

7. Protezione dei dati personali e della privacy

La prima parte di questo modulo didattico si occupa della privacy e del valore aggiunto della MIL.

La seconda parte, il MILAB, offre un approccio pratico al tema della privacy.

Alcune definizioni (si veda il glossario)

- Dati
- Big data
- Privacy
- Phishing
- Termini del servizio
- RGPD
- Sensibilizzazione del consumatore

Sintesi

PARTE I Costruzione delle conoscenze

1. La privacy in passato
2. La privacy nel mondo digitale
3. Caratteristiche
4. Opportunità e rischi
5. Obiettivi didattici, competenze e valore aggiunto della MIL
6. Valutazione
7. Materiali formativi

PARTE II MILAB

- Attività fase 1
- Attività fase 2
- Attività fase 3

PARTE I (4 sessioni da 45 MIN)

1. La privacy prima del mondo digitale (20 MIN)

La privacy è una condizione in cui non si è osservati o disturbati da altre persone. I segni, le immagini ed i simboli che formano la nostra identità sono tutti elementi che potremmo considerare privati e che non vorremmo fossero resi pubblici poiché sono intimi e/o potrebbero avere ripercussioni sulla nostra sicurezza.

La privacy è definita in termini legali in molti Paesi e dalla Dichiarazione Universale dei Diritti Umani (1948), all'interno della quale la protezione dei dati personali ha a che fare con l'integrità e la sicurezza dell'individuo:

- **Articolo 12 sulla privacy**
 - ⇒ “Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni.”

- **Articolo 3 sulla sicurezza**
 - ⇒ “Ogni individuo ha diritto alla vita, alla libertà ed alla sicurezza della propria persona.”

Suggerimento per l'insegnante:

I giovani spesso non sono d'accordo con gli adulti su cosa dovrebbe rimanere privato e cosa può essere pubblico o condiviso con gli amici.

Un dibattito su cosa gli studenti considerano “intimo” può rappresentare un buon punto di partenza.

Riferimenti:

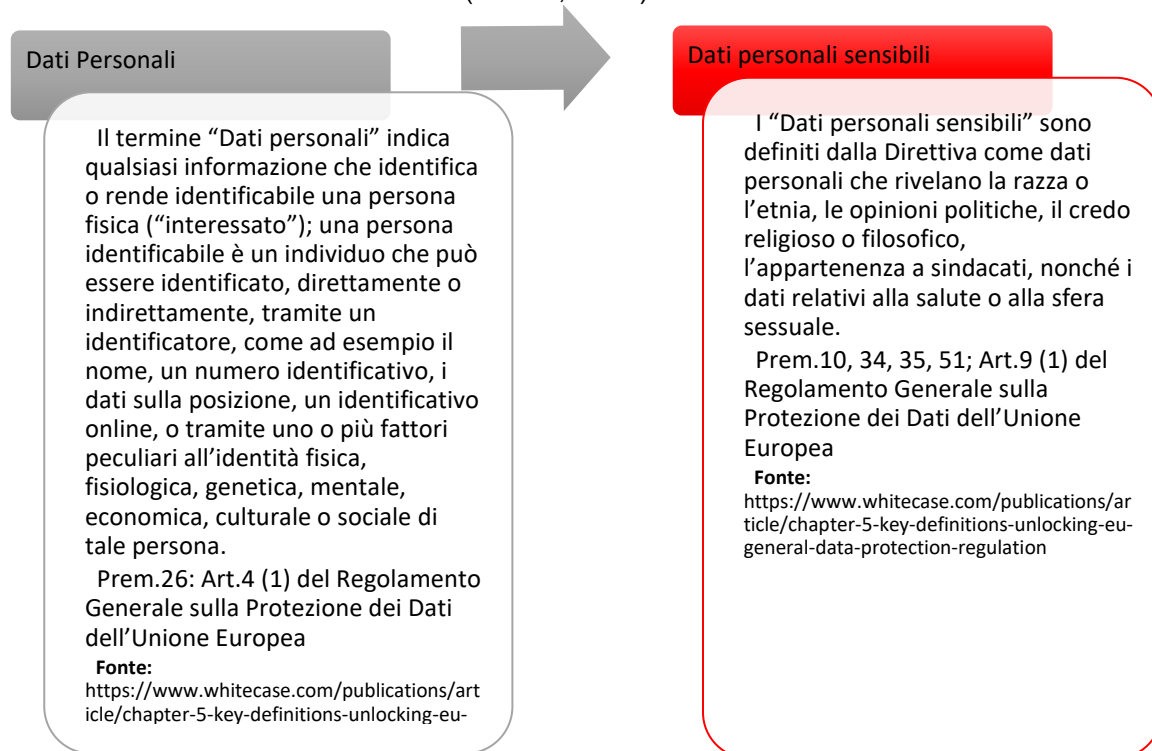


Per leggere l'intera dichiarazione online : <https://www.un.org/en/universal-declaration-human-rights/index.html>

2. La privacy e il mondo digitale (25 MIN)

❖ Come cambiano la privacy e i dati personali?

La privacy online si basa su due tipi di dati, come indicato nel recente Regolamento Generale sulla Protezione dei Dati (RGPD, 2018):



❖ La navigazione e le altre attività online lasciano delle impronte digitali!

Internet e le sue reti sono un’infrastruttura di servizi disponibili tramite un provider che richiede i nostri dati (indirizzo, pacchetto IP...) per la navigazione, lo streaming, il networking, ecc. Questi servizi sono altresì collegati ad altri dispositivi (es. webcam o microfoni del pc portatile) e raccolgono dati sulla nostra navigazione.

La nostra navigazione lascia delle impronte: cronologia, file temporanei di internet, geolocalizzazione, messaggi...

Sul web vengono raccolti due tipi di dati che possono rivelare elementi della nostra privacy:

- ⇒ dati **forniti volontariamente** (stato civile, indirizzo pubblico, pubblicazioni di testi e immagini, mi piace, voti...)
- ⇒ dati generati e **raccolti a nostra insaputa durante la navigazione** (cookie, cronologie di navigazione, ...)

Tali dati vengono raccolti, analizzati e utilizzati mediante algoritmi per varie finalità, per lo più commerciali. Le tecniche di profilazione, previsione e nudge necessitano dei nostri dati per potersi adattare alle nostre esigenze.

Negli Stati Uniti, anche prima dell’età digitale, la raccolta e l’uso di dati personali era regolata da leggi commerciali, e l’aggregazione di dati da vari database da parte di terzi è pertanto consentita. In Europa, in particolar modo con l’avvento del RGPD, tali attività non possono essere svolte senza il consenso degli utenti.

3. Caratteristiche della privacy (25 MIN)

❖ Discussione: quali sono le caratteristiche della privacy secondo te?

- ✓ Controllo delle impronte digitali
- ✓ Gestione delle impronte digitali e della reputazione e presenza digitale
- ✓ Caricare contenuti e pubblicare assicurandosi di mantenere dei confini tra la privacy/intimità e la sfera pubblica/privata.
- ✓ Contratto di condivisione (conversazioni private e pubbliche, commenti, collaborazioni con altri)
- ✓ Comprare e vendere online ed i problemi legati al phishing e al furto d'identità

Suggerimento per l'insegnante:

Far visitare agli studenti il sito web del centro nazionale per la protezione dei dati e mostrare i servizi che offre.

<https://www.cnil.fr/en/data-protection-around-the-world>

Riepilogo

- La violazione del diritto alla privacy può portare a una sgradita sorveglianza o a delle situazioni di stress
- La regolamentazione per il web è relativamente recente e varia significativamente tra Unione Europea, Stati Uniti e altre zone del mondo. Ciò può creare delle difficoltà in uno spazio senza confini come internet.

Suggerimento per l'insegnante:

Chiedere agli studenti se abbiano mai ricevuto spam o altre pubblicità invadenti dopo aver visitato un sito web. Chiedere come si sono sentiti e cosa avrebbero dovuto fare.

❖ Forme ed esempi di privacy e protezione in relazione alle capacità di sensibilizzazione del consumatore (20 MIN)

- ⇒ Termini del servizio
- ⇒ RGPD
 - https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en
- ⇒ Cookie
- ⇒ Geolocalizzazione

Sessione 3: 45 MIN

4. Opportunità e rischi della privacy e dei dati?

❖ Discussione (15 MIN)

Conosci la frase “*se è gratis, il prodotto sei tu*”, attribuita a **Andrew Lewis**.

Cosa può significare in riferimento al data mining e ai rischi per la privacy?



Suggerimento per l'insegnante:

Consultare la risposta data a tale citazione da un insegnante di fisica statunitense (si vedano i Riferimenti a seguire) per comprendere come abbia le stesse ripercussioni di un fenomeno storico.

Riferimenti:

Michael Treanor, ex Insegnante di Chimica/Fisica (1997-2017)

Risposta del 23 giugno, 2018 ·

<https://www.quora.com/Who-originally-suggested-that-if-youre-not-paying-for-the-product-you-are-the-product>

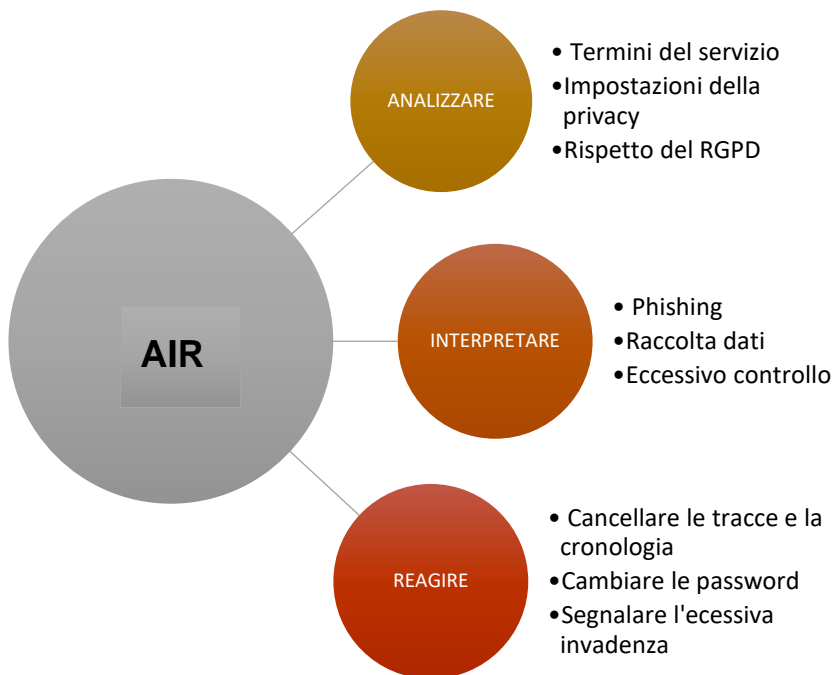
Riepilogo

- I rischi tendono a manifestarsi poiché internet ed i social media sembrano uno “spazio privato”, mentre in realtà sono uno spazio pubblico, con una portata globale. Gli utenti, in quanto consumatori, vengono esposti al phishing e al furto dei dati personali, allo sfruttamento dei dati per la profilazione (politica, commerciale...), alla sorveglianza, ad abusi come il cyberbullismo e i discorsi d’odio.
- Le opportunità si rinvergono in un senso di interconnessione e di interessi condivisi. Gli utenti, in quanto consumatori, vengono esposti alla reputazione e alla presenza digitale (influenza)

❖ Opportunità e rischi (15 MIN)

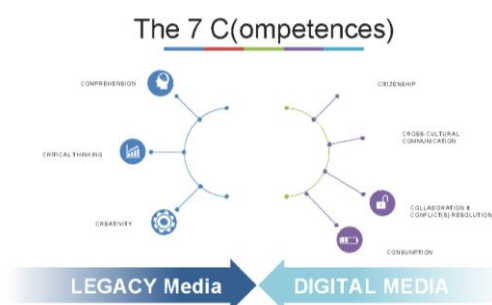


Costruzione delle capacità di pensiero critico



5. Focus sulle **COMPETENZE DI SENSIBILIZZAZIONE DEL CONSUMO/CONSUMATORE (7C) (15 MIN)**

Consente agli utenti di vedere i social media e gli altri spazi sociali virtuali come spazi pubblici in cui vengono venduti prodotti e servizi online. Comprendere le implicazioni della realtà commerciale degli spazi online è fondamentale per proteggere la privacy degli utenti.



Si vedano l'introduzione e il glossario

❖ **Divisione delle competenze MIL in categorie/indicatori delle **COMPETENZE DI SENSIBILIZZAZIONE DEL CONSUMO/CONSUMATORE****

Gli studenti dovrebbero essere in grado di:



❖ **Valore aggiunto della MIL per i diritti umani**

- ⇒ libertà d'espressione
- ⇒ privacy

6. Valutazione (45 MIN)

Mostrare 3 foto e chiedere agli studenti di dare un voto in termini di "privacy" (da 0, non sicuro, a 5 molto sicuro)

7. Materiali di supporto didattico (si veda la sezione aggiuntiva ai Moduli Didattici)

- ⇒ Riferimenti ad altri materiali e risorse (Manuale di alfabetizzazione digitale; Manuale didattico sulla cittadinanza digitale)
- ⇒ Link utili per animazione pedagogica
- ⇒ Glossario

- ⇒ Software per l'integrazione della MIL nei risultati didattici (Risorse online per Paese)
<https://docs.google.com/spreadsheets/d/10wxqYEe9O8GiSKo8kTjv8uQgpkOeHJp5k0ytBcZsdU/edit?usp=sharing>

Per approfondire

PARTE II - MILAB (4 sessioni da 45 MIN, a seconda del tempo assegnato alla MIL)

Le attività MILAB sono strutturate in tre fasi (1-avvio; 2-consolidamento; e 3-approfondimento). Le tre fasi sono indicative: possono essere seguite come suggerito o utilizzate secondo un approccio di "collegamento" o modulare a seconda del tempo assegnato alla MIL e/o al livello di risultato desiderato.

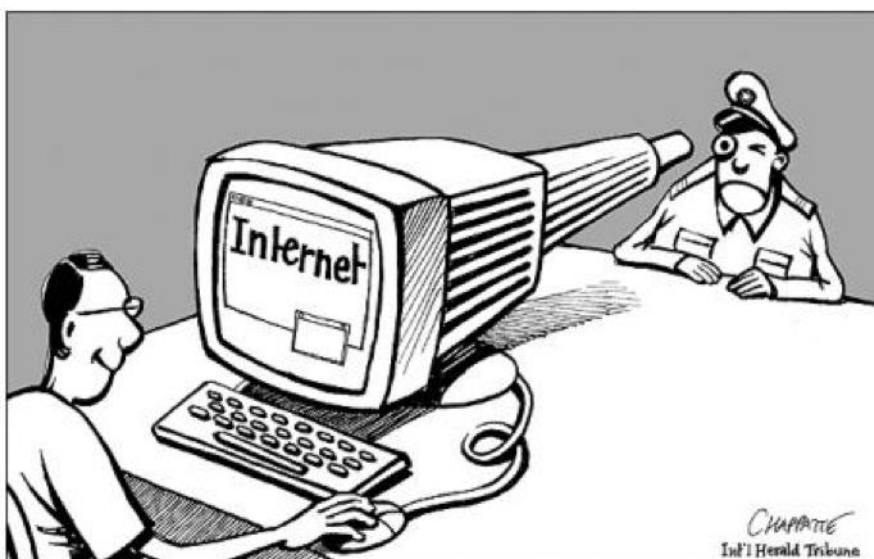
Le fasi prevedono varie attività pedagogiche, come ad esempio: workshop, giochi di ruolo, esercizi scritti e giochi. Sperimentano vari formati multimediali, come i blog, i video e gli articoli web, al fine di formare le capacità di pensiero critico degli studenti (AIR).

ESPLORAZIONE DELLE COMPETENZE DI SENSIBILIZZAZIONE DEL CONSUMO/CONSUMATORE:

Contributi ai social media tramite tweet, post, storie...

FASE 1 (15-16):

CAPIRE LA PRIVACY E LA PROTEZIONE DEI DATI



FONTE : <https://wisc.pb.unizin.org/commarts250/chapter/week-15-viewing-labor/>

Suggerimento per l'insegnante:

Introdurre l'argomento descrivendo una sua rappresentazione visiva divertente, come questa, provare a polarizzare i concetti di "vedere" ed "essere visti" attraverso l'uso di internet.

❖ Dibattito sul PHISHING (45 MIN)

Gestire un dibattito sulla pratica del phishing:

Far riflettere gli studenti sullo shopping online, le forme di pagamento accettate, le informazioni sui prodotti, gli http...ma anche sui rischi di furto d'identità, o di hackeraggio del proprio account...

Dividere la classe in squadre. Lasciare del tempo per delle ricerche online.

Suggerimento per l'insegnante:

Discutere di attività come l'eccessivo controllo, l'ottimizzazione delle pubblicità su misura per l'utente, ma anche la manipolazione e la propaganda.,

❖ Dibattito sul PHISHING (continuazione) (45 MIN)

In piccoli gruppi:

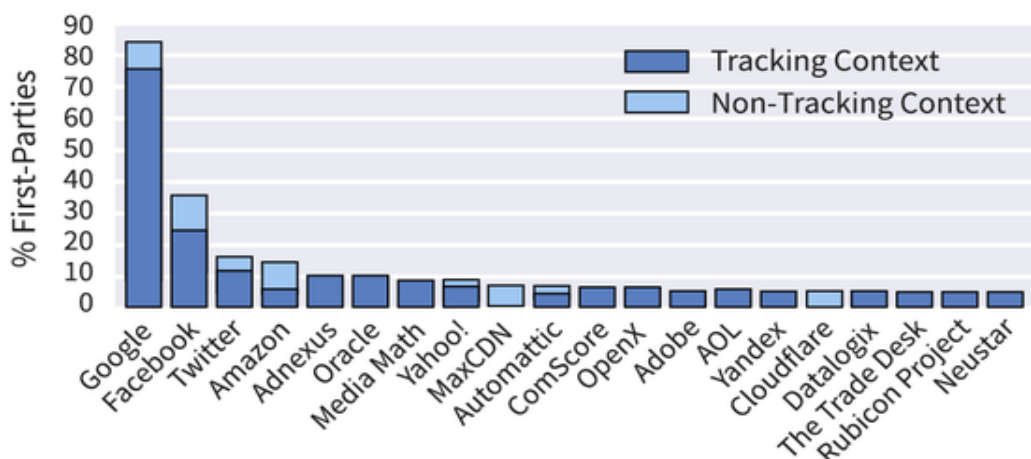
Aiutare gli studenti a delineare i pro ed i contro del dibattito per proteggere la propria privacy ed evitare il phishing; cercare buone pratiche e soluzioni tecniche, come ad esempio la crittografia.

Lasciare che gli studenti esponano le proprie argomentazioni, con un moderatore.

Tutti insieme: creare una lista di controllo di sicurezza dell'utente per la prevenzione dello spam/phishing, come ad esempio: strane richieste via e-mail (sui conti correnti); testo sospetto (annuncio di assegnazione di un premio o ricompensa); truffa della lista di contatti (tutti i contatti ricevono lo stesso messaggio); allegati da mittenti indesiderati (che contengono virus). Far scrivere agli studenti la soluzione per ogni punto (cancellare, gettare nel cestino, bloccare, segnalare, codificare) in base alle capacità di pensiero critico AIR.

❖ VALUTAZIONE E COMMENTO (45 MIN)

Osservare ed elencare le tre società nel diagramma sottostante con le più ampie reti di tracciamento. Cosa ci dice sull'esposizione personale a terze parti?



FONTE: [Princeton's WebTAP privacy project](#)

FASE 2 (16-17)

APPROFONDIMENTO SULLA PRIVACY ONLINE

❖ SIMULAZIONE (2 x 45 MIN)

Parlare del RGPD con gli studenti e dei loro diritti e responsabilità, nonché dei rimedi a loro disposizione

Link: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en

Chiedere agli studenti di considerare specifici diritti:

- 1. diritto di consultazione,*
- 2. diritto di correzione,*
- 3. diritto di soppressione dei dati personali,*
- 4. diritto alla portabilità dei dati,*
- 5. diritto di cancellazione.*

Dopodiché, far scaricare il modulo per l'esercizio del diritto di cancellazione.

<https://gdpr.eu/right-to-erasure-request-form/>

Chiedere agli studenti di considerare i motivi per la cancellazione ed i rimedi indicati all'articolo 4 del modulo. Cosa farebbero se avessero un problema legato alle modalità di utilizzo dei propri dati (in particolare in quanto ragazzi minorenni).

S Suggerimento per l'insegnante:

Chiedere agli studenti di discutere del diritto di cancellazione vs diritto al ricordo? Chiunque può cancellare i fatti e le azioni di qualcun altro a suo piacimento?

❖ RICERCA SU GOOGLE (45 MIN)

Cercare la parola "Cookie" e come si collegano alla cronologia di navigazione.

Raccogliere informazioni, e verificare le fonti, su come disabilitare i cookie e come utilizzare le estensioni del browser che segnalano e bloccano i cookie e le pubblicità.

S Suggerimento per l'insegnante:

Parlare di Ghostery o di uBlock Origin come modi per bloccare i cookie e le pubblicità.

❖ VALUTAZIONE E COMMENTO (45 MIN)

Far lavorare gli studenti in piccoli gruppi per discutere di come creare una buona password e spiegare la logica dietro la loro scelta. Possono aiutarsi con strumenti online come <https://www.wikihow.com/Create-a-Password-You-Can-Remember>

FASE 3 (18-19):

CREARE UNA PROTEZIONE SOSTENIBILE DELLA PRIVACY E DEI DATI PERSONALI ONLINE

❖ RICERCA ONLINE (2 x 45 MIN)

Chiedere agli studenti di individuare dei motori di ricerca che non traccino e non favoriscano la comparsa di annunci pubblicitari, come Qwant, DuckDuckGo, Ecosia, Lilo...

Cercare quanto da essi dichiarato all'interno delle rispettive mission, individuare il loro modello economico (in che senso sono sostenibili?)

Confrontare questi motori di ricerca con i principali motori di ricerca commerciali, come Google, Yahoo !...

❖ Dibattito (45 MIN)

Cosa ne pensano gli studenti del pluralismo dei motori di ricerca? Sono pronti a passare ad un motore di ricerca che possa proteggere la loro privacy? Come si sentono a vendere i propri dati personali a società private per fare soldi?

❖ VALUTAZIONE E COMMENTO (45 MIN)

Consultare la controversia spagnola, una delle prime sul tema del Diritto di Cancellazione (o diritto all'oblio). (e consultare il modello per la cancellazione).

Nel maggio 2014, la Corte di Giustizia europea si è pronunciata contro Google nel caso *Costeja*, un procedimento avviato da un cittadino spagnolo, Mario Costeja González, il quale aveva richiesto la rimozione di un link da un articolo digitale del 1998 apparso sul giornale *La Vanguardia*, relativo ad un'asta sulla sua casa pignorata, per un debito che egli aveva successivamente ripagato. Inizialmente, il Sig. González aveva tentato di far rimuovere l'articolo presentando reclamo all'Agenzia spagnola per la protezione dei dati, la quale aveva respinto il reclamo poiché l'articolo era legittimo e veritiero, ma accettò un reclamo nei confronti di Google e chiese a

a quest'ultimo di rimuovere i risultati. Google citò in giudizio l'Alta Corte Nazionale spagnola, che pose una serie di interrogativi alla Corte di Giustizia europea. La corte, nel caso *Costeja*, deliberò che i motori di ricerca sono responsabili per i contenuti da essi mostrati e pertanto Google fu costretta ad adempiere alle leggi europee sulla riservatezza dei dati. Il primo giorno di tale adempimento (30 maggio 2014) Google ricevette 12.000 richieste di rimozione dei dati personali dal proprio motore di ricerca.

FONTE: https://en.wikipedia.org/wiki/Right_to_be_forgotten

Quali erano le sue argomentazioni? Quali erano le argomentazioni di Google? Come è stata risolta la vicenda? Cosa ne pensi?

Suggerimento per l'insegnante:

Gli studenti possono usare come riferimento il modulo per il diritto all'oblio disponibile dal 2018.

<https://gdpr.eu/right-to-erasure-request-form/>