e i meccanismi di navigazione nella pagina. Le pagine che presentano lo stesso tipo di contenuti, per esempio tutte le pagine dei prodotti, devono possibilmente aderire allo stesso layout. Layout diversi possono invece essere definiti a seconda che la pagina sia centrale, ausiliaria o di accesso.

3.4.2. DISPOSIZIONE DEGLI ELEMENTI DI PAGINA

Questo passo richiede la definizione di regole per la disposizione di elementi di presentazione (per esempio unità di contenuto, barre di navigazione, form per la login e per la ricerca diretta) in determinate posizioni della griglia di pagina. Lo scopo è ottenere una disposizione coerente degli elementi dalla stessa semantica nelle varie pagine del sito, con l'effetto di incrementare

l'orientamento e ridurre lo sforzo dell'utente nell'individuare il ruolo dei vari elementi di contenuto e di navigazione.

3.4.3. DEFINIZIONE DELLO STILE GRAFICO

È necessario definire regole di formattazione (per esempio i caratteri del testo e i colori), da applicare a elementi di pagina ricorrenti come i testi, le ancore, le tabelle ecc.. La definizione di tali regole richiede di considerare le linee guida per l'accessibilità della presentazione, come quelle definite dal W3C-WCAG [19], al fine di assicurare l'accessibilità da parte di diversi utenti, dispositivi e agenti. Per poter incrementare la coerenza dello stile grafico in tutto il sito, le regole di formattazione possono essere specificate per mezzo di fogli di stile (*style sheets*).

4. UN CASO DI STUDIO

Al fine di chiarire ulteriormente i concetti fin qui enunciati, in questa sezione discuteremo l'accessibilità dei contenuti dell'applicazione web del *Dipartimento di Elettronica e Informazione* (DEI) del Politecnico di Milano. Useremo quindi il concetto di Web Mart per ricostruire e rappresentare la sua organizzazione generale.

L'applicazione DEI è un vasto sito istituzionale, composto da una parte pubblica, che giornalmente riceve circa 9.000 richieste di pagina da utenti esterni al dipartimento, e una intranet che permette di espletare alcune procedure amministrative interne al dipartimento. La nostra discussione farà in particolare riferimento a una vecchia versione dell'applicazione, recentemente sostituita da una nuova versione modellata con WebML².

La figura 4 illustra un frammento del contenuto dell'applicazione analizzata, specificato secondo la notazione E-R, che sarà oggetto della nostra discussione. Il diagramma evidenzia *PersonaleDEI* come concetto centrale, con un'entità di accesso, *CategoriaPersonale*, basata sulla classificazione

² La versione corrente del sito del DEI è raggiungibile all'indirizzo <http://www.dei.polimi.it>. La versione analizzata è temporaneamente disponibile all'indirizzo <http://intranet.dei.polimi.it/index.jsp>.

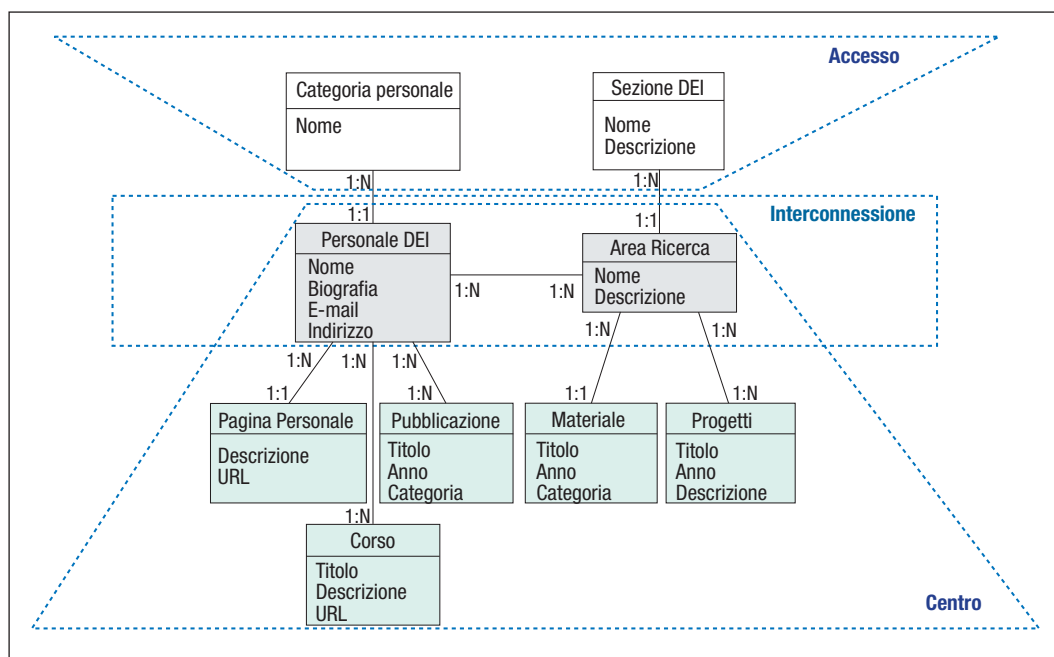


FIGURA 4
Un frammento dello schema dei dati del DEI

dei membri del dipartimento in categorie quali professori ordinari, professori associati, ricercatori ecc.. Le entità di dettaglio riguardano informazioni sulle pagine personali, sui corsi e sulle pubblicazioni di ciascun membro del personale.

AreaRicerca è un altro concetto centrale dell'applicazione DEI, che si riferisce alle varie aree della ricerca svolta dai docenti del dipartimento. L'accesso alle aree di ricerca è facilitato dalla loro classificazione in sezioni (per esempio "Elettronica", "Informatica" ecc). La descrizione delle aree di ricerca è arricchita da contenuti di dettaglio, riguardanti documentazione di varia natura resa disponibile sul web (per esempio le pubblicazioni, i link a siti di progetti ecc.), e descrizioni di progetti relativi alle varie aree di ricerca.

La relazione tra i due concetti *PersonaleDEI* e *AreaRicerca* è un esempio di interconnessione tra concetti centrali. Altri concetti centrali, non rappresentati nella figura per brevità, riguardano le attività didattiche del dipartimento e le relazioni con il mondo dell'industria.

A livello di progettazione preliminare, l'ipertesto della parte pubblica dell'applicazione è organizzato in quattro aree distinte (*Ricerca*, *Didattica*, *Industria* e *Personale*), che pubblicano i contenuti dei quattro concetti centrali individuati. Ogni pagina dell'appli-

cazione visualizza quindi nella sua parte superiore una barra di navigazione globale, i cui link permettono di accedere alle quattro aree. In aggiunta, all'interno di ogni area, le pagine visualizzano una barra di navigazione locale, che raggruppa i link ad alcune pagine rilevanti per l'area.

La figura 5 A mostra una pagina centrale, dedicata alla pubblicazione di informazioni sui singoli membri del personale del DEI. Oltre alle due barre di navigazione (globale e locale) per la navigazione tramite landmark, nella sua parte centrale la pagina mostra le informazioni relative al concetto centrale *PersonaleDEI*. L'accesso ai dati di dettaglio per il membro del personale selezionato è reso possibile da un indice delle pagine personali, e da alcuni link che portano alle pubblicazioni e ai materiali dei corsi tenuti dal docente. Un ulteriore indice, che nella pagina di esempio include una sola voce, punta poi alle aree di ricerca, rappresentando così l'interconnessione con il concetto centrale *AreaRicerca*.

Il modello della pagina per i membri del *Personale DEI* è rappresentato nella figura 5 B e prevede una unità di contenuto per la visualizzazione dei dati centrali, due link che puntano alle pagine ausiliarie relative ai corsi e alle pubblicazioni, un indice per la visualizzazione delle pagine personali, e un

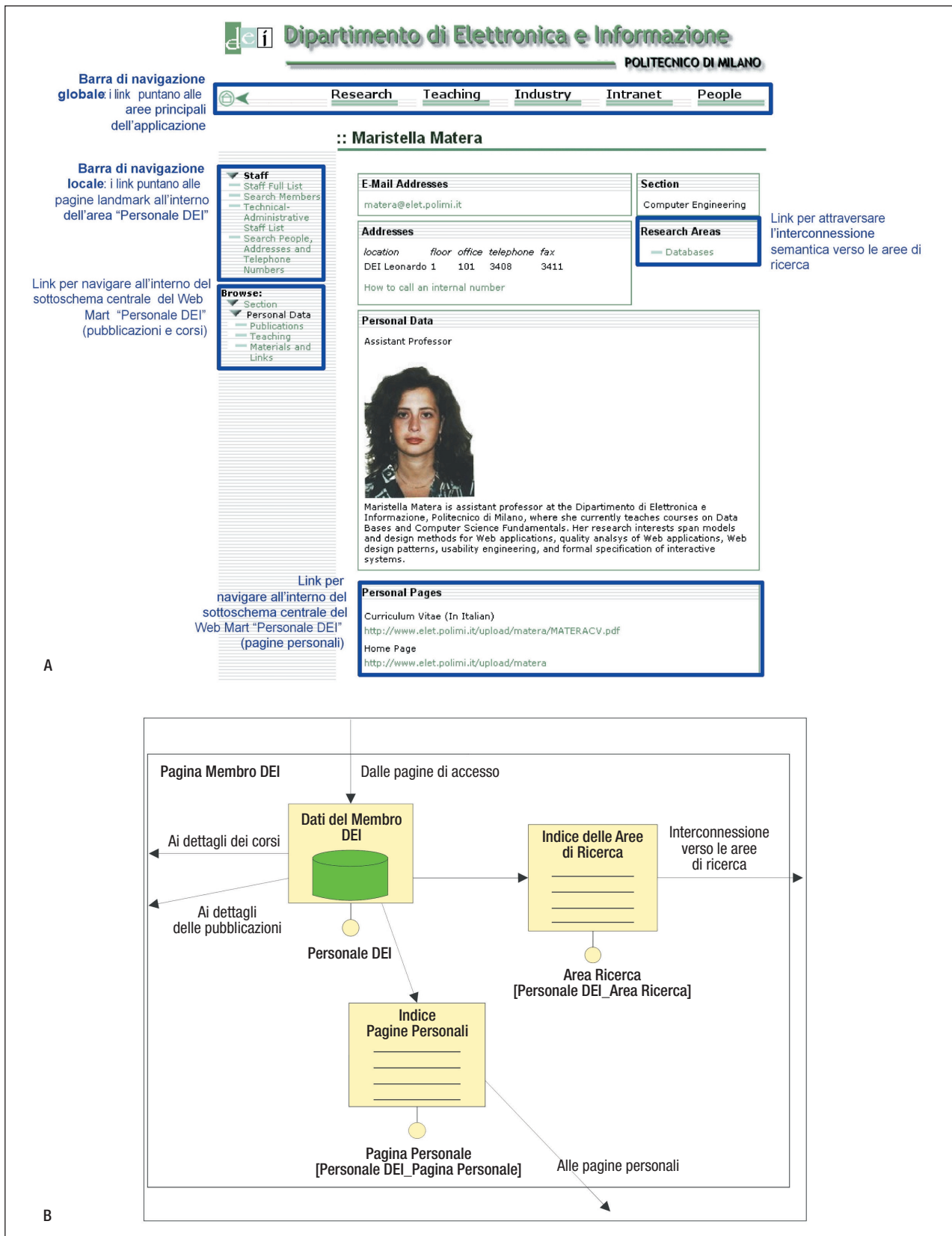


FIGURA 5

Una presentazione concreta per le pagine dedicate ai membri del personale del DEI (A), e il suo modello concettuale astratto (B)



indice che permette l'interconnessione con le aree di ricerca a cui il docente del DEI appartiene. Si noti che, essendo i landmark proprietà attribuibili alle aree e alle pagine, i link nelle due barre di navigazione persistenti non sono esplicitati nel modello della pagina riportata nella figura, mentre saranno rappresentati come proprietà delle loro pagine di destinazione.

La figura 5 B rappresenta "il modello astratto", mentre la figura 5 A è uno delle sue possibili "presentazioni" ottenuta applicando al modello uno stile di presentazione.

Il modello mantiene una chiara corrispondenza con lo schema del Web Mart: la pagina infatti pubblica i contenuti centrali e alcuni dettagli di un membro del personale, e fornisce meccanismi di navigazione per muoversi sia verso altri concetti di dettaglio, sia verso altri concetti centrali così come stabilito dallo schema di interconnessione. Infatti, a partire da un Web Mart è possibile derivare pattern di pagine web, che suggeriscono come pubblicare i componenti del Web Mart. Tale corrispondenza con lo schema dei Web Mart può inoltre essere sfruttata da strumenti di supporto alla navigazione, come per esempio i cosiddetti *web readers*: per ogni unità di contenuto in una pagina potrebbe infatti essere possibile fornire informazioni aggiuntive riguardo la semantica del contenuto a cui essa si riferisce e il ruolo di tale contenuto nello schema del Web Mart.

L'astrazione dei Web Mart può anche essere usata per un'analisi critica dell'accessibilità dei contenuti. Riflettiamo per esempio sulla visibilità delle pubblicazioni nella versione analizzata dell'applicazione DEI. Come mostrato dalla figura 4, a livello dei dati l'entità *Pubblicazione* è rappresentata come un dettaglio del concetto *PersonaleDEI* – non come un concetto centrale. Coerentemente con la scelta, le pubblicazioni sono raggiungibili solo a partire dalla pagina di un membro del personale (si confronti la Figura 5 B). Questa scelta di progetto impedisce però all'utente di accedere con facilità alle pubblicazioni, poiché la scoperta di tali contenuti è condizionata all'accesso alle pagine del personale.

Data la rilevanza delle pubblicazioni, que-

sta scelta iniziale è stata successivamente valutata come una carenza dal punto di vista della accessibilità di contenuti. Per questo, in una delle versioni successive dell'applicazione, la pagina delle pubblicazioni è stata arricchita con una *form* per la ricerca diretta sulle pubblicazioni. Ma anche questa scelta non è risultata particolarmente efficace. Un'analisi degli accessi all'applicazione, eseguita sui log delle richieste di pagina pervenute nell'arco di 15 giorni, ha rivelato che solo 2 su 440 accessi alle pubblicazioni sono stati eseguiti utilizzando il nuovo meccanismo di ricerca. In generale, l'omissione di un Web Mart in corrispondenza di un concetto centrale per l'applicazione e, in modo più specifico, la mancanza di un accesso di navigazione al concetto centrale non possono infatti essere compensati dall'aggiunta di meccanismi *ad-hoc* per la ricerca diretta. A seguito di questa e di altre analisi, si è deciso di procedere ad una revisione del progetto dell'applicazione, dando così origine alla nuova versione correntemente disponibile sul Web.

5. CONCLUSIONI

I lavori recenti sull'accessibilità delle applicazioni web si sono particolarmente concentrati sui requisiti posti da utenti disabili, con molta enfasi sulla presentazione, prescindendo in alcuni casi da altri importanti fattori, come la qualità e l'usabilità delle applicazioni web [11]. Buona parte della comunità di ricerca ritiene tuttavia che l'accessibilità sia un concetto universale, in grado di apportare benefici a ogni utente. L'accessibilità può infatti essere considerata un concetto più generale, strettamente legato all'usabilità e alla qualità delle applicazioni, che può andare incontro alla varietà delle tecnologie attualmente adottate nel web e alla diversità degli utenti, concentrandosi in particolar modo sulla facilità dell'accesso ai contenuti [12, 16]. Ed è proprio alla luce di risultati consolidati sull'usabilità e sull'accessibilità che è possibile comprendere perché l'accessibilità dei contenuti, così come definita nel contesto del nostro metodo di sviluppo, rivesta un ruolo importante per il successo delle applicazioni.

Secondo quanto definito da Nielsen [15] e da Shneiderman [17], un'applicazione "intuitiva" non dovrebbe richiedere esperienze precedenti con altre applicazioni dello stesso tipo: gli utenti dovrebbero essere messi in grado di applicare "modelli mentali precedenti" per interagire con successo con ogni nuova applicazione. Il riconoscimento di una struttura ripetitiva per il web [9], già discussa nella sezione 2, è quindi la migliore argomentazione a supporto della nostra ipotesi che i Web Mart costituiscono un modello di interazione semplice e intuitivo. La struttura suggerita dai Web Mart deriva dall'osservazione di strutture ricorrenti e di successo. Se adottata nelle applicazioni web, tale struttura non richiede quindi all'utente una specifica esperienza pregressa di interazione, se non quella accumulata visitando la maggior parte delle applicazioni web. Inoltre, la nozione di "concetto centrale", inteso come entità principale caratterizzata da un ricco insieme di proprietà, corrisponde alla classica "struttura dei concetti", riconosciuta dalla psicologia cognitiva come modello adottato dagli esseri umani per articolare la loro conoscenza [4].

L'utilizzo di un pattern ricorrente per la rappresentazione e l'organizzazione dei concetti è molto utile al fine di facilitare gli utenti nel ritrovare e navigare i contenuti. Tuttavia, è ulteriormente necessario assicurare che gli utenti non avvertano eventuali dissonanze tra le loro aspettative e i contenuti ritrovati tramite i meccanismi di navigazione offerti dall'applicazione [15, 17]; diversamente, essi sarebbero disorientati e non riuscirebbero facilmente a formulare e realizzare i loro obiettivi di ricerca dei contenuti. È essenziale quindi che ogni meccanismo di accesso, sia esso basato sulla navigazione o sulla ricerca diretta, restituisca esattamente i contenuti centrali desiderati, in un formato che sia conforme alle attese degli utenti. Una pratica di progettazione consolidata, a supporto di tale requisito, è quella di adottare strutture gerarchiche di informazione e indici di navigazione definiti su di esse, così da guidare gli utenti in un accesso *top-down*, basato su passi successivi di raffinamento [15, 17]. A ogni passo l'utente è in grado di valutare i risultati ottenuti e

quindi eventualmente calibrare i propri obiettivi di ricerca. L'applicazione deve inoltre mettere a disposizione meccanismi di ricerca diretta, per fornire all'utente una "via di uscita" quando le strategie *top-down* non hanno successo.

La modellazione del contenuto informativo di un'applicazione web riveste quindi un ruolo importante per l'accessibilità, forse più significativo del progetto della presentazione. Il concetto di Web Mart, se pur semplice ed intuitivo, induce un metodo di progettazione sistematico ed efficace, che permette di organizzare i contenuti, quindi l'intera applicazione web, in modo da potenziarne l'accessibilità.

Bibliografia

- [1] Batini C., Ceri S., Navathe S.B.: *Conceptual Database Design: an Entity-Relationship Approach*. Benjamin-Cummings, 1992.
- [2] Brambilla M., Celino I., Ceri S., Cerizza D., Della Valle E., Facca F. M.: *Model-Driven Design and Development of Semantic Web Service Applications*. ACM Transactions on Internet Technology - Numero speciale on Semantic Web Services, Febbraio 2008, in fase di stampa.
- [3] Brambilla M., Ceri S., Fraternali P., Manolescu I.: Process modeling in Web applications. *ACM Transactions on Software Engineering and Methodologies*, Vol. 15, n. 4, Ottobre 2006, p. 360-409.
- [4] Bruner J., Goodnow J. J., Austin G. A.: *A Study of Thinking*. Transaction Publications Inc., 1995.
- [5] Ceri S., Daniel F., Matera M., Facca F. M.: Model-Driven Development of Context-Aware Web Applications. *ACM Transactions on Internet Technology*, Vol. 7, n. 1, Gennaio 2007.
- [6] Ceri S., Fraternali P., Bongio A., Brambilla M., Comai S., Matera M.: *Designing Data-Intensive Web Applications*. Morgan Kaufmann, 2003.
- [7] Ceri S., Fraternali P., Matera M.: Conceptual Modeling of Data-Intensive Web Applications. *IEEE Internet Computing*, Vol. 6, n. 4, Luglio-Agosto 2002, p. 20-30.
- [8] Chen P. P.: The Entity-Relationship Model - Toward a Unified View of Data. *ACM Transactions on Database Systems (TODS)*, Vol. 1, n. 1, Gennaio 1976, p 9-36.
- [9] Dill S., Kumar R., McCurley K., Rajagopalan S., Sivakumar D., Tomkins A.: *Self-similarity in the Web*. Proc. of VLDB 2001, Rome, Italy, Settembre 2001, p. 69-78.



- [10] Fraternali P.: Tools and Approaches for Developing Data-Intensive Web Applications: A Survey. *ACM Computing Survey*, Vol. 31, n. 3, Marzo 1999, p. 227-263.
- [11] Hudson W.: Inclusive Design: Accessibility Guidelines Only Part of the Picture. *Interactions*, Vol. 11, n. 4, Luglio 2004, p. 55-56.
- [12] Hull L.: Accessibility: It's Not Just for Disabilities any more. *Interactions*, Vol. 11, n. 2, Marzo 2004, p. 36-41.
- [13] Kimball R., Ross M.: *The Data Warehouse Toolkit: The Complete Guide to Dimensional Modeling*. John Wiley & Sons, Seconda edizione, 2002.
- [14] Manolescu I., Brambilla M., Ceri S., Comai S., Fraternali P.: Model-Driven Design and Deployment of Service-Enabled Web Applications. *ACM Transactions on Internet Technology (TOIT)*, Vol. 5, n. 3, Agosto 2005.
- [15] Nielsen J.: *Web Usability*. New Riders, 2000.
- [16] Shneiderman B.: Universal Usability. *Communication of ACM*, Vol. 43 n. 5, Maggio 2000, p. 84-91.
- [17] Shneiderman B., Byrd D., Croft W. B.: Sorting out Searching. *Communication of ACM*, Vol. 41, n. 4, Aprile 1998, p. 95-98.
- [18] Stephanidis C., Savidis A.: Universal Access in the Information Society: Methods, Tools, and Interaction Technologies. *Universal Access in the Information Society*, Vol. 1, n. 1, 2001, p. 40-55.
- [19] Web Content Accessibility Guidelines 2.0: W3C-WAI Working Draft, 11 Marzo 2004.
- [20] WebModels, s.r.l. WebRatio. <http://www.webratio.com>.

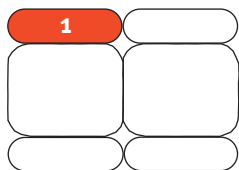
STEFANO CERi è professore ordinario di Basi di Dati presso il Politecnico di Milano. La sua ricerca si concentra sull'estensione delle tecnologie per le basi di dati per incorporare aspetti quali la distribuzione dei dati, le regole attive e i metodi orientati agli oggetti, e su metodi di progettazione e sviluppo per le applicazioni web "data-intensive". È uno degli inventori di WebML, un modello concettuale per la progettazione delle applicazioni Web (Brevetto US 6,591,271, Luglio 2003), e uno dei fondatori della WebModels, un'azienda spin-off del Politecnico di Milano, che commercializza WebML per mezzo del prodotto WebRatio (www.webratio.com).
E-mail: stefano.ceri@polimi.it

MARISTELLA MATERA è ricercatrice presso il Politecnico di Milano, dove insegna Basi di Dati. La sua ricerca si concentra su metodi e strumenti per la modellazione e lo sviluppo di applicazioni web, con particolare enfasi sull'adattività e la context-awareness, la modellazione di processi cooperativi, l'usabilità e l'accessibilità delle applicazioni Web. Su tali argomenti, ha scritto più di 50 articoli scientifici, pubblicati su riviste e atti di conferenze internazionali.
E-mail: maristella.matera@polimi.it



STORIA DELL'INFORMATICA E FORMAZIONE CULTURALE DEGLI STUDENTI

Paolo Giangrandi
Claudio Mirolo



L'Università di Udine aderisce all'iniziativa "Corsi AICA", volta a promuovere l'insegnamento della storia dell'informatica. Questo articolo presenta un'analisi condotta sugli esiti delle prove d'esame con l'obiettivo di esplorare la formazione culturale degli studenti. Dalle prime osservazioni emerge una fragile prospettiva storica, in particolare per quanto riguarda l'evoluzione della scienza, che rende loro difficile trasformare la spontanea curiosità per gli artefatti tecnologici in un più maturo interesse per gli sviluppi del pensiero e della società che li hanno resi possibili.

1. INTRODUZIONE

Negli ultimi anni si sta registrando a livello internazionale una crescita dell'interesse per le radici storiche dell'informatica, testimoniata da autorevoli proposte di introdurre lo studio nei programmi accademici [10, 11]. La prospettiva storica non è quindi considerata semplicemente come una curiosità o, detto con l'ironia di D. Knuth, come "uno dei modi per rendere più rispettabile l'informatica" [12], ma si ritiene possa anche contribuire ad allargare la formazione culturale degli studenti di una disciplina scientifico-tecnica.

In Italia l'AICA si è fatta promotrice dell'iniziativa illustrata in queste pagine da C. Bonfanti [4], volta a promuovere l'istituzione di corsi universitari sulla storia dell'informatica. Cogliendo tale opportunità, a partire dall'anno accademico 2005-06 la Facoltà di Scienze dell'Università di Udine ha attivato un insegnamento opzionale, indirizzato principalmente agli studenti dei corsi di laurea in discipline informatiche. Diversamente da quanto ci si poteva attendere, l'esperienza udinese si è caratterizzata rispetto a quella

delle altre sedi per il cospicuo numero di studenti che hanno scelto di inserire l'insegnamento nei loro piani di studio, diventando così un significativo banco di prova per valutare l'accoglienza e l'efficacia didattica degli argomenti trattati. Per questo motivo ci è sembrato utile mettere a disposizione i risultati della nostra analisi a conclusione del primo anno di attività, proponendo inoltre alcuni spunti di riflessione.

Analisi di questo tipo sono rilevanti, a nostro avviso, quando ci si interroga sugli obiettivi che possono essere realisticamente perseguiti in un corso di cultura generale, tenendo conto delle attitudini prevalenti tra gli allievi. Nel caso specifico dell'ateneo friulano, l'elevato numero di prove scritte d'esame disponibili, ben 260 nell'anno accademico 2005-06, e la forma di questionario con domande a risposta multipla hanno offerto una base particolarmente appropriata per l'indagine.

Prima di entrare nello specifico, richiamiamo per sommi capi i principali nodi su cui si confrontano gli storici della scienza e della tecnologia nel momento in cui si accingono a calare



questa materia in un contesto culturale diverso da quello delle scienze umane. Le difficoltà che incontrano gli educatori a fronte della complessità e della frammentazione dei saperi specialistici stanno infatti alimentando un dibattito sulle possibili ricadute didattiche dell'insegnamento della storia della scienza e della tecnologia, considerandone le potenzialità [5, 9, 14, 15, 17], ma anche i rischi di indurre concezioni erronee riguardo la natura della scienza, ovvero gli scopi e i metodi della ricerca storica [1, 3, 7]. Gli obiettivi perseguibili sono svariati, talvolta ambiziosi, sia sul piano culturale generale che su quello professionale:

- interpretare lo sviluppo delle conoscenze scientifiche e i rapporti tra scienza, tecnologia e società [18], al fine di maturare un punto di vista critico ed una maggiore autonomia di giudizio;

- arricchire la formazione generale, contribuendo a ridurre il divario fra sapere scientifico e sapere umanistico [17], affinché il cittadino sia in grado di partecipare responsabilmente ad un più ampio dibattito culturale;

- riflettere su natura e identità di una disciplina per scopi epistemologici o pedagogici [1, 6], in modo da "armonizzare l'esigenza di competenze specialistiche con la ricerca di un senso di cui si preoccupa l'educazione generale" [19];

- capire come "il cambiamento sia una caratteristica costante e ineluttabile della scienza e della tecnologia" [9], per imparare a farvi fronte assumendo una prospettiva a lungo termine;

- riconoscere i principali fattori che incidono sulla diffusione e sull'obsolescenza degli artefatti tecnologici, considerandone responsabilmente l'impatto sociale, psicologico ed economico.

Tuttavia è indispensabile chiedersi quali obiettivi sia realistico perseguire, e in quali termini in un contesto di formazione scientifico-tecnologica, tenendo conto da un lato delle attitudini vocazionali degli studenti, dall'altro del limitato spazio che può essere ritagliato dai curricula tradizionali per una simile attività. Alla luce della nostra esperienza, una parte non trascurabile degli studenti di discipline informatiche mostra di possedere un quadro storico e culturale ancora troppo fragile, su cui non si può fare affidamento per

agganciarvi i temi peculiari dello sviluppo scientifico e tecnologico. È perciò importante riuscire a capire in quale misura un corso di storia dell'informatica possa contribuire ad accrescere il bagaglio formativo generale degli allievi, motivandoli soprattutto a coltivare la sensibilità e l'interesse per i temi culturali anche al di là dell'impegno curriculare.

Con questo articolo ci proponiamo innanzitutto di avviare un dibattito, con l'auspicio che possa coinvolgere, oltre alla comunità accademica, anche gli ambiti scolastico e professionale. Nelle sezioni che seguono, dopo aver delineato sinteticamente l'impostazione del corso svolto a Udine, presentiamo il contesto e i risultati della nostra indagine. Infine, nell'ultima parte dell'articolo, discutiamo le interpretazioni che ne abbiamo tratto per concludere con alcune proposte preliminari.

2. IL CORSO DI STORIA DELL'INFORMATICA

Il corso di storia dell'informatica attivato presso l'ateneo di Udine è un corso opzionale rivolto agli studenti dei corsi di laurea di primo e secondo livello in discipline informatiche. Nei limiti delle 30 h di lezione allocate, i docenti del corso C. Bonfanti e P. Giangrandi hanno scelto di privilegiare gli obiettivi generali dei primi due ambiti individuati sopra. Si è giudicato infatti importante sia favorire l'ampliamento delle basi per una partecipazione responsabile alle scelte che la società moderna deve affrontare, sia dare rilievo alla stabilità nel tempo delle idee e dei principi generali in contrapposizione alla contingenza delle soluzioni tecnologiche di volta in volta adottate.

Seguendo percorsi talvolta divergenti, attraverso svolte concettuali e scoperte inattese che hanno determinato drastici cambiamenti, la storia dell'informatica ci presenta interessanti esempi di non linearità e non determinismo nello sviluppo scientifico [13]. Per queste ragioni, invece di seguire una sequenza strettamente cronologica, i contenuti del corso si articolano attorno ad alcuni moduli tematici che illustrano la grande varietà di approcci all'automazione del calcolo (Tabella 1). Possiamo ad esempio osservare come solo una sessantina di anni fa non fosse ancora scontato che l'elaborazione elettronica digi-



TABELLA 1

Programma corso,
a.a. 2005-06

1	Antichi strumenti di calcolo
2	Calcolatori meccanici analogici e digitali
3	Automi e macchine programmabili
4	Sistemi meccanografici
5	Pionieri del calcolo elettronico e architettura di von Neumann
6	Evoluzione delle tecnologie di CPU, memoria e dispositivi di I/O
7	Evoluzione del software e dei sistemi operativi
8	Algoritmi, cibernetica e intelligenza artificiale
9	Informatica in Italia
10	Sviluppo dell'industria e del mercato mondiale

CFU / Livello	E	D	C	B	A	Totale
[0, 40)	4	7	2	0	0	13
[40, 80)	8	12	11	5	0	36
[80, 130)	12	11	15	5	2	45
[130, 177)	0	5	6	14	6	31
[177, 300)	1	1	2	14	15	33
Totale	25	36	36	38	23	158

TABELLA 2

Distribuzione
degli studenti
del campione

tale avrebbe avuto il sopravvento su quella analogica. Inoltre, l'informatica rappresenta un caso emblematico di approccio multidisciplinare, dal momento che è nata dall'integrazione dei contributi di diverse discipline come la matematica, la logica, la fisica, l'elettronica, la linguistica e le scienze cognitive.

3. IMPOSTAZIONE DELL'ANALISI

L'analisi di cui qui ci occupiamo si riferisce alle prove scritte di cinque appelli d'esame (l'esame prevede anche una prova orale facoltativa i cui esiti non sono discussi in questa sede), ma non si propone come obiettivo di valutare il profitto degli studenti. Piuttosto, siamo interessati a capire meglio le conoscenze di base degli studenti e la loro attitudine verso tematiche culturali di ambito non prettamente tecnico. Non si tratta di un esperimento

didattico, preparato a tavolino, ma dell'osservazione di un "fenomeno non controllato" al fine di trarne quante più informazioni possibile, un *caso di studio* per cui "i confini fra il fenomeno e il contesto non sono del tutto chiari" [8] e le "domande di ricerca" vengono dopo la raccolta dei dati. Proporremo comunque alcune ipotesi interpretative, la cui generalità dovrà essere verificata estendendo l'analisi ad altri contesti.

3.1. Il campione di studenti

Gli studenti impegnati negli esami sono stati 158, la maggior parte dei quali iscritti da almeno due anni a un corso di laurea. Solo un gruppo ristretto ha seguito regolarmente le lezioni di storia dell'informatica, anche a causa di inevitabili sovrapposizioni di orario vista l'inattesa eterogeneità curriculare. La tabella 2 riassume inoltre la distribuzione degli studenti in relazione ai crediti maturati (CFU) e ai punteggi conseguiti nelle prove (livelli E-A). I crediti sono una misura della carriera degli studenti e possono essere rapportati ai 60 CFU corrispondenti al superamento degli esami di un anno di corso. I livelli quantificano il profitto in base alla percentuale di risposte corrette ai quesiti d'esame: E = 0-50%, D = 50-60%, C = 60-70%, B = 70-85%, A = 85-100% (dove nel caso di prova ripetuta è stato considerato il valore medio).

Probabilmente un risultato modesto (livelli E-C) indica che lo studente ha affrontato l'esame con un atteggiamento di tipo esplorativo, senza preoccuparsi seriamente di assimilare le nozioni del corso. Tuttavia, indipendentemente dall'assiduità di frequenza e dal profitto dimostrato, dal nostro punto di vista tutti i dati rilevati concorrono a caratterizzare il background generale degli allievi, ciò che qui ci interessa, a prescindere dalle nozioni specifiche di storia dell'informatica.

3.2. Le domande selezionate

Ogni prova d'esame consiste in una trentina di quesiti a scelta multipla. Per rispondere ad alcune domande di carattere generale non sono richieste competenze specifiche di storia dell'informatica, ma è sufficiente riflettere con un po' di buon senso su nozioni base di informatica e ricollegarsi al quadro storico sviluppato nella scuola secondaria (Tabella 3). Ai fini della

George Boole, Fibonacci, John von Neumann e Leonardo da Vinci sono personaggi di rilievo per la storia dell'informatica. Ordinali in ordine cronologico.

- [] Fibonacci, Leonardo, Boole, von Neumann
- [] Leonardo, Boole, Fibonacci, von Neumann
- [] Fibonacci, Leonardo, von Neumann, Boole
- [] Boole, Fibonacci, Leonardo, von Neumann
- [] Boole, Leonardo, Fibonacci, von Neumann

TABELLA 3

Esempio di quesito

nostra indagine abbiamo selezionato proprio le domande di questo tipo, in tutto 69 su un totale di 162, in quanto ci forniscono informazioni utili sul background degli allievi.

Una classificazione di queste domande per temi generali è schematizzata nella tabella 4, dove a fianco di ogni argomento è riportato il numero di quesiti pertinenti. Per *nozioni generali di storia della scienza* intendiamo le cognizioni che un allievo dovrebbe aver maturato nella scuola superiore; le *nozioni generali su tecnologie recenti* si riferiscono a strumenti comunemente considerati in ambito informatico, ancora in uso o comunque familiari per chi si interessa del settore; infine, la *familiarità con concetti e nozioni di base* riguarda il bagaglio culturale che lo studente dovrebbe aver acquisito frequentando un corso di laurea in informatica.

Argomenti dei quesiti	Numero di quesiti
<i>Nozioni generali di storia della scienza</i>	21
Problemi e strumenti	5
Personalità di rilievo	16
<i>Nozioni generali su tecnologie recenti</i>	26
Evoluzione nel secolo scorso	17
Principi di funzionamento	6
Tecnologie del software	3
<i>Familiarità con concetti e nozioni di base</i>	22
Concetti scientifici ricorrenti	4
Concetti matematici ricorrenti	6
Nozioni sugli algoritmi	2
Cultura informatica generale	10

3.3. Criteri dell'analisi

Le risposte fornite dagli studenti sono state analizzate applicando i seguenti criteri:

- i.** in relazione al numero di CFU, indice della maturità dello studente;
- ii.** come sopra, ma senza considerare le prove ripetute;
- iii.** in relazione al punteggio medio conseguito nelle prove, indice dello sforzo compiuto dallo studente per apprendere le nozioni di storia dell'informatica;
- iv.** come sopra, ma restringendo il campione agli studenti che hanno maturato da 80 a 176 CFU (terza e quarta riga di Tabella 2, cioè a studenti che hanno frequentato 2-3 anni di corso;
- v.** distinguendo studenti e studentesse, per verificare l'eventualità di un diverso atteggiamento (le allieve rappresentano circa il 15% del campione).

L'interesse per il punto (iv) deriva dal fatto che il corso di storia dell'informatica, per come è stato progettato, è prevalentemente in-

dirizzato alla corrispondente fascia di studenti; inoltre, questo campione appare meglio distribuito in relazione ai punteggi (si veda Tabella 2). D'ora in poi utilizzeremo il termine "campione ristretto" per riferirci a questo campione, distinguendolo dal "campione completo" che include tutti gli studenti che si sono cimentati nell'esame.

TABELLA 4

Classificazione dei quesiti analizzati

4. RISULTATI DELL'ANALISI

In questa sezione analizziamo le risposte degli studenti ai quesiti selezionati, seguendo lo schema di classificazione della tabella 4. Prima di entrare nel dettaglio, anticipiamo alcune osservazioni. Innanzitutto, dal confronto dei dati relativi ai punti (i) e (ii) si riscontra che i risultati non migliorano se si tiene conto delle prove ripetute; una possibile interpretazione di questo fatto è che le modalità di studio che gli studenti più deboli adottano incidono poco

sulle loro conoscenze culturali generali. Per quanto riguarda i punti (iii) e (iv), si rileva una correlazione fra nozioni di carattere generale e nozioni inerenti ai contenuti più specifici. Infine, in accordo con altri studi [2, 16], dai dati relativi al punto (v) emerge che gli studenti sono più interessati agli aspetti tecnologici rispetto alle studentesse, con uno scostamento più significativo per il campione ristretto.

4.1. Nozioni generali di storia della scienza

Riguardo a questa tematica, complessivamente poco più della metà delle risposte sono state corrette. Una selezione dei risultati è sintetizzata nella tabella 5, dove la seconda e terza colonna riportano il numero di risposte corrette rapportato al numero di allievi che si sono cimentati con il quesito, considerando rispettivamente il campione esteso e quello ristretto. Possiamo notare, per esempio, che i contributi di Church e di Wiener sono sconosciuti alla gran

parte degli allievi, mentre i ruoli di Boole e von Neumann vengono riconosciuti più facilmente, come ci si poteva aspettare per il frequente richiamo ai loro nomi in altri insegnamenti di base. Inoltre, i dati dell'ultima riga sono un indice della fragilità del quadro storico, dal momento che gli studenti faticano a collocare cronologicamente personaggi molto noti e appartenenti ad epoche chiaramente diverse.

4.2. Nozioni generali su tecnologie recenti

In questo caso le risposte corrette sono state circa i 2/3 del totale. L'impressione generale che se ne trae è che gli studenti sono incuriositi dagli artefatti e dagli strumenti tecnologici, ma non altrettanto interessati alle vicende e alle idee che ne hanno resa possibile la realizzazione. Talvolta anche l'identificazione di principi fisici o matematici alla base del funzionamento di un dispositivo risulta incerta. Una selezione dei risultati è riportata nella tabella 6.

TABELLA 5
Risposte
a una selezione
di quesiti su nozioni
storiche generali

Tipo di conoscenza oggetto del quesito: gli studenti...	Campione esteso	Campione ristretto
Sono in grado di riconoscere il ruolo preminente della geometria nella matematica della Grecia antica	20 / 50	6 / 24
Sono consapevoli delle proprietà distintive della rappresentazione numerica posizionale	26 / 60	16 / 33
Sanno identificare i principali ambiti dell'opera di Fibonacci, Nepero, Shannon	circa 50 %	10 / 29
Sanno riconoscere l'opera fondamentale di Frege o il problema chiave posto da Hilbert	25 / 50 26 / 44	circa 50 %
Sono in grado di associare i nomi di von Neumann e Boole ai rispettivi contributi più noti	46 / 50 19 / 20	circa 90 %
Sono in grado di collegare Wiener alla cibernetica e Church al lambda-calcolo	3 / 60 1 / 20	5 % o meno
Sono in grado di ordinare cronologicamente Fibonacci, Leonardo da Vinci, Boole, von Neumann	11 / 20	5 / 10

TABELLA 6
Risposte
a una selezione
di quesiti su aspetti
tecnologici

Tipo di conoscenza oggetto del quesito: gli studenti...	Campione esteso	Campione ristretto
Ricordano in quale decennio la RAM e la microprogrammazione furono introdotte	25 / 50 15 / 44	16 / 24 9 / 22
Sono in grado di ordinare cronologicamente dispositivi tecnologici recenti e ben conosciuti	44 / 60	23 / 33
Riescono a vedere il microprocessore come un'evoluzione dei circuiti integrati	11 / 20	3 / 10

4.3. Familiarità con concetti e nozioni di base

In questo ambito le risposte corrette sono state complessivamente meno della metà; una selezione è sintetizzata nella tabella 7. In alcuni casi abbiamo riscontrato una certa difficoltà a capitalizzare le conoscenze acquisite in altri corsi per rispondere ai quesiti proposti, forse perché la storia dell'informatica è percepita come una materia in cui il nozionismo prevale sulla riflessione. Alcuni studenti, tra l'altro, faticano a caratterizzare l'elaborazione analogica rispetto a quella digitale. Un'ulteriore considerazione pertinente questo tipo di quesiti: molti dei testi adottati presentano note di carattere storico, che includono gli argomenti oggetto delle ultime tre righe della tabella 7, ma evidentemente gli studenti non vi prestano attenzione o le considerano irrilevanti ai fini della loro formazione.

5. DISCUSSIONE

Tentiamo ora di formulare qualche ipotesi interpretativa dei risultati dell'analisi illustrati nelle sezioni precedenti. Nel fare questo è opportuno essere consapevoli delle condizioni in cui i dati sono stati raccolti: i campioni di studenti variano da una prova all'altra, ma non sono del tutto disgiunti perché era possibile ripetere la prova più volte; i quesiti presenti nei questionari sono stati formulati per

valutare il profitto e non ai fini di questa analisi; è verosimile che una parte degli studenti non abbiano affrontato seriamente lo studio del materiale del corso, ma in ogni caso le loro risposte riflettono le conoscenze maturate durante gli studi secondari e universitari.

La mancanza di nozioni come quelle a cui i quesiti fanno esplicito riferimento non è un problema di per sé stesso. Sapere che Church ha introdotto il lambda-calcolo ha poco a che vedere con la conoscenza del lambda-calcolo o del suo ruolo nella storia dell'informatica; analogamente, sapere che il test di Turing assume la forma di un gioco d'imitazione non implica alcuna cognizione della portata e della rilevanza del pensiero di Turing nel dibattito culturale. Tuttavia i risultati evidenziano un quadro culturale piuttosto modesto, ed è proprio in questo quadro generale che lo studente può collocare ogni nuova nozione o nuovo concetto. Per usare le parole di G. Gooday [9], "l'identità disciplinare di un fisico, di un chimico, di un biologo, di un chirurgo, di un ingegnere elettronico" e, aggiungiamo noi, di un informatico "fonda le proprie radici in questa conoscenza allargata dei rispettivi settori disciplinari".

Ecco, in sintesi, le nostre impressioni generali:

□ il quadro storico degli allievi appare incerto, come si è detto, specialmente per quanto riguarda lo sviluppo scientifico; da qui la difficoltà di mettere in relazione le acquisizioni

Tipo di conoscenza oggetto del quesito: gli studenti...	Campione esteso	Campione ristretto
Hanno familiarità con le proprietà dei dispositivi analogici e digitali	18 / 58	6 / 29
Hanno un'idea di quali costruzioni geometriche possono essere fatte con riga e compasso	36 / 50	16 / 24
Conoscono le principali applicazioni delle tavole logaritmiche	30 / 60	15 / 33
Hanno buona familiarità con la combinatoria dei codici binari	16 / 44	10 / 22
Riescono a identificare il <i>titolo</i> o l' <i>argomento</i> del principale articolo di Turing	26 / 50 10 / 20	9 / 24 6 / 10
Sono in grado di riconoscere la natura dell'esperimento concettuale noto come test di Turing	11 / 50	2 / 24
Sono in grado di caratterizzare correttamente lo scopo della macchina di Turing universale	7 / 20	4 / 10

TABELLA 7

Risposte a una selezione di quesiti su concetti e nozioni di base

pertinenti l'informatica con lo sviluppo generale delle idee;

□ emerge abbastanza chiaramente una certa curiosità per gli artefatti tecnologici, disposizione che si presta ad essere sfruttata per catturare l'attenzione degli studenti anche quando sono in gioco concettualizzazioni più astratte;

□ gli interessi culturali degli studenti sembrano concentrarsi prevalentemente nell'ambito tecnico, indicando un atteggiamento opportunistico verso la conoscenza, dove sono privilegiati gli aspetti funzionali all'applicabilità concreta.

A livello più informale, sulla base di alcuni commenti raccolti in aula, si può forse aggiungere che gli interessi degli allievi tendono ad orientarsi verso le vicende recenti a discapito di una ricerca delle radici culturali che si collocano più lontano nel tempo.

A nostro avviso il principale interesse di questa analisi risiede nelle domande che solleva in relazione agli obiettivi di conoscenze generali realisticamente perseguibili per integrare le competenze tecniche. Progettare un corso di storia dell'informatica che possa contribuire in modo efficace ad accrescere il bagaglio culturale non appare un compito facile, e comunque presuppone l'individuazione del quadro concettuale *tipico* degli studenti (il focus della nostra indagine), nonché la comprensione dell'atteggiamento prevalente nei confronti della cultura.

Si possono tuttavia già trarre alcuni suggerimenti per migliorare l'impostazione del corso di storia dell'informatica. In particolare, è necessario insistere sul contesto culturale di ciascuna delle epoche considerate, richiamando quanto appreso dallo studio della storia nella scuola secondaria ed enfatizzando il ruolo delle idee generali. Da un punto di vista storico, è inoltre opportuno distogliere l'allievo dalla tentazione di una visione esclusivamente *internalista* [14] dell'evoluzione tecnologica, centrata sugli artefatti piuttosto che sulle relazioni fra questi e i processi sociali. Infine, è opportuno prevedere dei collegamenti espliciti con la materia di altri insegnamenti curricolari, in modo che il corso si integri maggiormente nel programma di studi complessivo e non sia percepito semplicemente come una collezione di aneddoti e cu-

riosità; a questo proposito si potrebbero per esempio sfruttare le note storiche presenti nei libri di testo adottati, ma che gli studenti sono soliti ignorare, come abbiamo già osservato, perché le giudicano poco rilevanti.

6. CONCLUSIONI

Con questo articolo abbiamo cercato di stimolare una discussione sul ruolo di un corso che introduce la prospettiva storica in un curriculum a carattere prevalentemente tecnico per conseguire la laurea in informatica. Sebbene l'inattesa accoglienza del corso da parte degli studenti e i commenti raccolti in classe siano stati confortanti e tendano a confermare la validità dell'iniziativa, i risultati della nostra analisi ci hanno indotti a riflettere ulteriormente e potrebbero fornire degli spunti per migliorarne l'efficacia anche in contesti diversi da quello preso in esame.

In ogni caso è necessario tenere ben presenti i limiti di spazio che, in un curriculum standard, può essere realisticamente assegnato a un corso con queste caratteristiche. Poiché tale spazio non è comunque sufficiente a esaurire gli argomenti chiave per una comprensione dei processi storici, il principale obiettivo da perseguire è motivare gli allievi a porsi domande e a coltivare autonomamente un interesse culturale più ampio, che sappia andare oltre gli aspetti meramente tecnici.

Bibliografia

- [1] Abd-El-Khalick F.: History of science, science education, and nature of science: Conceptual change, discourse, collaboration, and other oversights! *History of Science Society Newsletter*, Vol. 30, n. 1, 2001.
- [2] Acker S., Oatley K.: Gender Issues in Education for Science and Technology: Current Situation and Prospects for Change. *Canadian J. of Education*, Vol. 18, n. 3, 1993, p. 255-272.
- [3] Allchin D.: How not to teach history in science. *J. of College Science Teaching*, Vol. 30, 2000, p. 33-37.
- [4] Bonfanti C.: Storia dell'informatica nelle università: un'iniziativa dell'AICA. *Mondo Digitale*, Settembre 2007, p. 33-39.
- [5] Condoor S.: *Importance of teaching the history of technology*. In IEEE Frontiers in Educat. Conf., 2004.



- [6] Dodig-Crnkovic G.: *Computer science in a theory of science discourse*. Master Thesis in Computer Science, Department of Computer Science Mälardalen University, 2004.
- [7] Duschl R. A.: *Using and abusing: Relating history of science to learning and teaching science*. In Proc. BSHS Conf., 2000.
- [8] Fincher S., Petre M., editors: *Computer Science Education Research*. Routledge Falmer (Taylor and Francis), 2004.
- [9] Gooday G.: *U-rated not X-rated: reassessing how science students could benefit from learning history of science*. In BSHS Annual Conference, 2003.
- [10] Hazzan O., Impagliazzo J., Lister R., Schocken S.: Using history of computing to address problems and opportunities in computer science education. *SIGCSE Bulletin*, Vol. 37, n. 17, March 2005, p. 126–12.
- [11] Impagliazzo J., Lee J. A. N., Williams M. R.: *Using history to teach computing*. In Proc. 33rd ASEE/IEEE Frontiers in Education Conf., 2003.
- [12] Knuth D. E.: Ancient babylonian algorithms. *Commun. ACM*, Vol. 15, n. 7, 1972, p. 671–677.
- [13] Pannabecker J.: Technological impacts and determinism in technology education: Alternate metaphors from social constructivism. *J. of Technology Education*, Vol. 3, n. 1, 1991.
- [14] Pannabecker J.: For a history of technology education: Contexts, systems, and narratives. *J. of Technology Education*, Vol. 7, n. 1, 1995, p. 43–56.
- [15] Pannabecker J.: Technology education and history: Who is driving? *J. of Technology Education*, Vol. 16, n. 1, 2004, p. 72–83.
- [16] Sanders J.: *Gender and Technology: A Research Review*. www.josanders.com, 2005.
- [17] Simard J.: Histoire des sciences et pédagogie. *Pédagogie collégiale*, Vol. 16, n. 2, 2002, p. 4–12.
- [18] Simard J.: *Science, technologie et société*. Le Saut Quantique, www.apsq.org/sautquantique, 2002.
- [19] Simard J.: L'épistémologie. *Pédagogie collégiale*, Vol. 16, n. 3, 2003, p. 11–16.

PAOLO GIANGRANDI, laureato in Informatica a Udine, insegna Matematica presso l'I.T.I.A. Malignani di Udine. Tiene inoltre da alcuni anni il corso di Storia dell'Informatica per la Scuola di Specializzazione per l'Insegnamento nella Scuola Secondaria e dal 2005-06 per i corsi di laurea in Informatica attivati presso l'Università di Udine. Nel 2000 e nel 2001 ha progettato e realizzato la mostra "Numeri e Macchine", organizzata con il contributo dell'Università di Udine, della Mathesis di Udine e del liceo scientifico N. Copernico di Udine. Ha al suo attivo diverse pubblicazioni scientifiche.

E-mail: giangran@dimi.uniud.it

CLAUDIO MIROLO è ricercatore presso la Facoltà di Scienze dell'Università di Udine e insegna nell'ambito del corso di laurea in Informatica e della Scuola di Specializzazione per l'Insegnamento Secondario. Coordina inoltre il Nucleo Dipartimentale di Ricerca in Didattica dell'Informatica e collabora con le scuole alla realizzazione di progetti didattici. I suoi principali interessi nel campo della ricerca riguardano gli algoritmi per risolvere problemi geometrici.

E-mail: claudio.mirolo@dimi.uniud.it



ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

Licenze software e Open Source

David D'Agostini, Antonio Piva

1. LICENZE SOFTWARE

Fin dalla sua comparsa, il software ha posto delle serie problematiche riguardo alla sua tutela giuridica. Prima del suo avvento, due erano i principali istituti giuridici di tutela delle opere dell'ingegno umano, il diritto d'autore e il brevetto industriale: il primo concepito originariamente per le creazioni artistico-espressive, il secondo per le invenzioni di carattere tecnico-industriale. Mentre il diritto d'autore mira a proteggere solo la forma espressiva dell'opera, la tutela brevettuale ha per oggetto il contenuto dell'invenzione. Il software si presenta però come un'opera atipica in quanto si colloca proprio a cavallo delle due categorie di opere dell'ingegno: la sua vocazione di opera destinata alla soluzione di problemi tecnici, lo avvicinerebbe ineluttabilmente alla categoria delle invenzioni dotate d'industrialità; d'altro canto, però, il software risulta carente del requisito della materialità, fondamentale per la brevettabilità.

Nel 1980 il legislatore statunitense stabilì quale disciplina applicare al software, ovvero la tutela per mezzo del copyright. Dopo un decennio, il legislatore italiano, recependo con il d. lgs. 518/1992 la direttiva comunitaria 1991/250/CEE, inserì il software tra le opere sottoposte a tutela del diritto d'autore. Il diritto continentale europeo e in particolare modo quello italiano, avverte la distinzione tra gli inalienabili diritti morali d'autore e quelli patrimoniali, ovvero tutto il fascio di diritti passibili di una valutazione economica (e quindi alienabili) che ruotano attorno alla gestione e alla diffusione dell'opera. Gli ordinamenti di *common law*,

come gli USA non presentano una simile dicotomia, considerando il diritto d'autore come sempre rilevante dal solo punto di vista patrimoniale.

Data la sussistenza dei diritti esclusivi derivante dalla tutela d'autore, è necessario che l'autore del software stipuli un contratto con l'utente, nel quale definisca di quali prerogative si spogli e di quali quindi possa essere investito l'utente, ovviamente per contro di un corrispettivo. Dal momento dell'ingresso del software nella schiera dei beni di consumo, gli autori iniziarono a stilare dei contratti di portata generale in cui esprimevano i termini della distribuzione e della riproduzione del programma su cui essi vantavano i suddetti diritti esclusivi: nacque così il tipo contrattuale della licenza d'uso software. [1]

Il software, a seconda del grado di libertà che il titolare dei diritti di tutela decide di attribuire agli utenti della sua opera, può essere classificato in un prospetto di categorie; in una scala di valore che parte da un grado minimo di libertà per l'utente verso il grado massimo, troviamo le seguenti ipotesi.

□ Software proprietario

Prevede molteplici e sovrapposte forme di distribuzione, tra le quali le più diffuse sono:

- *commerciale*, è il software rilasciato da una azienda per essere venduto su licenza, con o senza periodi di prova. Prevede il pagamento per l'uso della licenza da parte dell'utente per poter cominciare l'utilizzo del pacchetto software e/o per poter entrare in possesso del supporto (contenente il software eseguibile). L'accettazione della licenza e delle clausole

contrattuali da parte dell'utente avviene, alcune volte, per il solo fatto di aprire la confezione esterna in plastica trasparente del package, che equivale alla lettura e accettazione delle clausole contrattuali leggibili all'esterno della scatola, ovvero, con l'accettazione esplicita delle clausole contrattuali durante l'installazione del prodotto. Il software commerciale non consente la distribuzione libera ad altri utenti, anche se interni alla stessa organizzazione, ma è possibile distribuire, o consentire l'uso del software ad altri utenti solo se vengono acquistate le relative licenze.

- **Demo** (o versioni di prova), è il software di tipo commerciale che il fornitore ritiene utile distribuire in versione dimostrativa, con alcune funzioni inibite, o con alcune limitazioni d'uso (quali, ad esempio, il divieto di utilizzare il software in ambienti di produzione, ma solo in ambienti di laboratorio, progetti prototipali o progetti pilota), rispetto alla versione commerciale (piena) che può essere utilizzata in produzione. Dipende, quindi, da caso a caso se questo tipo di software può essere usato, copiato e distribuito liberamente, o no, concordemente con le clausole contrattuali siglate dal cliente con il fornitore.

- **Shareware**, sono i pacchetti software che si possono ottenere gratuitamente, in cui il programma, a differenza delle demo, si presenta completo delle funzionalità, ma con la possibilità di essere provato per un limitato periodo di

tempo. Allo scadere del periodo di prova, occorre pagare una certa somma all'autore, altrimenti il programma cessa di funzionare.

- **Ad-ware**, ovvero software gratuito che per l'utilizzo visualizza banner pubblicitari o installa nel computer dell'utente programmi spyware (software che raccolgono e inviano dati per usi solitamente commerciali). I costi di licenza sono così coperti in via indiretta dalle aziende inserzioniste.

- **Freeware** (da non confondere con Free Software), cioè software commerciale completo che viene ceduto in uso gratuito¹. In questo caso, l'aggettivo "free" è usato nel solo significato di gratuito, a differenza che nell'espressione "free software".

□ **Software Libero e Aperto**

È questa la categoria del software della quale fanno parte le due denominazioni di "free software" e software "open source" e la sottocategoria del copyleft.

□ **Public Domain Software**

Programmi che, per concessione dell'autore, non contengono alcuna indicazione di copyright, tanto da occultarne anche la paternità (aspetto "morale" del diritto d'autore); è perciò possibile utilizzarli, riprodurli e diffonderli liberamente, ma anche eventualmente modificarli e inglobarli all'interno di altro software non public domain (anche commerciale), in quanto non sussistono i limiti derivanti da licenza [2].

Nella tabella 1 sono riportate a confronto di-

	Open Source o Free		Proprietario		
	Non Copyleft	Copyleft	Chiuso	Shareware	Freeware
Codice sorgente disponibile	Si	Si	No	No	No
Libertà di ridistribuzione	Si	Si	No	Si	Si
Modifica	Si	Si	-	-	-
Restrizione	Si	No	No	No	No
Versioni modificate sono sempre libere	No	Si	-	-	-
Liberamente scaricabili	Si	Si	No	Si	Si
Limitazioni d'uso temporali	No	No	No	Si	No
Possibilità di ritorno economico	Si	Si	Si	Si	No

TABELLA 1

In tabella sono riportate alcune differenze fra le categorie di licenze Open Source o Free, nello spirito del copyleft o meno ed alcune licenze per software proprietario rispetto ad alcune libertà e/o limitazioni

¹ Nel Freeware viene concesso gratuitamente l'utilizzo del programma eseguibile mentre il codice sorgente rimane all'autore. Viene concesso in uso di solito per motivi promozionali, per esempio per puntare sull'aspetto della manutenzione e sulla personalizzazione.

verse tipologie di licenze rispetto ad alcune libertà e/o limitazioni.

2. COPYLEFT, FREE SOFTWARE E SOFTWARE OPENSOURCE

La parola Copyleft [3] è nata da un gioco di parole che deriva e rovescia il concetto di copyright. Un software copyleft viene dichiarato sotto copyright e poi vengono riversate le garanzie di libertà per l'utente all'interno della licenza, ribaltando così il ruolo della stessa e creando un vincolo di tipo legale fra la disponibilità del codice e le libertà di utilizzo, modifica e redistribuzione dello stesso.

Il copyleft consiste quindi nel convertire le licenze d'uso, da decalogo degli obblighi dell'utente, in una sorta di statuto dei suoi diritti, intoccabili nel tempo e invariati presso terzi.

In maniera più o meno sovrapposta a questa categoria di licenze, troviamo altre due definizioni di licenze software:

□ Software Libero (Free Software)

Tale dizione indica una categoria di licenze predisposte inizialmente da Richard Stallman e adottate dalla *Free Software Foundation* (FSF) [4]. Le caratteristiche principali di questa modalità di distribuzione del software sono descritte nella definizione di Free Software che recita testualmente: *L'espressione "software libero" si riferisce alla libertà dell'utente di eseguire, copiare, distribuire, studiare, cambiare e migliorare il software. Più precisamente, esso si riferisce a quattro tipi di libertà per gli utenti del software:*

- Libertà di eseguire il programma, per qualsiasi scopo (libertà 0).
- Libertà di studiare come funziona il programma e adattarlo alle proprie necessità (libertà 1). L'accesso al codice sorgente ne è un prerequisito.
- Libertà di ridistribuire copie in modo da aiutare il prossimo (libertà 2).
- Libertà di migliorare il programma e distribuirne pubblicamente i miglioramenti, in modo tale che tutta la comunità ne tragga beneficio (libertà 3). L'accesso al codice sorgente ne è un prerequisito.

□ Software Open Source

Tale dizione è frutto di una rivisitazione delle proposte della Free Software Foundation operata nel 1998 da un gruppo di persone (fra cui Todd Anderson, Chris Peterson e Eric Raymond che guidò alla costituzione della *Open*

Source Initiative (OSI) [5]), con l'obiettivo di avvicinare lo sviluppo del software libero a quello sviluppato dalle imprese commerciali. Questo ha portato all'elaborazione della cosiddetta *Open Source Definition* (OSD), che definisce dei criteri generali per riconoscere le licenze e le distribuzioni Open Source. La OSD contiene 10 condizioni che disciplinano gli aspetti informatici, economici e giuridici della metodologia Open Source. Le prime tre riportate di seguito, servono a garantire le libertà fondamentali:

- distribuzione Aperta (Libera e Gratuita): *diritto di fare copie del programma e di ridistribuirle liberamente;*
- accesso Aperto (al Codice Sorgente): *il codice deve essere disponibile a costo di distribuzione e non obnubilato;*
- modificabilità Aperta: *diritto di poter intervenire sul programma e modificarlo* (non si obbliga né si vieta che la licenza si propaghi al lavoro derivato).

Le rimanenti 7 garantiscono l'assenza di discriminazioni e definiscono i diritti e dignità degli autori. Queste sono:

- integrità del codice sorgente dell'autore;
- nessuna discriminazione contro persone o gruppi;
- nessuna discriminazione contro campi applicativi;
- i diritti offerti dalla licenza si applicano automaticamente a tutti i destinatari;
- la licenza non deve essere specifica ad un prodotto (cioè legata ad una particolare forma fisica di distribuzione);
- la licenza non deve porre vincoli su altro software allegato a quello licenziato (esempio, vincoli sui software che possono o meno essere utilizzati assieme a quello licenziato);
- la licenza non deve richiedere particolari tecnologie di accesso (esempio, vincoli sui prodotti utilizzabili per accedere/utilizzare il software licenziato).

Dunque, la OSD non è un modello di licenza per software Open Source, bensì una specifica di quanto è ammesso in una licenza software perché possa essere considerata Open Source. Attualmente la Open Source Initiative riconosce 59 licenze Open Source.

Dall'analisi delle definizioni di licenza Free Software e Open Source, si può notare come queste abbiano molti punti di contatto, tant'è che buona par-



te delle licenze Free Software risultano anche essere Open Source e viceversa. Tuttavia esistono licenze, anche se non molte, che sono Free Software ma non Open Source e viceversa [6].

Si presentano ora alcune tra le più importanti e diffuse licenze Open Source.

3. LICENZE OPEN SOURCE

3.1. GNU General Public License (GPL)

La GPL uscì nel 1989 ed esprime in sé stessa i principi del Free Software. La caratteristica principale della GPL è la sua “viralità”, vale a dire che ogni modifica a codice GPL e tutto il codice sviluppato per funzionare in associazione con software GPL, deve essere a sua volta coperto da licenza GPL. La licenza GPL è tale per cui si può affermare che il software regolato GPL è Open Source, inoltre, la sua viralità garantisce che le libertà dell'utente vengano mantenute nel tempo, quindi il software GPL fa anche parte della categoria del software copyleft.

Recentemente è stata pubblicata la terza versione della licenza GPL allo scopo di modificare alcuni aspetti della versione precedente, per meglio gestire in particolar modo l'uso di DRM (*Digital Right Management*) e del *tivoization*².

3.2. LGPL, Library General Public License

La viralità della licenza GPL pose un problema alla realizzazione di librerie di funzioni; infatti, una libreria protetta da GPL non sarebbe stata utilizzabile da sviluppatori di software proprietario e quindi la libreria avrebbe perso gran parte del suo potenziale; per questo motivo, nel 1991 uscì una seconda licenza, chiamata LGPL, *Library General Public License*. Questa è una licenza apposta per le librerie, che si presenta come una versione della GPL alleggerita di alcune restrizioni (per questo recentemente rinominata “Lesser GPL”). In tal modo, il software principale, che utilizza librerie LGPL, può essere rilasciato sotto qualsiasi licenza (anche proprietaria), ma le modifiche al codice LGPL sono comunque soggette a LGPL; tale particolarità pone la LGPL ai margini di ammissibilità fra le licenze copyleft.

3.3. BSD (*Berkley Standard Distribution*)

La licenza BSD (le cui prime versioni risalgono agli anni '80), è una licenza molto semplice, la cui applicazione si risolve nell'inserimento di una breve nota standard da inserire nei file che si intendono tutelare con la licenza. La nota deve riportare il nome di chi detiene il copyright, l'organizzazione cui appartiene e l'anno di realizzazione³. La licenza specifica che sono permesse la ridistribuzione e l'utilizzo del software tutelato in forma sorgente o binaria, con o senza modifiche, ma solo se vengono rispettate tre condizioni:

- ❑ le ridistribuzioni del codice sorgente devono mantenere la nota sul copyright;
- ❑ le ridistribuzioni in forma binaria devono riprodurre la nota sul copyright, l'elenco delle condizioni e la successiva avvertenza nella documentazione e nell'altro materiale fornito con la distribuzione;
- ❑ il nome dell'autore non potrà essere utilizzato per sostenere o promuovere prodotti derivati dal software licenziato, senza un apposito permesso scritto dell'autore.

La caratteristica principale di tale licenza è la possibilità di “chiudere” il software sotto qualsiasi altra licenza, anche proprietaria; lo stesso vale anche per le modifiche apportate al software. Questo aspetto la pone al di fuori del paradigma di “copyleft”, poiché non è garantita la trasmissione all'infinito dei diritti da essa concessi, i quali si interrompono nel momento in cui il codice (originale o modificato) viene chiuso sotto altra licenza. Simile alla BSD nella struttura e nello spirito generale è la MIT License, che prende il nome dal noto centro di ricerca del Massachusetts.

3.4. Mozilla Public License (MPL)

Sviluppata da Netscape nel 1998, la MPL è un ibrido tra le licenze GPL e BSD. Al suo interno distingue tra “Covered Code”, cioè il codice soggetto alla licenza, che è simile a GPL e “Larger Work” cioè il codice MPL che può essere combinato con altro codice (anche proprietario). In tal modo, la MPL si comporta come la GPL sul Covered Code e come la BSD sul Larger Work. All'interno di un progetto, la decisione sulla distinzio-

² Il termine indica la pratica di creazione di un sistema che incorpora software sotto i termini di una licenza copyleft, ma usa particolare hardware per evitare agli utenti la possibilità di eseguire versioni modificate del software su quell'hardware.

³ La BSD originale, prevedeva una clausola chiamata “pubblicitaria” che obbligava l'utente a “dare esplicito riconoscimento all'Università [Berkley] nelle eventuali inserzioni pubblicitarie previste per i programmi derivati”. Siccome la GPL proibisce ogni restrizione addizionale circa la ridistribuzione del software, la licenza BSD originale non era compatibile con la GPL. Nel 1999, quindi, tale clausola venne eliminata rendendo così la BDS, GPL-compatibile.

ne tra i due tipi di codice è lasciata agli sviluppatori. In essa, più che in altre licenze anteriori, sono presenti alcune rilevanti clausole mirate a tutelare gli sviluppatori del progetto Mozilla dalla malafede di coloro che avrebbero potuto approfittare della elasticità della licenza inserendo tacitamente parti di codice coperte da brevetto, per poi rivendicarne per vie legali il pagamento. La licenza Mozilla, tuttora usata per i browser Netscape, è incompatibile con la GPL⁴.

3.5. Q Public License

La QPL creata da Trolltech, cattura il significato generale della GPL, ma è incompatibile con essa

Licenze	Può essere miscelato con software commerciale?	Le modifiche possono essere mantenute private e non restituite all'autore originale?	Può essere ri-licenziato da chiunque?
GPL	no	no	no
LGPL	sì	no	no
New BSD	sì	sì	no
MPL	sì	sì	no
QPL	sì	sì	no
Public Domain	sì	sì	sì

TABELLA 2

Nella tabella sono riportate alcune differenze tra le licenze Open Source trattate nel presente articolo

Licenze	È una licenza di software libero?	È compatibile con la GPL?	È nello spirito del copyleft?
GPL	sì	sì	Sì
LGPL	sì	sì	non del tutto
New BSD	sì	sì	No
MPL	sì	sì	No
QPL	sì	no	non del tutto

TABELLA 3

Analisi delle licenze trattate in base ai parametri di software libero, compatibilità con la GPL e copyleft

nel senso che non è possibile unire assieme codice protetto da GPL e da QPL. Questa distingue tra il software originale e le modifiche apportate e come queste sono distribuite. Se le modifiche sono incorporate nel codice, allora la QPL si estende anche ad esse (come per la GPL). Se invece le modifiche sono distribuite sotto forma di patches (codice esterno), similmente a quanto accade nella BDS, queste possono essere soggette a qualsiasi licenza, anche proprietaria⁵.

Nella tabella 2 e 3 sono riportate a confronto le licenze trattate rispetto ad alcuni parametri fondamentali.

Alla luce di quanto visto, si può procedere ad una classificazione delle licenze Open Source nel seguente modo:

□ **propagative** (nello spirito del copyleft), sono quelle licenze ispirate alla GPL, che richiedono che tutti gli sviluppi del codice siano integrati solo con codice Open Source e siano pubblicati sotto una licenza GPL-compatibile;

□ **persistenti ma non propagative** (non propriamente copyleft), sono quelle licenze che consentono un linking dinamico con codice proprietario, ma ogni modifica al codice originale deve essere soggetto alla stessa licenza (esempio, LGPL, MPL, QPL). Gli sviluppatori che modificano il codice originale o estendono librerie esistenti devono rilasciare il codice sotto la stessa licenza (persistenza), ma il codice esterno collegato al codice originale, può essere distribuito sotto altra licenza (non propagazione);

□ **permissive non propagative né persistenti** (non copyleft), sono quelle licenze che ammettono una combinazione di codice OS con codice proprietario (esempio, BSD, MIT) e consentono di porre il codice così ottenuto sotto altra licenza (anche proprietaria) mantenendo solo una nota riportante i nomi degli autori del codice OS.

Un aspetto degno di nota è quello delle garanzie sul software. Il software libero in genere, è ceduto senza alcuna garanzia. La ragione dell'assenza di garanzia è conseguenza del fatto che l'autore originario rischia di essere chiamato in cause legali anche per modifiche non apportate da lui. Garantire questo tipo di software diventerebbe, quindi, un ostacolo alla sua diffusione ed esporrebbe l'autore a rischi legali e finanziari non pre-

⁴ Alcune licenze derivate dalla MPL sono Apple PL (Mac OS X e Darwin (Covered Code) + Quartz e altre porzioni proprietarie), Nokia OSL, Sun PL.

⁵ Per questo motivo tale licenza non può essere considerata pienamente nello spirito del copyleft. Un esempio di software QPL sono le librerie Qt (che però sono state rilasciate anche sotto GPL).

vedibili a priori. È concessa garanzia, ma limitata - come avviene per il software proprietario - solo in caso di diffusione commerciale. In questo caso è l'azienda che realizza la "distribuzione" che esegue le verifiche ed i test sul software utilizzato e che si assume la responsabilità di fornire una garanzia "limitata". La limitazione scelta nella maggior parte dei casi fa sì che si debba solo risarcire il prezzo del pacchetto software, oppure obbliga alla sostituzione del supporto danneggiato. La OSD non fa riferimento a questo tipo di garanzie, pertanto in una licenza Open Source non vi è obbligo né divieto di inserirle.

4. UN CONTRO ESEMPIO: LA LICENZA MS SHARED SOURCE

Microsoft ha proposto otto licenze di tipo *Shared Source* [7] le quali permettono la lettura del codice sorgente, ma vietano di ridistribuire il codice o di condividere il sorgente con terze parti. Le licenze per enti commerciali o governativi sono di tipo "read only", ovvero non consentono la modifica neanche per uso interno (ma è possibile proporre le patch a MS). Il ricevente è tenuto a trattare il sorgente come dati proprietari confidenziali di Microsoft. Pertanto uno sviluppatore che entra in contatto con il sorgente Microsoft, se successivamente sviluppa programmi competitivi, potrebbe essere citato per violazione di dati confidenziali.

5. CONCLUSIONI

Open Source è un modello di sviluppo innovativo, mirante alla qualità e l'affidabilità del software attraverso la revisione indipendente tra pari e l'evoluzione rapida del codice sorgente. La rilevanza economica del software Open Source è cresciuta rapidamente, soprattutto grazie al fatto che questi sistemi liberi sono disponibili a costi molto bassi, se non nulli, ma comunque ben inferiori a quelli di analoghi sistemi proprietari. Tuttavia, a causa delle loro caratteristiche, il loro uso richiede una buona cultura di base nel campo del software. Grazie alle spinte all'utilizzo di software Open Source negli Enti Pubblici, il *Centro Nazionale per l'Informatica nella Pubblica Amministrazione* (CNIPA) [8] ha costituito l'Osservatorio Open Source [9] e molti sono i provvedimenti legislativi presi a livello sia nazionale che regionale che mi-

rano alla promozione e l'uso del software Open Source anche nella Pubblica Amministrazione. Per essere Open Source, il software deve essere distribuito sotto una licenza che garantisca i diritti fondamentali espressi nelle 10 condizioni della *Open Source Definition* (OSD). È importante ricordare come questa definizione risulta abbastanza generale per cui non esiste un'unica licenza Open Source, ma è possibile scegliere (o proporre) la licenza Open Source più adeguata agli obiettivi e alle situazioni. La *Open Source Initiative* (OSI) mantiene sul suo sito ufficiale una lista delle licenze "Open Source compatibili".

Bibliografia

- [1] St. Laurent A. M.: *Understanding Open Source & Free Software Licensing*. O'Reilly, Agosto 2004.
- [2] Aliprandi S.: *Copyleft & opencontent l'altra faccia del copyright*. PrimaOra, marzo 2005.
- [3] Sito del Copyleft italiano: www.copyleft-italia.it
- [4] Sito Ufficiale della Free Software Foundation (FSF): www.fsf.org
- [5] Sito Ufficiale della Open Source Initiative (OSI): www.opensource.org
- [6] Baggi M., Piva A.: *Categorie di licenze per software libero*. Rivista di Informatica Giuridica, disponibile all'indirizzo: <http://217.141.103.211/alsiud/infogiur.htm>
- [7] MS Shared Source: <http://www.microsoft.com/resources/sharedsource/default.mspix>
- [8] Sito Ufficiale del CNIPA: <http://www.cnipa.gov.it/>
- [9] Osservatorio Open Source del CNIPA: <http://www.ossipa.cnipa.it/>

ANTONIO PIVA, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA. E-mail: antonio@piva.mobi

DAVID D'AGOSTINI avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA. E-mail: studio@avvocatodagostini.it



DENTRO LA SCATOLA

Rubrica a cura di

Fabio A. Schreiber

Con questo numero si conclude il ciclo di articoli "Dentro la scatola". Scopo dichiarato della rubrica era di presentare, in modo semplice e succinto, ma rigoroso, i concetti basilari dell'Informatica a coloro che, a vario titolo, di Informatica si occupano o con l'Informatica lavorano, pur senza avere una formazione tecnica specifica.

Il tema scelto per il 2004 è stato: "*Perché gli anglofoni lo chiamano "computer", ovvero: introduzione alle aritmetiche digitali*", e ha affrontato il modo di codificare l'informazione digitale. Per il 2005 il filo conduttore della serie è stato: "*Ma ce la farà veramente? Ovvero: introduzione alla complessità computazionale e alla indecidibilità*", con l'intento di guidare il lettore attraverso gli argomenti fondanti dell'Informatica e le loro implicazioni pratiche e filosofiche. La terza serie, negli anni 2006 e 2007, ha esplorato "*Come parlano i calcolatori*", ovvero i linguaggi di programmazione delle procedure e di interazione con i dati e i protocolli di comunicazione per i sistemi distribuiti. Non a caso la serie si conclude con un contributo sulla crittografia, argomento di grande attualità e di fondamentale importanza in un mondo sempre più informatizzato, nel quale la sicurezza e la privacy dell'informazione diventano una delle principali preoccupazioni a livello tecnico e sociale per lo sviluppo di nuove applicazioni.

Colgo l'occasione per ringraziare sentitamente tutti i colleghi che hanno compiuto il non piccolo sforzo di condensare in testi sintetici e divulgativi i loro contributi e il Consiglio Direttivo dell'AICA per aver intrapreso un'iniziativa, che ci auguriamo possa avere un seguito nel futuro.

Crittografia elettronica

Luca Breveglieri, Mariagiovanna Sami

Il problema di proteggere l'informazione da sguardi indiscreti – in particolare, anche se non solamente, quando l'informazione deve essere comunicata fra due partecipanti – si è presentato millenni fa; dopo la seconda guerra mondiale, con l'avvento dei calcolatori elettronici, la scienza della protezione dell'informazione mediante crittografia ha avuto grande sviluppo, dato che i nuovi strumenti consentono la realizzazione di sistemi complessi di codifica che non sarebbero stati praticamente applicabili con tecniche manuali.

In questo articolo, dopo un cenno ai diversi aspetti della *sicurezza* (*security*) dell'informazione, si presenteranno brevemente le metodologie principali per la *confidenzialità* ottenuta mediante codifica (e relativa decodifica), dal momento che proprio la *confidenzialità* è alla base di tutte le soluzioni di sicurezza. Si introdurranno le cifre di merito che portano a valutazioni delle diverse metodologie, e si indicheranno i metodi oggi più significativi miranti a infrangere la sicurezza.

1. INTRODUZIONE

Si può definire la *crittologia* (*cryptology*) come lo studio della messa in sicurezza dell'informazione, vale a dire come l'analisi e il progetto, da un lato, di metodi per proteggere l'informazione contro utilizzi indesiderabili e, in senso opposto, di metodi per infrangere (o "rompere") una tale protezione [1]. La *crittografia* (*cryptography*) [2, 3] raggruppa pertanto i metodi destinati alla protezione dell'informazione, mentre il suo contrario è la *crittanalisi* (*cryptanalysis*) [2, 3]: queste due discipline costituiscono complessivamente la crittologia. Qui l'attenzione sarà posta principalmente su metodologie e algoritmi (o "primitive crittografiche") in uso nella crittografia contemporanea, la quale è basata in modo essenziale sull'uso del calcolatore elettronico; prima di entrare in argomento si farà però un breve cenno storico.

La proprietà essenziale che si desidera conferire all'informazione è la *sicurezza* (*security*). In realtà tale termine naturale è un po' vago e va

precisato caso per caso specificando quali aspetti di sicurezza si vogliono considerare. L'esempio forse più immediato e intuitivo è dato dalla proprietà di *confidenzialità* (*confidentiality*), vale a dire la protezione dell'informazione, sia essa un messaggio da trasmettere o un dato memorizzato, contro l'interpretazione e di conseguenza lo sfruttamento da parte di un'entità, essere umano o macchina, non esplicitamente autorizzata a svolgere tale funzione.

L'operazione fondamentale per ottenere la confidenzialità è la *cifratura* (*encryption*), mediante la quale si altera e confonde la forma codificata dell'informazione al fine di renderla non interpretabile; l'operazione inversa, mediante la quale si ricostruisce la forma originale, si chiama *decifrazione* (*decryption*)¹. L'informazione in forma *non cifrata* e *cifrata* si chiama, rispettivamente, *testo in chiaro* (*cleartext* o *plaintext*) e *testo cifrato* (*ciphertext*). Le operazioni di cifratura e decifrazione si effettuano mediante *algoritmi* (o *primitive*) crittografici, e spesso all'insieme dei due algoritmi – di cifratura e di decifrazione – si dà nome di *crittosistema* (*cryptosystem* o *ciphersystem*).

La confidenzialità è tuttavia solo la prima e più semplice proprietà di sicurezza dell'informazione; ce ne sono altre più raffinate e specifiche, che si vedranno più avanti. È pur vero che la proprietà di confidenzialità funziona in molti casi come base per ottenere le altre proprietà più sofisticate. La crittografia contemporanea è interamente basata sull'uso del calcolatore elettronico. Tralasciando dunque interpretazioni cinematografiche fantasiose, non è neppure lontanamente pensabile che la cifratura di un blocco di informazione, e meno che mai la decifrazione, svolta mediante un algoritmo crittografico contemporaneo di uso commerciale (come DES o AES), sia effettuabile da parte di un essere umano a mente o al massimo solo con l'ausilio di carta, matita e poco altro. Non è tuttavia sempre stato così, e la crittografia per secoli fu applicata manualmente o tramite qualche ausilio meccanico piuttosto semplice.

Ecco una brevissima sintesi storica [6], relativa a sistemi crittografici miranti a garantire la funzione di confidenzialità per messaggi da spedire. I

primi algoritmi di cifratura di cui si abbia notizia, risalenti all'antichità, furono di tipo alfabetico a schema di sostituzione prefissato: i caratteri del testo in chiaro venivano sostituiti secondo uno schema fisso e naturalmente invertibile. Assai noto è l'algoritmo di Cesare, dove la lettera "A" viene sostituita da "C", "B" da "D", ..., "X" da "Z", "Y" da "A" e infine "Z" da "B". Naturalmente tale schema è invertibile, per potere decifrare. Lo schema di sostituzione prefissato costituisce un esempio elementare di *chiave segreta* o *privata di cifratura* (*secret* o *private key*). Nell'algoritmo di Cesare la chiave è data da due elementi: la specifica del tipo di schema e il numero di passi. In generale la chiave sarà costituita da tutti gli elementi e i parametri caratterizzanti lo schema. La proprietà di confidenzialità è garantita dal possesso esclusivo della chiave, che deve essere nota solo a chi o che cosa sia autorizzato a interpretare il contenuto del messaggio. La chiave segreta può restare in uso per sempre, oppure (per maggior sicurezza) la si può mantenere per un certo intervallo di tempo o per un dato numero di operazioni di cifratura, cambiandola poi con frequenza proporzionata al livello di confidenzialità che si desidera conseguire.

Lo scopo della crittanalisi consiste nel trovare la chiave segreta in uso, ovvero lo schema di sostituzione, avendo a disposizione come materiale di lavoro qualche esempio di testo cifrato e possibilmente anche qualche esempio di testo in chiaro corrispondente. Ingenuamente, si può sempre tentare la crittanalisi mediante *forza bruta* (*brute force*) provando tutte le chiavi segrete. Ne segue che per garantire un buon livello di protezione alla cifratura occorre garantire che l'insieme di chiavi ammissibili, o *spazio delle chiavi* (*key space*), sia adeguatamente ampio, sì da rendere impossibile o almeno non conveniente il ricorso a forza bruta.

Gli algoritmi crittografici a schema di sostituzione prefissato, alfabetici o più realisticamente a blocchi di caratteri, sono però vulnerabili all'*analisi delle frequenze* dei caratteri (*frequency analysis*). Il principio secondo cui analizzando le frequenze relative dei caratteri (o dei blocchi di caratteri) nel testo cifrato e confrontandole con quelle caratteristiche del testo in chiaro, possedendone un esemplare oppure facendo qualche ipotesi ragionevole su come esso sia fatto, si possa ritrovare lo schema di sostituzione (la chiave segreta), risale al tardo Medioevo

¹ Qualcuno purtroppo dice e scrive *crittare* e *decrittare*, *crittazione* e *decrittazione*.

e al Rinascimento; tale scoperta è accreditata a Leon Battista Alberti [6]. Ovviamente per poter adottare la *frequency analysis* occorre conoscere la lingua naturale in cui il testo è stato scritto ed è necessario che il testo cifrato sia sufficientemente lungo da consentire l'applicazione di sia pur semplici ragionamenti statistici. Un esempio letterario molto celebre è presentato in una delle avventure di Sherlock Holmes, "I pupazzi ballerini", dove a ogni lettera è sostituito un disegno schematico.

A fronte dello sviluppo delle tecniche di analisi delle frequenze vennero sviluppati metodi combinati di cifratura mediante sostituzione e permutazione di elementi di informazione (caratteri o blocchi), secondo schemi guidati da una chiave segreta. Infatti, applicando sostituzioni differenziate si riduce l'efficacia dell'analisi delle frequenze, e intercalando permutazioni (cioè cambiamenti di ordine) diverse si tendono a cancellare le regolarità ripetitive eventualmente presenti nel testo in chiaro. I crittosistemi di tale tipo in uso in età moderna furono numerosi, spesso incentrati su un repertorio prefissato ma abbastanza ampio di tabelle di sostituzione e permutazione, di uso manuale, da scegliere caso per caso come specificato dalla chiave segreta [6]. In séguito l'operazione di cifratura manuale venne accelerata mediante l'uso di sistemi elettromeccanici, quando tale tecnologia fu inventata, senza però cambiare il principio del metodo. Il culmine di tale tendenza fu raggiunto dalla notissima macchina elettromeccanica Enigma progettata poco prima e posta in uso durante la seconda guerra mondiale [6]. Essa sostituisce e permuta i caratteri del testo secondo schemi complicati selezionati dalla chiave segreta. Di fatto l'analisi delle frequenze di testi cifrati da Enigma risultava molto complessa con i metodi dell'epoca, e fattibile solo in casi speciali e fortunati.

Con la fine della guerra e la contemporanea invenzione del calcolatore elettronico inizia la storia della crittografia contemporanea, dove cifratura e decifrazione sono realizzate da strumenti elettronici. Il primo crittosistema, ideato secondo criteri che aspiravano a essere sistematici, documentato (almeno parzialmente) e realizzato sia in software sia in hardware, che risultò di rilevante successo commerciale, fu DES (*Data Encryption Standard*), progettato da IBM nel 1973-74 [2] e reso standard da NIST nel 1976. Con esso inizia ufficialmente la storia della crittografia

contemporanea. Oggi DES è superato da altre soluzioni più moderne, come AES (*Advanced Encryption Standard* - 2002) [2][5], ma con esso si può concludere la nostra breve rassegna storica. Nel resto dell'articolo si illustreranno sinteticamente i concetti e i metodi fondamentali della crittografia contemporanea basata su calcolatore elettronico: prima se ne presenteranno concetti e modelli di base (sezione 2), poi si descriveranno gli algoritmi commerciali attualmente in uso, a chiave segreta (sezione 3) e pubblica (sezione 4). Le conclusioni tratteggeranno alcune tendenze di ricerca attuali (sezione 5).

2. CONCETTI E MODELLI DI BASE

La crittografia può garantire diverse proprietà di sicurezza dell'informazione. Come già detto, la proprietà fondamentale (e più semplice) è la *confidenzialità*, in pratica la restrizione della facoltà di interpretazione e sfruttamento dell'informazione solo a entità specifiche, proprietà che si ottiene tramite la funzione di *cifratura*. La proprietà di *autenticazione* (*authentication*) consiste nella garanzia che l'informazione sia prodotta o riconosciuta da un'entità identificabile, e si ottiene mediante la funzione di *firma digitale* (*digital signature*), che si vedrà più avanti. La firma digitale può anche garantire la proprietà di *integrità* (*integrity*) dell'informazione, che consiste nella garanzia che l'informazione non sia alterata, accidentalmente o intenzionalmente, e anche la proprietà di *non-ripudio* (*non-repudiation*), che consiste nella garanzia che l'informazione prodotta o riconosciuta da un'entità non possa essere da questa misconosciuta in séguito. Infine la proprietà di *autorizzazione* (*authorization*) consiste nella garanzia che l'informazione (o il servizio) sia accessibile solo da parte di un'entità o di un gruppo esplicitamente autorizzato a tale funzione, e si ottiene tramite combinazioni delle funzioni citate in precedenza.

Ogni crittosistema è dotato di uno o più elementi di informazione che costituiscono la *chiave* (*key*), da cui dipende il livello di sicurezza del sistema. In definitiva la chiave è sempre rappresentabile come stringa di bit. I crittosistemi odierni sono progettati in conformità al cosiddetto principio di Kerchoff (formulato già nel 1883): *tutti gli aspetti del crittosistema sono pubblici* (struttura, algoritmi e parametri), *tranne la chiave*. L'idea è che un crittosistema con

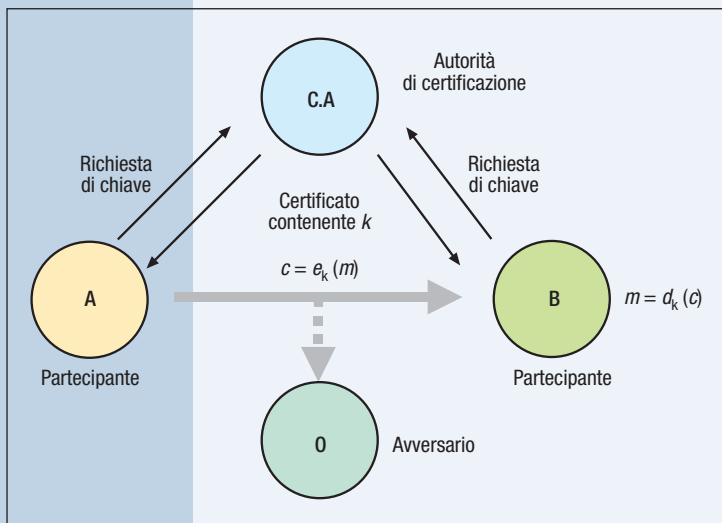


FIGURA 1

Modello generale di crittosistema (canale di comunicazione cifrato)

troppi aspetti segreti finisca per essere meno sicuro di uno con pochi. Infatti, poiché la crittografia oggi è diffusissima e primitive crittografiche si trovano realizzate in numerosi dispositivi elettronici, fissi e mobili, prodotti e distribuiti in milioni di esemplari, sarebbe del tutto vano illudersi di riuscire a celare, anche solo per breve tempo, gli aspetti strutturali e algoritmici o la configurazione di un crittosistema di successo commerciale. Senza contare che rendendo pubblico il crittosistema numerosi ricercatori possono studiarlo ed eventualmente scoprire per tempo difetti sfuggiti a una prima analisi. Il massimo che si riesca a fare, e d'altra parte il minimo indispensabile, è tenere segreta la chiave o parte di essa. Pertanto il principio di Kerchoff rappresenta un requisito formale del tutto coerente con l'uso concreto che oggi si fa della crittografia. La figura 1 mostra il modello generale di crittosistema, nel caso l'informazione da rendere confidenziale sia un messaggio. Le entità A e B sono i *partecipanti (partner)* del sistema. Ecco (1) il modello espresso in simboli:

$$c = e_k(m) \quad e \quad m = d_k(c) \quad (1)$$

dove $m, c, k \in M, C, K$

Gli elementi m, c e k sono il testo in chiaro (messaggio originale), il testo cifrato (messaggio cifrato) e la chiave, rispettivamente, e appartengono agli insiemi o spazi M, C e K del testo in chiaro, cifrato e della chiave, rispettivamente. Di norma il testo in chiaro e quello cifrato (m e c)

hanno dimensione (in bit) prefissata. I simboli e_k e d_k sono gli algoritmi di cifratura e decifrazione, rispettivamente. Li si suole formulare come funzioni a un solo argomento parametrizzate dalla chiave k , e naturalmente si ha l'identità $\forall m, k \quad d_k[e_k(m)] = m$.

L'entità O rappresenta l'*avversario (adversary)*, che si procura materiale vario, generalmente esemplari di testo cifrato ed eventualmente anche in chiaro, su cui lavorare per effettuare la crittanalisi e trovare la chiave k o almeno parte del testo in chiaro m .

La chiave k può essere la medesima per entrambi i partecipanti o differenziarsi tra i due. Nel primo caso si parla di crittosistema a chiave *segreta* (o *privata*) o *simmetrico*, nel secondo a chiave *pubblica* o *asimmetrico*. Nelle sezioni 3 e 4 se ne vedranno due esempi caratteristici. Per ora si prosegue supponendo unica la chiave, ma quanto si dirà vale anche per chiavi differenziate.

È necessario garantire che la chiave k sia nota solo ai partecipanti A e B, e che sia valida, cioè effettivamente legata alla coppia AB e non ad altri partecipanti. Insomma, si deve stabilire un legame sicuro tra chiave e identità del partecipante. È questo il problema di *distribuzione della chiave (key distribution)*. La soluzione generale è data dal *certificato (certificate)*: c'è una *terza parte fidata (trusted third party)*, intrinsecamente sicura, chiamata *autorità di certificazione* o CA (*Certification Authority*), che rilascia la chiave dietro richiesta del partecipante. La CA mantiene una base di dati dove registra i partecipanti afferenti e le rispettive chiavi. I partecipanti possono iscriversi alla CA, essere registrati e associati a una chiave, oppure ritirarsi (o essere espulsi) rilasciando la chiave.

Per esempio, il partecipante A richiede alla CA la chiave di A per la coppia AB, e la CA risponde inviando ad A un certificato (messaggio) contenente la chiave in questione; il partecipante B procede in modo simile. Naturalmente la CA deve essere un'entità la cui sicurezza è presupposta e indiscussa; spesso è un'autorità pubblica o legalmente riconosciuta. Il certificato deve essere autentico e integro, e pertanto molto spesso viene protetto con firma digitale, come spiegato prima. Si è riconosciuto che per ottenere la proprietà di confidenzialità (e di riflesso anche le altre) la funzione di cifratura deve possedere le due caratteristiche seguenti: *confusione* e *diffusione*. Confondere significa modificare le frequenze

relative dei simboli (caratteri, numeri, bit o blocchi) nel testo in chiaro in dipendenza dalla chiave, si vanificare la crittanalisi mediante frequency analysis. Diffondere significa permutare i simboli (come prima) secondo la chiave, si da cancellare le regolarità ripetitive eventualmente presenti nel testo in chiaro.

Numerosissimi algoritmi di cifratura, in particolare di tipo simmetrico, sono costruiti secondo una "ricetta" comune: suddividono il testo in blocchi di simboli, hanno struttura iterativa e il corpo del ciclo applica al blocco una successione, fissa o dipendente dall'iterazione, di trasformazioni costituite da sostituzioni e permutazioni di simboli pilotate dalla chiave, rispettivamente per confondere e diffondere il testo; in ingresso c'è il testo in chiaro e in uscita quello cifrato. Il crittosistema AES esposto nella sezione 3 ne è un'esemplificazione per così dire "da manuale". Nella crittografia odierna le trasformazioni applicate al testo sono quasi sempre di tipo matematico ben definito e sono generalmente formulate nell'ambito della teoria dei *campi* (o degli *anelli*) *finiti*, una branca dell'algebra. Il riquadro dà una sintesi di tale teoria.

Campo Finito [4]. Il *campo finito* o di *Galois*¹ (*finite* o *Galois field*) costituisce la *struttura algebrica* dove sono ambientati tutti o quasi i crittosistemi attuali. Un campo finito F è un *insieme finito* di elementi $a, b, c, \dots$, dotato di due *operazioni binarie* tra elementi: addizione $a + b$ e moltiplicazione $a \times b$, associative, commutative, dotate di elemento neutro e opposto o reciproco. Il campo finito può ridursi a un *anello finito*, cui manca solo la possibilità di definire il reciproco di ciascun elemento. Alcuni crittosistemi (come per esempio RSA) sono ambientati in anelli finiti.

¹ Dal nome dello scopritore, il matematico francese Evariste Galois.

Ci sono motivazioni precise che hanno contribuito a orientare la crittografia verso la matematica dei campi finiti. Ecco le due principali:

- L'insieme di elementi è finito ed essi sono pertanto rappresentabili in modo esatto.
- Le operazioni di addizione e moltiplicazione del campo modellano a grandi linee le trasformazioni di sostituzione e permutazione, e hanno dunque effetto confusivo e diffusivo.

Un esempio di campo è dato dagli interi con ad-

dizione e moltiplicazione modulo un numero primo $p > 1$. Per esempio, $2 + 4 \bmod 5 =$ resto di 6 rispetto a 5 = 1, e $2 \times 4 \bmod 5 =$ resto di 8 rispetto a 5 = 3. Esistono anche campi finiti i cui elementi sono polinomi. Insomma, il campo finito offre un ambiente matematico sistematico e ricco di proprietà utili dove costruire primitive crittografiche. Si può quantificare il *livello di sicurezza* (di confidenzialità ecc.) del crittosistema in tre categorie generali. Il parametro caratterizzante la dimensione del crittosistema è il numero di bit $n \geq 1$ necessari per codificare in binario la chiave (lunghezza di chiave). Ecco le tre categorie di livello:

- *assoluto*: non esiste in linea di principio nessun metodo di crittanalisi;

- *computazionale*: si dimostra matematicamente che l'algoritmo di crittanalisi computazionalmente più efficiente è NP-completo;

- *pratico*: l'algoritmo di crittanalisi computazionalmente più efficiente noto al momento ha costo economicamente non conveniente rispetto al valore dell'informazione in chiaro ottenibile. Il livello di sicurezza assoluto è conseguibile unicamente usando la chiave una volta sola per cifrare e sostituendola continuamente. Dato che non c'è riuso della chiave, la crittanalisi è impossibile in via teorica. I crittosistemi di questo tipo sono detti *usa-e-getta* (*one-pad*).

È molto arduo costruire un crittosistema collocato a livello di sicurezza computazionale, a causa della difficoltà matematica di dare una dimostrazione rigorosa di NP-completezza. Gli esempi noti di crittosistemi la cui analisi è stata dimostrata essere NP-completa sono pochi [1] e nessuno è di interesse commerciale rilevante. Di fatto quasi tutti i crittosistemi in uso commerciale si collocano a livello di sicurezza soltanto pratico.

Si conclude con un breve accenno alla crittanalisi. In generale essa ha lo scopo di trovare il testo in chiaro, partendo dal testo cifrato, senza conoscere la chiave. In pratica comunque mira quasi sempre a trovare proprio la chiave, perché una volta questa è nota qualunque esemplare di testo cifrato è decifrabile. Il metodo ingenuo e universale di crittanalisi è la *forza bruta*; la *frequency analysis* è un metodo meno generico ma pure universale², più o meno efficace. I metodi di crittanalisi *lineare* e *differenziale* sono molto generali e consistono nell'approssimare il crittosistema con funzioni lineari; sono tuttavia meto-

² Tranne che nel caso *usa-e-getta*.

di complessi, che richiedono parecchi aggiustamenti *ad hoc* dipendenti dal crittosistema in esame [7, 8]. Oltre a questi metodi in un certo senso universali, la crittanalisi si divide in famiglie particolari di cosiddetti *attacchi* (*attack*) mirati sul crittosistema specifico, i quali ne sfruttano le debolezze matematiche o i difetti di implementazione (in SW o in HW); gli attacchi saranno ripresi brevemente nelle conclusioni (sezione 5).

3. CRITTOSISTEMI SIMMETRICI

Un crittosistema mirato a garantire la confidenzialità dell'informazione è detto *simmetrico* o a *chiave segreta* se i due partecipanti A e B usano la stessa chiave k_s , detta appunto segreta (o privata); si rivedano la figura 2 e il modello (1).

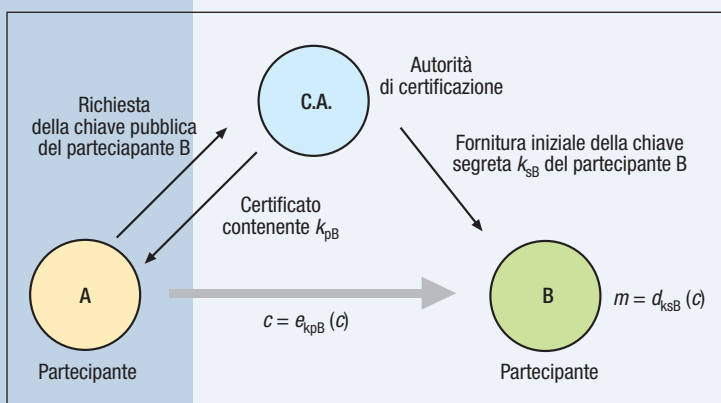


FIGURA 2

Modello di crittosistema asimmetrico (canale cifrato con chiave pubblica)

La chiave segreta k_{sAB} è dunque univoca per la coppia di partecipanti AB. Essa va calcolata inizialmente e deve essere conosciuta solo da parte di A e B; in generale può essere distribuita mediante certificazione.

Il primo crittosistema simmetrico standard di larga diffusione fu DES: ha testo in chiaro, cifrato e chiave segreta tutti di lunghezza 64 bit. Una variante, Triple-DES o 3DES, consiste nell'applicare in cascata tre cifrature DES con due chiavi differenti ed è talvolta ancora oggi utilizzata.

Il crittosistema standard oggi di maggiore diffusione è Rijndael (*Rijmen-Daemen* 2000) o AES (*Advanced Encryption Standard*) [5]. Lo standard AES è stato definito nel 2002 a séguito di un processo di selezione internazionale gestito dal NIST e durato due anni. Alla fine è stato scelto tra sei crittosistemi concorrenti e ha rapidamente rimpiazzato DES in numerose applicazioni. Ha la caratteristica importante di essere calcolabile in modo efficiente sia in software sia in hardware. Infatti lavora essenzialmente su byte, ed è efficiente anche se programmato su processori da 8 bit, di potenza limitata. È del tutto pubblico, molto studiato e ben documentato, e pertanto soddisfa al principio di Kerchoff. Per una breve presentazione del crittosistema [2, 5] si veda il riquadro.

Il crittosistema AES fornisce gli algoritmi di cifratura e decifrazione, e garantisce la proprietà

Crittosistema AES (o Rijndael) [2, 5]

Ambiente matematico: campo finito F_2^8 dei polinomi di grado max 8 (byte), a coeff. binari (0 e 1).

Testo in chiaro, cifrato e chiave segreta: stringhe m , c e k , ciascuna da 128 bit

Algoritmo di schedulazione della chiave (va effettuato *una-tantum*): pre-elabora la chiave segreta k (usando varie trasformazioni molto simili a quelle dell'algoritmo di cifratura), derivando da essa 10 chiavi di round k_r ($1 \leq r \leq 10$), ciascuna delle quali è una stringa di 128 bit.

Algoritmo di cifratura: suddividi il testo in chiaro m in 16 byte $m_{u,v}$, organizzati a matrice quadrata di tipo 4×4 ($1 \leq u, v \leq 4$), ed esegui il ciclo seguente (ciascuna iterazione si chiama "round")

for r **from** 1 **to** 10 **do**

- applica a ciascun byte $m_{u,v}$ la trasformazione (non-lineare) SubByte
- applica a ciascuna riga m_u della matrice la trasformazione (lineare) ShiftRow
- applica a ciascuna colonna m_v della matrice la trasformazione (lineare) MixColumn
- applica all'intero testo m la trasformazione (lineare) AddRoundKey(k_r)

end for

il testo finale elaborato dai 10 round del ciclo costituisce il testo cifrato c ; ciascuna delle quattro trasformazioni (o funzioni) interne al round SubByte, ShiftRow, MixColumn e AddRoundKey è biunivoca; per i particolari si veda per esempio, [5].

Algoritmo di decifrazione: il ciclo di cifratura, eseguito in ordine retroverso e con le trasformazioni SubByte, ShiftRow, MixColumn e AddRoundKey sostituite dalle rispettive inverse InvSubByte, InvShiftRow, InvMixColumn, InvAddRoundKey(k_{10-r}) (chiavi di round usate in ordine inverso).

di confidenzialità dell'informazione. Si colloca a livello di sicurezza pratico (non computazionale), poiché non è formalmente dimostrato che la crittanalisi di AES sia infattibile in tempo meno che esponenziale rispetto al numero di bit della chiave, benché di fatto oggi per infrangere AES non si sappia fare di meglio che esplorare l'intero spazio delle chiavi mediante forza bruta, ciò che implica circa $2^{128} \approx 10^{43}$ tentativi. Allo stato attuale la crittanalisi di AES è del tutto infattibile con i supercalcolatori più potenti disponibili.

Ci sono altri crittosistemi simmetrici concorrenti di AES, più o meno diffusi. Tra quelli più noti si trovano RC4 e RC5, molto semplici e talvolta usati per esempio in reti di sensori con potenza di calcolo limitatissima e alcuni altri, ma non molti.

4. CRITTOSISTEMI ASIMMETRICI

Una comunità di membri che usano a coppie un crittosistema simmetrico deve gestire in generale tante chiavi segrete quante sono le coppie possibili, e la distribuzione delle chiavi risulta pertanto onerosa e rischiosa. Un crittosistema mirante a garantire la confidenzialità dell'informazione è detto *asimmetrico* o a *chiave pubblica* se i due partecipanti A e B usano chiavi differenti; si veda la figura 1. Ecco (2) il modello espresso in simboli (questo particolare il modello (1)):

$$c = e_{k_s}(m) \quad e \quad m = d_{k_p}(c) \quad (2)$$

dove $m, c, k_s, k_p \in M, C, K_s, K_p$

Ciascun partecipante (qui A e B) è dotato di due chiavi: segreta k_s e pubblica k_p . Per cifrare il messaggio per B, A si serve della chiave pubblica di B, k_{pB} ; per decifrare B si serve della propria chiave segreta, k_{sB} ; lo stesso accade se B deve cifrare per A. La chiave pubblica di ciascun partecipante può essere resa nota a tutti gli altri partecipanti, mentre quella segreta è conosciuta solo dal partecipante cui si riferisce. Ne segue che la comunità di partecipanti usa molte meno chiavi che nel caso simmetrico.

Tuttavia, dato che deve valere l'identità $\forall m \in M : d_{k_p}[e_{k_s}(m)] = m$, le due chiavi di una coppia segreta-pubblica di un partecipante sono legate funzionalmente. Affinché il crittosistema sia sicuro deve essere computazionalmente infattibile trovare la chiave segreta cono-

scendo quella pubblica (poiché allora tutti potrebbero farlo e le chiavi segrete cesserebbero di essere tali!). Il proprietario della chiave segreta conosce dall'inizio la sua chiave e non ha mai bisogno di calcolarla.

Non esiste, o quanto meno oggi non si conosce, nessuna "ricetta" per definire crittosistemi asimmetrici. Di conseguenza ci sono a tutt'oggi ben pochi esempi di crittosistemi asimmetrici ed essi differiscono profondamente uno dall'altro.

Il crittosistema asimmetrico principale e più diffuso è RSA (*Rivest-Shamir-Adelman*), ideato nel 1977. Per una breve presentazione del crittosistema [2, 3] si veda il riquadro. Essenzialmente, RSA fornisce gli algoritmi di cifratura e decifrazione, e garantisce la proprietà di confidenzialità dell'informazione. Fornisce però anche l'algoritmo di firma digitale e garantisce le proprietà di autenticazione, integrità e non-ripudio. Si basa su un teorema di teoria dei numeri (si veda il riquadro); qui ci si

Crittosistema RSA [2]

Ambiente matematico: anello Z_n degli interi modulo $n > 1$, dove l'intero $n = pq$ (composto) è il prodotto di due fattori primi differenti $p, q > 1$ rappresentabili con circa il medesimo numero di bit.

Testo in chiaro e cifrato: numeri interi m e c ($0 \leq m, c < n$).

Fase di preparazione (va effettuata *una-tantum* per impostare il sistema):

- calcola la funzione di Eulero $\varphi(n) = (p-1)(q-1)$, dove $1 < \varphi(n) < n$
- scegli (a caso) un intero $a > 1$ [$e < \varphi(n)$] coprimo con $\varphi(n)$, cioè tale che il massimo comun divisore di a e $\varphi(n)$ sia 1, ovvero tale che $\text{m.c.d.}[a, \varphi(n)] = 1$
- calcola l'intero $b > 1$ reciproco di a modulo $\varphi(n)$, cioè tale che $ab = 1 \pmod{\varphi(n)}$ (b esiste ed è unico se e solo se $\text{m.c.d.}[a, \varphi(n)] = 1$, e si calcola facilmente)
- **chiave pubblica e segreta:** la coppia e la terna di interi $k_p = (a, n)$ e $k_s = (b, p, q)$

Algoritmo di cifratura: calcola l'esponentiale $c = m^a \pmod{n}$

Algoritmo di decifrazione: calcola l'esponentiale $m = c^b \pmod{n}$

Dimostrazione di correttezza del sistema: dato l'intero a e la condizione $\text{m.c.d.}[a, \varphi(n)] = 1$, vale il *teorema fondamentale* seguente:

$$\forall m \text{ si ha } [(m^a)^b] = [(m^b)^a] = m \pmod{n}$$

pertanto l'algoritmo di decifrazione è effettivamente l'inverso di quello di cifratura (e viceversa).

Valutazione del livello di sicurezza del sistema: per trovare l'intero b (segreto), indispensabile per decifrare, partendo dall'intero a (pubblico), bisogna conoscere $\varphi(n) = (p-1)(q-1)$, e dunque i fattori primi p e q di n ; però scomporre l'intero n in fattori primi ha complessità temporale esponenziale con l'algoritmo migliore noto (Crivello di Eratostene, con svariate ottimizzazioni); se ne conclude che il crittosistema RSA si colloca a *livello di sicurezza pratico* (non computazionale).

limita a enunciarlo, si vedano [2] o [3] per la dimostrazione.

RSA non si colloca a livello di sicurezza computazionale perché non esiste una dimostrazione formale che il problema della scomposizione in fattori primi sia NP-completo. In pratica oggi è possibile scomporre in fattori primi numeri rappresentabili con 600-700 bit, tramite mezzi di supercalcolo molto potenti. La lunghezza di chiave standard per RSA (il numero di bit per codificare n in binario) è fissata a 1024 bit, più che adeguata per applicazioni civili, e quella per applicazioni militari a 2048 bit, ben oltre ogni immaginabile possibilità di decifrazione.

Il crittosistema RSA è assai versatile e realizza facilmente la funzione di *firma digitale* (*digital signature*) per autenticazione, integrità e non-ripudio. Ecco come procedere a questo scopo.

□ Il partecipante A *firma* il testo m cifrandolo mediante la funzione $e_{k_{SA}}$ e la chiave segreta k_{SA} (non quella pubblica), cioè con l'esponente b (non a): la coppia (m, c) costituisce il *testo firmato* (m è il testo e c la firma).

□ Il partecipante B *verifica* la firma prendendo il testo firmato (m, c) , decifrando la firma c mediante la funzione $d_{k_{PA}}$ e la chiave pubblica k_{PA} (non quella privata), cioè con l'esponente a (non b), e confrontando il risultato della decifrazione con m (cioè con il testo in chiaro):

- se coincidono la firma c è valida e il testo m è autentico e integro;
- altrimenti non è valida e il testo m è da rifiutare in quanto falso o alterato.

Dato che la chiave segreta è in possesso solo del partecipante che firma il testo, questo non può misconoscere la firma in un secondo tempo. Pertanto anche la proprietà di *non-ripudio* del testo firmato è garantita. La funzione di firma digitale è ampiamente utilizzata per autenticare il certificato e garantirne l'integrità. L'insieme di regole standard che definiscono struttura, metodo di firma e modo di gestione del certificato è noto come *infrastruttura di chiave pubblica* o PKI (*Public Key Infrastructure*), ed è un componente molto importante dei sistemi crittografici applicativi.

5. CONCLUSIONI

Vale la pena di concludere illustrando le tendenze di ricerca attuali, di stampo scientifico

cioè mirate a scoperte nuove, e ingegneristico cioè mirate alla realizzazione. L'ideazione e messa punto di crittosistemi originali, simmetrici e asimmetrici, è un campo di ricerca scientifica sempre aperto, dove si mira a individuare nuovi crittosistemi con costo computazionale decrescente e livello di sicurezza crescente, senza però ampliare troppo lo spazio delle chiavi, anzi se possibile restringendolo. In questa direzione i crittosistemi asimmetrici *basati su curve ellittiche* [10, 11] sono di grande interesse perché ammettono numerose varianti algoritmiche, non tutte ancora identificate e ben studiate. La *crittografia quantistica* (*quantum cryptography*) è un approccio promettente [12] ma richiede a tutt'oggi sforzi di ricerca notevoli sia metodologici sia tecnologici. C'è infine una mole consistente di ricerca ingegneristica mirante a ottimizzare l'implementazione di crittosistemi già noti e in uso corrente, per evidenti ragioni di tipo applicativo e industriale.

In senso opposto, anche la crittanalisi è oggetto di ricerca, realizzativa e metodologica. Il primo approccio fa leva sull'aumento costante della potenza dei mezzi di supercalcolo. Invece i metodi universali di crittanalisi sono estremamente difficili da ottimizzare e i progressi in tale campo sono gradualmente e avvengono con una certa lentezza. Ben più fiorente, anzi oggi dominante, è lo studio dei metodi di *attacco*, cioè dei metodi di crittanalisi mirati sul crittosistema specifico. Qui l'interesse maggiore è diretto verso il campo vastissimo dei cosiddetti *attacchi collaterali* (*side-channel attack*), che sfruttano le debolezze dell'implementazione del crittosistema. In ambito industriale gli attacchi collaterali sono ben più temuti di ogni altra minaccia alla sicurezza di dispositivi elettronici.

Lo scopo dell'attacco collaterale è di raccogliere informazione rilasciata in modo inavvertito o imprevisto, sotto forma di grandezza misurabile o quantità valutabile, da parte del dispositivo crittografico, e di elaborarla successivamente per effettuare la crittanalisi e in definitiva trovare il testo in chiaro o meglio ancora la chiave. In ordine di tempo sono state scoperte tre famiglie principali di attacco di tipo collaterale, con numerose ramificazioni più o meno fini:

1. l'attacco *in tempo* (*timing attack*);

2. l'attacco in potenza (power attack);

3. l'attacco basato su induzione di guasto (fault-injection-based attack).

Nei primi due casi si misura una grandezza fisica: tempo di calcolo e potenza elettrica consumata o elettromagnetica irradiata, rispettivamente; nel terzo si valuta una quantità, ossia il risultato errato emesso in caso di guasto indotto intenzionalmente. Capita spesso che queste grandezze e quantità siano correlate in modo determinabile al testo in chiaro o alla chiave, e che pertanto rilevandole e poi analizzandole con metodi di carattere essenzialmente statistico, si possano inferire l'uno o l'altra. Per misurare con precisione il tempo di calcolo basta rilevare il segnale di clock del circuito, per la potenza consumata o irradiata basta ricorrere a oscilloscopio o altro strumento simile, e per indurre intenzionalmente un guasto (temporaneo) ben localizzato e sincronizzato si può ricorrere per esempio alla tecnologia laser (light-based fault attack).

Infine, giova ricordare che naturalmente si sviluppano in continuazione applicazioni dotate di funzionalità di sicurezza basata anche su crittografia, sia nel campo delle comunicazioni sia in quello delle basi di dati, e non di rado un'applicazione sicura tiene conto di entrambi gli aspetti.

Bibliografia

- [1] Simmons G.: *Contemporary Cryptology*. IEEE Press, 1992.
- [2] Menezes A., van Oorschot P.C., Vanstone S.: *Handbook of Applied Cryptography*. CRC Press, 1997.
- [3] Stinson D.: *Cryptography: Theory and Practice*. CRC Press, 1995.
- [4] Lidl R., Niederreiter H.: *Finite Fields*. 2ª edizione, Cambridge, University Press, 1997.
- [5] FIPS 197: *Announcing the Advanced Encryption Standard (AES)*. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>, 2001.
- [6] Singh S.: *Codici e Segreti*. Rizzoli, Milano, 1999.
- [7] Matsui M., *Linear Cryptanalysis Method for the DES Cipher*. Advances in Cryptology - EUROCRYPT '93, LCNS n. 765, Springer-Verlag, 1994, p. 386-397.
- [8] Biham E., Shamir A.: Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, Vol. 4, n. 1, 1991, p. 3-72.
- [9] Thomas S.: *SSL and TLS Essentials securing the Web*. New York, John Wiley & Son, 2000.
- [10] Menezes A.: *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.
- [11] Boneh D., Franklin M.: Identity Based Encryption from the Weil Pairing (IBE). *SIAM Journal of Computing*, Vol. 32, n. 3, 2003, p. 586-615.
- [12] Bennett C., Bessette F., Brassard G., Salvail L., Smolin J.: Experimental Quantum Cryptography. *Journal of Cryptology*, Vol. 5, n.1, 1992, p. 3-28.

Come detto nel riquadro iniziale, questa è l'ultima puntata di "Dentro la scatola".

Mondo Digitale coglie l'occasione per porgere un caldo "Grazie!" al prof. Fabio Schreiber che ha proposto la rubrica, ideato la sequenza degli articoli e seguito passo passo l'implementazione.

MARIAGIOVANNA SAMI è professore ordinario di prima fascia presso il Politecnico di Milano, nell'area dei Sistemi di Elaborazione. Dal 1987 al 1990 è stata Direttore del Dipartimento di Elettronica del Politecnico di Milano. È Direttore Scientifico del Master of Science in Embedded Systems Design presso l'Università della Svizzera Italiana a Lugano.

La sua attività di ricerca riguarda le architetture hardware dei sistemi digitali, con particolare riguardo alle metodologie di progetto di sistemi dedicati caratterizzati da elevate prestazioni, robustezza e basso consumo di potenza. È autrice o co-autrice di oltre duecento lavori scientifici in sede internazionale ed ha ricevuto alcuni premi per la sua attività di ricerca. È membro dell'Accademia Italiana delle Scienze (detta dei Quaranta).

E-mail: sami@elet.polimi.it

LUCA BREVEGLIERI, Nato nel 1962. Laureato in ingegneria elettronica nel 1986 e dottore di ricerca in ingegneria elettronica dell'informazione e dei sistemi nel 1991. Dal 1991 al 1998 è stato collaboratore tecnico (per la rete telematica) presso il Politecnico di Milano. Dal 1998 è professore associato di ingegneria informatica presso il Politecnico di Milano. Ha svolto attività di ricerca nel campo della progettazione digitale e delle architetture di elaborazione, in particolare per aritmetica del calcolatore ed elaborazione di segnale e immagine. I suoi interessi di ricerca attuali comprendono algoritmi e dispositivi per crittografia, e aspetti della teoria dei linguaggi formali.

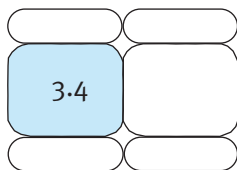
E-mail: luca.breveglieri@polimi.it



TECNOLOGIE WIRELESS PER LA LARGA BANDA

SCENARI EVOLUTIVI

Roberto Piermarini
Guido Vannucchi



L'offerta tecnologica di soluzioni per la larga banda "wireless" sta diventando sempre più ampia, con differenti soluzioni finalizzate all'offerta di connettività per qualsiasi tipo di applicazione in mobilità e obiettivi molto ambiziosi in termini di *bit-rate* (in *down* e *up-link*) e di efficienza spettrale. Nel presente articolo si offre un panorama su evoluzione e limiti di tali tecnologie contraddistinte anche dalla contrapposizione tra la "filiera 3GPP" che proviene dalla terza generazione di cellulari (UMTS) e la "filiera IEEE", derivata dalle *Wireless-LAN*, che porta avanti lo standard *WIMAX*.

1. PREMESSA

In questo articolo si desidera presentare un panorama dello sviluppo dei sistemi *wireless* verso la larga banda con qualche considerazione sulle problematiche connesse a tale sviluppo nel momento in cui i traguardi tecnologici si stanno ormai rapidamente approssimando al massimo sfruttamento della densità spettrale (limite di Shannon).

Il campo applicativo preso in considerazione non si limita alle sole tecnologie *wireless* nel senso stretto della parola, ma invade anche il campo della **convergenza fisso-mobile** e dei servizi puramente **diffusivi** per Mobile-TV. Questo dinamismo nel mercato per la larga banda *wireless*, è uno stimolo da un lato ad una sempre maggior (e forse eccessiva) concorrenza e dall'altra ad una continua accelerazione dei cicli di vita dei prodotti con le relative conseguenze non sempre positive.

Per aiutare il lettore interessato ad orientarsi in questa complessa materia - caratterizzata dall'impiego, anche nei prodotti di mercato, di un'eccessiva quantità di sigle tecniche di

cui spesso si ignora il significato - abbiamo ritenuto utile introdurre una **classificazione dei sistemi wireless** e tracciare un **profilo della loro evoluzione** storica e prevista. Ciò è utile da un lato per posizionare le tante sigle introdotte e dall'altro per cercare di individuare le ragioni della forte competizione creata tra le varie "filieri" in cui può essere allocata l'attuale offerta tecnologica.

Le ragioni che, in ogni caso, spingono al sempre maggior sviluppo della larga banda in mobilità sembrano potersi così riassumere:

- richiesta di ubiquità nell'accesso ai servizi a larga banda;
- stima che, almeno nel lungo termine, l'attuale utilizzo intensivo delle coppie in rame in tecnica ADSL sia destinato, con l'aumento di velocità, ad essere frenato da problematiche tecniche quali i problemi di diafonia tra coppie nel momento in cui l'impiego si estenderà a molti utilizzatori sullo stesso cavo;
- maggiore facilità a risolvere, con soluzioni *wireless*, i problemi di "Digital Divide";
- ampliamento del mercato a tutte le applicazioni "machine-to-machine".



Permangono tuttavia, nelle applicazioni in mobilità, problemi critici ai quali deve essere data una adeguata risposta, pena il successo sul mercato di tutte le nuove proposte. Possiamo citare, come sfide determinanti per il successo:

- l'importanza che il servizio in mobilità sia anch'esso del tipo "always on";
- la capacità di offerta di modelli tariffari adeguati a quelli delle reti fisse e di tipo flat anche se, nel caso del segmento mobile di accesso all'utente, occorre impiegare risorse condivise anziché dedicate (come è invece il caso delle reti cablate).

2. EVOLUZIONE DEI SISTEMI WIRELESS

Come già accennato, il **termine mobilità** (riquadro) è adottato in quest'articolo nel suo significato più generale e, corrispondentemente, le diverse famiglie (o filiere) indicate nello stesso riquadro coprono tutte le possibili applicazioni *wireless* (a parte la cortissima distanza).

Nell'ambito di questa classificazione, il presente paragrafo si propone di sintetizzare in modo semplice l'evoluzione storica e prospettica dei diversi apparati comparsi o che compariranno sul mercato, con particolare riferimento alle soluzioni tecnologiche che sono impiegate in Europa e in Italia.

Nei successivi due paragrafi si approfondiranno invece, con qualche maggiore dettaglio tecnico, le evoluzioni che si ritengono più importanti per la larga banda mobile del prossimo futuro, per poi passare ad accennare l'importantissima tematica dell'utilizzo dello spettro e concludere, nei due paragrafi finali, con una serie di considerazioni che coprono i vari tipi di problematiche.

2.1. La filiera 3GPP

Già dal 1982, si compiono in Europa i primi passi verso il primo sistema in tecnica digitale, denominato di "seconda generazione" (2G) per distinguerlo dai predecessori di tipo analogico come il TACS (*Total Access Communication System*). Nasce così lo standard europeo di grande successo denominato GSM (*Global System for Mobile communications*) che inizia ad essere operativo nel 1993. Il GSM è il primo sistema ad in-

stradamento (*roaming*) europeo, non clonabile, che consente comunicazioni crittografate e che permette uno sfruttamento dello spettro in modo significativamente più efficiente rispetto ai sistemi analogici. In Europa il GSM usa un totale di circa 120 MHz di banda, allocati in parte nella gamma del 900 MHz ed in parte in quella del 1800 MHz, in ambedue i casi con passo di canalizzazione di 200 kHz.

Uno dei componenti distintivi del GSM è la SIM (*Subscriber Identity Module*) ossia la scheda di memoria estraibile sulla quale sono memorizzati i dati dell'abbonato e che introduce un elevato standard di sicurezza nella gestione del servizio, sia per l'utente che per la rete.

IL TERMINE "MOBILITÀ" E LA CLASSIFICAZIONE DELLE "FILIERE" WIRELESS

Nel presente articolo si fa riferimento al termine "mobilità" in tutte le seguenti accezioni.

Accesso nomadico

Il terminale di utente, mentre è in funzione, viene considerato un terminale di accesso fisso e resta sempre associato alla stessa cella. In caso di spostamenti all'interno di una stessa cella la sessione non deve essere necessariamente ripristinata, ma la sua continuità non è comunque garantita.

Accesso "portable"

Il terminale di utente mantiene una sessione operativa mentre viene mosso all'interno della copertura di rete alla velocità tipica di una persona che si muove a piedi.

Accesso mobile

Il terminale di utente mantiene una sessione operativa (di norma con continuità di connessione) anche per applicazioni *real-time* e mentre ci si muove a velocità veicolare all'interno del raggio di copertura della rete. Le prestazioni di *hand-over* garantite tra celle differenti devono essere in grado di offrire continuità di servizio per tutte le applicazioni.

I sistemi *wireless* finora proposti possono classificarsi in **quattro grandi famiglie o "filiere"**:

A. Tecnologie cellulari di tipo radiomobile, nate per coperture geografiche estese, indicate come **"filiera 3GPP"** (*3rd Generation Partnership Project*). Questo gruppo include in particolare il sistema UMTS (*Universal Mobile Telephony System*) ormai in uso ed il sistema HSPA (*High Speed Packet Access*) che ne estende le funzionalità, ma anche da un lato il sistema capostipite iGSM e dall'altro il futuro sistema LTE (*Long Term Evolution*).

B. Tecnologie cellulari di tipo W-LAN (almeno storicamente parlando), originariamente concepite per realizzare LAN (*Local Area Network*) in tecnologia radio e che ora stanno evolvendo verso obiettivi di coperture più estese ed applicazioni *"full mobility"* del tutto equivalenti alla prima filiera. Tale famiglia di standard, spesso identificata come **"filiera IEEE"**, include, in particolare, Wi-Fi e WiMAX, in aggiunta ad altre varianti inizialmente proprietarie come il *Wi-Bro*.

C. Tecnologie satellitari, per accesso verso il singolo utente in modalità unicast.

D. Tecnologie diffusive multimediali per terminali mobili in modalità broadcast-multicast come il DVB-H (*Digital Video Broadcasting-Handheld*) e la famiglia DMB (*Digital Multimedia Broadcasting*). Appartiene a questa categoria anche il sistema MBMS (*Multimedia Broadcast Multicast Service*) che, di fatto, è una funzionalità dell'UMTS estesa a servizi di tipo diffusivo.

Con il GSM vengono anche introdotti i **primi servizi dati** e, in particolare, il servizio SMS (*Short Message Service*) che ottiene un successo superiore ad ogni aspettativa.

Con la versione denominata 2.5 G (*Seconda Generazione e mezzo*) viene introdotto il servizio GPRS (*General Packet Radio Service*), caratterizzato per i servizi dati dall'adozione della trasmissione a pacchetto (con un valore massimo di velocità dell'ordine dei 30-40 kbit/s per utente). Tale prestazione consente per la prima volta l'impiego del cellulare come "*wireless modem*" per navigare in Internet e accedere, utilizzando il protocollo di navigazione WAP (*Wireless Access Protocol*), ai siti Web direttamente dal telefono mobile.

La tecnica di accesso normalmente adottata per la famiglia GSM è il TDMA (*Time Division Multiplex Access*) in cui un canale radio, con spaziatura di 200 kHz, può essere assegnato a divisione di tempo ad un massimo di 8 utenti (nel caso del cosiddetto "*full-rate*" di compressione della voce).

Per la voce (campionata a 8 kHz con 13 bit) viene impiegata una codifica di compressione che porta la *bit-rate* a 12.5 kbit/s (**full-rate**), portata successivamente a 5,6 kbit/s (**half-rate**) con possibilità di coesistenza con la precedente. Nel 1998 è stata introdotta una più efficace tecnica di compressione denominata AMR (*Adaptive Multi-Rate*), oggi largamente impiegata, la quale adatta la velocità di trasmissione alle caratteristiche del canale.

Il multiplo delle conversazioni telefoniche impiega per la trasmissione una particolare modulazione di fase (GMSK) della portante studiata per ottimizzare l'occupazione spettrale.

Per quanto riguarda i **dati trasmessi a pacchetto**, il GSM sfrutta un singolo *time-slot* di un canale radio con *bit-rate* di 8, 12, 14.4, 20 kbit/s, a seconda di quattro possibili livelli di protezione di errore adottati. Più *time-slot* possono essere concatenati per realizzare un canale dati condiviso dagli utenti. Oggi le reti e i terminali consentono di aggregare fino a quattro *time-slot* che, a seconda delle codifiche impiegate, raggiungono valori di *bit-rate* che variano tra i 32 e gli 80 kbit/s. Le situazioni interferenziali di rete riducono normalmente questo valore attorno ai 40 kbit/s.

L'evoluzione più spinta della tecnologia 2.5 G è denominata EDGE (*Enhanced Data rates for GSM Evolution*) e consiste in un'evoluzione del GPRS. Questa è ottenuta attraverso la possibilità di utilizzare in modo adattativo la modulazione 8PSK (che porta il valore di *bit-rate* di picco teorico da 20 kbit/s a 60 kbit/s per *time-slot*) e nuovi schemi di codifica. In aggiunta sono presenti alcune ottimizzazioni nei protocolli orientate ad aumentare la rapidità di adattamento al canale e uno schema per la ritrasmissione dei pacchetti errati.

Negli anni '90 si comincia a pensare ad una **terza generazione (3G)** di sistemi cellulari puntando a sfruttare anche le bande attorno ai **2 GHz**.

L'ITU (*International Telecommunication Union*) si fa promotore di una famiglia di nuovi standard per la mobilità, denominati IMT-2000 (*International Mobile Telephony 2000*), essenzialmente centrati sull'impiego di tecniche di accesso multiplo di tipo CDMA (*Code Division Multiple Access*), ritenute più efficienti nello sfruttamento delle risorse radio. L'Europa sceglie, tra i sistemi della famiglia IMT-2000, lo standard UMTS (*Universal Mobile Telecommunication System*).

Nella tecnica a dispersione di spettro (*spread spectrum*) CDMA, ogni singolo utente occupa l'intera banda disponibile e tutte le sessioni di comunicazione sono sovrapposte tra loro nell'ambito dello spettro di canalizzazione adottato (5 MHz nel nostro caso in duplex per andata e ritorno). La demodulazione avviene attraverso tecniche di correlazione che sfruttano un particolare "codice" identificativo associato a ciascuna di esse.

In particolare, il sistema UMTS si identifica con l'adozione della tecnica di accesso radio W-CDMA (*Wideband Code Division Multiple Access*), sviluppata dai giapponesi della NTT e proposta all'ITU per ottenere maggiori prestazioni di velocità rispetto ai sistemi CDMA già esistenti. Essa prevede, tra le altre cose, un controllo di potenza adattativo sulla base del rapporto tra segnale utile e interferente. Con l'UMTS, la capacità teorica massima per i **dati** messa a disposizione di un singolo utente risulta pari a **384 kbit/s**, ossia significativamente maggiore di quella ottenibile con il GSM e le sue evoluzioni GPRS ed EDGE. Se si utilizza una configurazione che dedica tutta



la banda disponibile del sistema alle comunicazioni a pacchetto il **“troughput” per un’intera cella**, sui 5 MHz disponibili, risulta pari a 2 Mbit/s da suddividere tra i diversi utenti attivi nella cella.

L’UMTS, però, è solo la prima tappa della **roadmap 3G**.

Con il nuovo sistema HSPA (*High Speed Packet Access*), sempre con tecnica d’accesso W-CDMA, ma con modulazione della portante a 16 livelli, il *bit-rate* erogato aumenta ulteriormente (si è raggiunto il valore di 3.6 Mbit/s per cella già alla fine del 2006), con l’obiettivo di raggiungere una **velocità massima teorica** (denominata anche di **picco**) pari a 14.4 Mbit/s in *down-link* e di 5.8 Mbit/s in *up-link*, senza che per il singolo utente vi siano, almeno in linea di principio, limitazioni rispetto all’impiego pieno dell’intera capacità della cella qualora egli fosse l’unico utilizzatore.

Per questa tecnologia si adottano i termini **HSDPA** per il tratto in *down-link* ed **HSUPA** per quello in *up-link*.

Una tappa ulteriore del 3G è costituita dal cosiddetto HSPA evoluto, o **HSPA+** che, impiegando la modulazione a 64 QAM in luogo del 16 QAM, porta la capacità del sistema in *down-link* a 21,6 Mbit/s (6/4 di 14,4). Questa *bit-rate* può essere ulteriormente incrementata con l’adozione di sistemi di *diversity* di spazio in trasmissione e ricezione.

L’ulteriore traguardo tecnologico viene oggi indicata con la denominazione LTE (*Long Term Evolution*) e, attraverso l’impiego della stesso tipo di modulazione OFDM (*Orthogonal Frequency-Division Multiplexing*) adottato per il WIMAX, rappresenta una risposta dell’industria della filiera 3GPP a quella della filiera IEEE cui si accenna nel punto successivo.

2.2. La filiera IEEE

I primi sistemi commerciali di tipo *Wireless LAN*, ossia per **“Local Area Network”**, hanno fatto la loro comparsa già all’inizio degli anni ‘90. L’IEEE (*Institute of Electrical and Electronics Engineers*), organo primario di standardizzazione delle reti LAN, iniziò in tale periodo un progetto di standardizzazione in tecnologia *wireless*. La fase di progettazione si è conclusa nel 1997, con il pri-

mo standard per W-LAN (*Wireless LAN*), denominato **IEEE 802.11** operante nella banda del 2.4 GHz, gamma di frequenza non licenziata e pertanto condivisa tra i vari utilizzatori.

Nel 1999, l’IEEE modifica e potenzia lo standard, risolvendo i vari problemi di mancanza di interoperabilità e di capacità troppo limitata. Si dà così vita ad un’evoluzione che viene denominata *802.11b*, più nota con l’acronimo Wi-Fi (*Wireless Fidelity*). Il sistema impiega una modulazione a spettro espanso DSSS (*Direct Sequence Spread Spectrum*) e fornisce connettività con un massimo teorico di velocità pari a 11 Mbit/s. Per il protocollo impiegato, il sistema prende anche il nome di **“Wireless Ethernet”**, per sottolineare l’impiego di base come tecnologia di *cable replacement*.

Un ulteriore standard denominato IEEE *802.11a*, cerca di mantenere il passo con le LAN cablate. In particolare, l’impiego della modulazione OFDM consente a questo standard di raggiungere una velocità pari a 54 Mbit/s e la frequenza di lavoro viene spostata nella gamma del 5 GHz.

Le pressioni per l’impiego della banda del 2.4 GHz spingono nel 2000 all’uscita dell’ulteriore standard IEEE *802.11g* (combinazione dell’*802.11b* e del *802.11a*). Si tratta dell’evoluzione del Wi-Fi verso la tecnologia OFDM che porta a raggiungere una capacità di 54 Mbit/s (ed arriva fino a 108 Mbit/s adottando le tecnologie proprietarie di vari costruttori). In Italia esistono 2500 *hotspot* pubblici in grado di fornire accessi Wi-Fi, tecnologia che si è rapidamente diffusa con grande successo, anche se l’applicazione rimane confinata al caso nomadico e con coperture per lo più limitate all’interno di edifici pubblici.

Si pone a questo punto, in ambito IEEE, il problema di ottenere coperture geografiche maggiori e gli studi si spostano dalle reti LAN alle reti MAN (*Metropolitan Area Network*), ossia con più ampia copertura geografica. In tal modo l’IEEE tende ad entrare progressivamente in concorrenza con il 3GPP, cui sopra si è già accennato, ed i rispettivi campi di applicazione iniziano così a confondersi.

Il sistema per quest’obiettivo si chiama WIMAX (*Worldwide Interoperability for Microwave Access*), termine che sta ad indicare il marchio di

interoperabilità per la nuova famiglia di standard **IEEE 802.16**, nata nel 2001.

Il WIMAX nasce con requisiti di coperture *wireless* estese al cosiddetto "ultimo miglio", ponendosi obiettivi di qualità del servizio (QoS) e di gestione della sicurezza, anche se è importante ricordare che sia Wi-Fi che WIMAX non comprendono specifiche per l'intero collegamento *end-to-end*, come per i sistemi cellulari 3GPP, ma si concentrano esclusivamente sulla tratta di accesso radio. Per superare questa limitazione, il WIMAX Forum, organizzazione di operatori e produttori a sostegno del WIMAX, sta cercando di integrare il lavoro dell'IEEE con attività che rendono il sistema realmente implementabile e che prevedono anche lo studio di architetture *end-to-end*. Attività fondamentale del WIMAX Forum, è la definizione e certificazione dei vari profili, ognuno afferente ad una specifica banda e tecnica di *duplexing*.

Le maggiori ambizioni del sistema consigliano l'adozione di **frequenze di tipo "licenziato"** (paragrafo 5) che assicurano maggiori garanzie da interferenze. I costi più alti di aggiudicazione per porzioni di spettro licenziato sono normalmente bilanciati dalle migliori garanzie di controllo sull'uso dello spettro assegnato, anche se l'iter temporale di assegnazione può risultare, come spesso capita in Italia, significativamente più lungo.

Oggi si parla di due versioni fondamentali di WIMAX: la "**IEEE 802.16d**" (chiamata anche **versione 2004**) studiata per offrire servizi a larga banda per apparati fissi o nomadici e la "**IEEE 802.16e**" (indicata come **versione 2005**) che consente la piena mobilità dei terminali d'utente. I due standard non sono compatibili tra loro.

Le due versioni sono caratterizzate da diversi profili nelle **gamme di frequenze** 2.3, 2.5, 3.5, 3.7 e 5.8 GHz con larghezza dei **canali radio** flessibile da 1.25 MHz a 20 MHz.

La realtà europea del WIMAX-2004 vede inizialmente una prevalenza dei profili nella banda 3.5 GHz con canali da 3.5, 5, 7, 10 MHz e con una possibile estensione nel medio periodo alla banda 2.5 GHz (come già possibile in alcuni paesi europei). Per quanto invece riguarda i canali radio, la loro flessibilità è un obiettivo molto interessante. Pertanto, an-

che la filiera degli standard 3GPP che, come già detto, utilizza attualmente canali radio con banda fissa da 5 MHz, sta lavorando con l'obiettivo preciso di raggiungere, per il futuro sistema LTE, un'analogia flessibilità nell'uso dello spettro radio.

Come modulazione il WIMAX ha sposato la tecnologia della **modulazione OFDM** (sia per *down-link* che *up-link*) affermatasi ormai in svariati campi applicativi perchè gode (a meno di vincoli specifici da rispettare) di prestazioni superiori agli altri tipi di modulazioni. Per la versione 2004 con canalizzazione a 10 MHz, tale modulazione consente di raggiungere una **bit-rate** di picco per cella di **33 Mbit/s in down-link** e di **4 Mbit/s in up-link**. Su questa scia anche per il sistema LTE della famiglia 3GPP è stato deciso di abbandonare la modulazione W-CDMA per sposare la scelta OFDM per il *down-link*.

Si rimanda al successivo paragrafo 3 per maggiori dettagli sul cammino e sulle scelte tecnologiche operate dai due sistemi avanzati LTE e WIMAX-2005 che rappresentano, come caratteristiche e filosofia, i sistemi di riferimento del futuro e che, probabilmente, potrebbero tendere a convergere in un sistema unico.

2.3. La filiera satellitare "unicast"

I servizi satellitari per applicazioni commerciali sono complessivamente identificati come **MSS (Mobile Satellite Services)**.

Come è noto, i consorzi *Iridium* e *Globalstar* (che lavorano con satelliti in orbite basse) non hanno portato i ritorni di mercato sperati, nonostante il fatto che dal punto di vista tecnologico si siano compiuti grandi passi avanti ed hanno lasciato una certa diffidenza in investimenti nell'area mobile satellitare.

Immarsat ha lanciato la cosiddetta **B-GAN (Broadband Global Area Network)** in grado di offrire *bit-rate* fino a 492 kbit/s in terminali portatili ovunque sulla terraferma e sui mari, in particolare per situazioni di emergenza, in aree colpite da disastri o conflitti.

In definitiva il satellite, nella generazione 2G, ha avuto un ruolo nell'estensione geografica e complementarità dei servizi, ma non è riuscito a conquistare una porzione significativa del mercato di massa.

Per applicazioni satellitari puramente diffusi-

ve del tipo *multicasting* il ruolo che potrà giocare sembra però assai maggiore.

2.4. La filiera diffusiva multicast

Con la diffusione dei servizi di **Mobile-TV** si sta dando particolare attenzione a tutte le possibili soluzioni che permettano di estendere l'area di copertura e di interesse per tali servizi. Non vi è dubbio che tali sistemi rientrano nel quadro complessivo della multimedialità *wireless*, pur rappresentando un campo particolare. Per tale ragione non si entrerà in eccessivi dettagli che esulano dalle finalità.

In particolare come sistemi terrestri vanno ricordati: il **DVB-H** (**Digital Video Broadcasting-Handheld**) ed il **T-DMB** (**Terrestrial-Digital Multimedia Broadcasting**). Il primo nasce come *fall-out* della televisione digitale terrestre DVB-T e viene visto con particolare favore dai gestori di *broadcasting* televisivo, consentendo nell'ambito del Multiplex di trasporto, la trasmissione di 10-20 programmi del nuovo servizio in luogo di un programma televisivo normale. Il secondo è un'estensione multimediale, e perciò anche per Mobile-TV, del più noto sistema DAB per la trasmissione di segnali audio digitali.

Nell'ambito della filiera diffusiva va ricordato il sistema **MBMS** (**Multimedia Broadcast Multicast Service**) che deve considerarsi la risposta del 3GPP alle forme diffuse precedentemente citate. Il sistema può considerarsi una versione con protocollo *multicast* dell'HSPA che prevede il trasporto su canali radio comuni a tutti gli utenti, di servizi di tipo punto-multipunto anziché di servizi punto-punto (*unicast*) e verrà implementato nell'*up-grading* previsto delle reti 3GPP per introdurre HSPA. Attualmente, le limitate risorse in frequenza rendono questa prestazione scarsamente appetibile se si desidera trasmettere agli utenti un numero significativo di programmi di Mobile-TV tra i quali operare la scelta desiderata. Sono tuttavia previste evoluzioni di MBMS (*Release 7* ed *8*) che potranno porre tale tecnologia in diretta concorrenza con le altre tecnologie diffuse anche in termini di capacità.

Per applicazioni di Mobile-TV, un particolare interesse stanno invece assumendo nuovi sistemi satellitari o, per essere più esatti, **si-**

stemi misti satellitari-terrestri che operano nella stessa gamma di frequenze.

3. L'EVOLUZIONE CONVERGENTE DEI SISTEMI WIRELESS VERSO LA LARGHISSIMA BANDA

Data l'importanza che tali sistemi avranno in futuro, è opportuno approfondire qualche aspetto tecnologico dei futuri sistemi LTE e WIMAX-2005.

3.1. Evoluzione dell'UMTS verso LTE

I sistemi UMTS sono stati migliorati per incrementare il *data-rate* sia nella tratta *down-link* che in quella *up-link*. Le denominazioni **HSDPA** (**High Speed Down-link Packet Access**) e **HSUPA** (**High Speed Up-link Packet Access**), nate separatamente per indicare il miglioramento ottenuto nel funzionamento nelle rispettive tratte, sono oggi riunite, come già detto sopra, nell'acronimo unificato HSPA.

Per quanto riguarda la **tratta di andata**, ossia di *down-link*, il concetto base di HSDPA consiste nel migliorare il *throughput* medio nella cella agendo essenzialmente su due fronti: massimizzando le prestazioni a livello di singolo *link* (con uno schema di modulazione più efficiente e l'adozione di più codici in parallelo) e adottando, a livello di rete, la "**User Diversity**". Questa si concretizza in schemi di modulazione e codifica adattativi e in uno *scheduling* dinamico delle risorse da assegnare ai singoli utenti. Queste tecniche consentono sostanzialmente di ottimizzare in modo estremamente dinamico (con una scala temporale di 2 ms) l'allocazione delle risorse ai diversi utenti. Ciò consente di evitare, ad esempio, di assegnare modulazione e codifica inutilmente robuste (che determinano un basso *bit-rate*) ad un utente che, in un determinato momento, si trova in condizioni propagative particolarmente favorevoli.

Oltre a queste tecniche, vanno sottolineate l'ottimizzazione di alcuni protocolli e lo spostamento di alcune funzionalità nella stazione radio base per ridurre i tempi di risposta. Questo vale in particolare per il meccanismo di ritrasmissione dei blocchi ricevuti errati il cui algoritmo, inoltre, è stato sensibilmente ottimizzato. Per l'accesso alle risorse viene inviata a ogni terminale, da parte della sta-

zione radio base, l'informazione su quando porsi in ascolto sul canale condiviso e su quali, dei codici possibili (fino a 15 assegnati in parallelo ad un singolo utente), viaggia l'informazione a lui destinata. Le caratteristiche trasmissive del canale condiviso, in termini di livello di protezione delle codifiche e schema di modulazione, possono variare ogni 2 ms.

Le modulazioni utilizzate in *down-link* per la portante radio, nell'ambito delle evoluzioni della famiglia HSPA, sono il QPSK, il 16 QAM ed il 64 QAM.

Per quanto riguarda la **tratta di ritorno**, ossia di *up-link*, la necessità di contenere la potenza trasmessa dal terminale non consente di replicare il meccanismo visto in precedenza, anche se i concetti adottati per massimizzare il *throughput* sono sostanzialmente gli stessi. In questo caso si opera su un canale dedicato caratterizzato da una veloce assegnazione adattativa dei parametri trasmissivi (*Fast Link Adaptation*).

Per massimizzare il *bit-rate* a livello di *link* è stata introdotta la possibilità di utilizzare un codice con fattore di *spreading* più basso (richiede più potenza ma trasporta più informazione) e ciascun utente può utilizzare fino a 4 codici in parallelo. Per i miglioramenti a livello di rete si adotta la *user diversity* attraverso codifica e *scheduling* dinamici. In questo caso si opera con canale dedicato e lo *scheduling* viene effettuato stabilendo dinamicamente potenza e codifica che dovranno utilizzare i singoli terminali in modo da sfruttare nel modo più efficiente possibile il *Noise Rise Budget* (ossia il residuo incremento possibile di potenza di rumore complessivo in aria). Il tipo di modulazione adottato in *up-link* è il QPSK per contenere la potenza di uscita del cellulare.

Nella tabella 1 sono riportate le informazioni di base per l'HSPA come definito dal 3GPP.

L'ulteriore evoluzione dell'HSPA assume il nome di **HSPA+** e fa riferimento all'applicazione di tecniche di **diversity di spazio** per le

Release 3 GPP		Release 99/ Release 4	Release 5	Release 6	Release 7		
Principali innovazioni introdotte		W-CDMA	HSDPA	HSPA	HSPA+		
Tratta in Down Link	Modulazioni disponibili	QPSK	QPSK/16QAM	QPSK/16QAM	QPSK 16QAM 64QAM		
	Intervallo di trasmissione	10 ms	2 ms	2 ms	2 ms		
	Nuovi codici	-	15	15	15		
	MIMO	-	-	-	si (da 2 a 4 antenne)		
Tratta in Up Link	Modulazione	QPSK	QPSK	QPSK	QPSK 16QAM		
	Intervallo di trasmissione	10 ms	10 ms	2 ms	2 ms		
	Nuovi codici	-	-	4	4		
	MIMO	-	-	-	si (da 2 a 4 antenne)		
Velocità di picco in DL (Mbit/s su 5MHz)		0,384	14,4	14,4	21	28	42
					64 QAM	MMO 2x 16 QAM	MMO2x 64 QAM
Velocità di picco in UL (Mbit/s su 5MHz)		0,384	0,384	5,8	12		
Latenza (ms) Ping su 32 byte		120	65	65	<65		

TABELLA 1

Parametri generali della famiglia 3GPP



antenne denominate **MIMO (Multiple Input Multiple Output)** e di impiego di modulazioni a numero di livelli più elevato: 64 livelli anziché 16 in *down-link*, 4 livelli in *up-link* (un ramo di una modulazione 16 QAM). È prevista anche una semplificazione architetturale dell'UMTS per quanto riguarda la rete di accesso, legata all'esigenza di gestire le maggiori velocità con costi di rete contenuti.

Gli obiettivi principali dell'HSPA+ sono i seguenti:

- sostituire completamente la commutazione a circuito con quella a pacchetto anche per la voce;
 - portare al massimo potenziale il sistema UMTS con modulazione W-CDMA, prima di passare al futuro sistema LTE basato sulla modulazione OFDM;
 - predisporre la rete per consentire la coesistenza tra l'evoluzione HSPA+ con W-CDMA ed il futuro sistema LTE; il tutto mantenendo la compatibilità con i sistemi già operanti.
- Per quanto riguarda i sistemi HSPA ed HSPA+ è molto importante sottolineare che essi possono essere **introdotti come aggiornamenti software** e, in entità abbastanza contenuta, **hardware** delle reti UMTS esistenti, conservando in tal modo la compatibilità col passato. Questo è un aspetto assai importante perché tale politica consente un **notevole risparmio dei costi di rete** rispetto ad una soluzione completamente nuova.

A partire da Novembre 2004, il 3GPP ha avviato gli studi per un'ulteriore evoluzione della tecnologia d'accesso radio in grado di fornire un'alta velocità di trasmissione, ottimizzata per l'accesso a pacchetto e con bassi tempi di latenza. Questa iniziativa in ambito 3GPP ha preso il nome di **LTE (Long Term Evolution)** da cui l'acronimo associato a questo nuovo sistema. Tra le caratteristiche più significative il sistema deve garantire la coesistenza con gli standard GSM/GPRS e UMTS e deve fornire un bit-rate di picco di **100 Mbit/s in down-link e 50 Mbit/s in up-link per cella** nella banda di 20 MHz.

La tecnica di accesso radio cambia drasticamente passando dal W-CDMA sulla banda dei 5 MHz alla tecnica OFDMA in *down-link* e SC-FDMA in *up-link* con canalizzazione non più fissa ma flessibile (1.25, 2, 5.5, 10, 15, 20 MHz). La spaziatura tra le sottopor-

tanti OFDM è mantenuta costante a 15 kHz nell'ambito delle diverse canalizzazioni sopra citate. Le modulazioni utilizzabili per ciascuna sottoportante sono il QPSK, il 16 QAM ed il 64 QAM in *down-link* mentre per l'*up-link* è adottato il QPSK ed il 16 QAM.

È previsto l'uso di tecniche di diversity di spazio MIMO con l'impiego di un numero di antenne che va da due a quattro.

Si prevede la commercializzazione del sistema attorno al 2010.

3.2. Evoluzioni verso il WIMAX-2005

Come già accennato, il **WIMAX-2004** ha adottato la modulazione OFDM per la trasmissione punto-punto per le due tratte e l'accesso di tipo OFDMA per gestire gli accessi multipli.

Nel **WIMAX-2005** il passo delle sottoportanti del sistema OFDM è stato fissato in 10,94 kHz (SOFDMA: *Scalable OFDMA*). Sembra che, per non ridurre le dimensioni della cella, sia in revisione l'adozione dell'OFDM in *up-link* con tendenza a portarsi su modulazioni più semplici (tipo SC-FDMA).

La profonda diversità delle interfacce radio rende i due standard 2004 e 2005 non interoperabili e perciò incompatibili tra di loro.

I sistemi LTE e WIMAX-2005 prevedono sia la modalità **FDD (Frequency Division Duplex)** che quella **TDD (Time Division Duplex)**.

Con la tecnica FDD, invece, le due portanti *up* e *down* sono separate in frequenza ed opportunamente distanziate di una banda di guardia prefissata. Tale tecnica si basa, per sua natura, su apparati che devono ricevere e trasmettere simultaneamente richiedendo, pertanto, la presenza di filtri che possano disaccoppiare le due semigamme.

La modalità TDD prevede di impiegare le due tratte sulla stessa portante, ma in *timeslot* differenti. Con la tecnica TDD, d'altro canto, può essere necessario sincronizzare tutte le stazioni base appartenenti ad una rete omogenea attraverso, ad esempio, l'impiego di ricevitori satellitari GPS. La tecnica TDD consente di realizzare ricevitori più economici (non devono trasmettere e ricevere simultaneamente) ed è in grado di gestire in modo flessibile ed ottimale il rapporto tra i *bit-rate* di *down-link* e di *up-link* (variando il rapporto tra i tempi di trasmissione nei due versi) consentendo l'utilizzo di porzioni di spettro non

accoppiate. Per contro presenta delle forti criticità dal punto di vista interferenziale (due terminali vicini connessi a reti diverse potrebbero trovarsi uno a trasmettere l'altro a ricevere su canali adiacenti).

IEEE ha proposto di includere la sola TDD nella versione 2005, mentre FDD è la tecnica prevalente nelle implementazioni dello standard 2004.

Anche nei sistemi WIMAX è previsto l'impiego di tecnologie avanzate di antenna quali l'**AAS (Adaptive Antenna System)**, in grado di indirizzare il fascio di irradiazione per consentire di inseguire un terminale in movimento massimizzando la potenza trasmessa nella sua direzione. Inoltre, in alternativa od in aggiunta, è previsto l'uso del sistema MIMO già menzionato per incrementare il *bit-rate* fornito a parità di qualità od aumentare l'area di servizio a parità di *bit-rate*.

Per la versione WIMAX-2005 con **canalizzazione a 10 MHz**, per esempio, nel caso di un rapporto temporale 3:1 tra le due direzioni ed utilizzando il MIMO a due antenne trasmettenti e due riceventi, la velocità massima in **down-link è di 46 Mbit/s**, mentre in **up-link è pari a 4 Mbit/s**.

Nel prossimo futuro si prevede che le velocità in *down-link* possa raggiungere i 50-70 Mbit/s con l'introduzione di più portanti per ogni settore, congiuntamente all'utilizzo di tecniche AAS e MIMO di tipo avanzato.

La portata delle **coperture radio** dipende molto dalla banda di frequenza, ma è possibile comunque poter coprire distanze **fino a 10 km in zone rurali**, non densamente popolate. In ambienti urbani e in condizioni di mobilità, distanze e capacità si riducono, analogamente a quanto succede per gli altri sistemi radio mobili.

Uno dei primi **prodotti commerciali** ispirato allo standard del WIMAX per la mobilità è il **WiBro**, lanciato in Corea ed in alcuni altri paesi orientali. Il WiBro, basato sul TDD e funzionante nella gamma dei 2.3 GHz, è nato da "un salto in avanti" rispetto allo standard IEEE ed è recentemente confluito, dopo opportune modifiche ed estensioni, nello standard WIMAX-2005.

Fatta eccezione per il servizio avviato in Corea con il WiBro, al momento ci sono in esercizio commerciale solo sistemi WIMAX-2004, men-

tre si prevede il lancio commerciale della versione 2005 nella seconda metà del 2007 attraverso diversi piani di realizzazione di cui il più noto è quello annunciato nell'estate del 2006 da *Sprint Nextel*, che prevede il collegamento con WIMAX mobile di decine di milioni di utenti entro la fine del 2009 nella banda 2.5 GHz.

3.3. Alcune considerazioni su velocità di picco e "throughput" di utente nei sistemi wireless

In precedenza si è sempre parlato di *bit-rate* o velocità di picco per cella. Per le reti *wireless* a larga banda, è opportuno chiarire alcuni concetti di base per una corretta comprensione della differenza tra le velocità massime teoriche (picco) raggiungibili e quelle effettivamente disponibili ai clienti (*throughput*).

Nel caso di comunicazioni a pacchetto, a differenza delle comunicazioni a circuito utilizzate per la voce, i dati trasmessi devono essere consegnati con un tasso di errore trascurabile o nullo. Questo significa che sono necessari dei meccanismi di ritrasmissione dei pacchetti errati (protocolli ARQ) che, di fatto, riducono la capacità trasmissiva a disposizione dell'applicativo che sta usando quel canale radio.

Il degrado introdotto dal canale radio è quindi visto in termini di riduzione del *throughput* rispetto alla velocità di picco e come variazione del tempo di latenza per effetto del *jitter* introdotto.

I fattori che influenzano la diminuzione della velocità di picco sono legati ad una molteplicità di fattori quali la qualità della copertura radio, il carico di traffico della cella, l'eventuale strozzatura del collegamento dalla stazione radio-base alle infrastrutture dell'operatore, il dimensionamento insufficiente del *core* della rete con conseguente congestione.

Non è quindi semplice dare una risposta alla domanda su quale può essere il vero *throughput* di utente.

A titolo di esempio si può ricordare che Il Consorzio 3G-Americas ha fatto recentemente alcune campagne di misure su una rete UMTS dove è attivo l'HSDPA assieme alle tradizionali comunicazioni a circuito ed a pacchetto della rete UMTS standard. L'HSDPA considerato è la versione commercia-

le che presenta attualmente una velocità di picco per cella di 3,6 Mbit/s. I test si riferiscono ad un terminale in grado di gestire una velocità di picco di 1,8 Mbit/s con il quale si richiede la consegna di un file con il protocollo FTP (*File Transfer Protocol*). Nel caso di rete scarica e con buone condizioni radio con terminale non in movimento, il valore mediano del *throughput* (a livello applicativo) è risultato di circa l'80% la capacità del terminale. Con rete in condizioni degradate per quello che riguarda la propagazione e con terminale non in movimento, il valore mediano si attesta attorno al 50%. Infine, nel caso di terminale in movimento e condizioni di propagazione radio favorevoli, il valore mediano del *throughput* si attesta attorno al 65% della capacità massima del terminale.

4. CENNI ALLE ARCHITETTURE DI RETE PER LE RETI WIRELESS A LARGA BANDA

L'evoluzione dei sistemi di accesso radio verso la gestione efficiente di comunicazioni a pacchetto è legata alle evoluzioni delle architetture di rete.

Un'architettura di rete è il complesso dei principi, delle regole di progetto, delle configurazioni fisiche, dell'organizzazione funzionale, dei pro-

tolci necessari per realizzare e gestire una rete in grado di erogare una serie di servizi.

Le architetture di rete si dividono in **architettura di accesso e di core**. L'accesso si riferisce al modo con cui viene gestita la raccolta del traffico *wireless*, il core definisce tutto ciò che è necessario per erogare i servizi richiesti.

Le architetture tradizionali per i sistemi GSM ed UMTS devono gestire le due tipologie di traffico a circuito (per la voce) ed a pacchetto per i dati in modo differenziato. Esse presentano pertanto un'architettura di accesso e di core "verticale", ossia con funzionalità distinte per le due tipologie di traffico. Nella figura 1 è riportato lo schema generale dell'architettura per il GSM e l'UMTS. Si noti la separazione dei dati dalla voce a livello core e la presenza di un nodo di controllo per la gestione dell'accesso radio (BSC - *Base station Controller* nel GSM ed RNC - *Radio Network Controller* per l'UMTS).

Le nuove architetture (Figura 2) si basano sull'adozione del protocollo IP come **standard di trasporto multiservizio** e si semplificano, sia nella parte di accesso sia nel core, tendendo a strutture più "piatte", cioè con un minor numero di nodi consentendo tempi di latenza più ridotti rispetto al caso precedente.

In particolare, per quanto riguarda la rete d'accesso, scompare il nodo RNC e la gestione del-

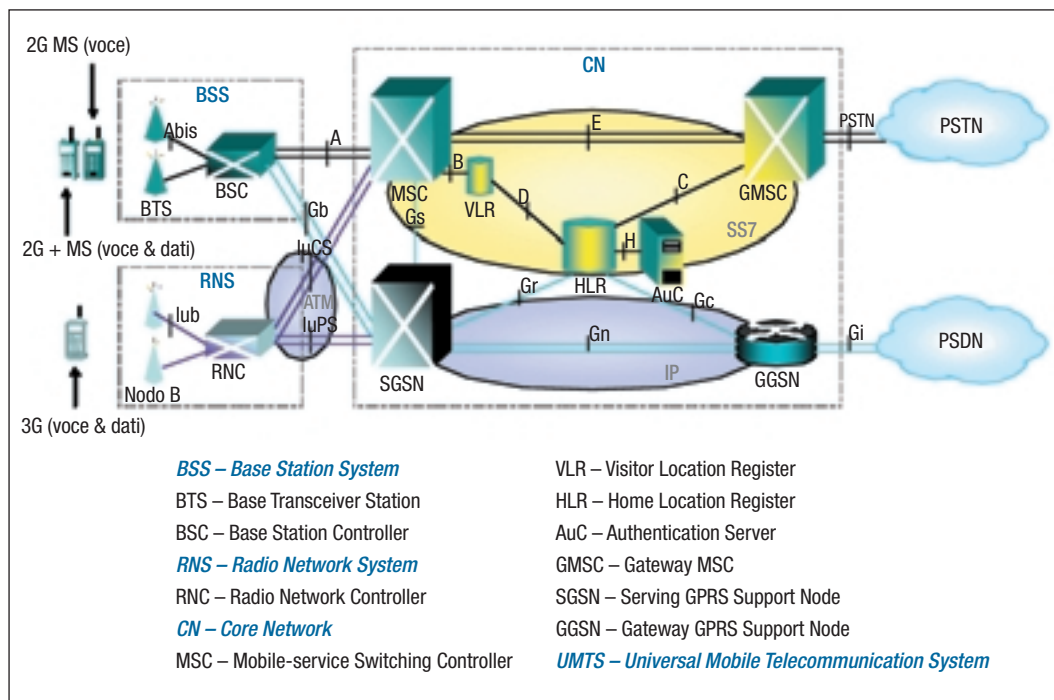
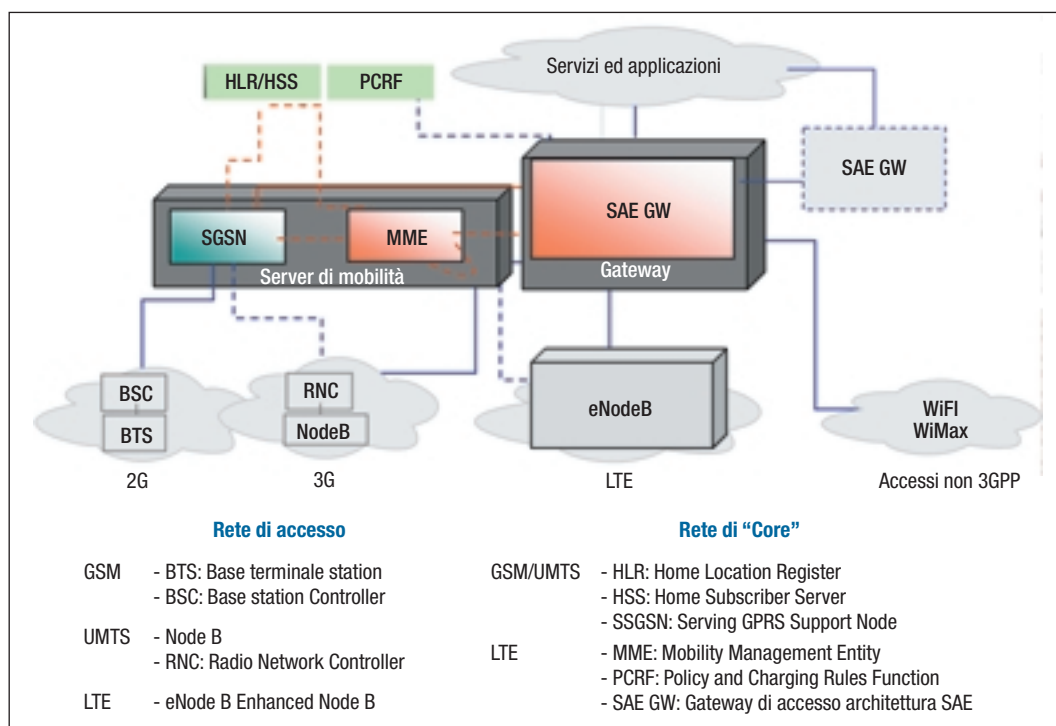


FIGURA 1
Architetture tradizionali GSM ed UMTS

FIGURA 2
Evoluzione
dell'architettura
delle reti
radiomobili a larga
banda



la comunicazione e della mobilità è demandata al cosiddetto eNodeB (*enhanced NodeB*) che dialoga verso un **Access Gateway**. Questo, a sua volta, ha il compito di interfacciarsi verso lo strato superiore dei servizi e delle applicazioni, di gestire le varie tecnologie di accesso e di collegarsi ad altre reti IP private o a Internet. Il nodo detto MME (*Mobility Management Entity*) ha il compito di gestire gli aspetti di mobilità e di accesso alla rete ed è una funzionalità che fisicamente potrebbe essere ospitata nello stesso apparato di *Access Gateway*.

L'HLR (*Home Location Register*), rispetto al passato, assume delle funzionalità più avanzate di profilatura del servizio del cliente necessarie per gestire le comunicazioni tra i vari accessi. La funzione PCRF (*Policy and Charging Rules Function*) ha il compito di assicurare la trasparenza delle politiche di qualità del servizio del cliente indipendentemente dalla tecnologia di accesso considerata. Sono scomparsi i nodi di commutazione in quanto *Gateway* specializzati provvedono alla interconnessione verso la tradizionale rete *PSTN*.

I concetti di base di questa architettura sono validi qualunque sia la tecnologia di accesso adottata. In questo modo il *core* della Rete a larga banda diventa agnostico ri-

spetto alle tecnologie di accesso utilizzate. In particolare la semplificazione dell'architettura di rete, permettendo di connettere un nodo di accesso radio con il *Gateway* per il traffico dati a pacchetto che raccoglie migliaia di stazioni radio, si traduce in un costo dell'infrastruttura poco dipendente dal traffico generato in rete, permettendo in tal modo una **struttura adatta a tariffe di tipo flat** (non basata cioè sul volume di traffico) che in tal modo potrebbe diventare sostenibile anche da parte degli operatori mobili. Resta tuttavia il vincolo importante di un'occupazione della risorsa spettrale comune agli utenti per quanto riguarda l'accesso nonché un corretto dimensionamento delle reti di *back-hauling*, in linea con le aumentate capacità di traffico generate.

5. GESTIONE DELLO SPETTRO NEI SISTEMI WIRELESS

La tabella 2 riassume le allocazioni attuali e le nuove opportunità spettrali per i servizi *wireless*. In particolare, può essere importante ricordare le seguenti posizioni assunte dall'ITU:

□ necessità e opportunità di una restituzione di frequenze nel passaggio dall'analogico al digitale in campo televisivo come conse-



Nome	Frequenze [MHz]	Assegnazione corrente	Possibili tecnologie	Applicazioni
III	(217,5 - 230)	Canali televisivi	TV A/ TDD	
UHF	(450 - 470)	Assegnata da WRC come estensione della banda per IMT-2000	TV A/ TDD, WIMAX	Solo 50 MHz, liberazione canali TV lunga e difficile in Italia
	(470 - 854)	In USA ed India è stata assegnata parte della banda per applicazioni WIMAX		
GSM	(900)	GSM 900	GSM, UMTS 900	In fase di estensione a UMTS
L	(1452 - 1492)	Banda L per T-DAB	T-DAB	
3G	(1900 - 2170)	IMT-2000 / UMTS	UMTS	Estensioni UMTS
MSS	(1900 - 2170)		MSS, SAT	Broadcasting Satellite/ Terrestre
Banda UC-WCS	(2305 - 2360)	Bande ISM, Reti private	WIMAX	WIMAX- Forum l'ha definita "banda standard WIMAX" (in uso in USA e Far East)
Banda ISM	(2400 - 2480)	Banda non licenziata per Wi-Fi, ISM, radioamatori	Wi-Fi	Banda densamente saturata da apparati eterogenei
Banda MMDS	(2500 - 2690)	Assegnata da WRC come estensione della banda per IMT-2000	UMTS, WIMAX.	Attualmente per IMT-2000 WIMAX-Forum chiede estensione per WIMAX-16e
	(2700 - 2900)	Radar meteorologici	UMTS, WIMAX	Non disponibile attualmente in Italia
Banda 3.3 GHz	(3300 - 3400)	Radar marini	WIMAX	Non disponibile in Italia WIMAX Forum spinge per estensione a 3.3 - 3.8 GHz
Banda 3.4 GHz	(3400 - 3600)	Banda licenziata per WIMAX. In Italia già assegnata al Ministero Difesa, ora a gara	WIMAX-UMTS	Attualmente una delle bande principali previste per WIMAX
Banda 3.6 GHz	(3600 - 4000)	Varie assegnazioni	WIMAX	Non disponibile in Italia WIMAX Forum spinge per estensione a 3.3 - 3.8 GHz
Banda 5 GHz	(5150 - 5350) (5470 - 5725)	Banda non licenziata Da ITU e WRC allocata per RLANs / Wi-Fi	Wi-Fi, Hiperlan, WIMAX	200 MHz. EU, Australia, China/HK limitano potenza
	(5725 - 5850)	In Italia è occupata da Ministero Difesa.		255 MHz per solo TDD. Applicazioni WIMAX outdoor

TABELLA 2

Elenco gamme di frequenza con relative tecnologie afferenti e possibili applicazioni

guenza del "dividendo digitale", definito come la possibilità, attuata dalla digitalizzazione, di moltiplicare sensibilmente, nell'attuale spettro impiegato, gli attuali servizi televisivi con conseguente esuberanza di programmi a fronte delle concessioni storiche;
 □ emissione di un singolo piano coordinato

per l'uso dello spettro *broadcasting* in Europa, *Middle-East* e Africa;

□ re-impiego di adeguate porzioni di banda per nuove tipi e forme di servizi multimediali, inclusi quelli mobili.

A seguito di quanto detto sopra, si prospetta una serie di potenziali opportunità per l'u-

tilizzo di risorse spettrali per i servizi mobili e diffusivi qui di seguito elencate:

- *quote di banda III-VHF (174-230 MHz) e banda UHF* da rilasciare dopo lo *switchover* al digitale televisivo;
- *riesame dell'utilizzo della banda GSM 900 MHz*, di cui viene chiesto l'ampliamento d'uso;
- *revisione della banda L (1452-1492 MHz)*, al fine di assicurare che future tecnologie e servizi per la mobilità non siano precluse dall'utilizzo in questa banda;
- *porzioni di spettro tra 1900-2170 MHz* per tecnologie 3G;
- *potenziali bande 1980-2010 MHz per up-link e 2170-2200 MHz per down-link* per tecnologie satellitari mobili MSS;
- *verifica della banda 2500-2690 MHz*, attualmente assegnata a UMTS, per possibile estensione anche al WIMAX.

La banda UHF ha innegabili vantaggi in termini di propagazione e quindi alla possibilità di realizzare ampie coperture con buone penetrazioni negli edifici, facilitando in tal modo lo sviluppo di sistemi *wireless* alternativi per affrontare il problema del "Digital Divide".

In Italia una tale tendenza risulterà un fattore critico dato l'atteggiamento storico fortemente negativo da parte dei gestori televisivi alla restituzione delle frequenze.

Le bande di frequenza per applicazioni MSS (1980-2010 MHz e 2170-2200 MHz), ossia per servizi mobili satellitari, sono attualmente allocate a livello ITU per servizi mobili. Il risultato potrebbe essere quello di sfruttare il segmento satellite anche per i servizi di Mobile-Tv.

La situazione nel nostro paese rimane sempre conservatrice ed arretrata rispetto agli altri Paesi con difficoltà continua e tempi lunghi per il reperimento di nuove frequenze per il mobile.

Per esempio, con notevole ritardo rispetto ad altri Paesi, si sta rendendo disponibile anche in Italia la banda dei 3.5 GHz (già assegnata al Ministero della Difesa) che permetterà, la messa in opera del WIMAX e la possibilità di creare estese reti *wireless* (pur con difficoltà di penetrazione *indoor*) per colmare il "Digital Divide" che penalizza ancora le popolazioni residenti in aree non densamente abitate.

Si vanno infine estendendo progetti a livello di zone metropolitane di reti *Wireless Mesh*

con accesso a 2 GHz e possibilità di impiego a 3.5 GHz del WIMAX come *backhaul*.

6. CONVERGENZA E COMPETIZIONE TRA LE FILIERE

È importante ribadire, come già accennato in Premessa, che nonostante l'accesa competizione tra le diverse filiere ed in particolare tra 3GPP ed IEEE, si rileva ormai una tendenza sempre più accentuata ad una **convergenza tecnologica tra queste due grandi famiglie** verso soluzioni simili come soluzioni tecniche e quindi come prestazioni che portano al massimo sfruttamento delle risorse radio. Questa convergenza tende oggi ad assumere il nome di 4G (*Quarta Generazione*) con valori di efficienza spettrale prossimi ai limiti teorici di Shannon. L'evoluzione temporale alloca al 2010 ed oltre la nascita dei sistemi 4G. Dopo il precedente approfondimento degli obiettivi e delle soluzioni realizzative di tali sistemi e delle tappe che stanno man mano portando a tali avanzate caratteristiche, impensabili fino a poco tempo fa, può essere utile ed interessante chiedersi quali siano state le cause scatenanti di una competizione sempre più accesa che, è ormai evidente, si giocherà più in termini economici che in termini tecnici.

Alcune ragioni possono trovarsi nel tentativo dei produttori provenienti dal mondo dei dati (LAN) di assicurarsi un'importante fetta del mercato della mobilità. A tale scopo essi hanno, in pratica, realizzato un'alleanza con alcuni tra i produttori legati al mondo TLC che hanno finora avuto un limitato successo, avendo anche sfruttato opportunamente un momento di criticità dell'UMTS, legato alle iniziali disattese rispetto alle prestazioni ipotizzate. A queste logiche si è aggiunto l'interesse, nel mondo della Ricerca, a esplorare strade alternative al WCDMA, con una sempre maggiore focalizzazione verso l'OFDM, percepita oltretutto come strada più sgombra da vincoli brevettuali.

Questa competizione riguarda il solo segmento dell'accesso e potrà eventualmente essere risolta con terminali *multistandard* in modo da permettere, anche attraverso reti in tecnologie eterogenee, la completa compati-



bilità di tutta la rete. Tale processo è semplificato dal fatto che la visione della *core network* è in ogni caso comune tra 3GPP e IEEE/WIMAX, con una piattaforma di servizi che si appoggia al sistema IMS (*IP Multimedia Subsystem*) sviluppato in ambito 3GPP.

In sintesi, in un'ottica temporale che porta al 2010, gli **obiettivi comuni** alle due filiere principali per i sistemi di Quarta Generazione risultano ormai sufficientemente chiari e possono così sintetizzarsi:

- **mobilità piena;**
- impiego di una **piattaforma di rete basata su IP**, completando in tal modo il quadro di evoluzione verso la futura rete NGN, anche in ottica di convergenza fisso-mobile;
- funzionalità **multicast** integrate nello standard per potere fornire servizi multimediali di *multicast-broadcast* in mobilità;
- ritardi (**latenza**) sotto i 10 ms per consentire la realizzazione di servizi avanzati con percezione soddisfacente (ritardi trascurabili) da parte dell'utente;
- **efficienza spettrale** attorno ai 5 bit/s/Hz, anche attraverso l'impiego di tecniche avanzate quali il MIMO;
- **uso flessibile dello spettro**, con possibilità cioè di supportare canalizzazioni multiple da 1,25 fino a 20 MHz.

7. CONCLUSIONI

Le tecnologie evolutive sopra illustrate seguendo le due grandi filiere degli enti di standardizzazione tendono ormai, come si è visto, ad essere sostanzialmente equivalenti. Si può ancora discutere sulla bontà o meno dei protocolli e delle modulazioni, ma il quadro che si delinea è di una sostanziale convergenza verso piattaforme multistandard, aggregate da un'architettura di rete core sempre più "piatta". L'orientamento che si prevede, nel lungo termine, è quello di adottare modulazioni OFDM, con meccanismi veloci e dinamici di gestione delle risorse radio in funzione dello stato della qualità del collegamento e con l'uso di tecniche MIMO.

L'impressione che emerge, guardando la storia degli standard esaminati, è che esiste una reciproca influenza ed emulazione la quale, di fatto, tenderà a creare nel tempo uno standard comune, ciò che sarebbe altamente au-

spicabile per semplificare i cellulari senza necessità di soluzioni multistandard.

Per l'evoluzione della larga banda *wireless*, non sarà mai sufficientemente sottolineato quanto importante sia il dimensionamento adeguato delle reti di raccordo (*backhaul*) in presenza di un così elevato aumento della capacità di traffico previsto nell'area di accesso. Tutti gli sforzi di ampliamento verso la larga banda delle reti *wireless* sarebbero totalmente vanificati in assenza di potenti reti di raccordo per la raccolta di tutto il traffico generato.

Una domanda che ci si può fare in riferimento alle comunicazioni mobili a larga banda è relativa, non tanto agli aspetti tecnici, ma a come questi sistemi potranno essere utilizzati con successo commerciale in un mercato saturo (come per esempio quello italiano) caratterizzato dalle seguenti fenomenologie tipiche:

- **"churn-rate"** (ossia il ritmo di cambiamento di operatore) elevato con molti utenti che posseggono almeno due Sim e seguono le promozioni degli operatori prevalentemente basate sui vantaggi di costo;
- ulteriore segmentazione del mercato per effetto degli **operatori mobili virtuali**, prevalentemente Società della grande distribuzione, che utilizzano il traffico, voce e dati, esclusivamente come promozionale per il *business* primario;
- sistema UMTS che, con l'introduzione dell'HSDPA, si vuole affermare come piattaforma per l'offerta dati, aggredendo anche il **mercato del fisso** con offerta di servizi dati e voce.

L'evoluzione verso l'HSPA già avviata è probabile che possa portare a limitare l'adozione del WIMAX ad un ruolo di tecnologia complementare, anche se a tale famiglia di standard va riconosciuta una notevole capacità d'innovazione che influenza sicuramente l'obiettivo comune a cui ormai tendono le due filiere.

Per la realizzazione delle reti *wireless* a larga banda è necessario avere disponibilità di banda per la connettività con il *core* di rete e già oggi gli operatori incontrano i primi problemi nell'aumentare la capacità di *backhauling* a costi sostenibili, non soltanto per i necessari ampliamenti di capacità delle tratte radio ma anche per la necessità di collegamenti in fibra non sempre disponibili.

Il tema della carenza delle infrastrutture di rete diventa un fattore limitante per l'uso del WI-

MAX, come soluzione al *digital divide*. Infatti, in questi casi la possibilità di usare configurazioni magliate consente comunque di collegare le stazioni tra loro fino ad un punto di raccolta. Tuttavia ciò comporta la diminuzione delle prestazioni del sistema in termini di capacità di *throughput* poiché risorse disponibili per l'accesso sono utilizzate per la connettività. Un'ultima considerazione importante. Le aspettative del larga banda *wireless*, oltre ai già accennati investimenti per la rete di *back-haul* necessari per essere garantiti dall'assenza di strozzature nella rete, sono anche fortemente legate alle tariffe che verranno applicate per questi servizi. Attualmente la navigazione è molto costosa e se, in prospettiva, non sarà possibile avere tariffe paragonabili a quelle della rete fissa, si possono fin d'ora nutrire dei dubbi sul successo di queste avanzate offerte tecnologiche.

Ringraziamenti

Il presente articolo aggiorna, rielabora e sintetizza alcuni degli argomenti trattati in una Giornata di Studio (dallo stesso titolo) organizzata nel Maggio del 2007 dall'Associazione AICT della Federazione AEIT in cui è stata anche presentata una pubblicazione AICT su questi argomenti. Si ringraziano tutti coloro che hanno contribuito a tale pubblicazione che è risultata una fonte importante per la preparazione del presente lavoro, che si ritiene utile allargare ad una platea molto più ampia di lettori. Un ringraziamento

particolare all'Ing. Silvia De Fina per una rilettura critica del presente testo e per le modifiche proposte.

Bibliografia

Per maggiori approfondimenti relativi a tutta la tematica dell'articolo e per il quadro dei servizi

- [1] Position Paper AICT: *Evoluzione dei Sistemi Wireless verso la larga banda*. Aprile 2007.

Per approfondimenti relativi a UMTS HSPA ed LTE

- [2] Holma H., Toskala A.: *WCDMA for UMTS-Radio Access for Third Gen. Mobile Comm.* Wiley 2005.
- [3] Holma H., Toskala A.: *HSDPA/HSUPA for UMTS*. Wiley 2006.
- [4] 3G Americas: *UMTS evolution from Release 7 to Release 8 HSPA and SAE/LTE*. July 2007.

Per approfondimenti relativi al WIMAX

- [5] IEEE Std 802.16TM-2004: *IEEE Standard for Local and metropolitan area networks. Air Interface for Fixed Broadband Wireless Access Systems*.
- [6] WIMAX Forum: *Mobile WIMAX: Part I: A Technical Overview and Performance Evaluation*. Febr. 2006.
- [7] WIMAX Forum: *Mobile WIMAX – Part II: A Comparative Analysis*. May 2006.
- [8] IEEE Std 802.16eTM-2005, IEEE Std 802.16TM-2004/Cor 1-2005: *IEEE Standard for Local and metropolitan area networks*. IEEE - New York, USA, 28 February 2006.

Per approfondimenti relativi al MIMO

- [9] Gershman A.B., Sidiropoulos N.D.: *Space Time Processing for MIMO Comm.* Wiley & Sons 2005.

ROBERTO PIERMARINI, laurea in Ingegneria Elettrotecnica all'Università dell'Aquila nel 1982. Dal 1985 al 1995 docente e ricercatore presso la SSGR, Scuola di Formazione della STET. Dal 1996 Responsabile Impianti TIM per il Centro Italia per lo sviluppo delle reti TACS e GSM. Nel 1998 partecipa allo start-up di WIND ed assume la responsabilità dell'Ingegneria per la Rete di Accesso Radiomobile (GSM-UMTS) e per i segmenti di Accesso e Trasporto della Rete fissa. Attualmente opera come consulente occupandosi di tematiche di convergenza, nuove tecnologie e scenari di business. Autore di numerose pubblicazioni per convegni e riviste. E-mail: roberto.piermarini@alice.it

GUIDO VANNUCCHI, laurea in Ingegneria Industriale all'Università di Bologna nel 1958, "Master Science EE" alla Stanford University nel 1963, Libera Docenza in Comunicazioni Elettriche nel 1971. Direttore Generale Telettra dal 1983 al 1990, "Senior Consultant" di Olivetti Telemedia, Vice Direttore Generale della RAI dal 1996 al 1998. Attualmente Docente al Politecnico di Milano di "Architetture per reti e sistemi multiservizio" e Presidente Associazione AICT della Federazione AEIT. Laurea "ad honorem" in Ingegneria delle Telecomunicazioni, conferita dall'Università di Padova nel 1998, per i contributi scientifici e manageriali nel campo della trasmissione dei segnali. E-mail: guido.vannucchi@fastwebnet.it