

## **L'EDUCAZIONE ALLA LEGALITÀ INFORMATICA: UNA NUOVA FRONTIERA DELLA FORMAZIONE TECNICA**

Michele Crudele, Centro ELIS e Università Campus Bio-Medico di Roma

Nonostante gli sforzi fatti per aumentare l'impatto dell'informatica nella scuola, la situazione attuale vede molti docenti impreparati ad affrontare la sfida di formare gli studenti ad un impiego responsabile delle tecnologie digitali. L'aumento del numero di laboratori ha evidenziato l'assenza di competenze specifiche per ridurre i rischi della navigazione su Internet e le azioni illegali. Manca una cultura della "legalità informatica": non si insegna ancora il rispetto dei beni "digitali", divenuti ormai tanto importanti quanto quelli "materiali" e gli studenti vedono spesso solamente gli aspetti sanzionatori delle violazioni, senza capire la *ratio* legislativa a volte offuscata dalla farraginosità e incongruenza di alcune norme. La proposta di programma formativo di educazione alla legalità informatica fornisce le nozioni fondamentali di carattere legale, tecnico, culturale e sociale per affrontare le attività pericolose e proibite in ambito informatico e di telecomunicazione, con il fine di difendere la scuola e tutti coloro che vi operano, rispettare i diritti altrui e trasformare i rischi in opportunità di sviluppo.

## Scenario

Negli ultimi anni è aumentato considerevolmente l'impatto dell'informatica nella scuola italiana, attraverso una maggior diffusione dei computer nei laboratori e, recentemente, l'introduzione delle lavagne interattive multimediali (LIM) in alcune aule. Il piano d'intervento descritto dal comunicato stampa dell'11 giugno 2009 del Ministero dell'Istruzione si articola in due fasi: la prima, proposta a gennaio 2009 e già operativa, prevede l'introduzione delle LIM, la seconda, denominata *cl@ssi 2.0* ha come obiettivo l'utilizzo delle tecnologie informatiche e di telecomunicazioni nelle scuole primarie e secondarie di I grado. Nell'anno scolastico 2009-10 dovrebbero essere state installate 16.000 LIM in altrettante classi della scuola secondaria di I grado, coinvolgendo 50.000 insegnanti in percorsi di formazione. Nel 2010-11 il piano si estenderà alla scuola secondaria di II grado e alla scuola primaria dove saranno distribuite 8.000 LIM e coinvolti circa 25.000 insegnanti.

Si avvicina inoltre il momento in cui l'art. 15 della Legge 133/2008 cominci ad avere vigore: *“A partire dall'anno scolastico 2011-2012, il collegio dei docenti adotta esclusivamente libri utilizzabili nelle versioni on line scaricabili da internet o mista”*.

È encomiabile, anche se non del tutto sufficiente, lo sforzo per formare i docenti dal punto di vista tecnico o didattico, ma manca un'esplicita preparazione ad affrontare i problemi di sicurezza della rete, connessi a quelli delle potenziali illegalità. Né si può pensare che il tema possa essere affidato *in toto* ai tecnici dei laboratori di informatica, sia perché sono presenti esclusivamente nelle scuole secondarie di II grado, sia perché neanche loro hanno avuto occasioni formative specifiche sulla sicurezza informatica.

Le scuole italiane sono spesso teatro di continue violazioni delle norme vigenti. Le reti sono utilizzate molte volte per scaricare illegalmente film e musica, duplicandoli utilizzando le risorse interne. Da reti scolastiche sono stati rilevati tentativi, falliti o riusciti, di attacco a siti nazionali o stranieri. Virus, cavalli di Troia e *malware* causano danni che comportano costi aggiuntivi non indifferenti.

Non è ben definito il ruolo dei responsabili delle reti scolastiche, né sono diffusi protocolli gestionali standard che consentano un maggior controllo delle risorse informatiche, senza inibirne l'uso, anzi promuovendolo.

I docenti sono generalmente impreparati ad affrontare la sfida di formare gli studenti ad un impiego responsabile delle tecnologie digitali. Manca una cultura della “legalità informatica” intesa come estensione del concetto generale di legalità, ben noto nelle scuole perché oggetto di numerose iniziative, soprattutto nel meridione. Non si insegna ancora il rispetto dei beni “digitali”, divenuti ormai tanto importanti quanto quelli “materiali” e gli studenti vedono spesso solamente gli aspetti sanzionatori delle violazioni, senza capire la *ratio* legislativa. Complicano il quadro la farraginosità e l'incongruenza di alcune norme, e la lentezza del legislatore nel rispondere ai mutamenti determinati dall'avanzare della tecnologia. In alcuni casi ci sono interessi contrapposti che non permettono di creare un quadro legislativo armonico: basti pensare al cosiddetto Decreto Pisanu nato per la repressione del terrorismo e rinnovato di anno in anno senza un assestamento normativo, che obbliga a conservare il traffico telematico per un lungo periodo [1], mentre il Garante della Privacy auspica una maggiore garanzia dei dati personali degli utenti [2]. In altre situazioni, come la tutela del diritto d'autore, i mezzi di comunicazione di massa contribuiscono a confondere i piani dichiarando che “è lecito scaricare musica” quando una sentenza sancisce la differenza tra “scaricare” e “condividere”, lasciando solamente quest'ultima azione nell'ambito penale, ma senza togliere la sanzione amministrativa per la prima.

In ambito internazionale si parla abitualmente di *computer ethics* indicando quell'insieme di comportamenti “corretti” che dovrebbero essere seguiti usando le tecnologie informatiche. Il termine “etica” comporta alcune riflessioni di carattere filosofico e obbliga per esempio a definire se stiamo riferendoci a un sistema di tipo aristotelico, basato sui “fini”, oppure kantiano, basato sui “doveri”. Ma, nonostante ci siano studi e ricerche teoriche e pratiche di *computer ethics* [3], nel

parlare comune spesso essa non si distingue dalla *netiquette*, cioè da un insieme di convenzioni sviluppatesi nel tempo per garantire un rapporto di rispetto con gli altri utenti. Non mi sembra quindi opportuno usare il termine “etica informatica” per riferirci all’insieme di norme e consuetudini che regolano, o dovrebbero regolare, l’Information and Communication Technology. È più consona la locuzione “legalità informatica” che fa immediatamente riferimento alle norme emanate ed è alla portata dell’insegnamento tipico scolastico, in analogia all’educazione civica. Ciò non toglie che, in assenza di legislazione specifica o in un quadro interpretativo confuso, si debba fomentare un comportamento “selvaggio”. È importante, in generale, insegnare che la giustizia non si identifica completamente con la legge: in tutti gli ambiti umani ci sono situazioni non regolate formalmente che richiedono però un discernimento personale per rispettare il diritto altrui, anche se non proclamato.

Non è l’obiettivo di questo articolo analizzare in dettaglio la legislazione nazionale ed europea sul tema, né le modalità di formazione specifica dei giovani di tutti i Paesi al rispetto delle norme vigenti e all’uso consapevole della rete. Risulta tuttavia utile il rapporto della Commissione Europea [4] pubblicato all’inizio del 2010 sull’educazione alla *Online Safety*, concetto incluso nella “legalità informatica” con l’accento sulla protezione personale. *“From 30 countries that participated in the study, education on Online Safety (OS) is included in the school curriculum in 24 countries/regions”*, dichiara il rapporto, aggiungendo che per l’Italia *“At present, the school curriculum doesn’t foresee any specific training on this subject, except for some initiatives or experimentations started up by individual schools according to their autonomy”*. L’iniziativa qui descritta ha proprio l’obiettivo di colmare il vuoto didattico istituzionale, utilizzando alcuni mediatori culturali e comportamentali privilegiati: i tecnici di laboratorio delle scuole.

## Metodologia

L’approccio al problema della mancanza di cultura della legalità informatica nelle scuole nasce con la mia chiamata, in quanto esperto di tecnologie e protezione dei minori in rete, alla Commissione “Bullismo a scuola”, creata dal Ministro della Pubblica Istruzione G. Fioroni alla fine del 2006 per rispondere al clamore mediatico suscitato dalla pubblicazione su Internet di un filmato con immagini di vessazioni nei confronti di uno studente disabile. Senza entrare nel merito dello specifico caso, che finora ha visto la condanna di Google per non aver rimosso immediatamente il filmato dalla rete, va considerato che il cosiddetto cyberbullismo si alimenta anche per la superficialità dei ragazzi nel gestire contenuti digitali: non comprendono che c’è un sostanziale salto di scala nella diffusione di una fotografia o un video dall’ambito locale a quello universale in rete, come è stato chiarito da una sentenza del Tribunale di Monza nel novembre 2009 quando uno studente è stato condannato a risarcire la professoressa per aver pubblicato su YouTube un filmato *“lesivo del decoro e della reputazione dell’insegnante”*. Purtroppo nei casi di bullismo la diffusione mediatica finisce per essere controproducente sia per la vittima, che resta etichettata come un “debole”, sia per il bullo che viene conosciuto da tutti come un “delinquente”, senza possibilità di riscatto. La permanenza delle informazioni su Internet costituisce per entrambi un danno irreversibile: quando saranno adulti molto probabilmente non potranno scrollarsi di dosso il passato, anche se si è trattato di un fatto isolato.

Nel cercare una soluzione strutturale al problema, partendo dai suoi aspetti tecnologici, è nata la proposta di un corso di educazione alla legalità informatica, svolto dall’Associazione Centro ELIS, istituzione dedicata alla formazione della gioventù da 45 anni, che con la Cedel e il Consorzio ELIS e il loro Cisco Academy Training Center d’Italia, ha forti competenze informatiche e di telecomunicazione, anche sul fronte della sicurezza, gestendo inoltre il portale [www.ilFiltro.it](http://www.ilFiltro.it) dedicato alla protezione dei minori su Internet. Il Ministero della Pubblica Istruzione designò come destinatari del corso gli assistenti tecnici dei laboratori di informatica perché costituiscono una categoria di operatori scolastici in grado di dialogare con gli studenti senza compiti di valutazione nei loro confronti e quindi in grado di recepire da questi ultimi anche “confidenze” o richieste di consiglio sull’uso di Internet.

La Direzione Generale per lo studente indicò la Sicilia come terreno iniziale di sperimentazione, con il tramite dell'IPSSAR Paolo Borsellino di Palermo. Nacque il corso pilota di educazione alla legalità informatica nell'anno 2007-8 al quale furono invitati inizialmente solo i 150 Istituti Professionali dell'isola, per privilegiare una categoria di scuole a volte svantaggiata nell'offerta culturale. La risposta limitata portò ad estendere l'invito alle altre 350 scuole secondarie di II grado di tutta la Sicilia. La partecipazione fu di 119 tecnici (in pochi casi le scuole inviarono professori) di cui 109 conclusero l'intero corso, tenuto in quattro turni, in sedi diverse, a Palermo, Catania, Caltanissetta e Siracusa.

Il risultato positivo portò il nuovo Ministero dell'Istruzione a una replica del corso, con il tramite dell'ITIS Meucci (poi assorbito dall'IIS Von Neumann) di Roma, per le 300 scuole dello stesso grado della Provincia di Roma, nell'anno scolastico 2009-10, con una partecipazione di 80 tecnici, di cui 77 hanno concluso l'iter formativo.

I moduli didattici sono stati replicati nelle due edizioni, con docenti provenienti dalle scuole ELIS, dalla Polizia delle Comunicazioni, dalla SIAE, dall'ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria, da studi legali informatici, da università e da associazioni dedicate alla tutela dei minori.

Il numero di partecipanti per ogni turno è stato limitato a quaranta per esigenze didattiche. Generalmente la prima sessione, di due giorni completi, è stata dedicata alla sicurezza delle comunicazioni IP, all'analisi, prevenzione e repressione dei crimini informatici, alla metodologia dell'autoaggiornamento e ai sistemi di tutela della navigazione dei minori su Internet. In questa sessione si è svolta anche l'esercitazione pratica: ogni partecipante aveva a disposizione un portatile *wireless* collegato in rete e a Internet. Il laboratorio di sperimentazione è stato allestito *ad hoc* in ogni sede per non interferire con le reti delle scuole ospitanti. In questo modo i tecnici hanno potuto simulare attacchi e difese e studiare le configurazioni ottimali. Nell'edizione romana è stato possibile analizzare le caratteristiche di protezione di Windows 7.

Dopo alcuni mesi si è svolta la seconda sessione, di un'intera giornata, completando il programma con normative, iniziative e proposte positive nell'uso della rete. La scelta della distanza temporale tra le sessioni risponde alla necessità di capitalizzare quanto imparato nella prima, mettendo in pratica le conoscenze acquisite e potendo avere un'ulteriore occasione di confronto con un bagaglio esperienziale arricchito. L'elenco completo delle lezioni è riportato nella tabella dei risultati, accanto al loro gradimento. Una parte delle lezioni è stata registrata e sincronizzata con le presentazioni, ed è liberamente disponibile in rete.

I tecnici hanno avuto a disposizione, per diversi mesi anche dopo la conclusione del corso, la piattaforma MyELIS basata su Moodle per la condivisione di materiali didattici, forum, test, calendari e altre risorse.

Prima dell'inizio di ogni corso sono stati somministrati test conoscitivi per tarare la profondità della formazione in relazione al grado di conoscenze tecniche dei partecipanti. Non essendoci infatti un livello di certificazione standard in Italia per gli assistenti tecnici dei laboratori di informatica, sono possibili grandi differenze di competenze professionali.

Nel corso romano, che si è svolto in due turni nella Scuola ELIS, è stata aggiunta un'iniziativa della Cisco Networking Academy ELIS in occasione del suo decennale (essendo stata la prima in Italia), offrendo l'accesso a tutti gli strumenti e contenuti didattici previsti dal programma sulle tecnologie ICT destinato a scuole ed università. Nei mesi di marzo e aprile 2010 hanno studiato il nuovo testo multimediale in italiano sulla sicurezza informatica e in laboratorio, e hanno condotto simulazioni avanzate di interconnessione di sistemi. Al termine del periodo di studio individuale e di sperimentazione, 39 di loro hanno voluto partecipare, ottenendo quasi tutti risultati brillanti, alla selezione per 15 borse di studio per la partecipazione gratuita ad un corso completo di certificazione come Istruttore per il percorso di Fondamenti d'Informatica e Reti.

## Risultati

Nel test informativo iniziale sono state poste alcune domande relative alle caratteristiche della rete della propria scuola. Il numero di computer gestiti varia nella maggior parte dei casi tra 20 e 100, trattandosi di scuole di dimensioni a volte molto diverse. Il sistema operativo è quasi in tutti i casi Windows XP, sia nell'edizione di tre anni fa che in quella dell'anno trascorso. In poche scuole sono presenti anche versioni più antiche, fino a Windows 98. Pochissimi sono i casi di sistemi basati su Linux e sempre accanto ad altri Windows. Rari anche i laboratori basati su Mac.

Altre domande riguardavano le aspettative e i contenuti desiderati: nella quasi totalità dei casi le risposte hanno ripreso i titoli e temi proposti nella presentazione del corso, con l'aggiunta di qualche dettaglio. Qualcuno ha sottolineato l'importanza di formarsi per difendere gli alunni e gli altri operatori scolastici.

Le domande più tecniche avevano la funzione di sondaggio di competenze. A tutto il questionario, incluse le domande a risposta libera sopra menzionate, bisognava rispondere in 7 minuti evitando di andare a cercare fonti di informazione. Era interessante valutare infatti la capacità di ricordare la situazione della propria rete, inclusi i sistemi di protezione adottati. Proprio quest'ultima domanda ha mostrato una situazione poco strutturata, con semplici antivirus, oppure *firewall* non gestiti o, peggio ancora, senza alcuna protezione (più frequentemente in Sicilia, molto meno a Roma). Rarissimi i casi di filtri di contenuti, tipo *parental control*.

Le domande a risposta chiusa, con una risposta esatta fra quattro proposte, hanno ottenuto i seguenti risultati:

EDIZIONE	DOMANDA	% ESATTE
RM	Il cyberstalking è ...	84%
Sicilia	Quale è la differenza tra virus e worm?	73%
RM	Un programma peer-to-peer ...	69%
Sicilia	Quando è utile o necessario utilizzare un firewall in rete?	62%
RM	Un firewall serve a ...	58%
RM	Il motivo principale per tenere aggiornato il sistema operativo è ...	58%
Sicilia	Ad oggi, non esiste un metodo di facile applicazione per filtrare la navigazione di un utente, proteggendolo dalla maggior parte delle insidie della rete. Vero o Falso?	57%
RM	Collegarsi a una rete wireless aperta sconosciuta per navigare gratis è ...	42%
Sicilia	In caso di violazione di norme sulle comunicazioni informatiche da parte di uno studente, la scuola non ha nessuna responsabilità. Vero, falso, oppure ...	38%

La percentuale altamente positiva nelle risposte sul *cyberstalking* fa pensare che la fonte di conoscenza prioritaria siano i mezzi di informazione di massa che parlano abbastanza spesso di questi fenomeni.

L'ultima domanda sulla violazione di norme a scuola è particolarmente complessa, ma denota una carenza di informazione giuridica in coloro che hanno spesso il compito di far rispettare la legislazione vigenti.

In quella sulla connessione a reti *wireless* aperte, la maggioranza si è soffermata su presunte questioni legali senza percepire che il rischio maggiore è il furto di dati in transito sulla rete da parte dell'anonimo proprietario o di altri malfattori.

Significativa la percezione non del tutto chiara del ruolo del *firewall*, confermata da quanto detto sopra in relazione alla consapevolezza della sua esistenza e funzionalità nel proprio istituto.

Al termine di ogni sessione, i partecipanti sono stati inviati a compilare questionari di gradimento per valutare l'efficacia soggettiva della formazione ricevuta. Nella tabella seguente sono riportate le percentuali su una scala di quattro valori, impostata volutamente senza valore centrale per obbligare a una scelta positiva o negativa.

GRADIMENTO GLOBALE	MOLTO		ABBASTANZA		POCO		PER NULLA	
	RM	Sicilia	RM	Sicilia	RM	Sicilia	RM	Sicilia
<b>Nel complesso come giudica tutto il corso di educazione alla legalità informatica?</b>	<b>82%</b>	<b>86%</b>	<b>18%</b>	<b>14%</b>	<b>0%</b>	<b>0%</b>	<b>0%</b>	<b>0%</b>
La giornata conclusiva ha soddisfatto le sue aspettative?	47%	56%	50%	44%	3%	0%	0%	0%
Le prime due giornate hanno soddisfatto le sue aspettative?	61%	38%	39%	62%	0%	0%	0%	0%

Appare chiaramente un giudizio positivo globale che va al di là della valutazione puntuale delle singole giornate condizionate a volte da alcune docenze meno gradite come è possibile leggere nella tabella successiva che analizza le singole lezioni. Il questionario è stato compilato in Sicilia dal 77% e a Roma dal 78% dei partecipanti e quindi può considerarsi ampiamente rappresentativo.

Ognuno ha potuto esprimere anche commenti liberi. A parte espressioni forse eccessive come *“È il primo corso dopo anni di lavoro nel pubblico impiego veramente valido, avrei solo incrementato un po' più di ore di pratica”*, sono significative frasi come *“Ritengo che le informazioni sulla legalità informatica vadano condivise con docenti e studenti”*, *“Estenderei il corso anche ai Dirigenti Scolastici, perché sempre per mia esperienza, non sono interessati a chi e come vengono utilizzati i laboratori; a loro interessa solo che funzionino per non ricevere lamentele”*, *“Propongo altresì l'istituzione di mini corsi rivolti, in maniera molto semplice, agli alunni di tutte le istituzioni scolastiche onde sensibilizzare gli stessi alla delicata problematica”*, *“Se tutti gli operatori di informatica si attenessero alle normali regole di legalità forse si correrebbero meno pericoli nella esplorazione della rete”* e ancora *“Sarebbe utile che i dirigenti scolastici frequentassero il corso di legalità informatica, escludendo la parte di laboratorio, per rendersi conto di ciò che è necessario fare e le responsabilità che ci assumiamo lavorando con gli studenti, soprattutto minori, senza adottare le adeguate protezioni”* e infine *“Ieri sera agli ultimi miei due figli ho dato delle nozioni sull'argomento”*.

Non ci sono stati commenti esplicitamente negativi e le critiche sono state quasi esclusivamente sulla durata di alcune sessioni, giudicata insufficiente.

Le preferenze analitiche delle diverse lezioni mostrano alcuni scenari di interesse.

LEZIONE	MOLTO UTILE		UTILE		POCO UTILE		INUTILE	
	RM	Sicilia	RM	Sicilia	RM	Sicilia	RM	Sicilia
Gli strumenti informatici di tutela dei minori su Internet	79%	73%	21%	27%	0%	0%	0%	0%
La normativa sulla legalità informatica	75%	58%	25%	41%	0%	1%	0%	0%
La prevenzione e la repressione dei crimini informatici	75%	56%	22%	39%	3%	5%	0%	0%
L'identità digitale e la sua protezione	72%	40%	27%	55%	1%	5%	0%	0%
Iniziativa ELIS Cisco Networking Academy	68%	-	29%	-	3%	-	0%	-
Le truffe e i sistemi di attacco di social networking	65%	59%	32%	36%	3%	4%	0%	1%
Metodologia dell'autoaggiornamento	65%	31%	34%	66%	1%	4%	0%	0%
Sicurezza delle comunicazioni IP e dei sistemi	62%	48%	38%	52%	0%	0%	0%	0%
Le indagini forensi informatiche	59%	-	38%	-	3%	-	0%	-
L'affidabilità dei siti Internet	59%	48%	41%	49%	0%	2%	0%	0%
Internet come risorsa educativa	58%	56%	39%	44%	3%	0%	0%	0%
La cultura della sicurezza informatica	53%	-	45%	-	2%	-	0%	-
Le attività delle associazioni in difesa dei minori	43%	74%	40%	23%	17%	3%	0%	0%
Tecniche di difesa della rete scolastica	42%	69%	53%	30%	5%	1%	0%	0%
Laboratorio informatico di sperimentazione	37%	35%	48%	59%	15%	6%	0%	0%
La tutela del diritto d'autore	10%	30%	62%	68%	23%	2%	5%	0%
Migliorare la legalità informatica a scuola	-	44%	-	54%	-	2%	-	0%

È notevole la differenza di apprezzamento delle lezioni di carattere giuridico. Al di là delle capacità espositive dei docenti, l'approccio al problema ha cambiato radicalmente la percezione dei partecipanti. È stato apprezzato il docente che ha raccontato la storia dell'informatica giuridica e dei suoi annessi e connessi, mostrando i pregi e le incongruenze della legislazione italiana dando anche qualche indicazione di comportamento ottimale nelle diverse situazioni tipiche degli ambienti scolastici, mentre l'impostazione istituzionale della SIAE nell'illustrare le norme sul diritto d'autore non ha sempre entusiasmato i partecipanti che tutti i giorni si scontrano con una realtà di abusivismo diffuso e incontrollato.

Il successo maggiore in entrambe le edizioni è stato ottenuto dalla lezione sugli strumenti informatici di tutela dei minori su Internet. È un segno positivo perché conferma l'interesse dei tecnici di laboratorio a lavorare per difendere gli alunni delle proprie scuole, oltre che i propri figli.

La Polizia delle Comunicazioni ha anche ottenuto un buon apprezzamento, soprattutto a Roma. È da segnalare la disponibilità dei dirigenti di questo servizio della Polizia di Stato che hanno ritenuto molto importante questa iniziativa, facendo partecipare sempre docenti molto esperti e, in un caso, lo stesso responsabile nazionale.

Una menzione particolare va alle attività delle associazioni in difesa dei minori. Un intervento in Sicilia da parte di don Fortunato Di Noto, dell'Associazione Meter, specializzata nella protezione dei bambini contro la pedofilia *on line*, ha avuto un tale successo che ha trascinato verso l'alto le statistiche globali di apprezzamento. In generale si è notata una forte sensibilità alle situazioni estreme e ai potenziali rischi per i bambini e gli studenti: c'è stata una richiesta continua di consigli di comportamento per arginare questi fenomeni delittuosi e per prevenirli.

Il laboratorio di sperimentazione, necessariamente ridotto nel tempo, è stato ritenuto utile ma ha suscitato alcune perplessità: dai commenti si deduce che le differenze di conoscenze specifiche tra i partecipanti hanno creato diverse velocità di apprendimento e quindi lamentele da parte dei più esperti che vedevano la lezione rallentata dai meno preparati.

Nella sezione "Progetti di formazione" del portale [www.ilFiltro.it](http://www.ilFiltro.it) sono riportati ulteriori dettagli, con l'elenco dei docenti delle singole materie, le relazioni complete di tutti i commenti dei partecipanti delle due edizioni e le lezioni registrate.

## Conclusioni

La risposta molto positiva da parte dei tecnici coinvolti nei corsi di educazione alla legalità informatica dimostra che si tratta di un tema rilevante nella formazione scolastica italiana. I "nativi digitali", cioè quei giovani che sono nati quando le tecnologie informatiche e di telecomunicazione erano già pervasive nella società, sono ormai arrivati all'adolescenza e hanno imparato da soli a sopravvivere nell'ecosistema digitale. Ma il loro atteggiamento assomiglia a volte a quello di "selvaggi digitali" difficilmente integrabili in una civiltà organizzata e dotata di regole di comportamento. Solamente quando sono toccati i propri interessi si rendono conto della necessità di rispettare norme che generalmente ritengono inutili. Accade quando sono privati in modo scorretto di beni digitali come un trofeo vinto in un gioco di ruolo, oppure quando sono soggetti ad atti di cyberbullismo, o ancora quando cominciano a produrre musica in modo professionale e si rendono conto che, se tutti la scaricano gratis, loro non guadagnano nulla.

Poiché è complesso e costoso, oltre che probabilmente lento, organizzare un piano di formazione per gli studenti adolescenti in tutta Italia, sembra più efficace cominciare a intervenire attraverso i mediatori scolastici privilegiati nel settore dell'ICT. I tecnici dei laboratori di informatica hanno infatti la possibilità di diffondere buone pratiche che vanno dalla spiegazione dei rischi alla tutela del diritto d'autore e all'uso dei programmi *open source* soprattutto in alternativa alla pirateria informatica. Il loro intervento potrà essere più efficace anche con docenti e dirigenti scolastici nella misura in cui sarà riconosciuta la loro competenza e definiti i loro compiti in relazione alla gestione delle reti di Istituto. Le normative ministeriali non sono ancora adeguate e richiedono un approfondimento e livelli formativi più alti per questi assistenti tecnici, considerata la complessità crescente, la diffusione quasi universale delle reti nelle scuole e la difficoltà di districarsi nella legislazione italiana.

Il punto più dolente resta la totale assenza di tecnici incaricati per le scuole secondarie di I grado e, ancor peggio, per quelle primarie dove frequentemente non esistono docenti in grado di supplire al compito di gestire le reti informatiche, mentre i rischi sono ancora maggiori trattandosi di bambini. In quest'ultimo caso gli alunni hanno maggiori abilità dei loro maestri, ma non hanno sviluppato ancora la capacità di autodifendersi, né conoscono i codici di comportamento sociale: se nessuno glieli insegna, si troveranno a dover fare esperienza sulla propria pelle, con conseguenze negative prevedibili. È come se un bambino dovesse imparare ad attraversare la strada da solo: prima di capire il sistema delle strisce pedonali e dei semafori, rischierà di essere investito più volte e probabilmente subirà qualche incidente. Se invece i genitori gli insegnano la "procedura" corretta, che varierà da città a città in relazione al grado di disordine del traffico, avranno maggiori possibilità di attraversare sempre indenni.

Auspichiamo perciò la continuazione e la moltiplicazione di corsi di educazione alla legalità informatica, anche da parte di altre istituzioni ed enti di formazione. La pubblicazione dei nostri programmi e metodologie risponde al desiderio di non conservare un *copyright* dell'iniziativa ma di farne un sistema formativo *open source* a beneficio di tutti.

## Ringraziamenti

Si ringrazia il Ministero dell'Istruzione, dell'Università e della Ricerca, che ha finanziato la realizzazione dei corsi, la Polizia delle Comunicazioni, la SIAE, l'ANSSAIF, i consulenti legali informatici, l'Associazione Meter e il Moige per la docenza, Telecom Italia per la disponibilità della connessione ad altissima banda presso la Scuola ELIS, Microsoft Italia per le licenze di Windows 7 e tutti gli Istituti che hanno ospitato le lezioni.

## Note

- [1] La Polizia delle Comunicazioni nei suoi numerosi interventi didattici nelle scuole invita spesso i responsabili delle reti a conservare i *log* di navigazione Internet a fini investigativi (senza quindi farne altro uso), tracciando tutti gli utenti ed evitando accessi anonimi alla rete. Tutto questo non è imposto formalmente dalle leggi vigenti e dal Decreto Pisanu, ma è una misura prudenziale opportuna in ambito scolastico, pubblico e privato. Nel corso sono stati riferiti casi di indagini della magistratura in difficoltà per non aver trovato nelle scuole le tracce di reati informatici indispensabili per individuare i colpevoli.
- [2] Il tema è illustrato nel provvedimento del Garante della Privacy del 17 gennaio 2008 accessibile su <http://www.garanteprivacy.it/garante/doc.jsp?ID=1482111> [2010-07-28] che contiene anche riferimenti a successive variazioni.
- [3] Interessanti sono gli studi che i convegni ETHICOMP promuovono dal 1995. Ebbi occasione di partecipare nel 1999 a quello organizzato dalla Luiss a Roma, nel quale presentai un'analisi su *Technological limits of parental control over the Internet*.
- [4] Euridyce, Education on Online Safety in Schools in Europe, December 2009, disponibile su [http://eacea.ec.europa.eu/education/eurydice/documents/thematic\\_reports/121EN.pdf](http://eacea.ec.europa.eu/education/eurydice/documents/thematic_reports/121EN.pdf) [2010-07-28]