Sicuri on line. Le competenze per la sicurezza DIGCOMP

Sandra Troia
Scuola Secondaria di I grado Vittorio Emanuele III - Dante Alighieri
Piazza Trieste e Trento 6, - 76123 Andria (BT)
sandra.troia@istruzione.it

Il saper tutelare la salute nell'ambiente digitale, il saper rispettare un adeguato codice di comportamento on line, il saper riconoscere e reagire dalle minacce in rete, l'essere in grado di proteggere la reputazione digitale sono elementi della competenza digitale. Il framework DIGCOMP offre un organico punto di riferimento per una progettazione didattica che supporti gli studenti, cittadini competenti digitali, in un percorso di crescita e riflessione critica sul proprio agire nella dimensione analogico-digitale. Per forzare le resistenze verso temi, come la sicurezza, ritenuti ostici l'impiego della didattica ludica può favorire l'engagement e la motivazione.

1. È "solo" digitale?

L'integrazione crescente tra la dimensione analogica e quella digitale richiama in modo costante la necessità di compiere una riflessione critica su come agiamo quando utilizziamo le tecnologie per **esercitare la cittadinanza** [Cameron-Curry et al, 2014]. La nostra presenza e la comunicazione nell'ambiente digitale influenza in modo concreto la qualità e la sicurezza della vita *off line*. È necessario acquisire **specifiche competenze (digitali)** per poter agire efficacemente in difesa della nostra e altrui sicurezza e salute. I rischi più comuni ai quali ci esponiamo e si espongono i minori sono molteplici: frode, violazione della privacy, violazione del *copyright* (norme a tutela del diritto d'autore), *grooming* (adescamento), *sexting* (invio di messaggi sessualmente espliciti anche con immagini), cyberbullismo. **Il mondo della scuola in Italia sta rispondendo ad esigenze nuove** di uno scenario che si evolve velocemente, si mostra, più che nel passato, disponibile e pronto a misurarsi con il rinnovamento di metodologie, strumenti e ambienti. Ha, non senza difficoltà, avviato un processo di rinnovamento che investe anche le competenze del personale docente e l'offerta formativa (Piano Nazionale Scuola Digitale). Tuttavia, nonostante siano stati compiuti significativi passi in avanti per portare il mondo reale in classe e mettere al centro l'esperienza dei soggetti come **cittadini digitali**, permangono in alcuni contesti forti resistenze o, peggio, disinteresse. Le ragioni di questo colpevole distacco possono essere verosimilmente connesse alle **incognite legate alla "guida" dei minori in una dimensione fluida analogico-digitale a cui si espongono i docenti** e alla

mancanza di un consolidato livello di competenze utile a gestire situazioni problematiche. Vivere la dimensione digitale interpretandola come “separata dal reale” (e per questo non importante) o fuggirla per timore di non essere in grado di gestirla sono atteggiamenti che l'ambiente formativo e la **società (digitale)** tutta deve impegnarsi a superare puntando sull'**acquisizione di competenze specifiche e a consolidare una cultura della collaborazione**. L'educazione al saper essere e fare digitale comprende la programmazione e l'uso degli strumenti, ma non può a questo limitarsi ed esaurirsi. È opportuno muovere delle riflessioni partendo da due quesiti: perché è indispensabile essere in possesso di competenze digitali in tema di *e-safety*? L'educazione alla cittadinanza digitale può considerasi un compito affidato in modo esclusivo alla scuola? Le **competenze digitali sono competenze per la cittadinanza**, devono essere apprese ed agite in modo integrato alle **8 competenze chiave per l'apprendimento permanente** (Raccomandazione 2006/962/CE del Parlamento europeo e del Consiglio, del 18 dicembre 2006, relativa a competenze chiave per l'apprendimento permanente), sono il perno intorno a cui ruota non solo l'inclusione del soggetto ma il suo essere libero, attivo, costruttivamente critico e **sicuro** nel XXI secolo. Le competenze digitali afferenti all'area della sicurezza hanno inoltre un **ruolo strategico per lo sviluppo economico**. Il livello di sicurezza digitale, sperimentato o percepito, influenza l'uso della rete da parte dei cittadini (nel ruolo di utenti/clienti di servizi). Vivere la condizione di non sentirsi in grado di tutelarsi nell'ambiente digitale, oltre a minacciare il benessere psico-fisico, pregiudica, a cascata, anche lo sviluppo dei mercati digitali a cui l'Europa punta con interesse. L'istituzione educativa non può dirsi in grado di formare cittadini competenti digitali se non coadiuvata dall'intera comunità e dalle famiglie, è necessario in primo luogo un intervento coordinato che miri all'educazione al saper essere cittadini in rete, rispettosi di norme e valori, sostenitori attivi della cultura della legalità, aperti alle differenze. Formazione che non può essere limitata all'orario delle attività scolastiche.

1.1 Verso un uso consapevole dei media digitali

Il tema della sicurezza negli ambienti digitali è spesso sottovalutato dai non addetti ai lavori. Trascurando in questa sede l'aspetto del rispetto delle norme di *copyright* e licenze, ci si soffermerà ad indagare il tema della sicurezza dei minori in relazione ad azioni di *cyber*-aggressione partendo da una delle indagini disponibili più recente. Il Censis (Centro Studi Investimenti Sociali) nel 2016 ha l'intervistato 1727 Dirigenti Scolastici italiani per la ricerca “Verso un uso consapevole dei media digitali” [Censis e Polizia di Stato, 2016] condotta in collaborazione con la polizia Postale e delle Comunicazioni. Sebbene i dati raccolti rappresentino il punto di vista di un'unica categoria (i Dirigenti Scolastici) e che solo il 10% delle scuole abbia predisposto un vero e proprio programma di monitoraggio (con questionari rivolti a studenti e genitori), le indicazioni ricavate fanno emergere l'urgenza di un'azione finalizzata a **rendere sistematica la riflessione sui comportamenti connessi all'utilizzo degli strumenti tecnologici** che coinvolga in modo attivo e congiunto allievi, genitori e personale scolastico. Dalla ricerca risulta che il 52% dei Dirigenti Scolastici

interpellati ha dovuto gestire casi di cyberbullismo, il 10% di *sexting* e il 3% di *grooming*. L'81% dei partecipanti all'indagine ha affermato, inoltre, che **i genitori tendono a minimizzare il problema**, il 49% ha sostenuto che la maggiore difficoltà da affrontare è **rendere consapevoli i genitori** della gravità dell'accaduto in casi di cyberbullismo e, infine, l'89% che l'esempio dei genitori influenza (molto o abbastanza) il comportamento dei cyber-aggressori. Il 39% delle scuole intervistate dichiara di aver già attuato alcune delle azioni specifiche contro il cyberbullismo previste dalle linee ministeriali, il 48% ha avviato programmi di contrasto al cyberbullismo, il 43% ha aperto uno sportello dedicato e il 51,8% ha attivato programmi di informazione rivolti ai genitori ai quali è stato registrato, per il 60%, un **livello basso di partecipazione** (pochi genitori). La ricerca, finalizzata a **definire nuove strategie ed azioni di contrasto** per i casi di aggressione subite da studenti e realizzate attraverso l'uso delle tecnologie, rende manifesto il **bisogno di una specifica formazione**. I temi di aggiornamento professionale di maggiore interesse indicati sono: adescamento on line e cyberbullismo, vittimizzazione sul web in danno di minori da parte di adulti, prepotenze on line tra minori. Fenomeni per i quali mancano riferimenti nell'ordinamento giuridico italiano e il cui vuoto normativo viene colmato riconducendoli a fattispecie di reato esistenti [Osservatorio per il contrasto della pedofilia e della pornografia minorile, 2016].

2. L'evoluzione digitale della formazione: DigCompOrg, DIGCOMP

L'apprendimento è oggi un **processo sociale** in cui le tecnologie e le competenze (analogico-digitali) giocano un ruolo chiave nella formazione del cittadino competente digitale [Troia et al, 2014]. Le organizzazioni educative vivono una profonda trasformazione e, come testimoniato dai dati del Censis per l'Italia prima citati, esse si trovano a gestire situazioni problematiche nuove (cyberbullismo, *sexting, grooming*) per garantire il benessere dei minori. Si assiste all'**allargamento della dimensione educativa e delle responsabilità ad essa correlate** al di fuori dell'ambiente scolastico. A conferma che ci si trovi di fronte ad una situazione di cambiamento strutturale è la predisposizione di uno strumento finalizzato all'auto-valutazione di scuole, università, enti di formazione elaborato dal Joint Research Centre europeo (JRC-IPTS): **il *framework* DigCompOrg.** Il DigCompOrg (*European Reference Framework for Digitally-Competent Educational Organisation*) è uno strumento, non prescrittivo, che guida le organizzazioni educative ad **auto-valutare la qualità e i progressi compiuti nell'integrazione ed impiego delle tecnologie**. Esso si compone di 7 elementi tematici fissi (leadership e gestione, insegnamento ed apprendimento, sviluppo professionale, valutazione, contenuti e curricula, collaborazione e reti, infrastrutture) ed 1 variabile, con relativi sub-elementi e descrittori. All'interno dell'elemento tematico "*Pratiche di insegnamento e apprendimento"* è contenuto il sub-elemento "*Promozione, standardizzazione e valutazione della competenza digitale"* in cui si evidenzia l'importanza per docenti e studenti di **dimostrare di essere in possesso dei livelli di**

competenza digitale necessari ad impiegare efficacemente le tecnologie digitali per l'insegnamento, l'apprendimento, la valutazione e la *leadership*. La responsabilità e l'impegno a prendersi cura del benessere di docenti e studenti mentre usano strumenti digitali (sicurezza e consapevolezza dei possibili rischi connessi al digitale) è affidata all'organizzazione educativa; uno tra descrittori recita infatti "sicurezza, rischi e comportamenti responsabili negli ambienti on line sono messi in primo piano" [Kampylis, 2015]. DigCompOrg è complementare al *framework* DIGCOMP anche questo elaborato dal JRC-IPTS. Il modello DIGCOMP del 2013, che a breve sarà aggiornato nella versione 2.0, è stato elaborato per concorrere allo sviluppo e al miglioramento delle competenze digitali dei cittadini declinandole in conoscenze, abilità e atteggiamenti [Ferrari et al, 2013]. Esso, inoltre, suggerisce possibili collegamenti rintracciabili tra le competenze digitali specifiche e quelle chiave dell'apprendimento permanente che possono risultare un utile riferimento per la definizione di progetti formativi. DIGCOMP, già impiegato in ambito educativo in alcune realtà europee per la creazione di programmazioni per la scuola dell'obbligo, la formazione degli insegnanti e corsi per adulti, non si concentra sull'uso di specifici strumenti ma è organizzato per **5 aree di competenza** che interpretano i bisogni di cui ogni cittadino della società dell'informazione e comunicazione è portatore: bisogno di essere informato (1.Informazione), bisogno di interagire (2. Comunicazione), bisogno di esprimersi (3.Creazione dei contenuti), bisogno di protezione (4. Sicurezza), bisogno di gestire situazioni problematiche connesse agli strumenti tecnologici ed ambienti digitali (5. *Problem solving*) [Ferrari e Troia, 2015]. Nel **Piano Nazionale Scuola Digitale**, documento di indirizzo del Ministero dell'Istruzione, dell'Università e della Ricerca, per il lancio di una strategia di innovazione della scuola italiana e del suo sistema educativo nell'era digitale, **nell'azione #14 *Un framework comune per le competenze digitali e l'educazione ai media degli studenti*** si fa espresso riferimento a DIGCOMP. Per raggiungere l'obiettivo di dotare il sistema scolastico di un *framework* chiaro e condiviso in materia di competenze digitali è prevista la valorizzazione di esperienze di mappatura e ricostruzione delle competenze già disponibili come il *framework Web Literacy* curato da *Mozilla Foundation*, il lavoro a cura della *Media Smarts* per il Governo Canadese e, come anticipato, DIGCOMP. Tra le 21 competenze digitali DIGCOMP possono essere ricondotte al tema della sicurezza le competenze **2.5 Netiquette** , **2.6 Gestire l'identità digitale** (attinenti all'Area 2: Comunicazione) e le competenze **4.1 Proteggere i dispositivi**, **4.2 Proteggere i dati personali**, **4.3 Tutelare la salute** (attinenti all'Area 4: Sicurezza).

2.1 Comunicare in sicurezza. Le competenze DIGCOMP

Per una comunicazione sicura come deve essere formato lo studente? Comunicare in rete in sicurezza richiede il possesso di competenze, non connesse solo agli strumenti tecnologici impiegati, ma alla **conoscenza della netiquette** e alla **gestione dell'identità digitale**. In DIGCOMP la competenza 2.5 **Netiquette** è descritta come il conoscere e il sapere applicare norme di comportamento per l'interazione in ambiente digitale; l'essere consapevoli degli

aspetti connessi alla diversità culturale; l'essere in grado di proteggere se stessi e gli altri da possibili pericoli in rete (tra i quali il cyberbullismo); l'essere in grado di sviluppare strategie attive per individuare comportamenti inappropriati. La necessità di **acquisire consapevolezza della diversità culturale** risulta un elemento di grande interesse per un paese che vive un crescente processo di integrazione legato ai fenomeni immigratori. Come si valuta la competenza in DIGCOMP? Il *framework* fornisce descrittori per tre livelli di competenza: base, intermedio (autonomo), avanzato. Consultando i livelli di *proficency* per la competenza 2.5 **Netiquette,** si apprende che il soggetto in possesso di un livello base di competenza conosce ed applica norme elementari di comportamento quando comunica utilizzando strumenti digitali. Un soggetto con un livello intermedio risulta più autonomo, conosce i principi dell'etichetta della comunicazione on line e li applica nel proprio contesto. È, invece, l'utente avanzato ad essere in grado di utilizzarli in ambienti digitali diversificati ed è in grado di sviluppare strategie utili ad individuare comportamenti inappropriati. Spesso i frequentatori della rete, adulti e minori, non considerano con la dovuta cautela la gestione della propria identità digitale. La pratica diffusa dell'**iscrizione ai social network da parte di soggetti con un'età inferiore a quella consentita** con l'indicazione di dati anagrafici falsi, talvolta con la silente complicità del genitore, può favorire nonostante **il diritto all'oblio**, una gestione poco opportuna dell'identità digitale. La competenza 2.6 **Gestire l'identità digitale** è declinata come il saper creare, modificare e gestire una o più identità digitali, essere in grado di proteggere la reputazione in rete; essere in grado di trattare i dati che un soggetto produce nell'utilizzo di account ed applicazioni. A livello base il soggetto è consapevole dei benefici e dei rischi connessi al possesso di un'identità digitale. Ad un livello autonomo è in grado di "dare forma" al proprio io digitale e di monitorarne le impronte (*digital footprint*). Un competente digitale avanzato, infine, può gestire diverse identità digitali appropriate per diversi contesti e scopi, riesce a monitorare le informazioni e i dati che produce attraverso la propria interazione on line. Sa come proteggere la propria reputazione in rete.

2.2 Proteggere e tutelare dispositivi, dati e salute. Le competenze DIGCOMP

La sicurezza nell'ambiente digitale è legata a tre elementi: hardware, software, *wetware* (il fattore umano). La protezione dei dispositivi, dei dati personali e la tutela della salute richiedono da parte dei soggetti conoscenze specifiche, un atteggiamento attivo e un'allenata capacità critica. Nell'ambito dell'area DIGCOMP dedicata alla sicurezza la competenza 4.1 **Proteggere i dispositivi** è inquadrata come il sapere proteggere i propri strumenti ed avere consapevolezza dei rischi in rete e delle minacce; conoscere le misure di protezione e sicurezza. Il **furto d'identità** espone i soggetti a diversi rischi tra i più comuni: l'invio di email e messaggi con contenuti offensivi, la pubblicazione di post nei social network da parte di estranei a proprio nome, la perdita di possesso di dati (anche riguardanti la sfera privata). Per tali motivi la protezione dei dispositivi rappresenta un'importante componente delle azioni utili a

contrastare possibili cyber-aggressori. I descrittori dei livelli di *proficiency* DIGCOMP inquadrano nel livello *foundation* i soggetti che, per proteggere gli strumenti, utilizzano soluzioni di base come, per esempio, anti-virus e password. Utenti digitali in possesso di un livello autonomo sono, invece, in grado di mantenere aggiornate le strategie di sicurezza. È nel livello avanzato che l'**aggiornamento delle strategie di sicurezza** è frequente ed è accompagnato dalla capacità di intervenire in caso di attacco da parte di virus, malware o hacker. Pensando ai dati personali, è comune l'errore di chi abita il digitale di trascurare l'importanza di proteggere oltre che i propri dati anche quelli degli altri. In possesso della competenza 4.2 **Proteggere i dati personali**, il soggetto comprende i termini di servizio comuni; protegge in modo attivo i dati personali; rispetta la privacy di altri soggetti; si protegge dalle frodi in rete, dalle minacce e dal cyberbullismo. Naturalmente il livello di autonomia è in relazione alla *proficiency.* Nel livello base la conoscenza è limitata al tipo di informazioni (proprie o di altri) che possono essere condivise in ambienti digitali. Nel livello intermedio il soggetto è in grado di proteggere la propria ed altrui privacy, comprende gli aspetti generali connessi a tale tema ed è in possesso di conoscenze di base relative a come i propri dati sono raccolti ed utilizzati. Arrivando **al livello avanzato spesso il soggetto modifica le impostazioni della privacy di *default* dei servizi on line** per migliorare la protezione dei propri dati, ha un'ampia e aggiornata conoscenza del tema della protezione della privacy e di come i propri dati siano raccolti ed utilizzati. L'impiego prolungato degli strumenti tecnologici e la frequentazione della dimensione digitale può, senza il rispetto di corrette regole di utilizzo, esporre gli utenti a minacce per il benessere fisico e psicologico (competenza 4.3 **Tutelare la salute)**. Di particolare rilievo è il **rischio di dipendenza dalla tecnologia**. I descrittori dei tre livelli di *proficiency* inseriscono nel livello base il soggetto che è in grado di evitare gli attacchi dei cyberbulli ed è consapevole che un cattivo uso delle tecnologie può risultare dannoso per la salute. Nel livello intermedio (autonomo) l'utente ha la capacità di saper proteggere se stesso e gli altri da attacchi di cyberbullismo, di comprendere i rischi associati all'uso delle tecnologie (da quelli legati ad una scorretta postura a forme di dipendenza). Nel livello avanzato vi è la consapevolezza di come utilizzare in modo appropriato le tecnologie per scongiurare problematiche di salute ed il saper **trovare il giusto equilibrio tra il mondo on line e quello off line**. L'acquisizione di tale competenza è particolarmente importante per i minori, e non solo, per comprendere che la dimensione digitale e la dimensione analogica sono nello stesso tempo integrate (le azioni digitali posso avere una ricaduta nella dimensione analogica) e diverse (l'identità digitale dichiarata da un soggetto in un social network può non essere la sua identità nel mondo analogico).

3. Coinvolgimento, gioco, educazione alla sicurezza on line

Chi è interessato alla sicurezza? L'esperienza di apprendimento dovrebbe essere emozionale, piacevole, rilevante, creativa, *social*, flessibile, personalizzata, certificabile. Una leva che può sostenere l'interesse e la

motivazione è l'***engagement,*** il coinvolgimento profondo. Le iniziative di didattica ludica, che propongo a giovani e studenti, genitori e docenti di misurarsi con il *coding* o con la robotica "giocando", hanno confermato la possibilità di approcciare temi percepiti dai più come ostici con entusiasmo e motivazione. L'***edutainment*** (intrattenimento educativo) consente di **forzare le resistenze al cambiamento attraverso il coinvolgimento attivo dei diversi attori**. Marshall McLuhan affermava *"Coloro che fanno distinzione fra intrattenimento ed educazione forse non sanno che l'educazione deve essere divertente e il divertimento deve essere educativo"*. Attraverso il gioco è possibile mettere in moto un meccanismo virtuoso di attenzione e consolidamento di competenze anche su temi quali la sicurezza digitale. Tra le esperienze e le risorse attualmente disponibili utili all'*engagement* di studenti tra gli 8 e 12 anni e, insieme, di figure adulte vi è Happy Onlife. **Happy Onlife**, a cura del Centro Comune di Ricerca della Commissione europea – Istituto per la protezione e la sicurezza dei cittadini, è una raccolta di attività ludo-educative e un *serious* game sui rischi ed opportunità dell'infosfera per promuovere la condivisione dell'esperienza digitale [Di Gioia et al, 2016]. Uno degli scopi dichiarati del documento, infatti, è quello di suggerire l'uso di strumenti (on ed off line) utili a **consolidare i legami tra i soggetti che compongono il gruppo che apprende** (insegnanti, genitori e minori). Le risorse selezionate guidano all'acquisizione di consapevolezza dei cambiamenti culturali in atto, connessi alla diffusione delle tecnologie, e facilitano il superamento del divario generazionale. Uguale attenzione è, inoltre, rivolta alla **prevenzione e alla soluzione di situazioni problematiche**. La scoperta e l'esperienza della dimensione digitale vengono vissute dagli studenti, principalmente, in autonomia e con il gruppo dei pari, vertendo in modo prevalente sugli aspetti ludici e di condivisione [Chaudron et al, 2015]. L'impiego del gioco per introdurre in modo non invasivo la presenza di figure adulte (genitori e docenti) consente di favorire il confronto e l'integrazione di conoscenze, competenze, letture ed interpretazioni di situazioni di possibile pericolo portate da target differenti. Il titolo stesso della raccolta Happy Onlife richiama l'attenzione sulla **connessione tra comportamenti competenti nell'ambiente digitale e benessere dei soggetti**. Nelle risorse della raccolta è **Happy Onlife game** con una struttura simile a quella del "gioco dell'oca" che si compone di quiz su tre argomenti principali (uso di internet, social network, giochi on line). L'attività ludico-didattica è strutturata in modo da consentire un **continuo confronto tra i partecipanti e i moderatori (adulti)**. È finalizzata a favorire la riflessione sul tema della sicurezza in rete, stimolare il confronto rispetto a situazioni problematiche ed indagare le opportunità di una partecipazione digitale attiva. Il gioco, disponibile nella versione cartacea (*board game*) e in quella digitale come applicazione è tradotto attualmente in lingua italiana e lingua inglese. L'adulto trova nel gioco l'occasione di rafforzare la comunicazione con i minori attraverso azioni che non sono percepite da questi come intrusioni-imposizioni ma naturalmente connesse all'attività in atto. Inoltre offre un'ulteriore opportunità, in particolare alla figura genitoriale, di **stimolo ad una riflessione sui pericoli e i corretti comportamenti dei giovani cittadini digitali in rete**. La partecipazione allargata (studenti, docenti, genitori) rende possibile

un'osservazione reciproca ed un'educazione reciproca. Minori ed adulti nel gioco si trovano ad essere un gruppo di “pari”, sono portatori di conoscenze e competenze diverse ed integrabili, apprendono insieme a muoversi in un contesto che muta rapidamente le proprie regole, richiede veloci adeguamenti e richiede di rinunciare alle “gerarchie”. Nel corso della “Europe Code Week 2015” il CCR della Commissione europea, sito di Ispra (VA), ha presentato e validato gli strumenti e attività Happy Onlife. Nel rapporto post-evento “Laboratorio Happy Onlife” ha inoltre inserito, nell'ambito della presentazione degli interventi condotti in Italia, richiami alle competenze di sicurezza DIGCOMP [Di Gioia e al, 2016].

3.1 Giocautori: dall’esperienza al gioco, dal gioco alla competenza

Un’ipotesi di lavoro per vivere il gioco come **laboratorio di competenze**, è quella di far vestire ai soggetti in formazione il doppio ruolo di giocatori ed autori. L’esperienza formativa in cui i soggetti sono “giocautori” è strutturata intorno a due elementi: **esperienza dei soggetti** e **competenze**. La struttura di gioco può essere ideata dagli studenti *ex novo* o, più semplicemente, mutuata da giochi già noti (selezionati considerandone il livello di complessità e la rispondenza ai bisogni formativi del *target* di riferimento). Elemento indispensabile è la presenza di **prove** che i giocatori, singolarmente o in squadra, siano chiamati a superare. Per garantire la personalizzazione dell’esperienza formativa e renderla significativa, al centro è posto il **racconto del vissuto dei soggetti come frequentatori della dimensione digitale**. Il docente-facilitatore, dopo aver presentato il modello DIGCOMP (o analogo *framework*), stimola il gruppo in formazione a descrivere azioni concrete svolte *on line* (navigazione, partecipazione a social network, creazione di account,…) e ad evidenziare eventuali situazioni problematiche vissute. Le esperienze raccontate vengono successivamente associate ed abbinate dagli stessi studenti a specifiche competenze e livelli di *proficiency*. Gli **studenti-autori** sono a questo punto pronti a strutturare, con la guida del docente, le prove del gioco (quesiti/compiti) in modo che il loro superamento possa attestare da parte del soggetto (o squadra) il possesso di una specifica competenza e relativo livello. Si richiede la redazione di almeno tre opzioni di risposta ai quesiti (vera, verosimile-non corretta, evidentemente non corretta) e l’indicazione di descrittori per la valutazione univoca dei task. Il ruolo di autore può essere altresì utilmente condiviso tra studenti-genitori-docenti. Terminata la fase di progettazione-redazione, gli **studenti-giocatori**, informati in modo critico su contenuti, obiettivi formativi e criteri di valutazione si mettono alla prova con il gioco da loro stessi implementato. L’attività di apprendimento ludico, secondo il modello sopra sinteticamente descritto, consente di realizzare **percorsi formativi personalizzati** (perché strettamente connessi al vissuto di chi apprende) e contrastare il rischio di **obsolescenza**. L’impiego di giochi con contenuti chiusi può risultare non ottimale se abbinato ad ambiti in continua evoluzione come la dimensione digitale (evoluzione degli strumenti, degli ambienti, delle dinamiche culturali-comunicative, delle normative, delle competenze stesse). È infine possibile ipotizzare la costruzione di ambienti *on*

line con la funzione di *repository* in cui raccogliere i quesiti e i task redatti, organizzati per target e competenze, intesi come *Learning Object* combinabili da parte degli autori. L'archiviazione organica di tali prove di conoscenza-competenza può essere, inoltre, intesa e letta come memoria collettiva del vissuto digitale dei soggetti in formazione relativamente ai bisogni formativi che essi hanno espresso.

4. Conclusioni

Formare nuovi cittadini digitali è renderli sicuri in rete con il possesso di competenze specifiche e sempre aggiornate. Perché i minori interiorizzino l'importanza della sicurezza nella dimensione digitale è **necessario che l'ambiente familiare e scolastico operino come modello positivo** di competenza, spirito critico, rispetto delle regole. Anche in tema di sicurezza digitale, pur con le difficoltà registrate e documentate, l'organizzazione scolastica non può prescindere dalla costruzione di una *partnership* forte con le famiglie per il benessere e la tutela dei minori. Allo scopo di favorire una prima conoscenza dei temi dell'*e-safety* potrebbero testarsi iniziative, analoghe a Happy Onlife, puntando su occasioni di intrattenimento educativo. Anche la scuola al proprio interno è chiamata ad un impegno costante di cooperazione da parte dell'intero *staff* per garantire la sicurezza digitale. L'organizzazione britannica Ofsted, operante nel settore degli standard nell'educazione e delle competenze, ha reso pubblico nel 2012 un manifesto che sintetizza in modo chiaro gli "elementi chiave" di *e-safety* per le istituzioni scolastiche. In breve la sicurezza connessa alla dimensione digitale nella scuola è presentata come l' impegno integrato di tutto il personale e la presenza di un sistema di regole e procedure ben definito. L'**obiettivo della sicurezza digitale è un obiettivo comune di tutti gli operatori della scuola** (personale docente e non docente); è prevista una puntuale attività di report con archiviazione delle segnalazioni; sono attivi percorsi didattici specifici rivolti a studenti ed operatori; sono predisposti, ed aggiornati frequentemente, regolamenti e procedure per l'uso di reti e strumenti; sono realizzati interventi costanti di monitoraggio e valutazione [Osfed, 2012]. **La sicurezza nella dimensione digitale è un processo continuo di apprendimento al saper essere e al saper fare** che è possibile realizzare sistematicamente ed attestare attraverso l'adozione di modelli di riferimento. La disponibilità di *framework* (DigCompOrg e DIGICOMP), predisposti dal Centro Comune di Ricerca della Commissione europea e frutto dell'integrazione di buone pratiche, interventi di esperti e *stakeholders,* costituisce una facilitazione. I *framework* europei agevolano il confronto nelle attività di studio, ricerca, aggiornamento in tema di apprendimento nell'era digitale e riconoscimento delle competenze (sia all'interno che all'esterno dei confini nazionali). **Per garantire l'e-*safety* è opportuno operare una scelta di cooperazione**: dall'attività all'interno delle scuole a cura di tutto il personale, alla partnership tra istituzioni scolastiche, studenti, famiglie, intera comunità, all'impegno alla reciproca tutela tra gli stessi minori, all'adozione di modelli di competenze riconosciuti in contesti il più possibile ampi.

Bibliografia

[Cameron-Curry et al, 2014] Cameron-Curry L.; Pozzi M.; Troia S.; Educare alla cittadinanza digitale, Tangram Edizioni Scientifiche, Trento, 2014.

[Censis e Polizia di Stato, 2016] Censis, Polizia di Stato, Verso un uso consapevole dei media digitali, Indagine sui dirigenti scolastici 2016 Estratto il 16/04/2016, da http://www.interno.gov.it/sites/default/files/allegati/indagine_censis_polizia_postale.pdf

[Chaudron et al, 2015] Chaudron S.; Di Gioia R. Gemo M.; Happy'Onlife!' Progetti ed attività per avviare e attrezzare bambini, docenti e genitori a una vita digitale piacevole, equilibrata e sicura, Ufficio delle pubblicazioni dell'Unione europea, 2015

[Di Gioia et al, 2016] Di Gioia, R., Gemo, M., Chaudron, S. (2016); Laboratorio Happy Onlife Rapporto post-evento; EUR 27698 IT; doi:10.2788/420548 (print); doi: 10.2788/632123 (online)

[Ferrari e Troia, 2015] Ferrari A., Troia S.; DIGCOMP Le competenze digitali per la cittadinanza. Estratto il 16/04/2016, da http://www.cittadinanzadigitale.eu/wp-content/uploads/2015/09/digcomp_Ferrari_Troia1.pdf.

[Ferrari et al, 2013] Ferrari A.; Punie Y.; Brecko B. N.; DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe, Publications Office of the European Union, Luxembourg, 2013.

[Kampylis, 2015] Kampylis, P., Punie, Y. & Devine, J. (2015); Promoting Effective Digital-Age Learning - A European Framework for Digitally-Competent Educational Organisations; EUR 27599 EN; doi:10.2791/54070

[Osfed, 2012] Osfed, Key features of e-safety in ‘good’ and ‘outstanding’ schools. Estratto il 16/04/2016, http://support.rm.com/_rmvirtual/Media/Downloads/OfstedLowdown.pdf

[Osservatorio per il contrasto della pedofilia e della pornografia minorile] Osservatorio per il contrasto della pedofilia e della pornografia minorile, Bullismo e cyberbullismo. Estratto il 19/04/2016, da http://www.osservatoriopedofilia.gov.it/dpo/it/bullismo_e_cyberbullismo.wpP

[Troia et al, 2014] Troia S.; Cameron-Curry L.; Pozzi M.; Dalla competenza digitale alla cittadinanza digitale: esperienze di apprendimento, DIDAMATICA 2014 Nuovi Processi e Paradigmi per la Didattica, Napoli, 2014, 867-876.