Istruzione e formazione delle competenze digitali come asset strategico

Cosimo Melella & Emilio Lo Giudice

Il cambiamento e il processo d'apprendimento sono aspetti fondamentali dell'agire umano e della sua psiche. Per porre le basi di una solida cyber hygiene *sarà necessario ripensare le attuali modalità di comunicazione e imparare a sfruttare i diversi mezzi disponibili. L'educazione agli strumenti informatici e alle sue dinamiche sociali va promossa a livello intergenerazionale, mutuando pratiche e metodologie improntate sul "paradigma di apprendimento" già attuate efficacemente da anni nella scuola primaria e secondaria. In quest'ottica sarà necessario adottare nuovi metodi didattici e nuovi ambienti di apprendimento, sia a livello giuridico che a livello organizzativo/istituzionale, coinvolgendo in particolare il mondo manageriale della Difesa e il comparto Sicurezza, anche attraverso brevi seminari dedicati al tema, migliorando le diverse* literacy *e approfondendo la questione dell'*information security*: persone, processi informatici e tecnologie devono correlarsi tra loro in modo armonioso per poter mantenere un ambiente sicuro.*

Il cambiamento e l'apprendimento sono aspetti fondamentali dell'agire e della psiche umana e per tenere il passo delle dinamiche socioculturali bisogna valorizzare il capitale umano, *asset* strategico per ogni Paese, investendo in istruzione, formazione, ricerca e cultura.

Il Parlamento Europeo e il Consiglio dell'Unione Europea con la Raccomandazione del 18 dicembre 2006[1] hanno definito il quadro normativo dei principi base per un'educazione permanente degli individui, la formazione del soggetto competente, il ruolo della competitività e dell'imprenditorialità. Da parte sua, l'Italia ha recepito le indicazioni europee sul piano della didattica, nel D.P.R. n° 89 del 15 marzo 2010 e col Piano triennale dell'offerta formativa[2].

[1] GUUE 30/12/2006 L 394/10.

[2] GU 15/03/2010 n.89; GU l.14/07/2015 n.107.

Citando Sicurello, "Non basta certo essere nativi digitali per essere anche consapevoli digitali. [...] [Bisogna] cercare di porre le basi per la stimolazione di momenti metacognitivi atti a motivare riflessioni sulle azioni compiute nell'uso dei new media che [...] non sono così spontanee"[3].

Il Piano Nazionale Scuola Digitale (PNSD)[4], sulla consapevolezza delle competenze digitali che i giovani devono avere per una "cittadinanza digitale", dichiara: "Tra le classi di "base" […] che costituiscono l'alfabetizzazione civica del cittadino digitale prevediamo [...]: i diritti della rete, a partire dalla Dichiarazione per i Diritti in Internet redatta dalla Commissione per i diritti e i doveri relativi a Internet della Camera dei Deputati; l'educazione ai media e alle dinamiche sociali online (social network); la qualità, integrità e circolazione dell'informazione (attendibilità delle fonti, diritti e doveri nella circolazione delle opere creative, privacy e protezione dei dati, information literacy)"[5].

Mentre i giovani a scuola imparano a riflettere in modo metacognitivo sugli strumenti digitali, gli adulti danno per scontato questo aspetto, rivelandosi impreparati[6]: l'educazione agli strumenti informatici e alle sue dinamiche andrebbe invece insegnata a tutte le generazioni. Si tratta di adottare pratiche e metodologie didattiche già attuate da anni nella scuola primaria e secondaria basate sul "paradigma di apprendimento" anziché sull'obsoleto "paradigma d'insegnamento"[7]. L'attuale formazione digitale è appresa incidentalmente, ma non è sufficiente saper usare un computer: serve uno studio intenzionale per ottenere conoscenze organizzate ed efficienti. Questo perché il principio dell'"economia cognitiva"[8] secondo cui si usano concetti prototipici per essere

[3] Sicurello, R., *Un percorso di media education nella scuola secondaria*, Media Education – Studi, ricerche, buone pratiche, 7, n. 1, 2016: pp 94-115.

[4] Ibidem nota 2.

[5] Piano nazionale scuola digitale, documento d'indirizzo, Ministero dell'Istruzione, dell'Università e della Ricerca, https://www.miur.gov.it/scuola-digitale.

[6] Ibidem nota 5.

[7] Belsito, F. & Milito, F. *Progettare e valutare nella scuola delle competenze*. Roma: Anicia, 2016.

[8] L'economia cognitiva mira a ribaltare l'assetto metodologico dell'economia neoclassica analizzando i processi attraverso i quali si formano preferenze e decisioni. Per approfondire Innocenti, A., *L'Economia Cognitiva*, Roma, Carocci, 2009.

più efficienti non funziona in quanto l'uso consapevole del digitale non è intuitivo[9].

Vanno dunque adottati nuovi metodi didattici e nuovi ambienti di apprendimento sia a livello amministrativo/giuridico che a livello organizzativo/istituzionale. Le competenze digitali richieste dalla società contemporanea sono state indicate come obiettivo europeo nella Strategia di Lisbona[10] e identificate nella Raccomandazione del 2006[11], secondo cui la competenza digitale consiste nell'uso consapevole e critico delle "tecnologie della società dell'informazione" e nel possesso di abilità nelle "tecnologie dell'informazione e della comunicazione"[12]. In particolare, le otto competenze di cittadinanza con funzione strategica sono: comunicazione nella madrelingua; comunicazione nelle lingue straniere; competenza in scienze matematiche e tecnologia; competenza digitale; "imparare ad imparare"; competenze sociali e civiche; spirito d'iniziativa e imprenditorialità; consapevolezza ed espressione culturale[13]. L'Italia ha recepito le indicazioni europee nel PNSD del 2007 e in quello del 2015[14], ma la strada è ancora lunga: andare oltre l'alfabetizzazione digitale è una questione soprattutto culturale, e richiede abilità tecniche e cognitive come la *media literacy* o la *information literacy*[15].

Per promuovere il capitale umano e avviare un processo di apprendimento autonomo delle competenze digitali bisogna usare diversi metodi (ad es. il metodo della

---

[9] Sicurello, R. *Un percorso di media education nella scuola secondaria, Media Education – Studi, ricerche, buone pratiche,* 7, n. 1, 2016: pp 94-115.

[10] Dagli atti del Consiglio Europeo straordinario, Lisbona, 23-24/03/2000, https://archivio.pubblica.istruzione.it/buongiorno_europa/allegati/lisbona2000.pdf.

[11] Ibidem nota 1.

[12] Bonazza, V. *Programmare e valutare l'intervento didattico. Fondamenti epistemologici*, Napoli, Guida Editore 2021.

[13] Ibidem nota 11.

[14] Ibidem nota 5.

[15] La *media literacy* definisce la capacità di interpretare criticamente testi multimediali, mentre per *infomation literacy* s'intende saper scegliere e utilizzare le tecnologie per reperire, analizzare, elaborare informazioni.

ricerca-azione[16] o il *cooperative learning*[17]) ed educare gli individui alla *digital literacy*, o alfabetizzazione digitale, ed alla *information security*[18] in ambito scolastico, negli ambienti della ricerca scientifica, come le università e gli enti pubblici preposti[19] e in quelli militari, sfruttando l'attuale percorso di formazione per la fascia dirigenziale degli ufficiali e sottoufficiali del settore Difesa[20].

Nel 2001 l'*Educational Testing Service* (ETS) negli Stati Uniti ha pubblicato un report[21] che definisce la *digital literacy* come la capacità di usare correttamente abilità e competenze informatiche per gestire e valutare informazioni, sviluppare e creare contenuti e comunicare efficacemente. Questo concetto include quelli di *information technology literacy*, *information literacy*, *visual literacy*, *media literacy* e *network literacy*: nozioni che richiedono una combinazione tra competenze e abilità di vario tipo: tecniche, cognitive/metacognitive, etiche e sociali[22].

Occorre migliorare le diverse *literacy*: la *ICT literacy*, ossia l'uso di *hardware* e *software*; la *internet literacy*, ossia l'uso consapevole della connettività, della sicurezza e della comunicazione (compresi i *personal device*); la *media literacy*, ossia la capacità di analizzare i messaggi "prodotti negli e dagli ambienti caratteristici dei diversi media" [23]. Legata all'*internet literacy* è la questione dell'*information security*: persone, processi

---

[16] La ricerca-azione è alla base di un metodo didattico di "progettazione partecipata" che stimola processi di negoziazione e dinamiche relazionali.

[17] Si tratta di un approccio che permette di sviluppare competenze di tipo cognitivo, operativo e relazionale.

[18] La totalità dei processi, dei mezzi e delle tecnologie volti a proteggere i sistemi informatici in termini di disponibilità, confidenzialità e integrità.

[19] Ad esempio: il Consiglio nazionale per la ricerca (CNR), l'Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA), l'Istituto nazionale di fisica nucleare (INFN) o l'Istituto nazionale di astrofisica (INAF).

[20] Ministero dell'Istruzione, dell'Università e della Ricerca, *Rapporto di approfondimento tematico. Scuola e società dell'Informazione*, 2015.

[21] International ICT Literacy Panel, *Digital Trasformation. A framework for ITC Literacy*, Princeton, New Jersey (U.S.A.), 2002.

[22] Parola, A. *Ricerca-azione e competenze mediali*. In Ricercazione, 6, n. 2, 2014.

[23] Ibidem nota 21.

informatici e tecnologie devono correlarsi tra loro per mantenere un ambiente sicuro. In particolare, il fattore umano è cruciale: la tecnologia sarà sempre inadeguata se questo aspetto viene trascurato. Invece l'essere umano, da anello debole nella catena della sicurezza, può diventare un *asset* strategico grazie ad un'adeguata educazione alla *internet literacy*. La sicurezza richiede quattro aspetti: formazione continua del personale; promozione di una cultura di consapevolezza; implementazione del modello *Zero Trust*[24]; uso adeguato delle *patch* e periodici aggiornamenti dei sistemi[25].

Per una solida *cyber hygiene* bisogna ripensare le modalità di comunicazione imparando a sfruttare i vari mezzi disponibili e ad applicare corretti protocolli di sicurezza e *patch*, pena possibili attacchi informatici[26]. Per far ciò serve un approccio proattivo integrato, come quello del modello di sicurezza informatica *Zero Trust,* che evidenzia la necessità di una corretta gestione delle identità. In passato, le organizzazioni erano concentrate solo sulla protezione e la difesa del perimetro: semplificando, sussisteva la convinzione che bastasse un antivirus efficacie per mantenere al sicuro i dati, senza prendere in considerazione che i *breach* potessero venire dall'interno[27].

Un esempio di minaccia interna è il comportamento suscettibile ad attacchi d'ingegneria sociale: per violare il perimetro od ottenere informazioni si fa leva sulla psicologia e sui comportamenti degli individui inducendoli a credere ad azioni ingannevoli, distrattive o comunque non autorizzate, avallando processi illeciti. Il modello *Zero Trust*, con accesso consentito solo con credenziali tecniche e fisiche adeguate risulterebbe efficace. Sarebbe dunque opportuno sviluppare protocolli con lo scopo di educare i dipendenti a proteggersi da attacchi d'ingegneria sociale. Infatti, nonostante gli individui sappiano

[24] Lo *Zero Trust* sostiene che non si debbano fornire facili accessi a informazioni all'interno o all'esterno del perimetro.

[25] Deluigi, R. *Interculturalità e formazione professionale: elementi di formazione e prospettive di ricerca*. In Deluigi R. (Ed.), *Formazione professionale e intercultura. Sfide pedagogiche tra pratica e riflessività* Milano, 2013.

[26] Rubinoff S.*, Cyber Minds: Insights on cybersecurity across the cloud, data artificial intelligence, blockchain, and IoT to keep you cyber safe,* Birmingham, 2020.

[27] Il caso Stuxnet è esemplificativo: B. Buchanan, The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics, Harvard University Press, 2020.

che certi comportamenti sono rischiosi, sottovalutano le conseguenze delle proprie azioni sopravvalutando le difese[28].

Per ridurre i rischi, rigorosi protocolli dovrebbero richiedere la cancellazione delle informazioni dopo il loro uso: infatti, quando diventano obsolete o non più significative per un dipendente, il livello di discrezione e l'attenzione diminuisce, ma rimarrebbero comunque preziose per un *threat actor* che le sfrutterebbe per ottenere la fiducia di altri utenti e avere accesso al perimetro. Il comportamento ignaro è facile da risolvere: educando gli individui a un'interdipendenza positiva e una responsabilità condivisa e cambiando comportamento, qualora avvenisse l'attacco, le persone lavoreranno in squadra per ridurre i danni.

Nessuno pensa di essere un *target,* ma i *threat actors* cercano di carpire più informazioni possibili da chiunque, così da poter sfruttare i dati in seguito. Molti non si rendono conto che i *social media* sono uno dei più grandi canali per violazione delle informazioni, tentativi di *phishing* e attacchi d'ingegneria sociale: un loro uso sconsiderato mina inevitabilmente la sicurezza informatica. Educare, quindi, all'*internet literacy* e alla *cyber mindfulness* è una tappa essenziale nel *long run* per un efficace investimento strategico del capitale umano.

COSIMO MELELLA ha conseguito una laurea magistrale in Giurisprudenza presso l'Università Bocconi, una seconda laurea magistrale in Scienze Politiche di Governo (focus su politiche pubbliche) e un Master di II livello in Cybersecurity presso l'Università degli Studi di Milano. Ha frequentato corsi specialistici presso il NATO CCDCOE ed è certificato Cisco. Attualmente, è ricercatore presso ITSTIME, cultore della materia in comunicazione e informazioni per la sicurezza presso l'Università Cattolica del Sacro Cuore ed è segretario di Socint (Società Italiana d'intelligence) in Lombardia.

---

[28] Rains T., *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*, Birmingham, 2020.

EMILIO LO GIUDICE ha una laurea magistrale in economia al DES presso l'Università Bocconi, ha frequentato sceneggiatura presso la Scuola Civica di Cinema di Milano e ha conseguito un Master di I livello in Metodologie Didattiche, Psicologiche, Antropologiche e Teoria e Metodi di Progettazione. Da sempre nel mondo della formazione, è contributor per Aleph-Analisi Strategiche, è stato speaker in una web radio, si è occupato di scrittura creativa e ha ricoperto il ruolo di Direttore Editoriale di un bimestrale.
