Curriculum sulla Protezione dei Dati

Università Pedagogica di Friburgo

Gennaio 2025

Lucie Brzáková, Deborah Krzyzowski, con Bernd Remmele e Zlatko Valentic

Co-funded by the European Union

Finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia Esecutiva per l'Istruzione e la Cultura (EACEA). Né l'Unione Europea né l'EACEA possono esserne ritenute responsabili.

Indice dei contenuti

1. Introduzione..... 3
2. Competenze in primo piano nel progetto DataPro.....4
3. Descrizione delle competenze.....5
3.1 I dati come bene di valore..... 6
3.2 La privacy come diritto umano.....8
3.3 Misure di protezione dei dati..... 11
4. Relazioni tra le competenze..... 13
5. Risultati di apprendimento più ampi.....15
6. Conclusioni per gli educatori.....16

1. Introduzione

Le tecnologie digitali pervadono ogni aspetto della nostra vita privata e pubblica e la capitalizzazione delle informazioni personali online ha reso la privacy un bene prezioso - per le aziende, il governo e gli individui[1]. La protezione dei dati personali tramite l'applicazione dei principi di minimizzazione dei dati e di misure di protezione dei dati è una preoccupazione cruciale.

DataPro è un progetto co-finanziato dal Programma Erasmus Plus dell'Unione Europea che riconosce la necessità di far comprendere ai giovani cittadini il valore dei loro dati, i loro diritti alla privacy e le misure di protezione dei dati. Nei tre anni di durata del progetto, i partner transdisciplinari svilupperanno strumenti di apprendimento sulla protezione dei dati per gli studenti. Il programma di studi approfondirà le tre aree menzionate riguardanti l'uso e la protezione dei dati, e consentirà ad insegnanti e partner di progetto di comprendere i concetti resi operativi negli strumenti educativi.

L'obiettivo più ampio del progetto DataPro è quindi quello di supportare gli insegnanti con un quadro educativo completo che aiuti gli studenti a diventare agenti digitali attivi e autonomi. La sensibilizzazione degli studenti sul valore dei loro dati come bene e sul valore della loro privacy per la democrazia sono le intenzioni alla base dell'insegnamento dei metodi di protezione dei dati. Educando gli studenti sulla natura multiforme dell'uso dei dati e sull'importanza critica della protezione delle informazioni personali, DataPro cerca di costruire una cittadinanza ben informata, in grado di sostenere e difendere i propri diritti riguardanti i dati personali.

Questo Curriculum stabilisce obiettivi di apprendimento specifici. Questi obiettivi devono essere raggiunti tramite una serie di competenze che migliorano la comprensione da parte degli studenti delle complessità della protezione dei dati e il riconoscimento della privacy come questione relativa ai diritti umani. Attraverso un approccio strutturato che prevede la raccolta, l'adattamento e lo sviluppo di strumenti di apprendimento innovativi, DataPro intende integrare conoscenze teoriche e comprensione pratica. Questa iniziativa non solo si concentra sulla diffusione di queste

[1] Si veda il concetto di "capitalismo di sorveglianza" in Zuboff, S. (2018) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Zuboff, Shoshana*. Disponibile all'indirizzo: http://archive.org/details/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019 (Accesso: 10 gennaio 2025).

risorse tra le scuole e gli attori del mondo dell'istruzione, ma sottolinea anche l'integrazione delle preoccupazioni e dei *feedback* di studenti e insegnanti. Un altro vantaggio degli strumenti di apprendimento è il loro compito di incoraggiamento degli studenti a diventare agenti digitali. Come agenti digitali, infatti, essi diventerebbero in grado di identificare e proteggersi dalle minacce digitali, quali, ad esempio, false influenze provenienti dalla disinformazione digitale, o attacchi coordinati ai dati che utilizzano tattiche di *social engineering*. Il Curriculum prende in considerazione anche ostacoli all'apprendimento già studiati in precedenza, come l'effetto desensibilizzante dell'uso quotidiano di Internet sulla privacy online[2]. Sulla base dell'attuale versione inglese del Curriculum, i suoi syllabi saranno tradotti per i gruppi target dei rispettivi Paesi partecipanti.

Integrando questo programma di studio nei contesti educativi, prevediamo di coltivare una generazione che non solo sia consapevole dell'importanza della protezione dei dati, ma anche esperta nell'implementazione delle migliori pratiche. Queste conoscenze fondamentali dovrebbero favorire l'atteggiamento sociale degli studenti nei confronti della protezione dei dati e dei diritti alla privacy, per lo sviluppo di cittadini digitali informati e responsabili.

2. Competenze in primo piano nel progetto DataPro

Il Curriculum sulla Protezione dei Dati informa gli insegnanti e i partner di progetto sulle conoscenze essenziali di cui i giovani cittadini hanno bisogno per navigare nelle complessità della protezione dei dati. La domanda centrale del progetto riguarda le competenze di cui gli studenti hanno bisogno per affrontare in modo sicuro le sfide digitali. I giovani crescono in un ambiente in cui i dati svolgono un ruolo centrale, sia attraverso i social media, che nell'apprendimento online o con la comunicazione digitale. Tuttavia, molti non sono consapevoli dei rischi e dei diritti associati all'uso delle tecnologie digitali. Il progetto DataPro mira a sviluppare strumenti di apprendimento ludici e creativi che consentano agli studenti di sviluppare meccanismi di gestione sicura dei propri dati.

Come introdotto nel capitolo introduttivo precedente, le aree di competenza previste si basano innanzitutto sulla conoscenza dei dati come bene di valore; comprendono i meccanismi di

[2] Krzyzowski, D. (2024) *Relazione sull'analisi quantitativa dei dati delle indagini*. Friburgo: Università Pedagogica di Friburgo, pagg. 21-23.

elaborazione dei dati, la capitalizzazione delle informazioni personali online, i sistemi di raccomandazione algoritmica e le inferenze tratte dal comportamento online, per citarne solo alcuni aspetti. Nella prossima sezione, il Curriculum presenta uno schema completo che contestualizza le implicazioni dei dati come bene per gli individui e la società. Dato che i dati sono il bene in questione, lo schema include anche le competenze rilevanti che gli studenti devono acquisire per proteggere con successo i propri dati online.

Il Curriculum si orienta sul Quadro DigComp[3] , mentre nel suo sviluppo sono stati implementati diversi cicli di *feedback* con i professionisti dell'istruzione. Sono stati raccolti consigli e suggerimenti dai membri del consorzio, dagli esperti di protezione dei dati e soprattutto dagli insegnanti. Questo dovrebbe garantire l'adeguatezza degli strumenti educativi per il gruppo target, ovvero gli studenti della scuola secondaria.

Il punto di partenza del Curriculum è gettare luce sul valore economico nascosto dei dati personali. Partendo da questa premessa cruciale, si sottolinea l'importanza dei diritti alla privacy per democrazie sane, e della protezione dei dati per l'autonomia individuale dei cittadini di tali società. Il Curriculum integra le tre aree tematiche per garantire che gli studenti acquisiscano le competenze necessarie per proteggere la propria privacy e agire in modo responsabile nello spazio digitale. Le dinamiche interconnesse tra questi temi della protezione dei dati saranno spiegate nella Sezione 4 del presente documento, con l'aiuto della visualizzazione in una Matrice delle Competenze (*Figura 1*).

3. Descrizione delle competenze

Le competenze DataPro sono strutturate in tre aree tematiche che coprono le diverse implicazioni dei dati digitali:

1. **I dati come bene di valore**: il "Cosa?" alla base del progetto. L'oggetto della protezione sono i dati personali online, che vengono commercializzati e gestiti come un bene scambiabile dai fornitori di servizi online e dalle piattaforme online.

[3] EU Science Hub e Commissione Europea (2022) *Quadro DigComp*. Disponibile all'indirizzo: https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en

2. **La privacy come diritto umano**: il "Perché" del progetto. Si tratta dell'importanza sociale di tutelare il bene in questione, a causa del ruolo vitale che la privacy individuale svolge per l'esercizio dei diritti fondamentali nelle democrazie.

3. **Protezione dei dati**: il "Come" del progetto. Dopo una sensibilizzazione orientata all'utente sui temi della capitalizzazione dei dati e della privacy online, si possono introdurre misure pratiche per la protezione dei dati degli studenti. Queste misure sono strumenti per una maggiore autonomia online e per l'autoefficacia nell'esercizio dei propri diritti.

Le competenze specifiche necessarie per navigare in questi gruppi di argomenti interconnessi sono trattate nella prossima sezione.

3.1 I dati come bene di valore

Il concetto di dati intesi come “bene di valore" è la premessa alla base della pressante importanza dell'educazione alla protezione dei dati. La privacy è un punto di dibattito politico da quando i governi e la stampa hanno iniziato a documentare le informazioni sui loro cittadini[4], ma la pubblicità algoritmica e la raccolta di dati per le compagnie assicurative hanno reso i dati una vera e propria moneta di scambio per servizi online gratuiti. DataPro cerca di spiegare questi meccanismi dell'industria dei dati, per incoraggiare gli studenti a trarre vantaggio dal valore dei loro dati. Il riconoscimento del valore economico dei dati è possibile quando gli studenti acquisiscono le seguenti competenze:

Competenze Cluster A	Misure pratiche
A.1 **Tradurre i dati in risorse**	***Trattare i dati come una valuta online*** Comprendere il valore dei propri dati personali, nella stessa maniera in cui si valuta il denaro. Ciò significa riconoscere quando e quali dati vengono elaborati dai servizi online, capire come i dati personali possono essere monetizzati, conoscere i rischi dello sfruttamento dei dati personali e prendere decisioni informate sulla condivisione dei propri dati.

[4] Per lo sviluppo storico del discorso sui diritti alla privacy, si veda Warren, S.D. e Brandeis, L.D. (1890), "The Right to Privacy", *Harvard Law Review*, 4(5), pp. 193-220. Disponibile all'indirizzo: https://doi.org/10.2307/1321160

	Consapevolezza della monetizzazione Conoscere i principali modi in cui le aziende traggono profitto dai dati personali e aggregati, ad esempio attraverso le piattaforme pubblicitarie e il miglioramento della pubblicità mirata (compresi gli annunci di stampo politico e di propaganda). Sapere che molti servizi di comunicazione gratuiti (come i social media) e contenuti online sono pagati dalla pubblicità o dalla vendita dei dati degli utenti. Questo modello economico si basa sulla monetizzazione dei dati personali.
A.2 **Distinguere i rischi di sicurezza della condivisione dei dati**	***Condivisione pubblica*** Sapere che tutto ciò che viene condiviso pubblicamente online (ad esempio, immagini, video, suoni) può essere utilizzato per addestrare i sistemi di intelligenza artificiale, che possono includere funzioni di tracciamento indesiderate. Bisogna essere cauti nell'individuare la portata della nostra condivisione di dati pubblici. ***Pratica di minimizzazione dei dati*** Mettere regolarmente in discussione la necessità di conservare e condividere i dati personali. Adottare pratiche come fornire solo le informazioni essenziali, e utilizzare indirizzi e-mail o numeri di telefono usa e getta, quando opportuno. ***Misure di sicurezza*** Essere consapevoli dei comuni attacchi di ingegneria sociale (phishing) attraverso vari canali di comunicazione, per prevenire l'acquisizione fraudolenta di beni (digitali).
A.3	***Valutazione critica***

Valutare le intenzioni alla base della monetizzazione dei dati	Chiedersi regolarmente chi c'è dietro le informazioni che si trovano su Internet, soprattutto sui social media. Identificare chi potrebbe avere interesse a creare camere d'eco (bolle). ***Consapevolezza della qualità*** Capire che la disinformazione può essere molto convincente, soprattutto con l'uso di tecnologie avanzate come l'IA, che possono creare visualizzazioni sofisticate. Mettere sempre in dubbio la qualità e la fonte delle informazioni.
A.4 Consapevolezza del controllo del comportamento	***Consapevolezza del meccanismo*** Sapere che molte piattaforme digitali utilizzano tattiche psicologiche come il *nudging*, la *gamification* e la manipolazione per influenzare il comportamento degli utenti. Riconoscere queste tattiche per evitare di essere indebitamente influenzati. Riconoscere che i modelli di utilizzo e i dispositivi connessi possono essere utilizzati per ottimizzare i servizi online e la pubblicità mirata. Ciò comporta il tracciamento del comportamento degli utenti per offrire contenuti personalizzati. ***Misure di controllo*** Imparare le strategie per controllare e limitare la portata del tracciamento comportamentale, ad esempio regolando le impostazioni sulla privacy e utilizzando tecnologie che migliorano la privacy. Sviluppare strategie per diminuire queste influenze, come la definizione di limiti personali di utilizzo e la valutazione critica dei contenuti consumati.

3.2 La privacy come diritto umano

Dal punto di vista dell'educazione generale, la dimensione della "privacy come diritto umano" sottolinea l'importanza della vita privata e dell'autodeterminazione informativa sia per gli individui che per le democrazie. La *Dichiarazione Universale dei Diritti Umani* protegge la "privacy, la

famiglia, la casa o la corrispondenza" di ogni individuo da qualsiasi tipo di "interferenza arbitraria"[5] . Come esempio negativo, questi diritti sono gravemente violati dall'uso illegittimo di *spyware* da parte dei governi, come ha confermato il caso *Pegasus*[6] . LIl concetto di privacy come diritto umano aiuta gli studenti a contestualizzare la propria privacy online all'interno della loro vita di membri di una democrazia (europea). Lo status speciale della privacy e una vita privata protetta da interferenze statali e aziendali dovrebbero anche far riflettere sul valore dell'autonomia individuale per l'intera società. La privacy è quindi un pilastro fondamentale per altri valori della democrazia, come la libertà di espressione e l'autodeterminazione informativa. Solo in assenza di controllo, sia esso da parte del governo, delle istituzioni o dei poteri del settore privato, gli individui possono formarsi opinioni autonome ed esprimerle in un discorso democratico. La privacy può quindi essere concettualizzata come l'assenza di conoscenze registrabili sull'individuo, uno status in cui l'individuo può sperimentare l'oscurità del proprio sé da parte di funzionari e autorità .[7]

Competenze Cluster B	**Misure pratiche**
B.1 **Comprendere l'ambito delle libertà**	***Riconoscere la libertà*** Riconoscere l'importanza della privacy per la nostra libertà. Proteggendo la nostra privacy, salvaguardiamo la nostra capacità di esprimere liberamente le nostre opinioni e di vivere senza inutili interferenze. Dobbiamo essere consapevoli che quando gli altri possono osservare o controllare il nostro comportamento, la nostra libertà personale può essere a rischio.
B.2 **Comprendere l'autodeterminazione**	***Controllo dei dati***

[5] Si veda l'articolo 12 della *Dichiarazione Universale dei Diritti dell'Uomo* delle Nazioni Unite (1948). Nazioni Unite. Disponibile all'indirizzo: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[6] Assemblea Generale delle Nazioni Unite (2022) *Il diritto alla privacy nell'era digitale*. Rapporto dell'Ufficio dell'Alto Commissario delle Nazioni Unite per i Diritti Umani* A/HRC/51/17. Consiglio dei Diritti Umani, pag. 2. Disponibile all'indirizzo: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf

[7] Confronta la concettualizzazione della privacy come oscurità in Selinger, E. e Hartzog, W. (2016) "Obscurity and Privacy", *Spaces for the Future: A Companion to Philosophy of Technology* [Preprint]. Disponibile all'indirizzo: https://scholarship.law.bu.edu/faculty_scholarship/3099

	Ricordare che abbiamo il diritto di controllare quali dati che ci riguardano vengono raccolti, elaborati e utilizzati. L'esercizio di questo diritto ci aiuta a mantenere la nostra autonomia personale e a gestire la nostra identità digitale. ***Protezione dell'automazione*** Essere consapevoli che la protezione dei dati include il diritto di non essere sottoposti a processi decisionali completamente automatizzati, che possono avere un impatto significativo sulle persone. ***Prevenzione dell'abuso*** La protezione dei dati personali aiuta a difendersi dalla sorveglianza indesiderata, dal furto di identità, dalla discriminazione e da altre forme di abuso dei dati personali. Essere consapevoli dei comuni attacchi di ingegneria sociale (phishing) attraverso vari canali di comunicazione, per prevenire l'acquisizione fraudolenta di beni (digitali).
B.3 **Conoscenza dei diritti della privacy (GDPR)**	***Diritti dei dati e necessità del consenso*** Conoscere i propri diritti nei confronti delle aziende che utilizzano i nostri dati, tra cui il diritto di accedere ai dati in nostro possesso, di rettificare le inesattezze, di cancellare i dati (diritto all'oblio), e di presentare reclami alle autorità. Comprendere che in genere le aziende devono ottenere il nostro consenso per trattare i nostri dati personali. Valutare regolarmente se è necessario dare tale consenso. ***Valutazione del consenso*** Valutare frequentemente la necessità di dare il consenso all'utilizzo dei dati per garantire che le informazioni personali non vengano sfruttate inutilmente.

B.4 **Consapevolezza dei diritti umani**	***Responsabilità digitale*** Essere consapevoli della propria responsabilità di salvaguardare la dignità umana, la libertà, la democrazia e l'uguaglianza quando si agisce su Internet. Ciò implica il rispetto della privacy e dei diritti dei dati degli altri e la difesa di pratiche responsabili in materia di dati.
B.5 **Valutare i rischi per la privacy individuale**	***Livelli di rischio*** Comprendere che esistono vari livelli di rischio per la privacy, associati a diverse pratiche di trattamento dei dati. Alcuni processi di trattamento dei dati, in particolare quelli che coinvolgono l'intelligenza artificiale, comportano rischi maggiori. ***Rischi dell'Intelligenza Artificiale*** Essere consapevoli che i processi e i servizi basati sull'intelligenza artificiale possono comportare diversi livelli di rischio per la privacy, spesso a causa della loro capacità di elaborare grandi quantità di dati e di dedurre informazioni sensibili.
B.6 **Valutare il potenziale di Internet**	***Riconoscere la dualità di Internet*** Bisogna essere consapevoli che Internet crea nuove opportunità di partecipazione alla società per i gruppi vulnerabili, ma può anche contribuire all'isolamento di coloro che non lo utilizzano.
B.7 **Verifica delle politiche sulla privacy**	***Valutazione delle politiche*** Sviluppare la capacità di esaminare e valutare in modo critico le politiche sulla privacy di app e servizi. Questo include la comprensione di quali dati vengono raccolti, di come vengono utilizzati e dei diritti che abbiamo sui nostri dati.

3.3 Misure di protezione dei dati

Proteggere i dati è l'obiettivo generale di apprendimento del Curriculum. Questa dimensione si basa sulla comprensione dei cluster tematici 1: I dati come bene di vaore, e 2: La privacy come

diritto umano. Le competenze del gruppo 3 si riferiscono alle misure pratiche di protezione dei dati e di sicurezza informatica che gli individui possono adottare quotidianamente.

Cluster di competenze C	Misure pratiche
C.1 **Gestione dell'identità**	***Consapevolezza dell'uso*** Interrogarsi regolarmente su come e dove utilizzare e condividere in modo sicuro le informazioni di identificazione personale. Comprendere i rischi associati alla condivisione dei dati personali. ***Misure di anonimato*** Utilizzare misure per nascondere la propria identità online, come VPN, strumenti di comunicazione criptati, e browser incentrati sulla privacy.
C.2 **Garantire la sicurezza dei dati**	***Misure di sicurezza*** Impiegare pratiche di sicurezza standard, come l'uso di password diverse e sicure per diversi servizi online, l'attivazione dell'autenticazione a più fattori, l'uso di strumenti biometrici, l'esecuzione di aggiornamenti software regolari, e l'installazione di software di protezione. ***Identificazione sicura*** Imparare a proteggere la propria identificazione elettronica con metodi come password forti e uniche e l'autenticazione a due fattori.
C.3 **Esaminare la tracciabilità online**	***Gestione della tracciabilità*** Implementare misure per limitare e gestire il tracciamento delle proprie attività su Internet, compreso l'uso di estensioni del browser che bloccano tracker e cookie. ***Controlli sulla comunicazione*** Conoscere e utilizzare le misure per non ricevere più messaggi o e-mail indesiderate, come i filtri antispam e le regole di posta elettronica.
C.4	***Controllo delle fonti***

Convalida delle informazioni	Essere pronti a consultare più fonti per verificare le informazioni. Questo aiuta a riconoscere e comprendere i diversi punti di vista o i pregiudizi che si celano dietro determinate informazioni e fonti di dati. ***Riconoscimento dei pregiudizi*** Imparare a identificare i potenziali pregiudizi nelle informazioni, comprendendo che ogni fonte di dati può avere un pregiudizio intrinseco basato sulla sua origine o sul suo scopo.
C.5 **Protezione reciproca dei dati**	***Considerazioni sulla condivisione dei dati*** Chiedere regolarmente se le informazioni di identificazione personale degli altri vengono condivise, e se possono essere utilizzate in modo improprio. ***Consapevolezza legale*** Sapere che la condivisione di informazioni su altre persone può avere gravi conseguenze legali. Chiedere sempre il consenso prima di condividere i dati personali di qualcun altro.

4. Relazioni tra le competenze

Le competenze necessarie per un uso autodeterminato e responsabile dei servizi online possono essere suddivise nei tre gruppi di argomenti presentati. I cluster sono interdipendenti. I *dati come bene di valore* e la *privacy come diritto umano* si sovrappongono nel soppesare gli interessi (legittimi) delle aziende che utilizzano i dati rispetto alla privacy. Il Curriculum affronta il tema dell'equilibrio tra gli interessi delle aziende nell'utilizzo dei dati e i diritti individuali alla privacy. Ciò aiuterà gli studenti a comprendere le implicazioni più ampie dell'economia dei dati, come le asimmetrie informative e gli squilibri di potere tra la società, le aziende e lo Stato.[8]

Le *misure di protezione dei dati* e la *privacy come diritto umano* si sovrappongono nella pragmatica di come proteggere i dati individuali tenendo conto dei diritti alla privacy degli altri. Ciò significa che il Curriculum non solo prevede di insegnare agli individui come salvaguardare i propri dati, ma

[8] Si veda ad esempio van de Waerdt, P.J. (2020) "Information asymmetries: recognizing the limits of the GDPR on the data-driven market", *Computer Law & Security Review*, 38, pag. 105436. Disponibile all'indirizzo: https://doi.org/10.1016/j.clsr.2020.105436

anche di instillare il rispetto per la privacy degli altri. La pratica reciproca dell'attenzione ai dati personali concettualizza la privacy come un bene interdipendente nelle democrazie, piuttosto che come una semplice preferenza personale. Il riconoscimento dell'interdipendenza aiuta gli studenti a capire che la mancata cura della propria privacy porta anche a un'erosione del diritto alla privacy nella società in generale, e che il mantenimento della privacy online per se stessi e per gli altri rafforza la democrazia.

La tautologia è completata dalla relazione tra le *misure di protezione dei dati* e i *dati come bene di valore*. Queste dimensioni si sovrappongono nella pragmatica di come utilizzare i propri dati alla luce delle asimmetrie informative. Questa intersezione si concentra sulle competenze pratiche necessarie per gestire e sfruttare i dati personali in modo responsabile ed efficace in vari contesti.

Le dinamiche e le interdipendenze tra le dimensioni dell'educazione alla protezione dei dati sono visualizzate nella seguente Matrice delle Competenze (*Figura 1*). Il Curriculum non discrimina l'importanza delle competenze di una dimensione rispetto a quelle di un'altra. Ogni competenza e la sua interazione con altre competenze sono considerate ugualmente fondamentali per l'autoefficacia e la libertà degli individui in una società dell'informazione. Queste competenze essenziali e la comprensione delle tre dimensioni della protezione dei dati
sono ritenute necessarie per navigare in un mondo digitalmente interconnesso in modo efficace e responsabile.

Figura 1: **Matrice delle competenze.** Il diagramma mostra i tre gruppi di argomenti ("I dati come bene di valore", "La privacy come diritto umano" e "Le misure di protezione dei dati") che formano un triangolo. Al centro si trova l'obiettivo generale, "Cittadinanza digitale informata", collegato a tutte le dimensioni per indicare la sua integrazione e la dipendenza dalla loro interazione.

5. Risultati di apprendimento più ampi

Tra gli obiettivi generali dell'educare gli studenti a prendere decisioni informate come cittadini digitali, un risultato di apprendimento indiretto dovrebbe essere il riconoscimento di comportamenti malevoli online. Questi potrebbero includere gli attacchi alla sicurezza informatica, come il phishing o il ransomware. Inoltre, gli attacchi alla libertà democratica e alla libertà di espressione potrebbero essere più difficili da distinguere, come nel caso delle campagne di disinformazione. Tali questioni non sono un argomento centrale del Curriculum, ma sono viste come vantaggi subordinati alla padronanza delle competenze DataPro. Quindi, sapere come le piattaforme online traggono profitto dall'attenzione dei loro utenti, sia positiva che negativa, presuppone la consapevolezza del fatto che i dati siano un *bene di valore*. Questa conoscenza

potrebbe aiutare gli studenti ad esaminare criticamente i titoli sensazionalistici e le informazioni manipolate, dotandoli di strumenti per identificare e affrontare la disinformazione online. Collegare le competenze del gruppo A - i *dati come bene di valore* - al gruppo B - la *privacy come diritto umano* - favorisce quindi la consapevolezza democratica e la resistenza ad attacchi come la disinformazione.

Conoscere i meccanismi di scambio dei dati e attuare pratiche e azioni di minimizzazione dei dati aiuta gli studenti a proteggersi dal controllo del loro comportamento online. I meccanismi di controllo del comportamento sono onnipresenti sulle piattaforme online, ad esempio nella pubblicità algoritmica e negli algoritmi che cercano di capitalizzare l'attenzione, aumentando il tempo di permanenza sullo schermo del servizio. L'interdipendenza tra il gruppo A - *Dati come bene di valore* - e il gruppo C - *Misure di protezione dei dati* - sostiene l'autonomia e l'autodeterminazione degli studenti online.

Quando si parla di sicurezza informatica, si intersecano il gruppo B - la *privacy come diritto umano* e il gruppo C - le *misure di protezione dei dati*. Creare una interconnessione tra il valore della privacy online e le misure pratiche per proteggerla aiuta gli studenti a costruire una resistenza alle pratiche ingannevoli. Esempi negativi della mancanza di privacy online sono lo sfruttamento delle informazioni personali da parte, ad esempio, di Stati autoritari o della criminalità organizzata. Rafforzare gli studenti contro gli inganni significa comprendere a fondo i rischi per la privacy e i modi pratici per mantenere la propria privacy online con l'aiuto delle competenze del gruppo C.

6. Conclusioni per gli educatori

Per trasmettere agli studenti una consapevolezza critica delle tecnologie digitali, incoraggiandone un uso vantaggioso ed efficace, l'insegnamento delle competenze dei gruppi A, B e C è fondamentale. Sulla base del Quadro di riferimento DigComp[9] , i seguenti elementi chiave del Curriculum saranno punti di orientamento per gli educatori:

[9] EU Science Hub e Commissione Europea (2022) *Quadro DigComp*. Disponibile all'indirizzo: https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en

Protezione dei dispositivi e dei contenuti digitali:

- Istruire gli studenti sulla protezione dei dispositivi digitali da minacce come malware e danni fisici, utilizzando software antivirus, aggiornamenti regolari e password sicure.
- Insegnare agli studenti a identificare e rispondere a minacce quali phishing, ransomware, furto di identità e cyberbullismo.

Comprendere le misure di sicurezza e protezione:

- Istruire sulle abitudini di navigazione sicure, sull'autenticazione a due fattori e sull'uso di reti sicure, come le VPN.
- Sottolineare l'importanza di proteggere i dati personali, capire cosa condividere online, e gestire password forti e uniche.

Protezione dei dati personali e della privacy:

- Evidenziare l'importanza di evitare la condivisione di informazioni sensibili su siti web non sicuri e di comprendere le politiche sulla privacy dei servizi digitali.
- Insegnare come impostare la privacy sui social media e su altre piattaforme.

Uso sicuro e condivisione delle informazioni personali:

- Educare alla condivisione sicura delle informazioni personali, alla crittografia dei dati sensibili e a riconoscere i potenziali danni derivanti da un uso improprio dei dati.

Comprendere le politiche sulla privacy:

- Spiegare l'importanza delle politiche sulla privacy nei servizi digitali e insegnare agli studenti a leggerle e comprenderle per prendere decisioni informate.

Evitare i rischi per la salute:

- Istruzioni per ridurre i rischi per la salute derivanti dall'uso prolungato dei dispositivi digitali, come l'affaticamento degli occhi, la postura scorretta e l'impatto sulla salute mentale.

Protezione dai pericoli digitali:

- Educare a identificare, evitare e segnalare il cyberbullismo, i predatori online e altri comportamenti dannosi.

Promuovere il benessere e l'inclusione sociale:

- Evidenziare gli aspetti positivi delle tecnologie digitali nel favorire le connessioni sociali e le pratiche inclusive.

Consapevolezza dell'impatto ambientale:

- Insegnare le implicazioni ambientali delle tecnologie digitali, compresi i rifiuti elettronici e il consumo energetico.

Monitoraggio e tutela del benessere:

- Monitorare attivamente le attività online per garantire il benessere e intervenire quando necessario per prevenire comportamenti dannosi.
- Essere pronti ad agire immediatamente contro le minacce al benessere degli studenti, come il cyberbullismo.

Consentire agli studenti di valutare i propri dati come se fossero denaro

- Un aspetto importante che non viene affrontato nel Framework basato su DigiCompEdu, ovvero nelle attività in corso, è il valore dei dati come risorsa.