Mario Gabbari
Antonio Gaetano
Roberto Gagliardi
Daniela Sacchi*

Educazione alla cittadinanza digitale e alla sicurezza in rete

La Rete Internet non è una realtà parallela, ma è diventata lo spazio in cui si svolge una parte sempre più importante della nostra vita.

Vita reale e vita virtuale sono sempre più connesse e la rivoluzione digitale trasforma, in dati e informazioni, porzioni sempre più rilevanti delle nostre esistenze e pone problemi nuovi per le nostre libertà.

Gli studenti per comunicare, imparare, lavorare e giocare in modo responsabile in quest'ambiente, devono sviluppare una molteplicità di competenze che consentano loro di sfruttare i vantaggi e le opportunità della rete, ma devono anche conoscere, per superarle, le insidie che incontreranno.

Un investimento in sensibilità e in educazione civica digitale

Nelle nostre scuole, il problema della sicurezza in rete viene ancora sottovalutato e si investe poco sia in termini di risorse economiche, sia in interventi di tipo culturale, anche nella formazione dei docenti.

È necessario invece fare uno sforzo per abituare gli studenti all'assunzione di responsabilità, in modo sempre più consapevole e maturo, verso sè stessi e verso l'interesse della comunità in genere.

Generalmente per "sicurezza" si intende la capacità di applicare le regole che stabiliscono chi può accedere alle risorse e alle informazioni e in che modo. Alcune di queste informazioni devono essere fruibili solo da chi è riconosciuto (autenticazione) e legittimato (autorizzazione) e il compito dei dispositivi di sicurezza è proprio quello di garantirne l'accesso. Riservatezza, integrità e disponibilità sono le parole chiave che accompagnano il percorso sulla sicurezza. Solo chi è "autorizzato", cioè solo chi ha avuto assegnato il diritto di accesso, deve poter garantire l'integrità dell'informazione, eventualmente modificarla e decidere se renderla disponibile.

La Rete è un "mare" che offre infinite opportunità, ma nei confronti del quale è necessario che gli alunni mettano a punto conoscenze specifiche di base e alcuni strumenti critici indispensabili, per capirne le dinamiche e navigare in modo responsabile e in sicurezza. Il mondo della rete Internet richiede la presenza e la formazione da parte dei docenti, di percorsi rivolti alla costru-

* Equipe Formazione Digitale di OPPI Milano.

zione di azioni e comportamenti per fornire, a tutti gli studenti un'educazione civica digitale finalizzata a un comportamento corretto.

L'educazione civica digitale rappresenta quindi la conquista di un nuovo spazio che aggiorna e integra l'apprendimento dell'educazione civica tradizionale.

Il tutto è orientato a consolidare lo sviluppo di capacità critiche, di una formazione che renda gli studenti protagonisti per una partecipazione e un coinvolgimento più attivo nella nuova società digitale.

L'Educazione Civica Digitale[1] è diventata pertanto uno spazio di formazione che ha come obiettivo la realizzazione di un mondo virtuale, ricco di occasioni, sanificato e utilizzabile da tutti.

I temi più efficaci, che devono necessariamente accompagnare la diffusione e la pratica dell'educazione civica digitale, sono lo sviluppo di:

- **Capacità critiche**, perché è fondamentale essere pienamente consapevoli che, accanto alle indiscusse potenzialità legate all'uso della tecnologia digitale, si nascondono anche profonde implicazioni sociali, culturali ed etiche;
- **Responsabilità**, poiché i media digitali hanno assunto non solo il ruolo di utilizzo, ma anche quello di produzione e di pubblicazione di messaggi con le implicazioni che ne derivano.

Grazie alle capacità critiche e alla responsabilità nasce e cresce l'abilità a migliorare le potenzialità offerte dalla tecnologia digitale (es. educazione, partecipazione, creatività e socialità) e a minimizzare gli aspetti negativi (es. sfruttamento commerciale, violenza, comportamenti illegali, informazione manipolata e discriminatoria).

[1] Si veda Legge 92/2019 Art. 5, in **gazzettaufficiale.it/eli/id/2019/08/21/19G00105/** (ultimo accesso novembre 2022). Nell'ambito dell'insegnamento trasversale dell'educazione civica, di cui all'articolo 2, è prevista l'educazione alla cittadinanza digitale. 2. Nel rispetto dell'autonomia scolastica, l'offerta formativa erogata nell'ambito dell'insegnamento di cui al comma 1 prevede almeno le seguenti abilità e conoscenze digitali essenziali, da sviluppare con gradualità tenendo conto dell'età degli alunni e degli studenti: 3. a) analizzare, confrontare e valutare criticamente la credibilità e l'affidabilità delle fonti di dati, informazioni e contenuti digitali; 4. b) interagire attraverso varie tecnologie digitali e individuare i mezzi e le forme di comunicazione digitali appropriati per un determinato contesto; 5. c) informarsi e partecipare al dibattito pubblico attraverso l'utilizzo di servizi digitali pubblici e privati; ricercare opportunità di crescita personale e di cittadinanza partecipativa attraverso adeguate tecnologie digitali; 6. d) conoscere le norme comportamentali da osservare nell'ambito dell'utilizzo delle tecnologie digitali e dell'interazione in ambienti digitali, adattare le strategie di comunicazione al pubblico specifico ed essere consapevoli della diversità culturale e generazionale negli ambienti digitali; 7. e) creare e gestire l'identità digitale, essere in grado di proteggere la propria reputazione, gestire e tutelare i dati che si producono attraverso diversi strumenti digitali, ambienti e servizi, rispettare i dati e le identità altrui; utilizzare e condividere informazioni personali identificabili proteggendo se stessi e gli altri; 8. f) conoscere le politiche sulla tutela della riservatezza applicate dai servizi digitali relativamente all'uso dei dati personali; 9. g) essere in grado di evitare, usando tecnologie digitali, rischi per la salute e minacce al proprio benessere fisico e psicologico; essere in grado di proteggere sé e gli altri da eventuali pericoli in ambienti digitali; essere consapevoli di come le tecnologie digitali possono influire sul benessere psicofisico e sull'inclusione sociale, con particolare attenzione ai comportamenti riconducibili al bullismo e al cyberbullismo.

Tra le diverse pratiche di utilizzo dell'Educazione Civica Digitale alcune hanno come obiettivo quello di limitare l'ostilità digitale in rete, ma anche gli altri detestabili fenomeni come la violazione della privacy, il cyberbullismo, l'uso irresponsabile dei social media, il riconoscimento delle fake news e il difendersi dal revenge porn.

Lo sviluppo di una piena e consapevole cittadinanza digitale deve soprattutto passare dalla capacità degli studenti di appropriarsi dei diversi media, per poter passare dal ruolo di consumatori passivi, a quello di consumatori critici e di produttori responsabili di contenuti leciti e di nuove strutture comunicative[2].

Insegnare la cittadinanza digitale

Recenti studi hanno analizzato milioni di siti web e piattaforme social quando è iniziata la pandemia da COVID-19. È stato rilevato un incremento del 70% di bullismo e linguaggio offensivo, tra i ragazzi e gli adolescenti, sui social media e nei forum di chat, un aumento significativo di comportamenti negativi nelle piattaforme di gioco e il 200% di picco di traffico su siti di incitamento all'odio.

Anche durante le lezioni in videoconferenza, si sono verificate intrusioni di anonimi, il cosiddetto "Zoombombing", in altre parole un utente non invitato irrompe in una videochiamata per disturbare compiendo gesti osceni, insulti razziali e altri atti illeciti.

Il modo migliore per insegnare la cittadinanza digitale è quello di educare all'empatia cioè all'attitudine ad offrire la propria attenzione a un'altra persona, mettendo da parte le preoccupazioni e i pensieri personali, senza giudicare, ma concentrandosi solo sulla comprensione dei sentimenti e dei bisogni dell'altro.

Naturalmente, per i docenti, la chiave del successo in empatia è essere, a loro volta, modelli protagonisti (edutopia[3]) di questo scenario, divenendo un esempio e quindi un riferimento e un'ispirazione per gli studenti. Infatti, sono

[2] Secondo i dati di una ricerca dell'Osservatorio Nazionale-Adolescenza, il proprio profilo sul social network rischia di diventare l'unico specchio nel quale riflettere la propria persona. Circa 1 adolescente su 10 decide di seguire una dieta per apparire più bello nei *selfie* già a partire dagli 11 anni di età. Sono quasi 3 su 10 gli adolescenti, da 14 ai 19 anni, e il 22% dagli 11 ai 13 anni, che dichiarano di provare ansia prima di pubblicare una foto, per paura che possa non piacere, che non ottenga consensi o che venga criticata. Il 60% dei giovani, senza differenze tra maschi e femmine, dai 14 ai 19 anni e il 65% dagli 11 ai 13 anni, raccontano di sentirsi felici quando ricevono tanti *like* ai *post* e tanti commenti postivi. Inoltre, l'ossessione da like non riguarda unicamente il numero dei "mi piace" ottenuti, ma anche, e soprattutto, da chi li mette. Il 66% degli adolescenti, infatti, controlla, minuziosamente, chi mette *like* a *post* e anche chi guarda le loro storie. Quando l'emotività e l'umore sono condizionati da un numero o dalle parole di un commento, vuol dire che ai ragazzi mancano basi solide su cui poggiare la percezione di sé.

[3] L'edutopia identifica almeno 4 strategie e comportamenti: • Modeling: essere il modello della classe per l'empatia. • Punto di vista: cioè mostrare come appaiono idee diverse da prospettive diverse. • Letteratura: Illustrare il punto di vista attraverso storie famose. • Ascolto: seguire i passaggi che sono Interrompi, Coinvolgi, Anticipa per comprendere meglio ciò che qualcuno dice. Citare la fonte se c'è.

i docenti che possono portare gli alunni a considerare i sentimenti degli altri in classe, incoraggiandoli a diventare più empatici e aiutandoli così a creare opportunità di successo a scuola, ma anche in altri aspetti della vita sociale e lavorativa.

Bisogna far presente agli studenti che, ogni volta che si accede alla rete, si lascia la propria "impronta digitale" poiché ogni volta che si visita un sito Web, si è monitorati tramite alcuni software che vedono la "tua impronta". Al proprio ritorno su quel sito Web, lo stesso software riconosce e abbina "l'impronta" precedente alla recente visita. Il risultato finale è che i siti Web sanno chi ha eseguito l'accesso, quante volte è stato visitato il loro sito Web e cosa è stato fatto durante la visita. Bisogna quindi far comprendere bene ai propri studenti che, quando usano Internet, sono di solito "osservati" da qualcuno.

Per incoraggiare gli studenti a parlare della loro esperienza online, è necessario promuovere un dialogo aperto ed empatico, mettendosi in ascolto e provando a costruire un dialogo. Quando online gli adolescenti s'imbattono in contenuti inappropriati, è importante che capiscano di non essere da soli, devono poter contare su una figura di riferimento che li supporti e a cui possano fare domande. Gli alunni di questa età hanno bisogno di contare su figure presenti, ma non invasive, cui chiedere aiuto senza sentirsi giudicati, sia se sono rimasti vittima di un comportamento lesivo, sia se si sono resi conto di aver fatto un errore.

Altro argomento da curare è l'alfabetizzazione informativa digitale intesa come la pratica di leggere le informazioni online e comprendere cosa significano, dove hanno avuto origine e se sono affidabili, in pratica saper distinguere le informazioni accurate da quelle della disinformazione presente online.

Gli studenti devono imparare come valutare correttamente la validità delle informazioni raccolte su Internet, come proteggere il contenuto che pubblicano e come dare credito al lavoro degli altri. Inoltre, devono apprendere le norme di sicurezza online di base come la protezione dei conti e della reputazione, l'importanza delle password forti e segrete[4] e come tenere aggiornati i computer e i dispositivi per difendersi da malware e truffe.

L'alfabetizzazione digitale deve includere quindi anche l'apprendimento dell'etica, la protezione online e la prevenzione del cyberbullismo.

Due concetti possono aiutare a comprendere meglio come valutare quello che troviamo in internet: il Clickbait e le Fake news:

- **Clickbait** (acchiappa clic): si riferisce a qualsiasi testo, titolo, nome del video, ecc. che è stato scritto deliberatamente per suscitare l'interesse di qualcuno e convincerlo a fare clic;
- **Fake news** (notizie false): si riferiscono a qualsiasi media che pubblica informazioni gravemente distorte o intenzionalmente false.

[4] Gli studenti e gli utenti in generale devono sapere che l'*e-mail* e l'*online banking* dovrebbero avere un livello di sicurezza decisamente più elevato e non utilizzare mai le stesse password impiegate negli altri siti. Devono utilizzare un sistema come *Last- Pass* (gestore di password) per l'amministrazione delle password o una app sicura in cui archiviare queste informazioni.

Altro elemento indicativo su cui indirizzarsi è il "benessere digitale", cioè la capacità di frequentare Internet e/o i media digitali per un tempo ragionevole. In altre parole, è la pratica di sapere quando "prendersi una pausa" dagli schermi[5].

L'ultimo elemento per diventare un buon cittadino digitale è la protezione e la sicurezza dei dispositivi digitali.

Questo rappresenta il fondamento perfetto per le lezioni di cittadinanza digitale perché comprende tutto ciò che gli studenti hanno imparato e che devono poi applicare anche a scenari di vita reale. Gli studenti devono sapere come proteggere i propri computer, smartphone e altro ancora. Mentre viaggiano su Internet devono posizionare, a garanzia, una specie di guscio protettivo attorno ai loro dati, per evitare i furti di identità. Devono essere messi in grado di bloccare e modificare i codici dello smartphone o i modelli d'identificazione. Se si utilizza il riconoscimento facciale, si devono assicurare che non siano pubblicate online foto somiglianti dei loro volti. Naturalmente, è importante saper gestire anche il software antivirus che deve essere sempre aggiornato e in grado di proteggere i dati e le informazioni da malintenzionati.

Un metodo per raggiungere l'obiettivo può anche essere quello di trasformare gli stessi studenti in docenti, chiedendo loro di creare dei tutorial o delle presentazioni su questi argomenti, ad esempio per esporre le truffe più comuni praticate in rete e per spiegare com'è possibile proteggersi contro le stesse.

Gli studenti, in questo modo, diventano protagonisti attivi e quindi più vigili e attenti.

Competenze per la cittadinanza digitale

La competenza digitale è una delle otto competenze chiave per l'apprendimento permanente individuate nella Raccomandazione del Parlamento europeo e del Consiglio del 2006[6].

Saper utilizzare con padronanza e spirito critico le tecnologie della società dell'informazione (TSI) richiede quindi abilità di

INFORMAZIONE:

1. Navigare, ricercare e filtrare le informazioni
2. Valutare le informazioni
3. Memorizzare e recuperare le informazioni

COMUNICAZIONE:

1. Interagire con le tecnologie
2. Condividere informazioni e contenuti
3. Impegnarsi nella cittadinanza online
4. Collaborare attraverso i canali digitali
5. Netiquette
6. Gestire l'identità digitale

[5] Il Safer Internet Day è una giornata dedicata alle riflessioni sui dati della ricerca realizzata da Generazioni Connesse, sulla quantità e sulla qualità delle ore passate in Rete dagli studenti in Italia. Il tempo trascorso online dai più giovani si riduce: il 42% dice di stare collegato dalle 5 alle 10 ore al giorno, contro il 59% dello stesso periodo dell'anno scorso. Gli studenti che si dichiarano "sempre connessi" scendono dal 18% del 2021 al 12% del 2022, complice anche il graduale ritorno alla normalità dopo le restrizioni del periodo più difficile della pandemia.

[6] Raccomandazione 2006/962/CE.

base nelle tecnologie dell'informazione e della comunicazione (TIC).

CREAZIONE DI CONTENUTI:

1. Sviluppare il contenuto
2. Integrare e rielaborare
3. Copyright e licenze
4. Programmare

SICUREZZA:

1. Proteggere i dispositivi
2. Proteggere i dati personali
3. Tutelare la salute
4. Proteggere l'ambiente

PROBLEM SOLVING:

1. Risolvere problemi tecnici
2. Identificare i bisogni e le risposte tecnologiche
3. Innovare e creare utilizzando la tecnologia
4. Identificare i gap di competenza digitale

Sicurezza in rete – Comportamento etico e legale

La sicurezza in rete, insieme alla competenza dell'utilizzo degli strumenti e del loro corretto impiego, deve diventare uno dei valori cui prestare maggiore attenzione sia per gli studenti che li utilizzano, sia per i docenti che li devono far utilizzare.

L'errato trattamento o la violazione di dati personali, previsto dalla Legge sulla Privacy[7], comporta sanzioni che vanno dalla multa fino alla reclusione. Non si tratta perciò di semplici e costosi "malfunzionamenti", ma di reati.

In classe è necessario che gli alunni, attraverso percorsi didattici formativi, apprendano le normative e adottino comportamenti che non diano adito ad attività illegali. Devono pertanto acquisire le competenze per comportarsi eticamente online e applicarle correttamente. Si suggeriscono alcune attività in rete per prendere confidenza:

Interland (Google) 	Sviluppato da Google, Interland è un gioco online gratuito che supporta alunni dai 6 ai 13 anni nell'apprendimento di concetti fondamentali relativi alla sicurezza sul web, alla tutela delle informazioni personale, alla comunicazione, alla condivisione in rete, alle truffe on line. Sviluppato come un platform, aiuta gli studenti e i docenti a vivere nel mondo on line in modo più consapevole ed è promosso dal Safer Internet Center Generazioni Connesse[8].
Datak (Radio Télévision Suisse - DNA Studios) 	Datak è un Serious game sviluppato per sensibilizzare gli studenti al tema della privacy e della tutela dei dati personali. Accessibile online gratuitamente, guida gli alunni a comprendere come sono usate le informazioni che si condividono in rete. Il giocatore è assunto come stagista dal sindaco di una città e viene incaricato della gestione dei social network. Si trova a dover affrontare dilemmi quotidiani: dalla sfera privata, alla collettività. Promosso dalla piattaforma dell'UFAS, si rivolge agli studenti a partire dai 15 anni e affronta temi come il trekking online, l'hackeraggio, l'indirizzo di posta elettronica, la geolocalizzazione, i metadati di video, la videosorveglianza, la carta fedeltà, la pubblicità profilata e le biobanche[9].

[7] GDPR N. 679/2016.

[8] **beinternetawesome.withgoogle.com/it_it/interland** (ultimo accesso novembre 2022).

[9] **https://datak.ch/#/play** (ultimo accesso novembre 2022).

Comunicare bene e correttamente: la Netiquette

La "netiquette" è una parola che unisce il vocabolo inglese network (rete) e quello francese étiquette (buona educazione).

È, dunque, un insieme di regole che disciplinano il buon comportamento, quindi è una sorta di "buona educazione" in rete. La conoscenza della netiquette è importante poiché permette di avere una buona qualità di dialogo e comunicazione indipendentemente dalle distanze fisiche con le persone con cui si interagisce.

Quindi, un vero e proprio galateo informatico che, così come quello dell"educazione quotidiana, deve far sì che, anche in rete, non ci si comporti in modo sgarbato.

Le regole ufficiali della netiquette sono state fissate nel 1995 con il documento RFC (Request for Comments). Alla presenza di comportamenti scorretti, pur mancando nella maggior parte dei casi, un carattere giuridico, vi è un sistema sanzionatorio che può portare all'esclusione da gruppi o liste.

Quando si comunica a distanza, bisogna tenere presente che, non sempre, si è in grado di vedere il nostro interlocutore e pertanto non si ricevono alcuni riscontri che facilitano la comunicazione, come il riconoscimento dello stato d'animo, la difficoltà nel mettersi nei suoi panni (empatia), la mancanza della prossemica, del tono della voce, del feedback, ...

Tutti questi elementi condizionano la nostra comunicazione e pertanto si richiede una maggiore attenzione, affinché il messaggio arrivi a destinazione, in modo efficace, utilizzando parole semplici e chiare che non creino disagio e/o offesa, punibili anche dalle disposizioni di legge.

Nelle regole di guida generali si possono declinare alcuni comportamenti come:

- interloquire con rispetto e riguardo con propri compagni e/o insegnanti, via e-mail o in qualsiasi altra modalità comunicativa online;
- utilizzare sempre un linguaggio chiaro, semplice e conciso;
- rispettare le tempistiche della comunicazione tra chi ascolta e chi scrive;
- ricordare che tutte le comunicazioni a livello scolastico dovrebbero essere scritte correttamente e con proprietà;
- cercare di evitare i termini gergali e/o le abbreviazioni di testo (es. come "nn" anziché "non");
- usare caratteri pensati per facilitare la lettura online (ad es. Sans serif) insieme a dimensioni coerenti e leggibili (almeno 14 pt.);
- non utilizzare la funzione di blocco maiuscole, poiché può essere interpretato come "un urlo";
- evitare l'uso di emoticon prive di un significato comunicativo;
- fare attenzione alle espressioni in cui si usa l'umorismo o il sarcasmo poiché potrebbero essere prese alla lettera o ritenute offensive;
- fare attenzione alle informazioni di carattere personale (violazione della privacy) che si decide di condividere online (sia le proprie che quelle degli altri);

- confutare l'argomento e non la persona in caso di contrasto, discutere, ma non litigare.

Inoltre, gli studenti nell'ambito delle attività di didattica a distanza (DaD), sono tenuti a rispettare tutte le norme concordate e previste anche in tema di privacy e di condotta e devono essere impegnati a

- conservare in sicurezza e mantenere segreta la password personale di accesso alla piattaforma di didattica a distanza e a non consentirne l'uso ad altre persone;
- comunicare immediatamente all'Istituto, attraverso e-mail, l'impossibilità ad accedere al proprio account, il sospetto che altri possano accedervi ed episodi come lo smarrimento o il furto della password;
- non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma di didattica a distanza in uso;
- non diffondere eventuali informazioni riservate di cui si venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
- non utilizzare la piattaforma in modo da danneggiare, molestare o offendere;
- non creare e/o trasmettere materiale commerciale o pubblicitario se non espressamente richiesto;
- condividere i documenti senza interferire, danneggiare o distruggere il lavoro degli altri utenti;
- non violare la riservatezza degli utenti;
- non effettuare registrazioni audio e/o video e non fotografare i docenti e/o i compagni durante l'attività didattica a distanza, se non preventivamente autorizzati;
- utilizzare i servizi messi a disposizione solo per le attività didattiche della scuola;
- non diffondere in rete, se non autorizzati, le attività realizzate con altri utenti (docenti/alunni);
- non diffondere in rete, se non autorizzati, screenshot o fotografie relative alle attività di didattica a distanza.

Queste norme di comportamento vanno puntualmente osservate, pena la sospensione, da parte dell'Istituto, dell'account personale dello studente e l'esclusione dalle attività di didattica a distanza e dai progetti correlati.

Tracce digitali e cookie

Come cittadini digitali dobbiamo essere consapevoli che, anche online, abbiamo una nostra identità che ci definisce, che lascia delle tracce nei vari "movimenti" che facciamo e che è rintracciabile in conformità a una serie d'informazioni che ci identificano.

Bisogna sfatare subito un mito: i cookies (biscotti) non sono pericolosi, né ci sono inviati per chissà quale fine occulto, anzi, senza di essi, molti siti web

non potrebbero funzionare. Il cookie è, infatti, un facilitatore per il sito web e per l'utente: permette al portale di funzionare correttamente e rende la navigazione dell'utente più facile e personale.

Esistono due macrocategorie di cookie:

- **Cookie tecnici**, che servono ad ottimizzare la navigazione e sono necessari per il corretto funzionamento dei siti web;
- **Cookie di profilazione**, che servono a creare un profilo dell'utente sulla base dei suoi interessi e che sono utilizzati per attività di marketing e pubblicità.

I plug-in sono dei moduli software, di per sé non autonomi, che interagiscono con altri programmi o applicazioni per ampliarne le funzioni[10]. Possono applicarsi a una app a sé stante o a un browser Internet. Per esempio, il plug-in di un browser espande le funzionalità dello stesso installando specifiche barre di strumenti, aggiungendo pulsanti, link o altre utili funzioni come il blocco dei pop-up.

Privacy e Cybersecurity

Utilizzare Internet iscrivendosi a forum, social network e chat, significa sacrificare parte della propria privacy. Nella maggior parte dei siti cui si accede e nei social, è necessario lasciare un indirizzo e-mail tramite il quale è possibile, volendo, risalire al proprietario. Su Internet l'anonimato vero e proprio non esiste.

Chi sa come fare, può conoscere tutto di noi, anche se siamo stati attenti e prudenti.

È necessario però, proteggere la propria privacy online mantenendo riservate alcune informazioni sensibili, come il numero della nostra carta di credito, le nostre password, dove siamo in ogni momento, cosa cerchiamo su Internet e così via.

Le varie informazioni riguardanti la privacy sono suddivise in categorie:

- i dati personali;
- i dati identificativi;
- i dati giudiziari;
- i dati sensibili.

In sostanza l'identificazione di una persona può condizionare:

- il lavoro;
- la possibilità di accendere un mutuo (credito);
- la possibilità di avere una copertura assicurativa;
- i nostri acquisti (variazioni di prezzo secondo censo);
- le informazioni a cui si può accedere.

È importante, pertanto, attivare privacy e sicurezza sia online, sia offline.

[10] Un meccanismo che limita la diffusione di dati che disperdiamo verso soggetti terzi è rappresentato da questo link **youronlinechoices.com/it/le-tue-scelte** (ultimo accesso novembre 2022). In questa pagina è possibile agire su degli interruttori che inibiscono l'acquisizione di numerose informazioni da parte di terzi.

Prima di creare o utilizzare una password, è necessaria la consapevolezza di quanto sia difficile proteggerla. Bisogna imparare come crearne una efficace, poiché è il primo step per mantenere i propri dati al sicuro. Una semplice regola è: inventare un codice facile da ricordare, ma complicato da indovinare per gli altri! Più lunga è la password, meglio è! Deve avere almeno 8 caratteri, meglio con quelli speciali e qualche maiuscola, senza riferimenti personali: questa è la ricetta di una password sicura!

"Meme" e "Internet Meme"

Il meme è un elemento culturale che si propaga, per imitazione, da un individuo a un altro. Secondo l'Oxford Dictionary, la parola meme[11] è usata per indicare un'immagine, un video o un pezzo di testo che è copiato e diffuso rapidamente dagli utilizzatori di Internet. Nel terzo millennio, la cultura di Internet ha dato alla parola "meme" un nuovo significato adottandola per indicare un'immagine divertente, un video o una porzione di testo che sono copiati, con variazioni, più o meno lievi, che, in molti casi, diventano caricature grazie alla decontestualizzazione e al diffondersi rapidamente sul Web. Purtroppo, in rete, sono presenti anche molti meme con commenti offensivi o diffamatori e/o d'incitamento all'odio e pertanto sono stati realizzati dei programmi che, con l'aiuto dell'intelligenza artificiale, estraggono e analizzano il testo o il video incriminato e lo rimuovono.

Infatti, in alcune piattaforme con buoni livelli di moderazione, un sistema ben funzionante è in grado di segnalare automaticamente testi e immagini potenzialmente problematici[12].

La creazione di un meme può rappresentare la violazione di alcuni diritti:

- diritto alla privacy;
- diritto di copyright;
- diritto a non subire il reato di diffamazione.

Le cosiddette "Internet meme" calzano bene con la metafora dei virus per descrivere come informazioni culturali e idee si diffondano in modo esponenziale.

Per i meme più popolari si usa, infatti, dire che diventano "virali".

Cyberbullismo e Blue Whale Challenge

Anche il cyberbullismo rientra in questo ambito dell'educazione alla cittadinanza attiva e digitale. Le dinamiche del bullismo, che ben conosciamo

[11] Questo termine è stato introdotto dal 1976 dal biologo evoluzionista Richard Dawkins nel libro *Il gene egoista*, per descrivere un elemento culturale o un tratto comportamentale che passa da persona a persona per imitazione, senza trasmissione genetica. L'autore ricorre alla parola greca "miméma", che significa "qualcosa di imitato copiato" utilizzando solo la radice *meme*, più somigliante alla parola "gene". Dawkins R., *Il gene egoista. La parte immortale di ogni essere vivente*, Oscar Mondadori, Milano, 2017.

[12] Facebook e Instagram hanno recentemente utilizzato in rete un programma chiamato "Rosetta" che con l'aiuto dell'AI, interviene sistematicamente.

nella vita reale, si trasferiscono in rete con l'aggravante della presunta impunità del cyberbullo e la diffusione istantanea delle offese, delle denigrazioni e delle prepotenze.

Molte ricerche convergono sul dato del 35% di ragazzi italiani vittime di cyberbullismo, ma solo la metà ne parla con i genitori.

C'è anche chi va oltre il cyberbullismo, cercando di spillare dei soldi tramite dei siti truffa, o anche chi cerca di spiare i nostri movimenti per farci del male, come nel caso di chi ha inventato il Blue Whale Challenge.

Blue Whale Challenge o Balena Blu, è un gioco dalle regole violente che in 50 giorni spinge al suicidio i ragazzi che vi partecipano.

Le forze dell'ordine ricevono ogni giorno moltissime segnalazioni di giovani che sono finiti nel tunnel della Blue Whale Challenge. Una follia che porta alla morte, ma che riesce ad attirare nella sua tela molti giovani studenti.

Ciò che prima sembrava assurdo, diventa una gara, qualcosa di misterioso da fare di nascosto dai genitori, cui non si riesce a dire di no.

Diversi psicologi hanno spiegato come questo gioco provochi un tunnel di sofferenza dal quale il ragazzo sente di poter uscire solo tramite il suicidio. Il tutto avviene manipolando la mente con video satanici, horror e osceni. Ecco perché non si deve cominciare, nemmeno per scherzo.

Ogni cosa che si scrive in Internet, ogni ricerca che si fa nel Web si sa che è tracciata: per questo motivo, visto il crescente pericolo del coinvolgimento di parecchi ragazzi, molti social stanno correndo al riparo. Da tempo, sia Facebook che Instagram e Tumblr hanno inserito, nel loro centro assistenza, alcune pagine dedicate alla prevenzione di comportamenti che inducono alla sofferenza, al suicidio e all'autolesionismo.

I Deepfake

Il deepfake è una nuova tecnica digitale, molto presente e usata nel mondo cinematografico, per la sintesi dell'immagine umana che, sfruttando l'intelligenza artificiale basata sull'implementazione di algoritmi di apprendimento automatico, sovrappone il volto di una persona a un'altra ripresa in un altro video[8].

Il termine è un neologismo nato dalla fusione dei termini fake (falso) e deep learning, che deriva dalla tecnologia sottostante, che è una forma d'intelligenza artificiale (AI). Gli algoritmi di deep learning insegnano, da soli, a risolvere i problemi quando sono forniti grandi set di dati mappati da caratteristiche facciali e vengono utilizzati per scambiare volti nei contenuti video e digitali, creando supporti falsi dall'aspetto realistico. Tramite il deep learning, i volti di due individui sono così sostituiti (face swapping), modificando o ricreando, in modo veramente realistico, le caratteristiche e i movimenti

[13] Combinazione e sovrapposizione di immagini e di video esistenti con video o immagini originali, tramite una tecnica di apprendimento automatico, conosciuta come "rete antagonista generativa" (Generative Adversarial Networks).

di un volto o di un corpo, per far dire a chiunque tutto quello che si vuole, riproducendo o imitando la voce e sincronizzando il labiale e rendendo, con estrema difficoltà, la possibilità di individuare la manipolazione.

Questa tecnica può anche essere usata per scopi malevoli o criminali gravi (truffe informatiche sofisticate), nel mondo politico, ma anche in quello finanziario; inoltre, può essere impiegata per produrre falsi video pornografici di celebrità e revenge porn (porno vendetta ed anche pornografia non consensuale), ma può essere utilizzata anche per produrre fake-news, compiere atti di cyberbullismo e vari altri crimini informatici per denigrare, irridere e screditare le persone coinvolte, o addirittura per ricattarle, chiedendo soldi o altro in cambio della mancata diffusione del video.

Vi sono situazioni in cui anche immagini di alunni sono state raccolte e utilizzate per generare deepfake sessualizzati.

È fondamentale che i docenti, i genitori e i professionisti della vigilanza siano consapevoli e preparati ai rischi che questa forma di abuso sessuale (senza contatto) può creare. In molti casi esaminati, le stesse vittime non erano consapevoli del fatto che le loro immagini fossero state raccolte e utilizzate, in modo improprio e sconveniente, per realizzare dei deepfake.

Tuttavia, proprio come tutto ciò che offre Internet, questa tecnologia in sé non è il problema: è l'applicazione di questi media che rappresenta una potenziale minaccia per gli studenti e le scuole.

Le preoccupazioni sui deepfake hanno portato a una proliferazione di contromisure e molti paesi stanno cercando di impedirne l'uso illegale. Alcune piattaforme di social media, tra cui Facebook e Twitter, li hanno banditi dalle loro reti.

Tuttavia, il primo e più efficace strumento di difesa è rappresentato sempre dalla responsabilità e dall'attenzione degli utenti. I docenti, per tutelare chi viene loro affidato, devono assicurarsi che tutti i dispositivi che gli studenti possiedono o a cui abbiano accesso, siano provvisti dei migliori programmi di sicurezza e devono controllare che i ragazzi limitino l'accesso pubblico alle loro immagini sui diversi social media.

Ecco allora i suggerimenti proposti dal Garante della privacy:

- Evitare di diffondere in modo incontrollato immagini personali o dei propri cari. In particolare, se si postano immagini sui social media, è bene ricordare che le stesse potrebbero rimanere online per sempre o che, anche nel caso in cui si decida poi di cancellarle, qualcuno potrebbe già essersene appropriato;
- Anche se non è semplice, si può imparare a riconoscere un deepfake. Ci sono elementi che aiutano: l'immagine può appare pixellata (cioè un po' "sgranata" o sfocata); gli occhi delle persone possono muoversi a volte in modo innaturale; la bocca può apparire deformata o troppo grande mentre la persona dice alcune cose; la luce e le ombre sul viso possono apparire anormali, la pelle del viso può apparire leggermente diversa rispetto al resto del corpo;

- Se si ha il dubbio che un video o un audio siano un deepfake realizzato all'insaputa dell'interessato, occorre assolutamente evitare di condividerlo (per non moltiplicare il danno alle persone con la sua diffusione incontrollata). E si può magari decidere di segnalarlo come possibile falso alla piattaforma che lo ospita (ad esempio, un social media);
- Se si ritiene che il deepfake sia stato utilizzato in modo da compiere un reato o una violazione della privacy, ci si può rivolgere, a seconda dei casi, alle autorità di polizia (ad esempio, alla Polizia postale) o al Garante per la protezione dei dati personali.

Oltre all'introduzione di tecnologie di rilevamento dei deepfake, è fondamentale che le scuole implementino strategie di sicurezza informatica per ridurre al minimo i rischi. Le scuole e i docenti devono svolgere un ruolo importante nella lotta al rischio rappresentato dall'uso ingannevole o non consensuale dei media pericolosi come deepfake. È pertanto indispensabile tanta preparazione ed educazione e una maggiore consapevolezza e padronanza degli strumenti informatici, per essere in grado di distinguere il falso dal vero, ovvero per facilitare la capacità degli studenti di analizzare criticamente i media digitali e di assumere atteggiamenti di scetticismo sui loro contenuti. In questo modo gli effetti dannosi dei deepfake e delle altre tecnologie e/o applicazioni potenzialmente dannose potrebbero essere ridotti al minimo.

Si suggerisce di adottare un mix d'istruzione formale e conversazioni informali con gli studenti per sviluppare e promuovere queste capacità di pensiero critico.

La cittadinanza digitale interculturale

La scuola e in genere tutte le agenzie educative hanno la responsabilità di lavorare congiuntamente per creare una società universalmente pluralista e autenticamente inclusiva per la costruzione di una cultura delle interdipendenze e delle interazioni costruttive.

Il docente deve formarsi e acquisire competenze nel campo dell'Intercultura e dell'inclusione per facilitare la partecipazione e il coinvolgimento attivo di tutti gli alunni.

La rete digitale Internet, tramite la sua ricca pluridisciplinarità e mondialità, rappresenta un mezzo veramente efficace per il raggiungimento di tali obiettivi.

In questa nuova scuola, indirizzata alla cittadinanza digitale interculturale e inclusiva, tutti gli alunni devono essere messi nelle condizioni di "esercitarsi" a convivere per una costruzione collettiva della società e della sua cultura, in una pluralità diffusa utilizzando le stesse aule come spazi laboratoriali di didattica interculturale, d'interazione positiva, di rispetto, di coinvolgimento operativo e di nuova cittadinanza digitale. Per raggiungere gli obiettivi interculturali richiesti, il percorso didattico non deve prevedere però tempi rapidi, ma un'intensa progressività.

Bibliografia

- Pascucci G., *La cittadinanza digitale. Competenze, diritti e regole per vivere in rete*, Il Mulino, Bologna, 2021.
- Celot P., Franceschini R. e Salamini E., *Educare ai nuovi media, Percorsi di cittadinanza digitale per l'educazione civica*, Pearson, Torino, 2021.
- Curry C.L., Pozzi M. e Troia S., *Educazione alla cittadinanza digitale, Un viaggio dall'analogico al digitale e ritorno*, Tangram Edizioni Scientifiche, Trento, 2020.
- Bruno P., *Il cittadino digitale*, Mondadori Informatica, Milano, 2002.
- Testa C., *La sicurezza sul lavoro nella scuola*, EPC Editore, Roma, 2018.

Sitografia (ultimo accesso novembre 2022)

- *Educazione civica* in **raicultura.it/webdoc/educazione-civica/index.html#indice**.
- *Educare alla cittadinanza digitale* in **cittadinanzadigitale.eu/cittadinanzadigitale/**.
- Ferrari A., e Troia S., DIGCOMP *Le competenze digitali per la cittadinanza* in **cittadinanzadigitale.eu/wp-content/uploads/2015/11/digcomp_Ferrari_Troia.pdf**.
- *SafetyDetectives* in **safetydetectives.com/best-password-managers/**.
- Sicurezza in rete, consigli per i bambini, materiale realizzato dalla Polizia di Stato in **slideplayer.it/slide/929269/**.
- Alaimo L.B., *Come insegnare la tutela della privacy ai ragazzi?*, in **mamamo.it/educazione-digitale/buone-prassi/come-insegnare-la-tutela-della-privacy-ai-ragazzi/**.
- *A proposito di virale e meme* in **accademiadellacrusca.it/it/consulenza/a-proposito-di-virale-e-meme/904**.
- Commissariato di P. S. online, *Blue Whale – consigli*, in **commissariatodips.it/notizie/articolo/attenzione-invio-false-e-mail-equitalia-con-oggetto-avviso-di-rimborsopagamento/index.html**.
- Nurra M., *La disinformazione è una bestia dai mille volti: impariamo a riconoscerla*, in **valigiablu.it/disinformazione-fake-news-propaganda/**.
- Saraceni G., *Fake News e Post-Verità: La Chiamata Alle Armi*, TED X Vicenza, in **youtube.com/watch?v=6vpgkQ9_cHc**.
- Baglioni F., *Scienza e bufale: perché il nostro cervello si fa ingannare*, TED X Rovigo, in **youtube.com/watch?v=5WCOaNmGjAk**.