Contenuto prodotto da Stefano Pasta - CREMIT

Impronte digitali

La traccia di dati che ciascuno genera online

L'impronta digitale (o *footprint* digitale) è la traccia di dati che una persona genera, sia attivamente che passivamente, quando utilizza Internet, inclusi i siti web visitati, le email inviate e le informazioni trasmesse online. Quando qualcuno è online e utilizza il suo dispositivo per interagire con siti, app, forum e file, lascia dietro di sé tracce di dati. **Queste tracce di dati costituiscono la tua impronta digitale.**

Tendenzialmente ciascun utente del web genera un'impronta digitale, ma le sue dimensioni possono essere diverse: crescono man mano che, ad esempio, si pubblicano contenuti sui social media, ci si iscrive a una newsletter, si lascia una recensione online o si fa shopping online. Non è sempre evidente che si sta contribuendo ad alimentare il proprio footprint digitale. I siti, ad esempio, possono tracciare le attività degli utenti installando cookie nel dispositivo e le app possono raccogliere dati a loro insaputa. Se un'organizzazione viene autorizzata ad accedere alle informazioni di un fruitore, potrebbe vendere o condividere i dati con terze parti. Ancora peggio, le informazioni personali potrebbero venire compromesse a seguito di una violazione dei dati.

Il processo di costruzione dell'impronta digitale può essere sia "attivo" sia "passivo", dimensioni che comunque sono tendenzialmente entrambe presenti in ciascuno.

Impronta digitale attiva

L'impronta digitale attiva di un utente (fruitore e produttore al tempo stesso…) si implementa quando questi ha deliberatamente condiviso informazioni personali, ad esempio pubblicando contenuti, oppure partecipando a siti di social network o forum online. Se un utente ha effettuato l'accesso a un sito web con un nome o un profilo registrato, tutti i post pubblicati fanno parte del suo footprint digitale attivo.

Altri esempi di attività che contribuiscono ai footprint digitali attivi – tutte incentrate sulla condivisione di dati – sono la compilazione di un modulo online, come l'iscrizione a una newsletter, o il consenso ad accettare i cookie nel browser, la pubblicazione sui social media o sui forum online, l'invio di email e il gaming online. In generale, chi condivide molto avrà un'impronta digitale attiva molto ampia.

Impronta digitale passiva

L'impronta digitale passiva viene implementata quando vengono raccolte informazioni sull'utente a sua insaputa (o senza la sua consapevolezza esplicita o il suo coinvolgimento attivo), come avviene, ad esempio, quando i siti raccolgono informazioni sul numero di visite effettuate dagli utenti, sulla loro provenienza e sul loro indirizzo IP. Questo è un processo nascosto, di cui gli utenti potrebbero non rendersi conto. Un altro esempio di footprint passivo è l'utilizzo che i siti di social network e gli inserzionisti fanno dei like, condivisioni e commenti per profilare gli utenti e indirizzare a loro dei contenuti specifici. Alcune fonti comuni in cui i dati vengono raccolti in modo invisibile includono: l'indirizzo IP, che segnala quante volte si visita un sito, come vi si arriva, i dispositivi domestici smart, le registrazioni finanziarie.

Singolarmente non sono gravi come una violazione dei dati, ma insieme possono diventare molto potenti.

Monitorare la propria impronta digitale…

Educare allo spirito critico e alla responsabilità, ossia a valutare le conseguenze delle nostre azioni nel digitale, include anche promuovere consapevolezza e monitorare l'impronta digitale per vari motivi; ne riportiamo alcuni.

- Un footprint digitale può determinare la reputazione digitale di una persona, che in taluni contesti è rilevante almeno quanto quella offline; ad esempio, i datori di lavoro possono controllare i footprint digitali dei potenziali dipendenti, in particolare i social media, prima di decidere se assumerli; è quello che si indica con il termine "web reputation".
- Le impronte sono relativamente permanenti e, una volta che i dati sono pubblici, o persino semipubblici, come nel caso dei post social, il proprietario ha un controllo decisamente limitato su come gli altri li utilizzeranno.
- Contenuti destinati a un gruppo privato possono essere divulgati a una cerchia più ampia di persone, rischiando di danneggiare relazioni e amicizie.
- I cybercriminali possono sfruttare l'impronta digitale utilizzandolo, ad esempio, per scopi come il phishing per l'accesso agli account o la creazione di false identità basate sui vostri dati; si tratta di un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Per approfondire

Pasta, S., Rivoltella, P.C. (eds.) (2022). *Crescere onlife. L'Educazione civica digitale progettata da 74 insegnanti-autori*. Brescia: Scholé.