DataPro

Curriculum

sulla Protezione dei Dati

Bernd Remmele, Zlatko Valentic

University of Education Freiburg

Friburgo, 2024

Cofinanziato dall'Unione europea

Indice dei contenuti

Introduzione

In un'epoca in cui le tecnologie digitali pervadono ogni aspetto della nostra vita, la salvaguardia dei dati personali emerge come una preoccupazione cruciale. DataPro, un'iniziativa educativa pionieristica nell'ambito del programma Erasmus Plus dell'Unione Europea, riconosce la necessità imperativa di incoraggiare una profonda comprensione della protezione dei dati come diritto umano fondamentale tra le giovani generazioni. Questo programma di studi è stato progettato per affrontare l'intricato panorama dell'uso e della protezione dei dati, con l'obiettivo di fornire agli studenti le conoscenze e gli strumenti necessari per navigare in questo campo complesso.

La nostra società è sempre più guidata dai dati, con grandi quantità di informazioni che vengono elaborate quotidianamente e che hanno un impatto sulla *privacy* individuale e sulla sicurezza collettiva. In questo contesto, il progetto DataPro offre un quadro educativo completo per illuminare le giovani menti sull'importanza della *privacy* dei dati e sulle considerazioni etiche che essa comporta. Educando gli studenti sulla natura multiforme dell'uso dei dati e sull'importanza cruciale della protezione delle informazioni personali, DataPro cerca di coltivare una cittadinanza ben informata, in grado di sostenere e difendere i diritti sui propri dati.

Il programma di studi stabilisce una serie di obiettivi e finalità specifiche volte a migliorare la comprensione da parte degli studenti delle complessità della protezione dei dati e il riconoscimento della questione come vitale per i diritti umani. Attraverso un approccio strutturato che prevede la raccolta, l'adattamento e lo sviluppo di strumenti didattici innovativi, DataPro intende integrare conoscenze teoriche e comprensione pratica. Questa iniziativa non si concentra solo sulla diffusione di queste risorse tra le scuole e gli attori del settore educativo, ma sottolinea anche l'impegno attivo di studenti e insegnanti in un processo di apprendimento dinamico.

L'impatto previsto di DataPro è profondo. Integrando questo programma di studio nei contesti educativi, prevediamo di formare una generazione non solo consapevole dell'importanza della protezione dei dati, ma anche esperta nell'implementazione delle migliori pratiche in tal senso. Si prevede che questa conoscenza di base favorisca il miglioramento delle misure di tutela della *privacy* e influisca sull'atteggiamento più ampio della società nei confronti della protezione dei dati e dei diritti alla *privacy* in un mondo sempre più digitale.

Attraverso la sua metodologia strutturata e gli sforzi di collaborazione sotto gli auspici del programma Erasmus Plus, DataPro si impegna a raggiungere questi risultati, contribuendo in

modo significativo allo sviluppo di cittadini digitali informati e responsabili. Questo programma di studi funge da faro per l'innovazione educativa, guidando i giovani verso un futuro in cui siano capaci e sicuri di proteggere i propri dati in un'era digitale interconnessa.

1. Preambolo

Il Curriculum sulla Protezione dei Dati, parte del progetto DataPro nell'ambito del programma Erasmus Plus dell'Unione Europea, mira a fornire ai giovani le conoscenze e le competenze essenziali per comprendere e navigare nelle complessità della protezione dei dati. Il Curriculum si basa su una matrice di competenze completa, suddivisa in campi educativi rilevanti. Le sezioni seguenti forniscono una panoramica dettagliata della struttura del Curriculum.

Nel mondo digitale di oggi, la protezione dei dati personali è di fondamentale importanza. I giovani crescono in un ambiente in cui i dati svolgono un ruolo centrale, sia attraverso i *social media*, l'apprendimento *online* o 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 una soluzione educativa completa che consenta agli studenti di gestire i propri dati in modo competente e sicuro.

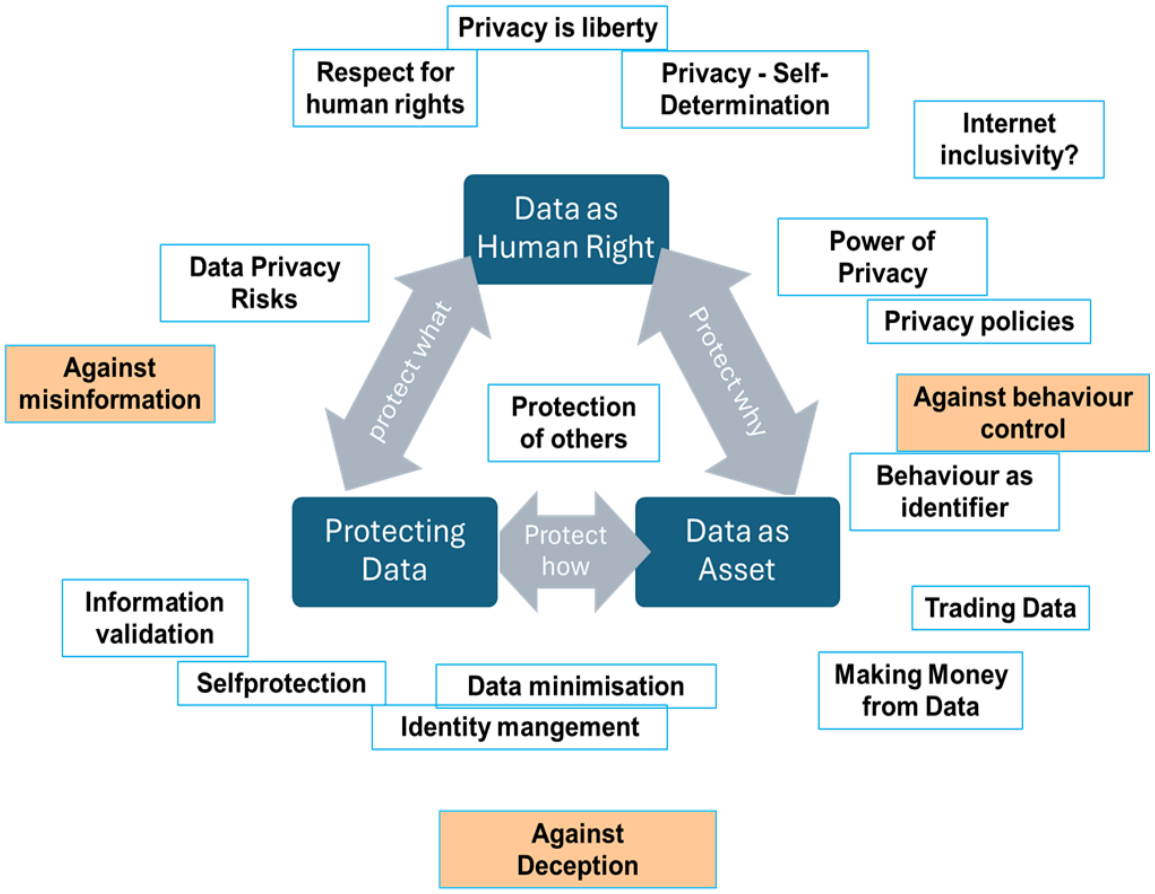
Il programma di studi riflette campi di attualità, ognuno dei quali copre competenze specifiche e tiene conto degli ostacoli all'apprendimento precedentemente studiati. Sulla base del programma di studi, verranno adattati sillabi specifici per ciascun gruppo target. I prototipi di formazione del Work Package 3 si baseranno sulle basi teoriche dei risultati del Work Package 2.

Sebbene il programma di studio si ispiri in larga misura al Quadro DigComp[1] , il suo sviluppo selettivo ha incluso diversi cicli di *feedback* con i membri del Partenariato e degli esperti di protezione dei dati, assicurando la sua completezza e praticità. Il programma trasmette, da un lato, l'idea che la protezione dei dati è un diritto individuale e una pratica che comporta rischi per gli altri e, dall'altro, quella che i dati hanno un valore economico spesso nascosto. Il programma di studi DataPro integra queste dimensioni per garantire che agli studenti di acquisire le competenze necessarie per proteggere la propria *privacy* e agire in modo responsabile nello spazio digitale.

[1] https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en

2. Descrizione delle competenze

Nella sezione seguente, il Curriculum viene descritto utilizzando il grafico fornito, che serve come rappresentazione visiva della matrice delle competenze. Il Curriculum DataPro è strutturato in tre campi sovrapposti: ***Protezione dei dati***, ***Privacy come diritto*** e ***Dati come bene***. Riflette i requisiti richiesti a un membro attivo, autonomo e responsabile di una società di mercato democratica e guidata dai dati e dalle informazioni.



Il programma di studi si concentra su tre argomenti interconnessi:

- Protezione dei Dati: è la parte più ovvia, in quanto si riferisce agli aspetti pratici della protezione dei dati e della sicurezza informatica, come previsto da molte linee guida.
- I Dati come Diritti Umani: da una prospettiva di educazione generale, questo aspetto si riferisce all'importanza dell'autodeterminazione informativa come diritto umano.
- I Dati come un Bene, un valore: da una prospettiva economica, questo aspetto spiega, da un lato, come funziona l'industria dei dati e, dall'altro, come gli individui possono beneficiare del valore dei loro dati.

Nel complesso, quindi, le competenze possono essere chiarite rispondendo alle tre domande seguenti: A. Come posso proteggere i miei dati personali (e la mia fiducia nelle informazioni)?; B. Cosa rende la protezione dei dati un diritto umano?; e C. Cosa rende i dati preziosi (economicamente)?

I tre focus non sono dimensioni separate, ma si sovrappongono pesantemente. La protezione dei dati e la *privacy* come diritto si sovrappongono nella pragmatica di come proteggere "cosa", e nella considerazione dei diritti alla *privacy* degli altri. Ciò significa che il programma di studi non solo insegna agli individui come salvaguardare i propri dati, ma inculca anche il rispetto per la *privacy* degli altri.

La *privacy* come diritto e i dati come bene si sovrappongono nel soppesare gli interessi (legittimi) delle aziende che utilizzano i dati rispetto alla propria *privacy*. Il programma di studi affronta il tema dell'equilibrio tra gli interessi aziendali nell'utilizzo dei dati e i diritti individuali alla *privacy*, aiutando gli studenti a comprendere le implicazioni più ampie dell'economia dei dati.

La protezione dei dati e i dati come bene si sovrappongono nella pragmatica di come utilizzare i propri dati. Questo campo si concentra sulle competenze pratiche necessarie per gestire e sfruttare i dati personali in modo responsabile ed efficace in vari contesti.

Il Curriculum DataPro non prevede livelli di competenza, perché l'elenco delle competenze fornite è considerato fondamentale per una società dell'informazione. Queste abilità e comprensioni essenziali sono ritenute necessarie affinché gli individui possano operare in modo efficace e responsabile in un mondo digitalmente interconnesso.

Vengono evidenziate in particolare le competenze per riconoscere e gestire i comportamenti malevoli su Internet.

A. Come proteggere i miei dati personali (e la mia fiducia nelle informazioni)?

Per proteggere i dati privati e mantenere la fiducia nelle informazioni, prendete in considerazione i seguenti obiettivi di apprendimento, che si concentrano sul mettere gli studenti in condizione di navigare nel mondo digitale in modo più sicuro e responsabile.

A.1 Gestione dell'identità:

a) *Identificazione sicura*: Imparare a proteggere la propria identità elettronica attraverso metodi come password forti e uniche e l'autenticazione a due fattori.
b) *Consapevolezza dell'uso*: Chiedersi regolarmente come e dove utilizzare e condividere le informazioni di identificazione personale in modo sicuro. Comprendere i rischi associati alla condivisione dei dati personali.
c) *Misure di anonimato*: Utilizzare misure per nascondere la propria identità online, come VPN, strumenti di comunicazione criptati e *browser* incentrati sulla *privacy*.

A.2 Autoprotezione:

a) *Controlli della comunicazione*: Conoscere e utilizzare le misure per impedire la ricezione di messaggi o e-mail indesiderati, come i filtri antispam e le regole di posta elettronica.
b) *Gestione del tracciamento*: 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.
c) *Misure di sicurezza*: Impiegare pratiche di sicurezza standard, come l'uso di password diverse e forti per i diversi servizi online, l'attivazione dell'autenticazione a più fattori, l'uso di serrature biometriche, l'esecuzione di aggiornamenti software regolari e l'installazione di software di protezione.

A.3 Contro la disinformazione:

a) *Valutazione critica*: Chiedersi regolarmente chi c'è dietro le informazioni che si trovano su Internet, soprattutto sui social media. Identificare chi potrebbe avere interesse a diffondere *fake news*, come i *social bo*t, i propagatori di discorsi d'odio o coloro che creano camere d'eco (bolle).
b) *Consapevolezza della qualità:* Capire che la disinformazione può essere molto convincente, soprattutto con l'uso di tecnologie avanzate come l'intelligenza artificiale, che possono creare visualizzazioni sofisticate. Interrogarsi sempre sulla qualità e sulla fonte delle informazioni.

A.4 Convalida delle informazioni:

a) *Verifica delle fonti*: 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.
b) *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.

A.5 Protezione degli altri:

a) *Considerazioni sulla condivisione dei dati*: Chiedere regolarmente se le informazioni di identificazione personale altrui vengono condivise e se potrebbero essere utilizzate in modo improprio.
b) *Consapevolezza legale*: Essere consapevoli 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.

A.6 Minimizzazione dei dati:

- *Interrogarsi sulla necessità*: 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.

A.7 Contro gli inganni:

- *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).

B. Cosa rende la protezione dei dati un diritto umano?

Per quanto riguarda la protezione dei dati come diritto umano, considerate i seguenti obiettivi di apprendimento, che si concentrano sulla comprensione della protezione dei dati e delle sue implicazioni:

B.1 La privacy è libertà:

- *Libertà fondamentale*: La *privacy* è essenziale per la libertà, in quanto consente agli individui di esprimere liberamente le proprie opinioni e di vivere senza indebite interferenze. Se altri possono osservare o controllare il nostro comportamento, la nostra libertà personale è compromessa.

B.2 Privacy - Autodeterminazione:

a) *Controllo dei dati*: Ogni persona ha il diritto di decidere quali dati che la riguardano vengono raccolti, elaborati e utilizzati. Questo diritto all'autodeterminazione è fondamentale per mantenere l'autonomia personale.
b) *Protezione dell'automazione*: Bisogna 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.
c) *Prevenzione degli abusi*: La protezione dei dati personali aiuta a prevenire la sorveglianza indesiderata, il furto di identità, la discriminazione e altre forme di abuso dei dati personali.

B.3 Potere della privacy:

a) *Diritti sui dati*: È importante conoscere i propri diritti nei confronti delle aziende che utilizzano i nostri dati, tra cui il diritto di accedere ai dati in possesso, di rettificare le inesattezze, di cancellare i dati (diritto all'oblio) e di presentare reclami alle autorità.
b) *Necessità del consenso*: 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.
c) *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 Rispetto dei diritti umani:

- *Responsabilità digitale*: Essere consapevoli della propria responsabilità di salvaguardare la dignità umana, la libertà, la democrazia e l'uguaglianza quando si opera 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 Rischi per la *privacy* dei dati:

a) *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.
b) *Rischi dell'Intelligenza Artificiale*: Essere consapevoli che i processi e i servizi basati sull'IA possono comportare diversi livelli di rischio per la *privacy*, spesso a causa della loro capacità di elaborare grandi quantità di dati e dedurre informazioni sensibili.

B.6 Internet Inclusivo:

- *Consapevolezza della 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 Politiche sulla privacy:

- *Valutazione delle politiche*: Sviluppare la capacità di esaminare e valutare in modo critico le politiche sulla *privacy* di applicazioni e servizi. Ciò include la comprensione di quali dati vengono raccolti, di come vengono utilizzati e dei diritti di cui si dispone in merito ai propri dati.

C. Cosa rende i dati preziosi (economicamente)?

Poiché i dati hanno un valore economico significativo che riguarda anche gli studenti, si considerino i seguenti obiettivi di apprendimento, che si concentrano piuttosto su una comprensione economica generale:

C.1 Guadagnare con i dati:

a) *Modelli di guadagno*: Scoprire 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 politici).
b) *Economia dei servizi*: Riconoscere che la maggior parte dei servizi Internet gratuiti sono forniti da aziende orientate al profitto, che spesso monetizzano i dati degli utenti per generare entrate.

C.2 Il comportamento come identificatore:

a) *Utilizzo dei dati*: 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 monitoraggio del comportamento degli utenti per offrire contenuti personalizzati.
b) *Strategie di controllo*: Imparare le strategie per controllare e limitare la portata del tracciamento comportamentale, come la regolazione delle impostazioni sulla *privacy* e l'uso di tecnologie che migliorano la *privacy*.

C.3 Contro il controllo comportamentale:

a) *Consapevolezza dei meccanismi* esistenti: Essere consapevoli del fatto 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.
b) *Misure di controllo*: Sviluppare strategie per diminuire queste influenze, come la definizione di limiti personali di utilizzo e la valutazione critica dei contenuti consumati.

C.4 Dati di trading:

a) *Consapevolezza sulla monetizzazione*: Essere consapevoli del fatto 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.

b) *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. Per questo motivo, è importante essere cauti nel definire l'entità della condivisione pubblica dei dati.

3. Conclusioni per gli educatori e le loro competenze

Per trasmettere agli studenti una consapevolezza critica delle tecnologie digitali, incoraggiandone l'uso benefico ed efficace, sono fondamentali le seguenti competenze basate sul DigiCompEdu Framework[2] :

Protezione dei dispositivi e dei contenuti digitali:

- Istruire gli studenti sulla salvaguardia 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.

[2] Quadro delle competenze digitali per gli educatori (fonte: https://joint-research-centre.ec.europa.eu/digcompedu_en)

Curriculum sulla protezione 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 sociale e l'inclusione:

- 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 un bene monetario

Un aspetto importante che non viene affrontato nel Framework basato su DigiCompEdu, ovvero nelle attività in corso, è il valore dei dati come *asset*, cioè beni. Pertanto, vorremmo aggiungere la seguente competenza da acquisire: **Valorizzare i dati come beni di valore.**

Gli studenti devono essere educati a comprendere il valore dei loro dati personali, analogamente a come valutano il denaro. Ciò significa riconoscere l'importanza di proteggere i propri dati, capire come possono essere monetizzati o sfruttati e prendere decisioni informate sulla condivisione dei propri dati.