6 La cittadinanza digitale

Quando si parla di cittadinanza digitale si intende la possibilità per ogni cittadino di entrare a far parte della «società online», assumendosene tutti i rischi, i diritti e i doveri come in qualsiasi altro tipo di collettività. Ognuno di noi deve quindi essere in grado di cogliere ed esercitare questa opportunità, imparando a utilizzare in modo critico e consapevole i media e la rete, rispettandone le norme specifiche e, soprattutto, proteggendosi dalle insidie che essa nasconde. Il testo che segue vuole essere un piccolo aiuto in questa direzione.

Essere cittadini digitali

Per far parte di una società digitale occorre innanzitutto avere la possibilità di accedervi: negli ultimi anni è sicuramente aumentata quella che si definisce «**inclusione digitale**», ma sussistono ancora numerosi ostacoli che impediscono ad alcune categorie sociali di farne parte, per esempio le persone meno privilegiate economicamente o le donne in taluni Paesi o contesti familiari.
Il solo utilizzo della tecnologia informatica, inoltre, non basta per essere automaticamente un **cittadino digitale**: per non restare ai margini di questa particolare società non bisogna essere semplici fruitori, ma occorre partecipare attivamente alla sua organizzazione, in maniera responsabile e senza perdere mai di vista i meccanismi e la logica che stanno alla base delle tecnologie.
Ma in quale caso ci si può definire veri cittadini della rete?
Quando, grazie alle tecnologie digitali:

- si portano avanti alcuni princìpi di cittadinanza attiva come l'inclusione sociale e la collaborazione con gli altri;
- si propongono idee e innovazioni per raggiungere obiettivi personali e/o sociali;
- si sfruttano le diverse capacità personali a fini commerciali in un mercato legale e di libera concorrenza;

- si riesce a essere critici sulla validità e sull'affidabilità delle informazioni raccolte in rete;
- si riesce a operare attivamente senza perdere mai di vista i princìpi etici;
- si rispettano specifiche norme come quelle della privacy e del diritto d'autore.

I rapporti dei cittadini digitali con la Pubblica Amministrazione

Con il Decreto legislativo n. 217, pubblicato sulla Gazzetta Ufficiale nel gennaio 2018, si è fissata una normativa chiamata **Carta della cittadinanza digitale** che permette ai cittadini «di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale […] al fine di garantire la semplificazione nell'accesso ai servizi alla persona» e «riducendo la necessità dell'accesso fisico agli uffici pubblici».
Grazie alle tecnologie digitali legate a tale normativa, per esempio, l'identità, il domicilio, le firme digitali, il rapporto tra cittadini, imprese e Pubblica Amministrazione può essere semplificato e migliorato.

Il diritto digitale

Spesso in rete si verificano furti e atti criminali, esattamente come succede nella società reale, di conseguenza anche la rete è regolata da una serie di normative. Ricordate sempre che l'appropriazione indebita, ossia il non rispetto della licenza d'utilizzo, potrebbe danneggiare il lavoro di altri utenti. Gli atti criminali digitali più comuni sono quelli relativi alla creazione di virus, all'hacking di informazioni, al plagio, al furto di identità digitale e al download illegale di musica e film.
Una riflessione a parte va poi fatta sul crescente fenomeno del **cyberbullismo**. Nel 2017 è entrata in vigore una nuova legge (Legge 29 maggio 2017, n. 71) che definisce giuridicamente il cyberbullismo come «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online».
Il cyberbullismo, come il bullismo, è una forma di **prevaricazione prolungata nel tempo** di una persona (o un gruppo di persone) nei confronti di un'altra considerata più debole, e si concretizza nell'invio alle vittime di insulti e minacce, foto o video compromettenti attraverso smartphone, pc, tablet.
Purtroppo la diffusione attraverso la rete di questo materiale può avvenire sia di giorno che di notte, è veloce e difficilmente controllabile. Altrettanto difficoltosa è poi l'identificazione immediata del cyberbullo, che si nasconde spesso dietro una falsa identità.

Fake news

Quando si naviga in rete è facile imbattersi nelle cosiddette **fake news**: si tratta di **notizie false**, in parte o completamente, che tuttavia trovano una veloce diffusione tra gli utenti grazie agli strumenti digitali di oggi. Le fake news sono potenzialmente **pericolose** perché diffondono una visione distorta della realtà e spesso sono utilizzate per disorientare, confondere, oppure per condizionare le idee e i comportamenti delle persone. Gli effetti di queste notizie false sono a volte istantanei, mentre invece per «smascherarle» e dimostrare la loro infondatezza è richiesto sempre del tempo. Pertanto, ogni volta che si legge una notizia, è necessario **valutarla** con attenzione, **confrontarla** con altre fonti, ed **evitare di diffonderla** lasciandosi prendere dall'emozione, positiva o negativa, che suscita: le fake news sono notizie tossiche che compromettono la nostra visione del mondo ed è anche responsabilità di ogni individuo intervenire affinché non trovino diffusione.

Il *digital divide*

Il mondo è sempre stato diviso fra Paesi ricchi e Paesi poveri e oggi le cose non sono cambiate. La ricchezza si misura ancora in beni materiali, rispetto al passato, però, è cambiato un elemento fondamentale: l'**accesso alle informazioni** è la condizione per lo sviluppo economico. E in questo senso, il mondo è ancora profondamente diviso: gli esperti parlano di ***digital divide*** («divario digitale») per descrivere lo squilibrio tra Paesi ricchi, altamente connessi alla rete e in grado di sfruttarne tutte le potenzialità, e Paesi poveri o in via di sviluppo, nei quali l'accesso alla rete è ancora insufficiente e costoso.

Glossario di educazione civica digitale

Algoritmo: nel linguaggio dell'informatica è una serie di istruzioni che permette di svolgere un'operazione o di risolvere un problema.

Backup: è una procedura che permette di salvare i dati presenti in un computer o in uno smartphone e conservarne una copia di sicurezza.

Cyberbullismo: sono azioni di bullismo attuate attraverso l'uso degli strumenti digitali.

Cybersecurity: comprende i sistemi di sicurezza per prevenire e fronteggiare minacce e attacchi informatici.

Digital footprint: l'«impronta digitale» è la traccia che le nostre informazioni lasciano (in termini di gusti, preferenze, abitudini ecc.) quando navighiamo in internet.

Fact checking: è un termine del giornalismo che significa «verifica dei fatti» e delle fonti; è una pratica fondamentale per individuare le fake news.

Filter bubble: la «bolla di filtraggio» è un sistema che seleziona per ogni utente i contenuti in base ai gusti, alle idee e alle abitudini, limitando la possibilità una visione più ampia della realtà.

Hacking: è una pratica illegale che consiste nell'accedere e modificare i sistemi informatici.

Hate speech: comprende le espressioni di odio e di incitamento all'odio che trova diffusione in certi media digitali.

Infosfera: è l'insieme dei mezzi di comunicazione e delle informazioni che circolano in essi.

Intelligenza artificiale: è un campo dell'informatica che si occupa di progettare e costruire elaboratori elettronici intelligenti.

Machine learning: l'«apprendimento automatico» è una branca dell'intelligenza artificiale che permette alle macchine di imparare attraverso l'esperienza.

Moderazione: sui nuovi media è l'intervento di controllo su affermazioni e commenti volgari, infamanti e pericolosi.

Privacy: è il diritto che ogni individuo ha alla riservatezza e alla protezione dei propri dati personali.

Realtà aumentata: è l'arricchimento della realtà fisica con contenuti e informazioni attraverso i dispositivi digitali.

Realtà virtuale: è un ambiente tridimensionale generato attraverso l'uso di computer e simulatori.

Trolling: è l'attività di disturbo e di provocazione che ha il solo intento di ottenere visibilità nella comunità virtuale.

Buone pratiche

Per diventare un buon cittadino digitale occorre molto tempo, tanto impegno e un bagaglio di conoscenze tecnologiche e di esperienze pratiche. Le piccole attività che seguono vi potranno aiutare in questo cammino.

- Fai sul tuo quaderno una sintesi delle tue riflessioni e delle nuove conoscenze apprese. Parti dal primo paragrafo nel testo e rifletti sul concetto di «inclusione digitale»: scopri se esistono Paesi nel mondo in cui i cittadini non hanno la possibilità di accesso alla rete ed eventualmente spiegane le motivazioni.
- Nel brano sono presenti i termini «identità», «domicilio», «firme digitali»: scopri di che cosa si tratta.
- Tra gli atti criminali viene citato l'«hacking»: trova informazioni che ti permettano di definire meglio tale fenomeno.
- Utilizzando le informazioni del testo e quelle nuove da voi trovate, predisponete alcune precise domande e organizzate un'intervista da sottoporre ad alcune persone adulte. Lo scopo è quello di scoprire quanti, tra i cittadini intervistati, siano anche cittadini digitali. Con i dati raccolti create grafici e realizzate cartelloni esplicativi della situazione intorno a voi.
- Il problema del cyberbullismo è purtroppo di grande attualità. Chiedete a un vostro insegnante di aiutarvi a organizzare una discussione in classe per confrontarvi (possibilmente tutti seduti in cerchio), in cui ciascuno di voi si senta libero di esprimere le proprie impressioni in merito a tale delicato argomento.

Barra con una x la risposta esatta.

1. Un vero cittadino della rete:

A opera seguendo i princìpi dell'individualità.
B è in grado di riconoscere una notizia vera da una falsa.
C non fa distinzione tra realtà e realtà virtuale.
D rispetta le norme sulla privacy, ma non sul diritto d'autore.

2. In che cosa consiste il cyberbullismo?

A Ad esempio, inviare insulti, minacce o foto/video compromettenti tramite la rete con intento di ricatto o diffamazione.
B Proporre nuovi princìpi etici per raccogliere informazioni in rete.
C Non rispettare la licenza d'utilizzo di un contenuto online.
D Acquisire informazioni rilevanti in rete sull'identità altrui.