

# La cittadinanza digitale

Sicuramente utilizzi strumenti tecnologici digitali in molte occasioni: per metterti in contatto con i tuoi amici, per ascoltare musica, per guardare un video, per scambiare i compiti con i compagni e molto altro ancora. Internet e gli strumenti digitali hanno acquisito una consistente presenza nella nostra vita e hanno modificato le nostre abitudini: molte azioni che prima si svolgevano offline (informarsi, comunicare con altre persone, ma anche pagare servizi pubblici o privati, iscriversi a scuola...) adesso si compiono attraverso la rete. L'uso responsabile delle nuove tecnologie è fondamentale, soprattutto per limitare i rischi a esse connessi; l'insieme delle regole di comportamento che consentono di impiegare le tecnologie digitali in modo consapevole e le opportunità che queste offrono costituiscono la cittadinanza digitale.



**L'avvento di Internet e il digital divide.** Alcuni aspetti della nostra vita sono profondamente cambiati in seguito all'avvento del web, per esempio cercare un lavoro: oggi è infatti possibile inviare curriculum senza pagare buste e francobolli, consultare migliaia di annunci senza uscire di casa, candidarsi per un lavoro in un'altra città o nazione senza spostarsi. Questo crea una profonda differenza tra chi ha competenze e possibilità di muoversi in rete e chi non le ha e quindi resta inevitabilmente escluso dalle opportunità che il web offre. Questo divario è chiamato **digital divide**. Identificarlo e riconoscere che chi ha un accesso limitato a Internet ha anche minori opportunità di esercitare i propri diritti costituzionali ha portato, soprattutto nei Paesi più avanzati, a una riflessione su come evitare che la rete possa contribuire a creare cittadini di serie A, facilitati dall'accesso al web, e cittadini di serie B, che rimangono esclusi.

Il concetto di cittadinanza è antico e i diritti/doveri del cittadino sono codificati attraverso la Costituzione e le leggi dello Stato. Al contrario, il concetto di cittadinanza digitale è recente e la definizione e regolamentazione dei diritti e doveri del cittadino digitale sono meno definite.

**La definizione di cittadinanza digitale.** Oggi è diventato necessario definire quali strumenti e servizi debbano essere resi disponibili per ogni cittadino, quali conoscenze si debbano avere per muoversi correttamente in rete e quali norme possano garantire a tutti l'accesso e l'utilizzo del web (quali **diritti?**). Nello stesso tempo, bisogna stabilire delle norme che regolamentino l'utilizzo degli spazi digitali (quali **doveri?**). Per ribadire l'importanza del web nella vita di ogni cittadino e la sua appartenenza alla società digitale, si è ripreso il concetto di cittadinanza, coniando una specifica definizione di **cittadinanza digitale**, intesa come **capacità di un individuo di partecipare alla vita online**. Come la cittadinanza tradizionale, anche quella digitale comporta un insieme di diritti e doveri, che, grazie al supporto di strumenti e servizi digitali, regolamentano e semplificano il rapporto tra cittadini, Stato e imprese.

**Il diritto di accesso a Internet.** La cittadinanza digitale comporta per ogni cittadino il **diritto di accesso alla comunità virtuale**, in cui vengono prese decisioni, conosciute persone, condivise conoscenze, avviati lavori, prodotta economia. Esserne fuori non significa soltanto perdere opportunità, ma venire lesi nei propri diritti. In alcune condizioni politiche, non avere accesso a Internet significa non poter disporre di informazioni o esprimere la propria opinione. Il **diritto di accesso a Internet** è quindi da considerare un diritto fondamentale che favorisce l'esercizio di altri **diritti fondamentali**: dalla libertà di espressione a quella di informare e di essere informati, dall'iniziativa economica alla possibilità di innovare, ed è condizione necessaria per il pieno sviluppo individuale e sociale della persona. Questo diritto non è dato per acquisito in tutto il mondo: accanto a Stati che hanno stabilito che nessuna autorità può disconnettere un cittadino, altre nazioni hanno limitato o impedito l'accesso alla rete o a determinati suoi servizi. In Cina, per esempio, un grosso **firewall** blocca ai cittadini cinesi l'accesso online impedendo loro di leggere la posta, guardare video o cercare informazioni via Internet attraverso i principali motori di ricerca; molti siti sono oscurati.

**La regolamentazione del web.** Non è facile creare una legislazione che prenda in carico i diritti e i doveri dei cittadini digitali, innanzitutto perché Internet è uno **strumento sovranazionale**: una persona può in pochi secondi accedere a contenuti provenienti da ogni parte del mondo. Un sito di informazione italiano potrebbe, per esempio, registrare le sue notizie su un server americano, includere video da uno russo e sfruttare applicazioni residenti su uno norvegese. Ecco perché le leggi nazionali cercano di riferirsi a normative di più ampio respiro, in particolare nel caso dell'Italia a quelle europee. Tra queste ultime assume un particolare rilievo il **Regolamento UE sull'accesso a Internet e sui diritti degli utenti** del 2015 dove, oltre a enunciare i diritti dei singoli cittadini digitali, sono affrontate tematiche

## BIETTIVI PER LO SVILUPPO SOSTENIBILE

Anche l'Agenda 2030 dell'ONU pone il tema della disponibilità di un collegamento a Internet per tutti. L'obiettivo 9 indica infatti la necessità di aumentare in modo significativo l'accesso alle tecnologie di informazione e di comunicazione attraverso l'impegno, da parte dei Paesi più avanzati, di fornire a quelli meno sviluppati un accesso a Internet universale ed economico.



di carattere più generale, come quelle sulla sostenibilità della gestione del traffico e alla trasparenza nel trattamento dei dati.

**Identità digitale e privacy.** Accedere al web, oltre che un nostro diritto, è una **responsabilità**: esistono infatti doveri e norme che regolano la presenza e la comunicazione in Internet. Partiamo dall'**identità digitale**, ovvero l'insieme di tutte le informazioni e i dati presenti in rete che ci riguardano, inseriti da noi o da terzi, che comunicano un'immagine di noi stessi. Da una parte abbiamo il **diritto di conoscere le informazioni su di noi** che lo Stato o un'azienda privata possiede;

dall'altra abbiamo la responsabilità di ciò che noi stessi comunichiamo e il **dovere di rispettare l'identità digitale degli altri**. Nel momento in cui pubblichiamo su un social network un "selfie" di gruppo, scattato a una festa, stiamo comunicando a tutti i nostri contatti dove sono i nostri amici, che cosa stanno facendo, come sono vestiti, chi stanno frequentando... In altre parole, essere presenti in rete ci costringe a **dover tutelare anche la privacy di chi sta con noi**, ossia il diritto alla riservatezza della propria vita privata e al controllo dei propri dati personali. Quando parliamo di "privacy" facciamo in particolare riferimento ai seguenti dati relativi a una persona:

- **anagrafici** (nome e cognome, indirizzo mail, indirizzo di residenza e domicilio, numero di telefono ecc.);
- **finanziari** (codice fiscale, conto corrente, numero di carta di credito ecc.);
- **identificativi** (fotografie, video ecc.);
- **sensibili** (informazioni su nazionalità, opinioni politiche, convinzioni religiose ecc.);
- **giudiziari** (processi, denunce ecc.).

La foto di una persona in qualsiasi contesto venga ripresa contiene molti dati identificativi e sensibili che potrebbero non rispettare la sua privacy e la sua identità digitale.



**La web reputation.** Imparare a gestire la propria (e altrui) privacy è il primo passo per navigare correttamente in Internet. Oltre che riguardare la propria sicurezza, ciò che postiamo ha a che fare anche con l'immagine che lasciamo in rete di noi stessi, ovvero la **web reputation**.

La **web reputation**, ossia l'insieme di informazioni e dati presenti in rete riguardo a una persona (ma anche a un'azienda o a un prodotto), comprende tutto ciò che noi pubblichiamo su noi stessi, tutto ciò che inseriscono gli altri (documenti anagrafici, iscrizione a determinati servizi ecc.), nonché le conversazioni online che ci riguardano, di cui possiamo essere o meno consapevoli. Sappiamo bene che anche prima della nascita del web si scattavano fotografie in luoghi pubblici con altre persone o ci si lamentava con gli amici di qualcuno o di qualcosa. Perché con la rete questi comportamenti sono differenti? Perché quando postiamo su un social network una fotografia o scriviamo un commento, questi diventano disponibili a un **pubblico potenzialmente mondiale**, anche se noi siamo convinti che saranno visti soltanto dalla nostra cerchia di conoscenti. Una frase denigratoria su una persona potrà essere letta dai nostri amici, ma anche dall'interessato, dai suoi genitori o dai professori... Non dobbiamo scordarci che ciò che postiamo potrebbe rivelarsi lesivo, oltre che degli altri, anche di noi stessi: nel web il contenuto permane, e una foto o un commento che oggi consideriamo innocente potrebbe invece crearci dei problemi anche dopo diversi anni.



**La sicurezza informatica.** Infine, dobbiamo accennare al tema della **sicurezza informatica** (*information security*), che si riferisce alle strategie da adottare affinché:

- le informazioni che una persona ha raccolto o creato siano accessibili secondo le sue preferenze (per esempio solo alla sua cerchia di amici e non ad altri);
- le comunicazioni digitali avvenute via mail, chat o altri sistemi di messaggistica siano conosciute soltanto dai partecipanti alla comunicazione stessa;
- i dati contenuti nelle comunicazioni non vengano corrotti, modificati o distrutti per errore.

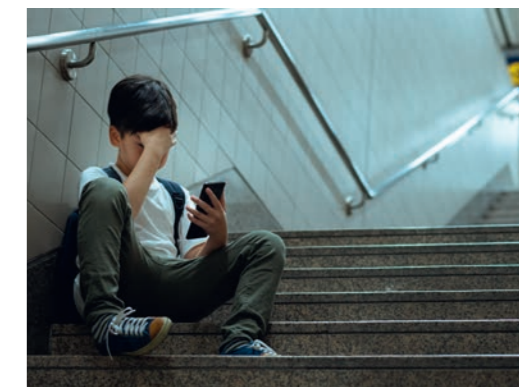
Sicurezza informatica significa anche **protezione dei propri strumenti digitali** affinché nessun altro li usi e possa trarne informazioni su di noi o sui nostri contatti, per esempio attraverso l'uso di password sicure.

### CONSIGLI PER UNA CORRETTA GESTIONE DELLA PROPRIA PRIVACY

- Evitate di diffondere informazioni personali come l'indirizzo di casa e della scuola, o il numero di telefono, a meno che non siate certi che rimangano all'interno di piattaforme (per esempio quella della scuola o quella del Ministero per l'iscrizione scolastica) dove sono chiaramente indicate le modalità di gestione della privacy.
- Ogni volta che pubblicate una foto, chiedetevi se vi darebbe fastidio che la vedesse un amico, un genitore, un insegnante, un futuro datore di lavoro. Nel dubbio, evitate di pubblicarla.
- Quando pubblicate una foto con altre persone chiedete sempre l'autorizzazione. Se nella foto sono presenti passanti o estranei, evitate di postarla o cancellatene il volto prima della pubblicazione.
- Utilizzate password per i servizi e gli ausili informatici che usate. Le password devono contenere maiuscole, minuscole, lettere e simboli ed essere differenti tra loro. Comunicatele soltanto ai vostri genitori.
- Controllate sempre le impostazioni dei social network che utilizzate e, dove possibile, scegliete di aumentare la privacy rendendo visibili post e informazioni personali unicamente ai vostri conoscenti diretti.

**Quando le informazioni arrecano danno.** Esistono alcune situazioni in cui vengono diffuse informazioni (vere o presunte) con la finalità di arrecare un danno a qualcuno, per esempio con la diffusione di **informazioni riservate su un'azienda o un prodotto** per influenzare il mercato o con la divulgazione di **notizie private e personali** su un personaggio famoso allo scopo di influenzare l'opinione pubblica. Un terzo caso su cui è fondamentale concentrare l'attenzione, perché riguarda la vita dei più giovani, è il **cyberbullismo**, ovvero, secondo la definizione fornita dalla legge n. 71/2017 «*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito dei dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche*

Il cyberbullismo è un fenomeno grave che colpisce le fasce giovani della popolazione che il web ha contribuito a diffondere.



uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo».

È un fenomeno grave, che riguarda principalmente i ragazzi, a cui le leggi cercano di fornire strumenti nuovi per difendersi.

### Rifletti e rispondi

1. La cittadinanza digitale:
  - A corrisponde al concetto di cittadinanza tradizionale
  - B a differenza della cittadinanza tradizionale non prevede specifici diritti e doveri
  - C si riferisce alla capacità di una persona di partecipare alla vita online
  - D vale solo per chi sa usare in modo consapevole i servizi Internet
2. Il digital divide indica:
  - A il divario generazionale tra chi è nato prima o successivamente alla nascita di Internet
  - B il divario tra chi ha accesso alle tecnologie dell'informazione e chi ne è escluso
  - C l'uso consapevole e corretto dei Internet
  - D un sistema di sicurezza che può bloccare il traffico in entrata o in uscita da una determinata rete
3. La web reputation indica:
  - A tutte le forme di violazione della privacy
  - B la condizione di chi è soggetto a forme di cyberbullismo
  - C l'insieme delle informazioni e dei dati presenti in rete con riferimento a una persona
  - D l'insieme dei dati sensibili di un soggetto

### EMPLOYABILITY SKILLS Competenze digitali ●●

Fai una ricerca nel web su te stesso e verifica se il profilo che emerge corrisponde all'immagine che vuoi dare di te. Prova a immedesimarti nei tuoi genitori, in un tuo docente, in un futuro datore di lavoro e valuta se è opportuno che conoscano le informazioni personali che hai reso pubbliche. Per svolgere questo compito:

- Tieni traccia di tutti i passaggi che fai, segna i link visitati e le informazioni raccolte.
- Inserisci il tuo nome e cognome tra virgolette (es. "Mario Rossi") su due o più motori di ricerca. Aggiungi caratteristiche che ti riguardano, come la città di provenienza o la tua attività sportiva (es. "Mario Rossi" Bologna, "Mario Rossi" alunno, "Mario Rossi" calcio ecc.).

- Sugli stessi motori di ricerca, seleziona la voce Immagini e verifica quante e quali "immagini" di te sono presenti. Apri le pagine web e controlla quali altre informazioni contengono (nomi di società sportive o scuole, eventi a cui hai partecipato, luoghi che frequenti).
- Controlla i tuoi profili sui social network e analizza le informazioni presenti. Su alcuni social le impostazioni per la gestione della privacy permettono di rendere visibili alcuni contenuti a un determinato pubblico. Spesso, offrono la possibilità di selezionare la modalità per vedere se le impostazioni sono corrette. Verifica l'elenco dei gruppi cui appartieni.