

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale



Lezione 1 Identità Digitale

SAMSUNG

Parola all'esperto: Barbara Volpi



Psicologa, psicoterapeuta, PhD in Psicologia Dinamica e Clinica Sapienza-Roma. Collabora con il Dipartimento di Psicologia Dinamica e Clinica della Sapienza. È autrice di numerose pubblicazioni, articoli di ricerca e interventi sulla genitorialità e sull'educazione digitale in tutto il territorio nazionale.

Tra le sue recenti pubblicazioni:

B. Volpi [2021], Docenti Digitali. Insegnare e sviluppare nuove competenze nell'era di internet, Il Mulino;
 B. Volpi [2017] Genitori Digitali. Crescere i propri figli nell'era di internet;
 B. Volpi [2014], Gli adolescenti e la rete, Carocci [2° rist. 2021].

Identità digitale: che cos'è?

L'identità digitale è l'insieme delle informazioni e dei dati che l'utente immette in rete sia per accedere a determinati siti o per poter usufruire di determinate applicazioni, sia come tracce di sé che lascia o che altri lasciano senza la sua autorizzazione nella navigazione come foto, video, contenuti che possono essere raccolti per determinare l'identificazione di una persona. Navigando in rete lasciamo orme digitali [digital footprint] che determinano di riflesso la nostra conformazione identitaria sia in forma di dati personali come nome cognome, indirizzo di residenza, codice fiscale, numero di telefono, sia sotto forma di gusti personali, hobbies, desiderata che possono essere proliferati orientando le nostre stesse scelte comportamentali.

L'identità digitale è il nostro biglietto da visita con il quale gli altri possono trovarci in rete, conoscere i nostri gusti, le nostre preferenze, visionare le nostre azioni e i nostri comportamenti, arrivare a conoscere i nostri dati personali con i rischi ed i pericoli che ne possono derivare.

Identità Digitale: perché parlarne

Nella società del riflesso delle identità sugli screen il promuovere e tutelare l'identità digitale di ciascuno di noi è uno dei tasselli cardine dell'educazione digitale e della tutela del benessere digitale delle nuove generazioni. Gli obiettivi educativi della società attuale nella riconfigurazione digitale devono orientarsi alla tutela della privacy della vita privata e delle relazioni interpersonali e al controllo e al monitoraggio dei propri dati personali all'interno della rete nel rispetto dei suoi diritti e della sua dignità personale.

L'input e l'output con il quale attiviamo le nostre azioni in rete non è mai indelebile ma lascia sempre traccia del nostro percorso. Un po' come le serie Tv che riassumono nelle puntate successive quanto emerso in quelle precedenti facendoci comprendere a che punto della nostra conformazione identitaria siamo arrivati.

Oggi nel 2020 non ha più molto senso parlare della distinzione tra mondo reale e mondo virtuale in quanto siamo tutti inseriti in un e-life costante in cui il dentro e il fuori lo schermo ha riconfigurato e riconfigura incessantemente la nostra società. L'ormai datata distinzione tra immigrati e nativi digitali viene superata dalla considerazione generale che TUTTI, bambini e grandi, tecnologicamente abili o meno, sono a tutti gli effetti cittadini digitali con il diritto e il dovere di utilizzare con competenza la tecnologia che anche se invisibile (basti pensare all'Internet of Things) orienta i nostri comportamenti in tutte le sfere del vivere quotidiano (dal lavoro alle relazioni sociali, all'apprendimento). Compito della società è quello di orientare i cittadini verso la costruzione di una cittadinanza digitale responsabile e consapevole avvalendosi di un percorso di educazione digitale o "screen education" che parte dall'infanzia fino all'età adulta lungo una traiettoria educativa che tiene conto dei bisogni e della capacità di acquisizione nelle diverse fasce del ciclo vitale.

I genitori devono essere consapevoli che immettere le foto del loro bambino in rete è un primo tassello della costituzione dell'identità digitale del proprio figlio prima ancora che lui stesso ne sia consapevole.

Quel che accade dentro lo screen e tra gli screen non appartiene solo allo spazio digitale ma di riflesso, nell'interconnessione costante tra il dentro e il fuori lo schermo, si rispecchia nella vita quotidiana agendo da amplificatore del disagio qualora in rete vengano immessi dati personali e agiti espressivi poco

edificanti. Nella nuova scrittura digitale che segue le sue regole espressive nulla viene dimenticato e ogni passo è segnalato per comprendere i passi procedurali di una società in profonda e rapida trasformazione. Le linee guida preventive per arginare il disagio in rete mettono in evidenza l'azione capillare dell'attenzione dapprima genitoriale, poi della scuola e solo in ultimo degli adolescenti come dimensione primaria per strutturare con competenza e dare valore alla propria identità digitale e per rispettare quella dell'altro.

In questa prospettiva il bambino sin da piccolo deve essere indirizzato verso la protezione dei suoi dati personali e non può essere lasciato da solo con lo schermo in mano prima ancora di essere pervenuto ad una distinzione tra ciò che vede nello screen e ciò che è parte del suo ambiente di vita. Prima infatti di arrivare a fenomeni di derisione e di scherno che in rete si diffondono in modo epidemico assumendo il profilo identitario del cyberbullismo occorre sensibilizzare i bambini e i ragazzi a mantenere viva l'attenzione e la riflessione sulle azioni azionate da touch impulsivi e poco riflessivi. Sin da piccoli i bambini devono essere sollecitati a parlare in famiglia delle loro attività con i device, sia a casa che a scuola. Parlare delle esperienze digitali è il primo passo preventivo per agire con consapevolezza, spirito critico e valore etico in rete.

Attenzione alla protezione dei dati personali, alla privacy che non è solo relativa al nome e al cognome ma anche agli agiti che lasciano tracce di sé nel digitale, così come all'invio di screenshot per testimoniare con dati alla mano il tradimento di turno, vuoi che sia dell'amico che del fallimento di una relazione sentimentale. Prima di arrivare a commettere reati in rete, a creare profili falsi per ingannare l'altro, ad entrare senza l'autorizzazione nei profili dell'altro per immettervi foto o notizie che ledono la reputazione e l'immagine personale commettendo dei veri e propri reati punibili per la legge, occorre attivare una rete di sensibilizzazione tesa alla prevenzione del disagio e al corretto comportamento in rete a partire dalla tutela e della protezione della nostra identità digitale così tanto importante nella società attuale. Se siamo vittime di attacchi diretti alla nostra identità digitale, se diveniamo il bersaglio mediatico di diffamazioni, minacce e insulti in rete dobbiamo sapere che ogni comportamento sia il nostro che quello dell'altro può essere tracciato, ricostruito e denunciato. Abbiamo il dovere di segnalare di essere stati vittime e il diritto di essere tutelati e di far cancellare l'attacco alla nostra identità. Abbiamo il diritto all'oblio, a cancellare tracce che noi non abbiamo prodotto e che testimoniano l'altra faccia della medaglia di agiti criminali che come società responsabile ed eticamente fondata dobbiamo punire aiutando la persona offesa a riconfigurare la sua vera identità nella rete.

D'altra parte nella costruzione di una società di alto valore etico occorre strutturare un percorso di rieducazione per i soggetti che hanno violato le buone prassi di condotta digitale tendendo conto, soprattutto per i minori, delle implicazioni psicologiche dei diversi acting out.

Barbara Volpi

Obiettivi formativi

- Definire le “norme” comportamentali del cittadino digitale
- Approfondire temi legati al comportamento del cittadino digitale con particolare attenzione al tema dei dati personali e della privacy
- Approfondire il tema del cyberbullismo fornendo indicazioni sia sull’entità che sulla portata del fenomeno
- Sensibilizzare alla prospettiva legale dei reati online

Indice lezione

1. Orme digitali e cookie
2. Dati e privacy
3. Cyberbullismo
4. Prospettiva legale
5. Attività con la classe



Capitolo 1: Orme digitali e cookie

In quanto 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 sulla base di una serie di informazioni che ci identificano.

I cookie

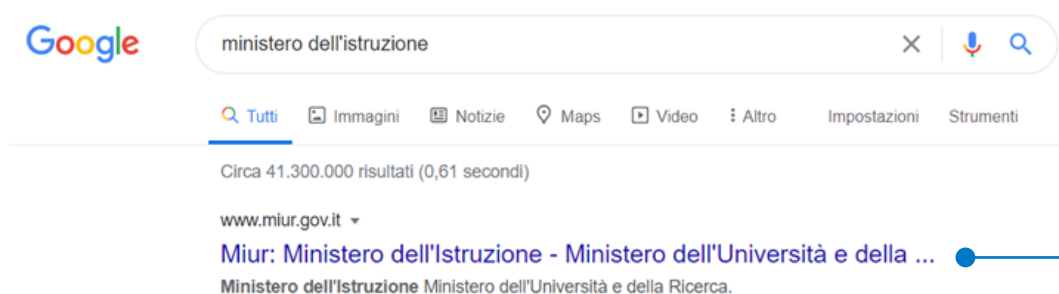
Quando navighiamo in rete, lasciamo infatti delle tracce del nostro passaggio che servono a migliorare la nostra esperienza di navigazione e a raccogliere dati sui nostri interessi e sulle nostre preferenze.

Queste orme digitali prendono il nome di “cookie”.

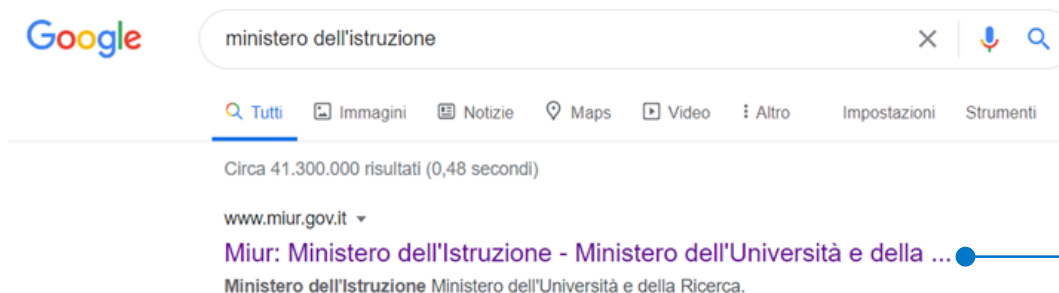
I cookie sono dei file che vengono creati automaticamente quando visitiamo dei siti web e che vengono salvati dal nostro browser, cioè il programma che utilizziamo per navigare su Internet (ad es. Google Chrome). Questi file memorizzano i dati della

nostra navigazione e tengono traccia delle nostre attività, generando una sorta di codice identificativo anonimo che viene associato all'utente.

Se, ad esempio, facciamo una ricerca Google e apriamo uno dei risultati, facendo la stessa ricerca dallo stesso dispositivo e dallo stesso browser tempo dopo, nella pagina dei risultati vedremo in viola il risultato che avevamo già aperto.



Risultato della ricerca senza cookie di navigazione, prima di aver visitato questo sito



Risultato della ricerca con i cookie di navigazione, dopo aver già visitato questo sito

Ciò significa che la prima volta che abbiamo aperto il sito “www.miur.gov.it” è stato creato un cookie che ha memorizzato questa attività. La volta successiva, quindi, quel sito ci viene presentato in cima all'elenco dei risultati ed è contrassegnato con il colore viola, ad indicare che abbiamo già visitato quel sito e che quindi è probabilmente ciò che stiamo cercando.

I cookie, quindi, da un lato migliorano la nostra esperienza online, permettendoci di salvare le nostre preferenze e di trovare più facilmente le informazioni che stiamo cercando, ma dall'altro raccolgono i nostri dati per fini commerciali e pubblicitari.

Esistono infatti due macro-tipologie 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. Vi sarà sicuramente capitato di cercare un prodotto online e di visualizzare poi, per un certo periodo di tempo, moltissime pubblicità relative a quello stesso prodotto: questo è reso possibile proprio dai cookie di profilazione.

Dal 2015, secondo la legge italiana ed europea, tutti i siti che utilizzano cookie di profilazione sono obbligati ad informarne l'utente, che potrà scegliere se accettarli o meno. Quando apriamo un sito, infatti, vediamo comparire in primo piano un banner che ci informa sull'utilizzo dei cookie e ci permette di accettare o meno l'utilizzo di quelli relativi ai fini pubblicitari: questi cookie non sono necessari per il funzionamento del sito, quindi se decidiamo di rifiutarli potremo comunque navigare senza limitazioni. Se non clicchiamo sul banner, ma continuiamo a visitare il sito, accettiamo implicitamente l'informativa.



Capitolo 2: Dati e privacy

Le “orme” attraverso la navigazione in rete sono di fatto dati personali. Cosa sono questi dati nello specifico? Perché è così importante comprendere come vengono tracciati e trattati?

Dati personali

Iniziamo cercando di capire quali sono le varie tipologie di dati che tutti i giorni girano sul web. I dati presenti online vengono raggruppati in due macro-categorie:

- I dati non personali
- I dati personali

Vengono considerati **dati non personali** tutti quei dati che non possono essere collegati a una persona identificata o identificabile. Le informazioni di questo tipo includono per esempio i dati meteorologici, i dati prodotti da dispositivi industriali, i dati relativi al monitoraggio di strutture o di processi e, in generale, tutti quei dati generati da dispositivi.

I **dati personali** costituiscono qualsiasi informazione relativa a una persona fisica identificata o identificabile, incluse quindi quelle informazioni che conducono all'interessato solo indirettamente, o effettuando controlli incrociati. Sono dati personali il nome, il codice fiscale, la voce, l'impronta digitale, gli indirizzi IP (Internet Protocol address), i cookie e i dati di geolocalizzazione, i dati telefonici, gli account, i dati sulle opinioni politiche ecc. Per la legge italiana ed europea, i dati personali possono riferirsi solamente a una persona fisica, non a una persona giuridica, come per esempio un'azienda.

I dati personali a loro volta si differenziano per tipologia ed è prevista una tutela maggiore per quei dati che possono essere utilizzati per discriminare gli individui, i cosiddetti dati particolari (o come venivano chiamati una volta, dati sensibili).

Vediamo nel dettaglio quali tipologie di dati costituiscono i dati personali:



- **Dati identificativi**, ovvero quei dati che permettono l'identificazione diretta, come i dati anagrafici, o indiretta, come un numero di identificazione, dell'interessato. Fanno parte di questa categoria nome e cognome, indirizzo di casa, indirizzo mail, numero di passaporto, numero di telefono, indirizzo IP del proprio computer, dati di geolocalizzazione, numero di targa ecc.
- **Dati particolari (sensibili)** sono dati soggetti a trattamento speciale, ovvero quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici e i dati biometrici (es. l'impronta digitale, la forma fisica della mano, del volto, dell'iride o della retina), i dati relativi alla salute, i dati relativi all'orientamento e alla vita sessuale della persona e i dati giudiziari.

L'utilizzo dei dati personali è dettagliatamente regolamentato dalla normativa europea.

Secondo la Carta dei diritti fondamentali dell'Unione europea, infatti, il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo e il 25 maggio 2018 in tutti i paesi dell'UE è entrata in vigore una nuova importante normativa, frutto del lavoro di diversi anni all'interno dell'UE, denominata General Data Protection Regulation (GDPR), Regolamento Generale sulla Protezione dei Dati.

Si tratta di un passo molto importante che ha rafforzato la protezione dei dati personali di cittadini e residenti UE.

Ma perché è così importante proteggere questi dati?



Proteggere i propri dati

I dati che immettiamo ogni giorno in Internet sono tantissimi. Quando utilizziamo la posta elettronica, effettuiamo delle ricerche su Google o ci muoviamo all'interno di una pagina web veniamo costantemente monitorati (le impronte di cui si parlava prima). Tutti questi dati, anche se apparentemente non ci sembrano "preziosi", hanno in realtà un importante valore economico.

Le tracce che lasciamo, incluse quelle sulla nostra mobilità, vengono raccolte e permettono a chi ha ottenuto il dato di "profilare" ognuno di noi, di avere quindi un quadro abbastanza chiaro di quello che ci interessa, dei luoghi virtuali e fisici che frequentiamo e di tanti altri aspetti che possono interessare chi usa Internet per pubblicizzare i propri prodotti o servizi, o per influenzare il pubblico.

La profilazione, infatti, determina il tipo di contenuti che visualizziamo online. Questo può tornarci molto utile quando siamo alla ricerca di qualcosa di particolare, o quando vogliamo ritrovare velocemente una pagina che avevamo già visitato, perché in quel caso il web ci verrà in aiuto proponendoci suggerimenti che potrebbero facilitare il

nostro lavoro (pensiamo a quando si cerca un paio di scarpe su un motore di ricerca e si visualizzano poi annunci di scarpe per giorni e giorni).

Talvolta, però, la profilazione fa sì che le notizie e le informazioni che troviamo online siano "filtrate" dal tipo di utente che siamo, influenzandoci quindi nelle nostre opinioni e scelte. Basti pensare al caso di Cambridge Analytica, la società che ha raccolto senza consenso esplicito i dati personali di milioni di account Facebook per rivenderli a scopo di propaganda politica. Uno scandalo che ha reso chiaro a tutti come sfruttando i dati personali e le informazioni condivise sui social sia possibile influenzare le decisioni di milioni di persone.

Non è necessario che questi dati vengano considerati tutti assieme per avere valore: sapere anche solo la fascia d'età, il sesso di una persona, il paese in cui vive e quali sono le ricerche che effettua su Google sono informazioni sufficienti per essere utilizzate.

Per questo motivo è importante che ognuno di noi sia consapevole di quello che accade mentre naviga in Internet, e che adotti delle misure per tu-



telare la propria privacy, ovvero la riservatezza dei propri dati personali.

Vediamo assieme alcune misure che possiamo adottare:

- Quando ci iscriviamo a un servizio o creiamo un account, leggiamo l'informativa privacy e aiutiamo i più giovani a capire di cosa si tratta. Leggendo le varie informative noteremo che non sono tutte uguali, e impareremo a identificare quali sono gli aspetti a cui prestare attenzione. Ogni informativa infatti è composta più o meno dagli stessi elementi, che dovrebbero aiutare gli utenti a capire diversi aspetti, tra cui chi eroga il servizio e detiene i dati, quali sono

esattamente i dati che detiene, per quanto tempo e con quali finalità, come fare per cancellare i propri dati ecc.

- Impariamo a distinguere i motori di ricerca: ognuno ha la propria policy in termini di dati che vengono raccolti. Firefox e Qwant, ad esempio, sono motori di ricerca che non profilano le informazioni degli utenti.



Link e informazioni utili

- Il 28 gennaio viene celebrata la giornata europea della protezione dei dati personali, per sensibilizzare e promuovere l'importanza della privacy e della protezione dei dati
- Garante per la protezione dei dati personali
www.garanteprivacy.it/
- Link Google per verificare quali informazioni relative alla nostra identità e alle nostre attività sono tracciate per decidere se eliminarle o meno
<https://myaccount.google.com/dashboard>
- Link Facebook per modificare le impostazioni sulla privacy
<https://it-it.facebook.com/help/325807937506242>
- Link Instagram per modificare le impostazioni sulla privacy
<https://www.facebook.com/help/instagram/116024195217477/>
- Modulo Google per richiedere di far rimuovere dai risultati delle ricerche i contenuti ritenuti lesivi (che non vengono quindi più indicizzati)
https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637369701910557419-3025121284&rd=1
- Modulo per il Reclamo al Garante per la protezione dei dati personali
<https://www.garanteprivacy.it/modulistica-e-servizi-online/reclamo>
- Altri link utili:
www.garanteinfanzia.org
www.agcom.it
www.commisariatodips.it
www.miur.gov.it
www.famiglia.governo.it
www.generazioniconnesse.it



Capitolo 3: Cyberbullismo

Un aspetto fondamentale legato alla nostra presenza online riguarda il comportamento che adottiamo nei confronti degli altri utenti. Non avere davanti una persona fisica porta spesso le persone a comportarsi in modi che, nella vita reale, non prenderebbero neanche in considerazione. Lo schermo, in questi casi, per molti funge da barriera, ma in quanto utenti e cittadini digitali dobbiamo ricordarci che i nostri comportamenti sul web hanno lo stesso valore di quelli che adottiamo offline.

Con lo sviluppo del mondo digitale si è sviluppato anche il fenomeno, di cui ormai abbiamo tutti sentito parlare, del cyberbullismo, ovvero di tutti quegli atteggiamenti che avvengono online e che costituiscono episodi di bullismo.

Non so chi è stato ma i miei genitori si sono rivolti alla Polizia Postale per identificare il colpevole. Non sono riuscita più ad entrare nel mio profilo di Instagram, la password non era più quella ma il profilo era attivo.

Hanno iniziato a pubblicare mie foto e video di me fuori dalla scuola deridendomi facendo credere che fossi io a farlo quando invece non sapevo nulla di nulla. Mi hanno seguito, mi hanno fotografato e hanno pubblicato tutto a mia insaputa.

È stato difficile anche farlo capire ai miei che inizialmente non mi credevano ma poi hanno visto in tempo reale un video pubblicato quando ero davanti a loro e avevano il mio telefono in mano.



La legge italiana

La [Legge 29 maggio 2017 n. 71](#) prevede delle misure di contrasto del fenomeno del cyberbullismo lo definisce 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 on line aventi ad oggetto 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”*.

Pertanto possono essere sanzionate penalmente le singole condotte di cyberbullismo qualora ricadano nelle fattispecie di reato (quali minaccia, estorsione, sostituzione di persona).

Uno screenshot, una foto ritoccata, un video. Il cyberbullismo può iniziare da un'azione semplice, una di quelle che tutti noi compiamo ogni giorno. Proviamo a pensare a qual è la differenza tra una presa in giro tra amici e un'aggressione online. Nel primo caso si tratta di una interazione tra amici che utilizzano espressioni scherzose in maniera affettuosa senza l'intento di far soffrire qualcuno. Nel secondo caso invece si tratta di episodi in cui una o più persone rivolgono scherzi e battute contro una persona sola con l'intenzione di farle del male ed emarginarla dal gruppo, stabilendo una relazione che tra le parti che non è alla pari.

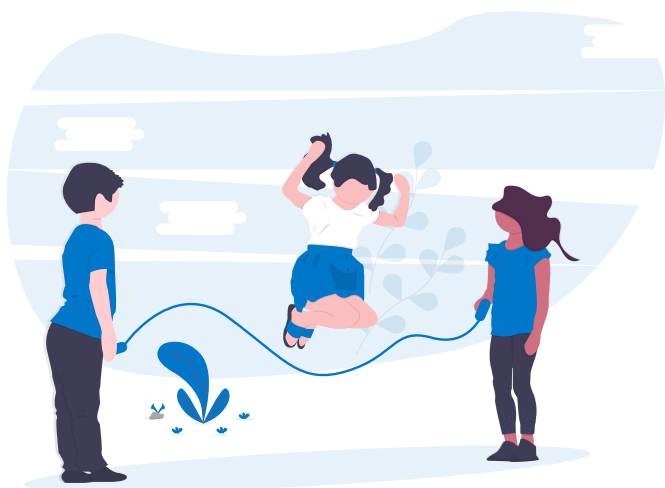
Qualche dato

Secondo un'indagine conoscitiva effettuata su bullismo e cyberbullismo dall'ISTAT¹, il cyberbullismo riguarda il 22,2% di tutte le vittime di bullismo.

Secondo l'indagine, tra i ragazzi di età compresa tra gli 11 e 17 anni che utilizzano quotidianamente il cellulare (85,8% del totale), ben il 22,2% riferisce di essere stato vittima di cyberbullismo.

Dall'indagine emergono anche due aspetti interessanti:

- **Le ragazze sono più colpite dei ragazzi.** Il 7,1% delle ragazze 11-17enni che hanno accesso a Internet o possiedono uno smartphone ha subito episodi ricorrenti di cyberbullismo, contro il 4,6% dei ragazzi. Questa differenza è probabilmente dovuta anche al fatto che le ragazze di questa età utilizzano il cellulare in maniera maggiore rispetto ai propri coetanei (l'88% delle ragazze usa il cellulare tutti i giorni, contro l'84% dei ragazzi).
- **I giovani sono più colpiti degli adolescenti.** Il 7% dei bambini tra 11 e 13 anni ha subito episodi ricorrenti, contro il 5,2% dei ragazzi di età compresa tra i 14 e i 17 anni.



Varie forme di cyberbullismo

Come abbiamo visto il fenomeno del cyberbullismo si basa su alcune condizioni: l'intenzionalità, la persistenza nel tempo, l'asimmetria nella relazione e il mezzo telematico. Le forme con cui si manifesta questo fenomeno però sono molteplici. Gli esperti hanno identificato le seguenti modalità:

- **Cyberstalking (cyber-persecuzione)** Consiste nel molestare e denigrare ossessivamente una persona online per incutere paura e terrore generando in essa una sensazione di insicurezza e facendola temere per la propria incolumità.

SMS anonimo:

Te la farò pagare. Hai ancora pochi giorni e poi finalmente sarà finita. Ti voglio MORTO.

- **Exclusion (esclusione)** Consiste nell'escludere deliberatamente e senza motivo una persona da un gruppo online per ferirla.

In chat:

Dai, di questo parliamone nell'altra chat che qui non sanno neanche cosa vuol dire!

- **Exposure o outing (rivelazioni)** Consiste nel diffondere online le informazioni confidate spontaneamente da un compagno.

Chat di classe:

Perché, non lo sapevate che Matteo è follemente innamorato di Greta? Guardate qua, le manda anche sue foto in Direct!

Screenshot chat privata

¹ ISTAT, Commissione parlamentare per l'infanzia e l'adolescenza, [Indagine conoscitiva su bullismo e cyberbullismo](https://www.istat.it/it/archivio/228976) (2019) <https://www.istat.it/it/archivio/228976>

- **Harassment (molestie)** Consiste nell'inviare in maniera ossessiva e ripetuta messaggi contenenti insulti a una singola persona, che causano disagio emotivo e psichico.

SMS anonimo:

Ti odio, anzi ti odiano tutti. Sei un'inutilità e faresti meglio a sparire!

- **Flaming (dall'inglese flame, fiamma)** Consiste nell'inviare messaggi offensivi e/o volgari online al fine di danneggiare gratuitamente una persona, solitamente su social network, forum e siti di discussione online.

Chat tra giocatori che stanno giocando online live:

- *Niko97 sei un pivello, neanche mia nonna gioca così male*
- *Sì Niko97 fuori di qui!*
- *Non farti rivedere!*

- **Happy slapping (dall'inglese, schiaffeggio allegro)** Consiste nel molestare fisicamente qualcuno con l'obiettivo di riprendere l'aggressione e di pubblicare il video sul web.

Riprendendo un ragazzo mentre viene picchiato da un gruppo:

Dai bello, fai un sorriso per i tuoi fan, fai vedere come sanguini bene!

- **Trolling** Consiste nel disturbare le conversazioni altrui online pubblicando messaggi provocatori o senza senso.

Commenti ripetuti a un post pubblico:

- *Stai zitto, i vaccini sono una truffa!*
- *Basta vaccini, basta casta!*

- **Masquerade (sostituzione di persona) o identity theft (furto d'identità)** Consiste nel rubare l'identità di una persona con l'obiettivo di pubblicare a suo nome contenuti volgari.

Post Facebook sulla bacheca di una ragazza, scritto a sua insaputa da compagni che le hanno rubato la password dal diario:

Ciao, sono brava in tutto, se mi volete chiamatemi (+39 555 1234 567)

- **Denigration (denigrazione)** Consiste nel divulgare nella rete notizie sulla vittima, allo scopo di danneggiarne la reputazione o le amicizie. Colpisce generalmente aspetti centrali della personalità del soggetto come l'orientamento sessuale, l'appartenenza etnica, difetti fisici, difficoltà scolastiche e situazioni familiari.

Mailing list della scuola:

Oggetto: Sorpresa
Testo: Eccolo qui il più gay della scuola
Allegati: foto di un compagno di scuola con il suo ragazzo

- **Trickery (inganno)** Consiste nel conquistare la fiducia di una persona per ottenere informazioni private e/o imbarazzanti con la finalità di renderle pubbliche.

Chat privata:

Ma quindi vai dallo psicologo? Perché?
Dai raccontami, di me puoi fidarti!

Abbiamo visto che in moltissimi casi le forme di cyberbullismo riguardano la condivisione non autorizzata di informazioni, vere o false, relative alla vittima. Riguardo a questo è interessante sottolineare che secondo le statistiche lo strumento principale del cyberbullismo sono le foto.

Secondo i dati riportati dall'Indagine Telefono Azzurro e DoxaKids, rispetto ai ragazzi intervistati:

- Il 30% ha dichiarato di aver trovato online proprie foto non autorizzate
- Il 20% ha dichiarato di aver trovato online proprie foto imbarazzanti
- Il 15% ha dichiarato di aver trovato online propri video non autorizzati
- Il 10% ha dichiarato di aver trovato online propri video imbarazzanti

Cosa fare

Come abbiamo visto, il cyberbullismo può assumere diverse forme e non è solo evitando di mettere in atto in prima persona comportamenti violenti che il problema può essere eliminato.

Nel cyberbullismo la responsabilità può essere estesa e condivisa anche da chi “semplicemente” visiona un video e decide di inoltrarlo ad altri, ride o rimane indifferente. In questo senso il ruolo del gruppo assume nel bullismo elettronico un'importanza ancora più evidente e delicata.

L'astante o spettatore che frequenta i siti e fruisce delle immagini, diventa uno “strumento” fondamentale per lo scopo del cyberbullo e assume un ruolo di responsabilità attiva nei confronti delle vittime anche se, paradossalmente, non le conosce affatto.

Quando vediamo situazioni anomale, ma non ne parliamo o non denunciando il fatto perché non ci sembrano affari nostri, diventiamo complici di atti di cyberbullismo. Lo stesso vale quando ci rendiamo conto che una persona a noi vicina viene ber-

sagliata e prendiamo parte allo scherzo per non sentirci esclusi.

Per combattere il cyberbullismo possiamo:

- evitare di diffondere screenshot, foto o video intimi, denigratori o imbarazzanti, nostri e di persone che conosciamo;
- non partecipare a chat o pagine Facebook aperte esclusivamente per bersagliare qualcuno;
- parlare con un docente o con un nostro familiare se ci sembra di vivere o di assistere a una situazione anomala;
- far caso ai comportamenti e alle reazioni dei compagni più sensibili e avvicinarli o avvertire qualcuno se ci sembra che si stiano isolando;
- non praticare mai hate speech sui social e ignorare o segnalare chi utilizza un linguaggio aggressivo.

Un'associazione italiana no profit, Parole Ostili, ha pubblicato il Manifesto della comunicazione non ostile, per rendere i rapporti più distesi nella vita e online. Consideriamo sempre che ogni contenuto condiviso online può avere forti impatti anche nella vita reale di ogni giorno.

Seguire le 10 regole del manifesto può aiutarci a lavorare contro l'hate speech, non solo evitando in prima persona di usare linguaggi e metodi comunicativi aggressivi e violenti, ma anche promuovendo uno stile di comunicazione più positivo centrato sull'importanza del rispetto della dignità dell'altro.

È possibile trovare il manifesto a questo link.

<http://paroleostili.com/manifesto/>

- Il Servizio del Dipartimento per le Politiche della Famiglia-Presidenza del Consiglio dei Ministri ha istituito un numero verde attivo o 24 ore su 24, il **114**, per dare supporto e soluzioni alle vittime di bullismo e di cyberbullismo.
- Ogni secondo giorno della seconda settimana di febbraio (9 febbraio 2021 il prossimo) si celebra il 'Safer Internet Day', una giornata istituita per fare appello alla gentilezza e per ricordare che, a livello mondiale, **1 studente su 3** è stato vittima di cyberbullismo .
www.saferinternetday.org
- Indagine conoscitiva su bullismo e cyberbullismo dell'ISTAT:
www.istat.it/it/archivio/228976
- Indagine Telefono Azzurro e DoxaKids 2020:
https://azzurro.it/wp-content/uploads/2020/02/Dossier-Doxa_2020_web_singole.pdf



Capitolo 4: Prospettiva legale

La [Legge 71/2017](#), oltre ad aver introdotto per la prima volta la definizione di “cyberbullismo”, ha anche indicato alcune misure per il suo contrasto. Tra queste, le misure di maggior rilievo sono le seguenti:

- Ciascun minore ultraquattordicenne (o soggetto esercente la responsabilità del minore) che sia stato vittima di atti di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un’istanza per l’oscuramento, la rimozione o il blocco dei contenuti. Entro 24 ore, il gestore deve provvedere. In mancanza, l’interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore (art. 2 L. 71/2017);
- Il dirigente scolastico che venga a conoscenza di atti di cyberbullismo informa tempestivamente i genitori dei minori coinvolti. I regolamenti scolastici dovranno prevedere esplicite sanzioni disciplinari, commisurate alla gravità degli atti compiuti (art. 5 L. 71/2017);
- Per i minori autori di atti di cyberbullismo, fra i 14 e i 18 anni, fino a che non intervenga una denuncia per i reati di cui agli articoli 594, 595 e 612 del codice penale, può essere applicata la c.d. “procedura di ammonimento”: il questore convoca il minore insieme ad almeno un genitore per un ammonimento formale, che può avvenire anche in forma scritta (art. 7 L. 71/2017).

Si osservi che la Legge 71/2017 non ha introdotto una fattispecie autonoma di reato per atti di cyberbullismo, limitandosi a prevedere misure per il suo contrasto. Nondimeno, le condotte alla base delle varie forme di cyberbullismo (pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d’identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali) possono configurare fattispecie perseguibili penalmente, punite finanche con la reclusione.

Così, ad esempio, flaming, denigration e masquerade possono configurare atti di diffamazione puniti, ex art. 595 cod. pen., con la reclusione fino a due anni, ovvero con la multa fino a 2.065 euro.

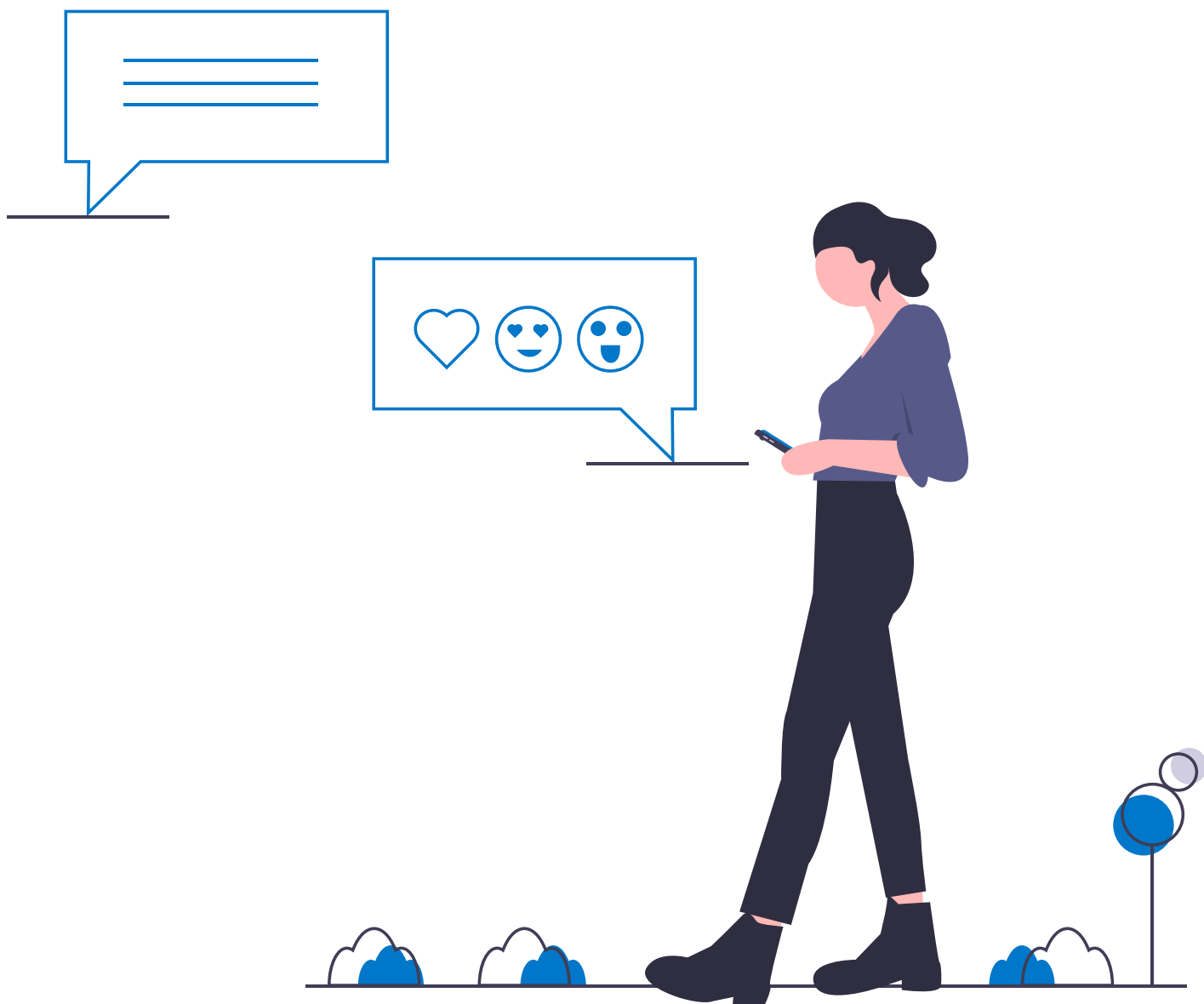
Flaming e masquerade possono astrattamente arrivare ad integrare il reato di minaccia di cui all’art. 612 cod. pen. (punito con la multa fino a euro 1.032).

L’exposure e il trickery (ove quest’ultimo sia finalizzato alla diffusione dei dati personali) sono sanzionati dall’art. 167 del D.lgs. 196/2003 con la reclusione da sei a diciotto mesi, laddove vengano diffusi dati della vittima senza il suo consenso e da tale condotta derivi un danno alla persona offesa (occorre tuttavia osservare che la tutela è in questo caso indebolita dall’esigenza di un profitto per l’agente: raramente il cyberbullo agisce per profitto, mirando piuttosto all’umiliazione della vittima).

Il cyberstalking (le cui condotte sono costituite materialmente da molestie) rientra nell’ambito del reato di atti persecutori ex art. 612 bis cod. pen. *“è punito con la reclusione da sei mesi a quattro anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l’incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita”*. Laddove l’ipotesi non comporti veri e propri atti persecutori, potrebbe comunque essere integrata la contravvenzione di molestie ex art. 660 cod. pen.

Occorre a questo proposito ricordare che se il colpevole è un minore con meno di 14 anni, esiste una esclusione totale di imputabilità, cioè non si è perseguibili. Per chi, invece, ha più di 14 anni ma meno di 18, le pene sono ridotte.

Sul piano civile, l'autore degli atti di cyberbullismo – indipendentemente dal fatto che questi si qualificino come reato – può certamente essere chiamato al risarcimento dei danni causati alla vittima.



ATTIVITÀ CON LA CLASSE

Attività 1 - I soliti ignoti

- Materiale necessario: due fogli e due pennarelli
- Obiettivo: rendere gli studenti consapevoli della quantità di azioni che compiamo per costruire la nostra identità digitale

La nostra reputazione digitale è nelle nostre mani dal primo accesso online e ogni impronta concorre a formarla e caratterizzarla. Ma come si costruisce un'identità digitale?

Sulla falsariga del gioco "I soliti ignoti", i ragazzi vengono stimolati a indovinare quante identità possiamo avere nel mondo digitale. Vengono chiamati due volontari, maschio e femmina, che si posizionano davanti alla classe. Prima di alzarsi avranno scritto su un foglio il loro nome virtuale – es. Marco e Anna – da attaccare addosso con lo scotch. L'insegnante elenca informazioni sui loro gusti e hobby (es. guarda film di fantascienza, il suo animale preferito è il gatto, è fan di Billie Eilish..) e i compagni devono indovinare, per alzata di mano, a chi piace cosa. In questa fase emerge il fatto che le informazioni sono generiche, dicono qualcosa di loro senza metterne a rischio la privacy. Successivamente l'insegnante condivide con la classe informazioni sui due personaggi (es. abita in Corso Como 25, va nella tal scuola, ha due sorelle di nome...) e invita gli studenti a riflettere sull'opportunità di condividere questo tipo di informazioni, sul concetto di privacy e dell'importanza e delicatezza del dato.

Modalità Didattica a Distanza

L'attività si può svolgere allo stesso modo anche a distanza, scegliendo due volontari che scrivono i loro nomi virtuali su un foglio da piegare e posizionare davanti allo schermo (oppure da attaccare addosso con lo scotch) in modo che tutti i compagni vedano.



ATTIVITÀ CON LA CLASSE

Attività 2 – L'identikit del cyberbullismo

- Materiale necessario: stampe
- Obiettivo: scoprire le diverse sfaccettature che può assumere il fenomeno dandogli un nome preciso. Rispondere alla domanda: "cosa potrei fare se mi trovassi in questa situazione?".

Dopo un breve brainstorming (il dibattito può essere ravvivato da frasi/domande stimolo fornite dall'insegnante) riguardo i possibili tratti che possono caratterizzare il fenomeno del cyberbullismo, si divide la classe in due squadre. Ad ogni squadra verranno consegnati diversi bigliettini prestampati con su scritto dei termini e altri contenenti una spiegazione. La squadra dovrà trovare la giusta associazione stilando così un vero e proprio identikit che aiuta a riconoscere le situazioni in cui si può parlare di cyberbullismo.

FLAMING	Offesa pura e gratuita, spesso volgare, per "tappare la bocca" della vittima e ricoprirla di insulti, con lo scopo magari di far ridere gli altri
HARASSMENT	Dall'inglese "molestia", è l'invio ripetuto di messaggi dal contenuto offensivo mirati a ferire una determinata persona e causarle un evidente disagio sia emotivo che psichico
TROLLING	Un "troll", nel gergo di Internet, è un soggetto che interagisce con gli altri tramite messaggi provocatori, irritanti, fuori tema o semplicemente senza senso per disturbare la comunicazione e fomentare gli animi
CYBERSTALKING	Rivolgere a qualcuno minacce, molestie e violenze con lo scopo di incutere nella vittima terrore e paura per la propria incolumità fisica
EXPOSURE/OUTING	Ottenere la fiducia di qualcuno con l'inganno per poi diffondere, pubblicare e condividere in rete le sue informazioni private, rivelandone i segreti
EXCLUSION	Escludere intenzionalmente qualcuno da un gruppo su un social network con l'obiettivo di provocargli un sentimento di emarginazione
DENIGRATION	Insultare o diffamare qualcuno online con pettegolezzi, menzogne e commenti crudeli, offensivi e denigratori per danneggiare gratuitamente e con cattiveria la sua reputazione
TRICKERY	Conquistare la fiducia di una persona per ottenere informazioni private e/o imbarazzanti con la finalità di renderle pubbliche
HAPPY SLAPPING	Molestare fisicamente qualcuno con l'obiettivo di riprendere l'aggressione e di pubblicare il video sul web
MASQUERADE/IDENTITY THEFT	L'aggressore si sostituisce alla vittima, utilizzando le sue informazioni personali per crearsi un profilo fittizio da cui spedire messaggi o pubblicare contenuti deprecabili con lo scopo di danneggiarne l'immagine

Modalità Didattica a Distanza

Proiettare la tabella con le dieci parole e definizioni senza rispettare la corrispondenza parola-definizione. Gli studenti provano a fare delle ipotesi di associazione e condividono a voce o via chat quelli che secondo loro sono i reali abbinamenti.

Si può concludere con una riflessione sulle differenze tra il bullismo offline e il cyberbullismo. Cosa cambia?

Esempio: assenza di limiti spazio-temporali, maggiore visibilità, apparente anonimato del bullo...

Copyright 2020 Samsung Electronics Italia SpA