

# La cittadinanza digitale

## SVILUPPO SOSTENIBILE

9 IMPRESE,  
INNOVAZIONE  
E INFRASTRUTTURE



VIDEO

9c. Aumentare in modo significativo l'accesso alle tecnologie di informazione e comunicazione e impegnarsi per fornire ai paesi meno sviluppati un accesso a Internet universale ed economico entro il 2020



“ L'accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.

(Dichiarazione dei diritti in Internet, art. 2.1)

## Che cos'è la cittadinanza digitale

La cittadinanza, cioè la **condizione di cittadino**, è caratterizzata da un insieme di diritti e di doveri stabiliti dal sistema legislativo di uno Stato. Si definisce "cittadinanza digitale" l'insieme dei diritti e dei doveri che devono essere rispettati quando si utilizzano **le tecnologie dell'informazione e della comunicazione (TIC)**: tale concetto indica dunque la posizione giuridica degli individui in quanto partecipi di una **società digitale**.

Non ci troviamo di fronte a una nuova forma di cittadinanza in sostituzione di quella tradizionale, ma piuttosto a un ampliamento e a un adattamento di quest'ultima alla luce dello sviluppo delle TIC, e al fatto che la società digitale è diventata una dimensione ineludibile entro cui si realizza l'attività delle persone. Di fronte a questo cambiamento e alle nuove esigenze che ne derivano, lo Stato ha il dovere di assicurare ai cittadini gli strumenti e i servizi per poter accedere a Internet, ha l'obbligo di garantire a ciascuno la possibilità di acquisire le competenze per servirsi delle nuove tecnologie, infine ha il dovere di regolamentare la partecipazione agli spazi digitali.

# 1 ORIGINI E CARATTERI DELLA CITTADINANZA DIGITALE ALL'ALBA DEL TERZO MILLENNIO

## 1 Dalla diffusione dei nuovi media alla cittadinanza digitale

La diffusione delle **tecnologie dell'informazione e della comunicazione (TIC)** – in particolare Internet e i social media – a partire dagli anni Novanta del secolo scorso ha rapidamente modificato non soltanto il rapporto tra le persone, ma anche quello tra i cittadini e le istituzioni: attraverso Internet è possibile ad esempio gestire pratiche burocratiche e sviluppare un'attività lavorativa.

Proprio l'importanza assunta dagli strumenti digitali ha determinato da un lato la necessità di garantirne l'accesso e la fruizione da parte di tutti, dall'altro il bisogno di elaborare una normativa che ne regolamenti l'uso. È emersa in altre parole l'esigenza di definire **nuovi diritti e nuovi doveri dei cittadini**, che fino a quel momento non erano stati esplicitamente previsti dalla normativa (Carte costituzionali o legislazione ordinaria): a partire dai primi anni del nuovo millennio, per indicare tali diritti e doveri si è iniziato a utilizzare l'espressione "**cittadinanza digitale**".

## 2 L'esigenza di norme e di principi etici relativi alle TIC

Uno degli aspetti caratteristici della cittadinanza digitale è la difficoltà di **adeguare efficacemente la legislazione** – la cui elaborazione necessita di procedure complesse e tempi distesi – **alle novità tecnologiche** – che si susseguono invece con una velocità crescente: il rischio è che le norme si dimostrino obsolete prima ancora di essere approvate e di entrare effettivamente in vigore.

Anche per questo motivo è diventato particolarmente importante che, accanto a norme giuridicamente vincolanti (leggi, decreti ecc.), si affermino tra gli utenti delle TIC nuove **regole etiche** ampiamente condivise e una diffusa consapevolezza circa le possibili conseguenze – positive o negative – dell'utilizzo di quelle tecnologie.

▼ Elaborazione grafica sul tema dell'interconnessione digitale nella società contemporanea.



## 2 LA PROSPETTIVA ATTUALE

### L'ACCESSO A INTERNET

#### Le competenze digitali

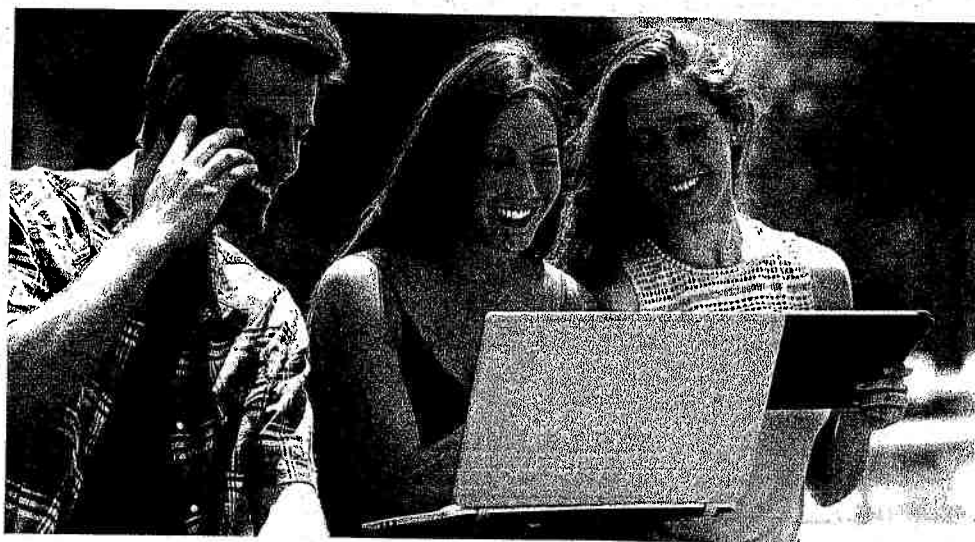
**Le tre categorie di utenti digitali** Dal punto di vista del rapporto con le TIC, la popolazione può essere divisa in tre grandi categorie: i nativi digitali, gli immigrati digitali e gli analfabeti digitali.

I **nativi digitali** sono gli individui più giovani – all'incirca quelli nati a partire dagli anni Novanta del secolo scorso –, i quali sono cresciuti in un contesto sociale e culturale già ampiamente permeato dalla diffusione delle TIC, che hanno imparato a usare fin dai primi anni di vita.

Gli **immigrati digitali** sono invece coloro che, appartenendo alle generazioni precedenti, hanno iniziato a utilizzare quelle tecnologie soltanto in età adulta.

Vi sono poi gli **analfabeti digitali**, i quali possono essere ulteriormente distinti in due tipologie: assoluti e funzionali. Gli analfabeti digitali **assoluti** – in genere la parte più anziana della popolazione – sono coloro che non sono in grado di usare un computer o altri dispositivi digitali nemmeno a un livello basilare. Gli analfabeti digitali **funzionali** sono invece le persone che, pur capaci ad esempio di azionare un computer, scrivere un testo su un file e collegarsi a Internet, non sono però in grado di svolgere le funzioni digitali più complesse, in particolare di usare la rete in maniera efficace e consapevole.

**Il diverso utilizzo delle tecnologie digitali** Significative differenze sono riscontrabili nel modo in cui vengono impiegate le TIC rispettivamente da parte dei nativi e degli immigrati digitali. I primi, infatti, proprio perché nati e cresciuti in un mondo già sostanzialmente digitalizzato, hanno nei confronti delle TIC una

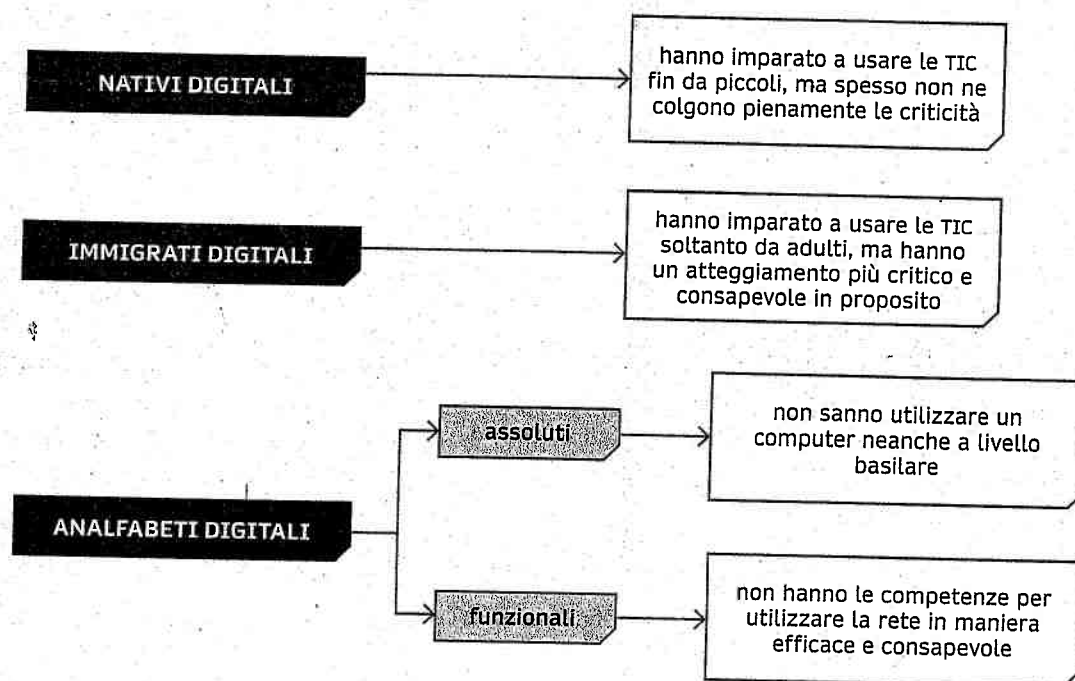


► Tre giovani "nativi digitali" impegnati nell'uso di dispositivi elettronici.

**dimestichezza quasi naturale**, che non può appartenere agli immigrati: sanno usare con grande velocità e destrezza gli strumenti informatici e telematici. Al tempo stesso, l'immersione totale nel mondo digitale rende **più difficile** alle nuove generazioni riflettere con il necessario **distacco critico** sulle potenzialità delle TIC e soprattutto sulle loro eventuali problematicità. Questa particolare situazione spiega almeno in parte un apparente paradosso relativo alla diffusione dell'analfabetismo digitale nelle società sviluppate. In effetti, se l'analfabetismo assoluto riguarda soprattutto la parte più anziana della popolazione, quello funzionale risulta più diffuso tra i nativi che tra gli immigrati digitali. Questi ultimi, infatti, proprio perché consci delle lacune conoscitive da cui partono, sono più spesso consapevolmente impegnati nell'acquisizione di **competenze digitali complesse e raffinate**. Molti nativi, invece, malgrado la loro familiarità con il computer, non acquisiscono per questo solo fatto le competenze proprie di un'alfabetizzazione digitale funzionale, ad esempio la capacità di estrapolare informazioni significative dai dati, riconoscendo gli errori e distinguendo le fonti inaffidabili da quelle attendibili.

In tale situazione, le politiche orientate alla promozione della cittadinanza digitale presso tutte le fasce della popolazione devono mirare da un lato a realizzare **programmi di alfabetizzazione di base** rivolti alle generazioni più anziane, dall'altro a diffondere un **uso consapevole e funzionale** delle TIC soprattutto da parte dei nativi digitali. ► **LA QUESTIONE**, p. 106

### Le categorie della popolazione digitale





#### LE PAROLE DEL DIRITTO

##### **digital divide**

Espressione inglese che indica il divario tra chi ha le possibilità e le competenze per accedere alla rete e usufruire di essa, e chi invece ne è escluso.

## Il digital divide

**La Dichiarazione dei diritti in Internet** L'esigenza di garantire a tutti il diritto di accesso a Internet è stata riconosciuta in Italia nel 2015 con l'approvazione della Dichiarazione dei diritti in Internet, il cui articolo 2 sancisce che

“L'accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità.

**Il divario geografico** La questione del diritto di accesso a Internet è strettamente connessa a quella del **digital divide**, che presenta differenti aspetti. Esiste innanzitutto un divario geografico. Infatti, **non tutte le aree sono ugualmente coperte da efficaci connessioni Internet**. Questo è vero innanzitutto a livello mondiale: in vaste regioni dell'Africa e dell'Asia i collegamenti sono ancora difficili. Aree poco servite sono tuttavia presenti anche in molti paesi sviluppati, tra cui l'Italia: si tratta in particolare di zone montane o scarsamente popolate, i cui abitanti rischiano di essere di fatto almeno parzialmente esclusi da un effettivo accesso alla rete. È quindi necessario che le pubbliche istituzioni intervengano per garantire uguali diritti in tal senso.

#### LA QUESTIONE

### La digitalizzazione: opportunità di sviluppo o rischio di esclusione?

Nel 2012 il nostro paese ha adottato l'Agenda digitale italiana, un documento che fissa le strategie per realizzare la piena diffusione delle tecnologie dell'informazione e della comunicazione nella pubblica amministrazione, nelle imprese private e presso tutti i cittadini. Il 16 maggio 2019 il responsabile per l'attuazione dell'Agenda ha presentato il Manifesto per la Repubblica Digitale, relativamente al quale riportiamo alcune dichiarazioni.

“Il Commissario Straordinario per l'attuazione dell'Agenda Digitale Luca Attias oggi ha presentato il “Manifesto per la Repubblica Digitale”. In sede di Forum PA, la manifestazione nazionale dedicata al mondo della Pubblica Amministrazione, Attias ha ufficializzato il «documento rivolto a istituzioni e privati che fissa alcuni principi per diffondere consapevolezza e competenze con l'obiettivo dell'inclusione digitale».

Con il motto “L'Italia è fatta, facciamola digitale!”, l'obiettivo è quello di un impegno condiviso per realizzare azioni concrete a favore dell'educazione digitale, la cittadinanza digitale e l'etica digitale. Quindi puntare su scuole, programmi, iniziative mediatiche, senza contare la rimozione di ogni tipo di ostacolo per l'uso di servizi pubblici e privati digitali.

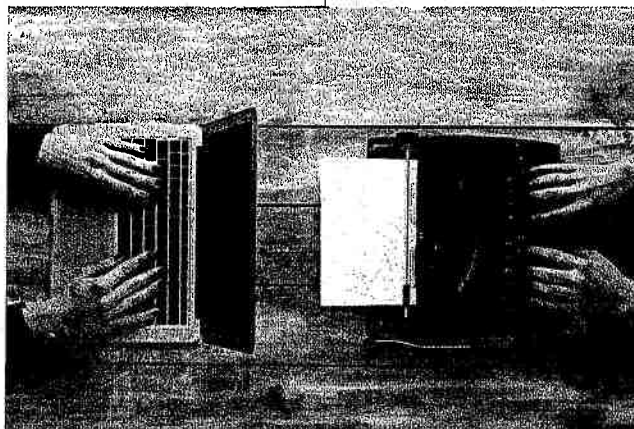
«In Italia ci sono dai 9 agli undici 11 milioni di persone che non sono in condizione di usufruire dei servizi digitali, anche dei migliori servizi digitali che possiamo sviluppare, perché mancano di sufficiente alfabetizzazione digitale e di consapevolezza de-

**Il divario economico** Un secondo aspetto del *digital divide* è quello più propriamente economico: molte persone, specialmente (ma non esclusivamente) nei paesi scarsamente sviluppati, **non hanno i mezzi necessari per acquistare** sia lo hardware necessario (computer, telefoni cellulari ecc.), sia i servizi di connessione forniti dalle compagnie telefoniche.

**L'analfabetismo digitale** Un terzo aspetto del *digital divide* è legato alle competenze digitali dei potenziali utenti. Malgrado l'enorme e crescente diffusione di Internet, sono infatti ancora moltissime nel mondo le persone che non possiedono le capacità minime necessarie per utilizzare gli strumenti informatici e telematici, sono cioè in una condizione di analfabetismo digitale assoluto.

**Il divario digitale come moltiplicatore delle disuguaglianze** In tutte le sue forme, il divario digitale rischia di essere un moltiplicatore delle disuguaglianze economiche e sociali. Infatti, per le sue svariate applicazioni l'accesso a **Internet**, e più in generale alle tecnologie dell'informazione e della comunicazione, è oggi un **fattore fondamentale di sviluppo**.

▼ Vecchie e nuove tecnologie a confronto.



gli strumenti messi a disposizione dalla tecnologia», ha ricordato Attias. «[...] Quello dell'inclusione digitale è un capitolo che non può essere ignorato, è parte integrante del processo di trasformazione digitale che come struttura siamo chiamati a gestire e accelerare».

Insomma, dovrebbe nascere un'alleanza tra Stato, cittadini, formazioni sociali e imprese per «sviluppare la cultura scientifico-tecnologica della popolazione e contrastare ogni forma di analfabetismo digitale – per le stesse ragioni e con la stessa determinazione con la quale, nel secondo dopoguerra, si superò l'analfabetismo linguistico – nonché ogni forma di discriminazione nell'accesso agli strumenti di cittadinanza digitale». ”

(D. D'Elia, *Manifesto per la Repubblica Digitale: obiettivo alfabetizzazione*, in tomshw.it, 16 maggio 2019)

## ATTIVITÀ DI RICERCA E DI DISCUSSIONE

L'articolo riportato solleva l'importante questione dell'inclusione digitale.

- Effettuate una ricerca in Internet per acquisire ulteriori informazioni sull'argomento, ad esempio su progetti di alfabetizzazione digitale nelle scuole, su corsi rivolti alla popolazione più anziana, sulle iniziative pubbliche e private volte a diffondere le TIC.
- Confrontatevi quindi in un dibattito in classe, sulla base del seguente interrogativo: la diffusione delle tecnologie digitali rappresenta un'occasione di crescita per tutti o costituisce un rischio di esclusione e marginalizzazione per le fasce più deboli della popolazione?
- Al termine del dibattito, dividetevi in due gruppi ed elaborate due distinte relazioni (max 3000 caratteri al computer) in cui riportare i principali argomenti a favore dell'una e dell'altra risposta.

Pertanto, proprio le persone e le società più deboli dal punto di vista economico e culturale, le quali spesso sono anche quelle che rischiano di essere escluse dal pieno utilizzo di tali tecnologie, vengono private di alcuni degli strumenti che potrebbero consentire loro di uscire da una condizione di difficoltà, e finiscono così in un circolo vizioso in cui la povertà tende ad autoalimentarsi.

## DIRITTI E DOVERI NELLA RETE

### La netiquette

**Le regole di buona educazione in rete** Una volta garantito l'accesso a Internet, si pone una serie di questioni relative ai diritti e ai doveri degli utenti della rete. Esistono in primo luogo **regole di comportamento non giuridicamente vincolanti**, bensì riconducibili a principi etici o anche semplicemente alla buona educazione. Si tratta, in particolare, della cosiddetta *netiquette*, espressione coniata unendo la parola inglese *net* ("rete") e quella francese *étiquette*, che significa appunto "buona educazione". La *netiquette* consiste in alcune semplici regole che è necessario seguire per essere considerato un utente di Internet – soprattutto di strumenti di comunicazione come posta elettronica, social media, blog e forum – corretto e rispettoso degli altri.

#### AGENDA 2030

**L'accesso alle tecnologie digitali come condizione di uno sviluppo sostenibile**

**OBIETTIVI**  **PER LO SVILUPPO SOSTENIBILE**

**L'impegno per la diffusione delle TIC** L'accesso alle TIC costituisce una condizione imprescindibile per la crescita economica, perché, fra l'altro, favorisce l'operatività delle imprese, rendendone più veloci ed efficienti i processi produttivi, i meccanismi amministrativi e le attività di comunicazione e commercializzazione. Tale accesso riveste importanza anche per le possibilità di promozione sociale dei singoli individui, offrendo loro visibilità e permettendo di far conoscere le proprie attività. Per questo motivo, nella prospettiva di una crescita globale equilibrata l'**Agenda 2030 per lo Sviluppo Sostenibile**, adottata dalle Nazioni Unite nel 2015 si propone (**Obiettivo 9, traguardo c**) di «Aumentare in modo significativo l'accesso alle tecnologie di informazione e comunicazione e impegnarsi per fornire ai paesi meno sviluppati un accesso a Internet universale ed economico entro il 2020».

**I dati sull'accesso a Internet** Secondo uno studio dell'Università di Oxford, nel **2015**, anno di approvazione dell'Agenda, la Cina era già il paese con più utenti di Internet (600 milioni), ma ancora oltre metà della popolazione di quello Stato non aveva accesso alla rete. Nel complesso, quasi **due terzi degli abitanti della**

**Terra ne rimaneva escluso.** Tra i paesi con almeno 10 milioni di abitanti, soltanto Paesi Bassi, Regno Unito, Giappone, Canada, Corea del Sud, Stati Uniti, Germania, Australia, Belgio e Francia avevano una percentuale della popolazione con accesso a Internet superiore all'80%. Alla fine del **2018**, secondo una stima dell'ITU (International Telecoms Union), **il 51,2% della popolazione mondiale era ormai connesso a Internet.** Negli Stati più sviluppati la quota degli utenti della rete aveva superato l'80%, mentre nei paesi in via di sviluppo essa si attestava in media soltanto a circa il 45%, ma il tasso di crescita era molto intenso. **L'Africa**, in particolare, aveva assistito al più rapido incremento del numero degli utenti di Internet, anche se nel 2018 restava il continente con la quota più bassa di popolazione con accesso alla rete, inferiore al 25%.

Le proporzioni del divario digitale tra le nazioni del mondo evidenzia come il traguardo 9c dell'Agenda 2030 risulti estremamente importante. La sua urgenza è dimostrata anche dal fatto che, mentre l'Agenda fissa al 2030 la scadenza per il raggiungimento della maggior parte dei propri obiettivi, in questo caso la **anticipa al 2020.**

**Alcuni esempi** Ad esempio, è importante fare un uso moderato dei **caratteri maiuscoli** perché, secondo le convenzioni vigenti nella rete, tale modalità di scrittura equivale ad "alzare la voce" e quindi esprime perlopiù **rabbia ed aggressività**. Oppure, per limitarsi alla posta elettronica, non è opportuno inviare un unico messaggio a un gran numero di persone senza utilizzare la funzione CNN (Copia carbone nascosta) – che impedisce a ognuno dei destinatari di vedere gli indirizzi mail di tutti gli altri –, a meno che non sia stata data un'esplicita autorizzazione: un tale comportamento, infatti, rappresenterebbe una **violazione della riservatezza dei propri corrispondenti**.

## Il cyberbullismo: tipologie e caratteristiche

**Le violenze attraverso la rete** Vi sono comportamenti nella rete che configurano veri e propri reati. Particolarmente grave è il fenomeno del cosiddetto cyberbullismo. Il termine è composto dal prefisso *cyber-*, che si riferisce alle situazioni caratterizzate da uno stretto rapporto tra essere umano e computer, e dalla parola "**bullismo**", che indica un'ampia gamma di comportamenti in cui un individuo è sottoposto a forme di violenza fisica o psicologica perlopiù da parte di gruppi di persone.

Il cyberbullismo è quindi un tipo di bullismo che utilizza le nuove tecnologie della comunicazione. Tale genere di comportamento può riguardare qualsiasi fascia di età, ma è molto diffuso tra gli adolescenti. Proprio per questo motivo, oggi si preferisce usare il termine soprattutto in riferimento alle situazioni in cui sia le vittime sia gli aggressori sono minorenni.

**Le varie forme di cyberbullismo** Il cyberbullismo si manifesta in molteplici forme. Tra le altre, possono essere ricordate:

- le **molestie**, consistenti nell'invio ripetuto alla vittima di messaggi offensivi;
- la **denigrazione**, che si verifica quando si diffondono online contenuti (informazioni, foto, video ecc.) mirati a danneggiare la reputazione di qualcuno;
- l'**esclusione** da un gruppo virtuale (come una chat o un social network) allo scopo di ingenerare un sentimento di emarginazione;
- il **cyberstalking**, consistente nell'invio reiterato di messaggi minacciosi finalizzati a incutere paura.

**Le specificità del cyberbullismo** La specificità del bullismo online consiste in primo luogo nel fatto che in esso il **carattere virtuale delle azioni** – cioè il fatto che vengono messe in atto attraverso la mediazione della rete – riduce i freni inibitori e quindi favorisce **comportamenti aggressivi o persecutori**. In effetti, gli stessi soggetti, che difficilmente utilizzerebbero di persona espressioni pesantemente offensive o denigratorie, lo fanno più agevolmente attraverso gli strumenti telematici, che possono spesso garantire l'anonimato: in tal modo, il cyberbullo tende a non essere del tutto consapevole della gravità delle proprie azioni, e a non sentirsene pienamente responsabile.

Un'altra caratteristica del bullismo online è il fatto che in molti casi i comportamenti che lo caratterizzano hanno **effetti di ampia portata e duraturi** nel tempo. Ad

### LE PAROLE DEL DIRITTO

#### cyberstalking

Il verbo inglese *to stalk* significa "avvicinarsi furtivamente", "seguire con insistenza", "assillare". Unito al prefisso *cyber-*, indica il reato che comporta l'utilizzo di dispositivi informatici di comunicazione come Internet o la posta elettronica con la finalità di molestare una persona.





anche 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.

L'intento principale della legge non è repressivo, anche perché i cyberbulli sono spesso essi stessi minori, e come tali parzialmente o totalmente non punibili sul piano penale. Essa si pone piuttosto prioritariamente l'obiettivo di **prevenire e contrastare gli atti di cyberbullismo**.

**La rimozione dei dati personali** In particolare, l'**articolo 2** della legge prevede, per la famiglia di un minore vittima o per il minore stesso se abbia già compiuto i quattordici anni di età, la possibilità di ottenere la rimozione dei dati personali dalla rete. A tal fine deve rivolgersi in prima istanza ai gestori dei siti o dei social su cui siano stati illecitamente pubblicati e, qualora questi non ottemperino alla richiesta, al Garante per la protezione dei dati personali.

**L'aspetto educativo** Particolare importanza è riservata dalla legge all'aspetto educativo. L'**articolo 4** stabilisce che

“Ogni istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio. [...] le istituzioni scolastiche di ogni ordine e grado [...] promuovono l'educazione all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche.

È in effetti fondamentale che tutti gli utenti di Internet – giovani o adulti – siano educati a un **uso responsabile della rete**. Molti di loro non sono pienamente consapevoli dei pericoli cui si può andare incontro navigando nel web, e corrono così il rischio non soltanto di diventare vittime di reati ma anche, paradossalmente, di commetterne senza neppure saperlo. È il caso della diffusione di immagini che possono ledere la dignità di una persona: un comportamento che qualcuno potrebbe irresponsabilmente considerare uno scherzo innocuo, ma che è invece penalmente perseguibile.

## ▲ **Lo hate speech**

**Le caratteristiche del fenomeno** Un fenomeno per alcuni aspetti analogo al cyberbullismo è lo *hate speech*, “discorso di incitamento all'odio”. Con tale espressione si indica la diffusione in rete, in particolare attraverso l'uso dei social network, di messaggi violenti e aggressivi mirati a creare un clima di intolleranza nei confronti di gruppi di persone, perlopiù minoranze, caratterizzate dalla comune appartenenza etnica, religiosa o politica, oppure ancora da disabilità o da particolari orientamenti sessuali. Anche in questo caso gli strumenti telematici tendono a favorire l'**esasperazione**

**razione del linguaggio:** per quanto riguarda i social, il fatto di diffondere i propri messaggi in primo luogo tra persone con valori e convinzioni comuni rende più facile radicalizzare le posizioni. Si presume infatti gradito o accettato all'interno del gruppo l'utilizzo di termini ed espressioni estremi che in un contesto più diversificato, in cui fossero presenti anche altri punti di vista, ci si vergognerebbe di scrivere o pronunciare.

**La normativa vigente** Come già si è visto a proposito del cyberbullismo, nella maggior parte dei paesi non esiste una normativa specifica per combattere i comportamenti di *hate speech*, ma alcuni di essi possono configurare reati previsti dal codice penale. In Italia, ad esempio, la cosiddetta **legge Mancino** (decreto legge 122 del 26 aprile 1993) punisce «con la reclusione sino a tre anni chi diffonde in qualsiasi modo idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero incita a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi».

Anche quando lo *hate speech* non rappresenta un vero e proprio reato può tuttavia essere combattuto in diversi modi, in particolare attraverso **forme di autoregolamentazione** attuate dagli stessi gestori degli spazi virtuali. Ad esempio, alcune testate giornalistiche hanno deciso di vagliare preventivamente i commenti postati dagli utenti nel proprio sito prima di pubblicarli e renderli così visibili a tutti i lettori. Anche molti social network vietano l'incitamento all'odio, riservandosi di rimuovere i post che non rispettino tale divieto. È comunque importante notare che – in rete come nei media più tradizionali – si pone sempre il problema di conciliare il divieto dello *hate speech* con la libertà di espressione e di stampa, garantita in Italia dall'**articolo 21** della Costituzione: «Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure».

## **Il Regolamento generale sulla protezione dei dati**

**Il phishing** Tra le numerose attività illecite di cui si può diventare vittime nella rete vi sono diversi tipi di **frode informatica**, ad esempio il cosiddetto *phishing* (variante del termine *fishing*, che significa “pescare”, nel senso di “recuperare dati privati attraverso Internet”). Tale genere di truffa consiste in genere nella falsa richiesta via mail da parte della propria presunta banca o di altri istituti e aziende, di effettuare particolari operazioni con la carta di credito o sul conto corrente: se la vittima cade nel tranello e risponde ingenuamente alla richiesta, il truffatore entra in possesso dei codici di accesso che gli consentono di sottrarre somme di denaro anche assai ingenti.

**La tutela dei dati personali** Questo fenomeno, insieme ad altri, ha fatto emergere l'esigenza di tutelare i dati personali dei cittadini, in particolare quelli raccolti con strumenti informatici e telematici, contro un loro uso illegittimo. Su tale questione l'Unione europea è intervenuta in forma sistematica nel 2016, emanando il **Regolamento UE 2016/679**, comunemente noto come **Regolamento generale**

sulla **protezione dei dati** o GDPR (*General Data Protection Regulation*), entrato in vigore in Italia nel 2018. Si tratta di un provvedimento assai complesso, di cui si possono tuttavia indicare i punti principali.

Il Regolamento definisce come **"dato personale"** qualsiasi informazione relativa a una persona identificata o identificabile: si tratta ad esempio del nome, di dati relativi all'indirizzo, o di elementi caratteristici della sua identità. Il Regolamento prevede che per raccogliere dati personali qualsiasi azienda privata o ente pubblico debba ottenere dall'interessato un consenso «dato liberamente, specifico, informato e chiaramente indicato» ed esplicitare in maniera chiara il modo in cui quei dati verranno elaborati e utilizzati.

Nella norma sono previsti il **diritto alla rettifica dei dati** (cioè che i dati precedentemente raccolti possano essere corretti su richiesta dell'interessato) e il **diritto all'oblio** (ovvero che i dati vengano cancellati dopo che siano cessate le esigenze per cui erano stati raccolti). Essa stabilisce inoltre precise responsabilità per le aziende e gli enti in merito alla conservazione dei dati raccolti, in particolare in formato digitale, per evitare che possano essere anche accidentalmente divulgati e utilizzati per scopi diversi da quelli per cui erano stati ottenuti.

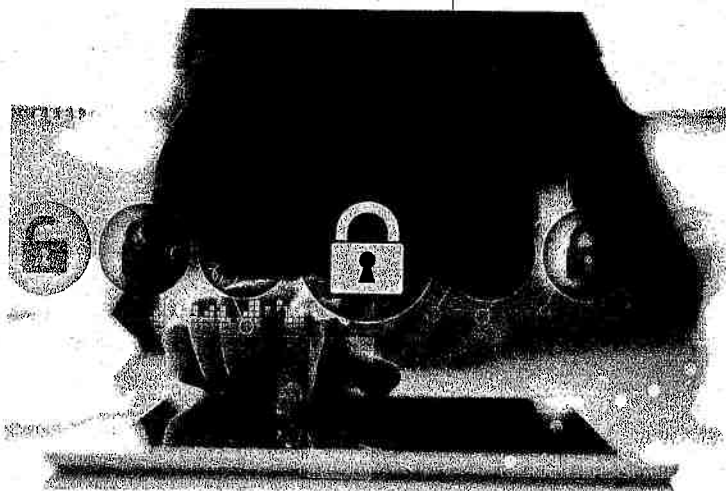
**Il divieto di trattamento dei dati particolari** Molta attenzione viene riservata ai **"dati particolari"**, ovvero i dati personali relativi all'origine etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, oppure all'appartenenza sindacale, all'orientamento sessuale, nonché i dati genetici, quelli biometrici (quali impronte digitali o immagini facciali) e quelli sulla salute fisica e mentale. Il GDPR vieta il trattamento di tali dati, salvo eccezioni esplicitamente specificate, ad esempio quando sia «necessario per motivi di interesse pubblico nel settore della sanità pubblica»: si pensi al caso in cui conoscere i dati sulla salute di una persona (anche se privati) sia fondamentale per impedire il diffondersi di un'epidemia.

## LA PUBBLICA AMMINISTRAZIONE NELLA SOCIETÀ DIGITALE

### ▲ La Carta della cittadinanza digitale

Le tecnologie digitali hanno modificato profondamente il rapporto delle persone con le istituzioni e con le pubbliche amministrazioni, talvolta contribuendo a semplificarlo. Da questo punto di vista, le prerogative dei cittadini digitali sono state fissate in Italia con la Carta della cittadinanza digitale, approvata dal Parlamento nel

▼ Elaborazione grafica sul tema della protezione dei dati personali nel web, che costituisce una tematica importante e delicata connessa alla società digitale.





## LE PAROLE DEL DIRITTO

## legge delega

Si tratta di un provvedimento legislativo con cui il Parlamento delega il governo a legiferare su un determinato argomento.

2015 e concepita come una **legge delega** che stabilisce alcune linee guida cui devono ispirarsi successivi decreti in materia. Uno degli obiettivi fissati dalla Carta è quello di

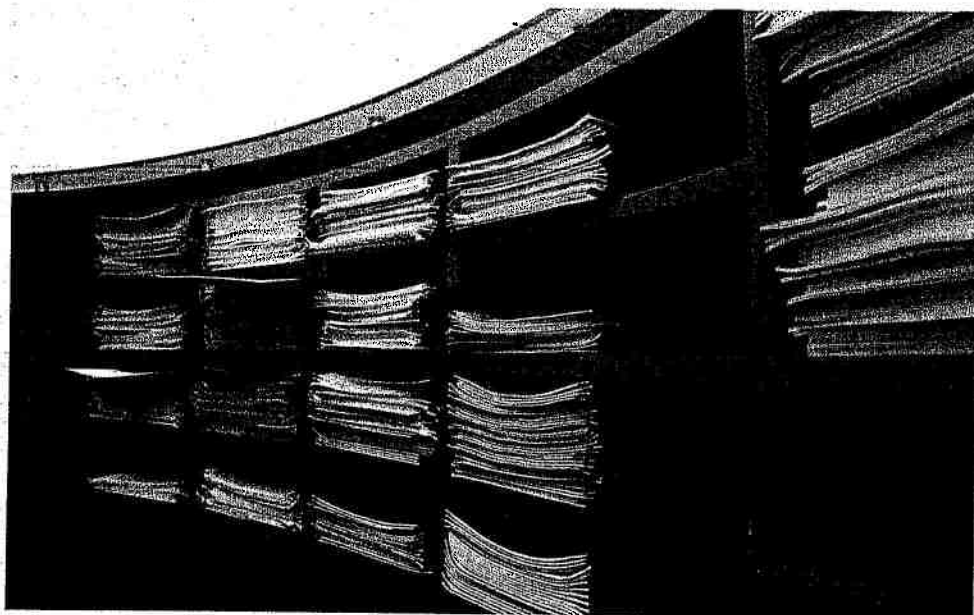
■ garantire ai cittadini e alle imprese, anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale, nonché [...] garantire la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici.

In concreto, questo significa che lo Stato si impegna a diffondere in maniera capillare le TIC nella pubblica amministrazione, in modo che il maggior numero possibile di pratiche burocratiche (come la richiesta di documenti o certificati, pagamenti ecc.) sia **espletabile online**, senza doversi recare personalmente negli uffici.

### ▲ La semplificazione della burocrazia

**Il sistema pubblico di identità digitale** Per rendere ancora più semplice l'accesso telematico ai servizi della pubblica amministrazione, la Carta della cittadinanza digitale prevede che nei rapporti con quest'ultima si possa largamente far uso del **Sistema pubblico di identità digitale** (SPID), già diventato operativo con il decreto ministeriale del 24 ottobre 2014. Lo SPID prevede che ogni cittadino e ogni impresa possano dotarsi, facendone richiesta ad alcuni enti autorizzati (tra cui gli uffici postali), di un'**identità digitale** – in pratica un username e una password – e utilizzarla per gestire autonomamente online gran parte dei propri rapporti con la pubblica amministrazione (dichiarazione dei redditi e altre pratiche fiscali, pratiche pensionistiche, richiesta di documenti a comuni e regioni ecc.). Oltre che nella possibilità

► Documenti archiviati in un ufficio pubblico. In Italia la pubblica amministrazione è tenuta a facilitare progressivamente l'accesso online a documenti e pratiche per il cittadino.



di operare a distanza, la novità dello SPID consiste nel fatto che gli utenti possono svolgere per mezzo di un'unica identità digitale una **varietà di operazioni** con una molteplicità di distinte pubbliche amministrazioni. È questo soltanto un esempio di come lo sviluppo delle TIC possa facilitare e semplificare la vita dei cittadini, ma la Carta si occupa anche di altre analoghe questioni.

**La firma digitale** In particolare, essa promuove la diffusione della firma digitale. Si tratta di un sistema con cui l'utente titolare di tale servizio – utilizzando un username, un numero di identificazione personale (PIN) e una password – può **modificare un file** in modo che esso risulti **legato univocamente alla propria identità digitale**. Il meccanismo è concettualmente identico a quello della firma autografa su documento cartaceo, ma con il vantaggio derivante dal fatto che il file firmato digitalmente può essere trasmesso online – ad esempio via mail o caricandolo sulle piattaforme telematiche di enti pubblici o privati – senza alcun trasferimento o spostamento fisico.

**La condivisione delle informazioni** Inoltre, grazie alla sempre più ampia diffusione delle TIC, tutte le pubbliche amministrazioni possono facilmente condividere informazioni e documentazioni. Questo genera ancora una volta vantaggi per i cittadini, ma facilita anche importanti attività quali la **lotta all'evasione fiscale**. Infatti, incrociando i dati in possesso di differenti amministrazioni pubbliche possono essere evidenziate incongruenze, ad esempio tra le spese e i patrimoni dei contribuenti da un lato e le loro dichiarazioni dei redditi dall'altro, permettendo di ipotizzare che queste ultime possano essere non veritiere.

## LABORATORIO DI CITTADINANZA ATTIVA

### ARGOMENTARE E DIBATTERE

Navigando in Internet su blog, siti, forum ecc. ti è capitato di leggere frasi contrarie alla *netiquette* o manifestazioni di *hate speech*? Che impressione ti hanno fatto? Argomenta le tue opinioni in proposito in un testo di circa 3000 caratteri. Quindi confronta la tua esperienza con quella dei tuoi compagni, avviando un dibattito in classe sull'argomento moderato dall'insegnante.

### COMPITO DI REALTÀ

Immaginate di essere i referenti nella vostra scuola per la prevenzione e il contrasto del cyberbullismo, e di dover elaborare un'iniziativa che possa essere realizzata direttamente dagli studenti.

Dopo una discussione in classe, un gruppo ristretto viene incaricato di riassumere la proposta in un testo scritto di non più di 3000 caratteri. Il testo deve essere valutato dall'intera classe (con l'apporto di eventuali modifiche), al fine di pervenire a una versione definitiva da presentare al Consiglio di Istituto tramite i rappresentanti degli studenti in tale organismo. L'obiettivo è che la proposta sia esaminata ed eventualmente messa in atto.