

L'illusione dell'anonimato e la reputazione digitale. L'impronta che lasciamo

Quando comunichiamo attraverso uno schermo possiamo avere l'impressione che tra ciò che facciamo online e ciò che accade nella vita reale esista una separazione. Utilizziamo un nickname, non vediamo direttamente la persona a cui stiamo parlando, possiamo scrivere un commento e allontanarci immediatamente dalla conversazione. Tutto questo può portarci a dire o fare cose che probabilmente non faremmo trovandoci faccia a faccia con il nostro interlocutore.

Allo stesso tempo, possiamo avere la sensazione opposta: che ciò che facciamo online sia momentaneo. Una storia scompare dopo poche ore, un messaggio può essere cancellato, un commento eliminato, un account chiuso. In realtà fotografie, messaggi e informazioni possono essere copiati, fotografati tramite screenshot, inoltrati ad altre persone o conservati sui sistemi delle piattaforme, contribuendo nel tempo a costruire quella che viene comunemente definita la nostra **impronta digitale** (*digital footprint*).

Anonimato e permanenza sembrano quindi muoversi in direzioni opposte: da una parte possiamo sentirci meno riconoscibili e meno responsabili, dall'altra le nostre azioni possono lasciare tracce molto più persistenti di quanto immaginiamo. Comprendere questi due aspetti è fondamentale per sviluppare una maggiore consapevolezza delle conseguenze della comunicazione online, tutelare i propri dati personali e quelli degli altri e imparare a costruire relazioni digitali basate sul rispetto e sull'empatia.

1. L'illusione dell'anonimato e l'effetto di disinibizione online

Nel 2004 lo psicologo John Suler ha utilizzato l'espressione **online disinhibition effect**, "effetto di disinibizione online", per descrivere la tendenza delle persone a dire e fare su Internet cose che probabilmente non direbbero o farebbero nella comunicazione faccia a faccia. Suler distingue una disinibizione *benigna*, che può facilitare l'espressione di sentimenti, richieste di aiuto o confidenze personali, da una disinibizione *tossica*, che può invece manifestarsi attraverso linguaggio aggressivo, insulti, minacce e comportamenti ostili.

Secondo Suler, questo effetto può essere favorito dall'interazione di diversi fattori:

a) **Anonimato dissociativo**: quando una persona ritiene che le proprie azioni online non siano facilmente riconducibili alla propria identità reale, può percepire una minore responsabilità personale. Il nickname o un account anonimo possono creare una separazione psicologica tra "quello che faccio online" e "chi sono realmente". Questo non significa, naturalmente, che l'anonimato sia sempre negativo: può essere fondamentale, ad esempio, per chiedere aiuto o parlare di esperienze delicate. Il problema nasce quando viene interpretato come sinonimo di impunità.

b) **Invisibilità**: nella comunicazione digitale spesso non vediamo la reazione immediata dell'altra persona. Non osserviamo il cambiamento dell'espressione del volto dopo un insulto, il silenzio dopo una frase offensiva o il disagio provocato da una battuta. L'assenza di questi segnali può diminuire la percezione dell'impatto emotivo delle nostre parole.

c) **Asincronia**: molte comunicazioni online non avvengono nello stesso momento. Possiamo scrivere un commento, inviarlo e leggere la risposta ore dopo. Questa distanza temporale può rendere più semplice esprimere qualcosa di aggressivo perché non siamo costretti ad affrontare immediatamente la reazione del destinatario.

d) **Introiezione solipsistica**: quando comunichiamo soprattutto attraverso parole scritte, possiamo inconsapevolmente immaginare tono, voce e intenzioni dell'interlocutore, attribuendogli caratteristiche che derivano anche dalle nostre aspettative. Una frase neutra può così sembrarci sarcastica o provocatoria, alimentando conflitti che nella comunicazione faccia a faccia potrebbero essere chiariti più facilmente.

e) **Immaginazione dissociativa**: l'ambiente online può essere vissuto come uno spazio separato dalla vita quotidiana, quasi fosse un gioco nel quale le normali regole sociali hanno un peso minore. Espressioni come "era solo Internet" o "era solo una chat" mostrano proprio questa possibile separazione tra ciò che accade online e le sue conseguenze reali.

f) **Minimizzazione dell'autorità**: online possono diventare meno visibili alcuni segnali tradizionali di status e autorità. Questo può favorire relazioni più paritarie e libere, ma può anche contribuire alla sensazione che non esistano regole o conseguenze per quello che si fa.

Questi fattori non producono automaticamente aggressività. Lo stesso anonimato che può favorire un insulto può permettere a una persona in difficoltà di raccontare un problema che non riuscirebbe a condividere altrimenti. Il punto centrale è comprendere che **l'ambiente attraverso cui comunichiamo può modificare il nostro comportamento** e che la distanza dello schermo può ridurre alcuni dei segnali che normalmente ci aiutano a regolare le relazioni con gli altri.

2. Dal distacco emotivo all'aggressività online

Quando la disinibizione online assume una forma negativa può contribuire alla diffusione di insulti, umiliazioni, molestie e altre forme di aggressività verbale. Lo schermo non crea necessariamente questi comportamenti, ma può rendere più semplice dimenticare che dall'altra parte della comunicazione esista una persona che sperimenta conseguenze emotive reali.

Un elemento fondamentale della cittadinanza digitale è quindi quella che possiamo definire **empatia digitale**: la capacità di riconoscere emozioni, dignità e diritti delle persone anche quando l'interazione è mediata da uno schermo. Prima di pubblicare un commento potremmo chiederci, ad esempio, se utilizzeremmo le stesse parole trovandoci fisicamente davanti alla persona coinvolta, oppure come reagiremmo se quel commento fosse rivolto a noi.

Non tutte le forme di aggressività online sono però uguali. È importante distinguere almeno due concetti molto utilizzati: *hate speech* e cyberbullismo.

2.1. Hate speech

Con l'espressione **hate speech**, o discorso d'odio, non si indica semplicemente qualsiasi frase maleducata o offensiva. La Raccomandazione CM/Rec(2022)16 del Consiglio d'Europa comprende nel concetto le forme di espressione che incitano, promuovono, diffondono o giustificano violenza, odio o discriminazione,

oppure denigrano persone o gruppi sulla base di caratteristiche personali reali o attribuite, come origine nazionale o etnica, religione, età, disabilità, sesso, identità di genere o orientamento sessuale.

È importante questa distinzione perché definire qualsiasi insulto come *hate speech* rischierebbe di rendere il termine poco utile. Una discussione accesa tra due utenti può contenere offese senza essere necessariamente un discorso d'odio; diverso è il caso di una comunicazione che colpisce una persona in quanto appartenente, o ritenuta appartenente, a un determinato gruppo.

Anche il contrasto allo *hate speech* non può essere ridotto soltanto alla cancellazione dei contenuti. Il Consiglio d'Europa sottolinea infatti la necessità di combinare, in maniera proporzionata alla gravità dei diversi casi, strumenti giuridici con educazione, sensibilizzazione, sostegno alle persone colpite e diffusione di narrazioni alternative.

2.2. Cyberbullismo

Il **cyberbullismo** riguarda invece comportamenti aggressivi e dannosi rivolti soprattutto ai minori attraverso strumenti digitali. In Italia la legge n. 71 del 2017, modificata dalla legge n. 70 del 2024, comprende nella definizione di cyberbullismo forme di pressione, aggressione, molestia, ricatto, denigrazione, diffamazione, furto d'identità, manipolazione o trattamento illecito di dati personali realizzate per via telematica in danno di minorenni, nonché la diffusione online di contenuti finalizzati prevalentemente a isolare, danneggiare o mettere in ridicolo un minore o un gruppo di minori. La riforma del 2024 ha rafforzato inoltre l'approccio preventivo ed educativo, coinvolgendo scuole, famiglie e altre organizzazioni che lavorano con i giovani.

Cyberbullismo e *hate speech* possono sovrapporsi, ma non coincidono. Un attacco contro un compagno di scuola può essere cyberbullismo senza riguardare l'appartenenza a un gruppo discriminato; un messaggio d'odio rivolto genericamente contro una comunità può essere *hate speech* senza configurare un caso di cyberbullismo.

Un altro aspetto importante riguarda la convinzione che ciò che viene fatto attraverso lo smartphone non produca conseguenze. In realtà un comportamento online può avere conseguenze scolastiche, relazionali e, a seconda dei fatti concreti, anche giuridiche. "Cyberbullismo", infatti, non significa automaticamente uno specifico reato: sono le singole condotte poste in essere — ad esempio minacce, diffamazione, furto d'identità o illeciti relativi ai dati personali — a dover essere valutate in base alle norme applicabili.

La legge italiana prevede inoltre strumenti specifici di tutela: in determinate circostanze il minore ultraquattordicenne, oppure chi esercita la responsabilità genitoriale, può richiedere al gestore del sito o del social l'oscuramento, la rimozione o il blocco di contenuti riconducibili ad atti di cyberbullismo e, in caso di mancato intervento, rivolgersi al Garante per la protezione dei dati personali.

3. L'impronta digitale: le tracce che lasciamo

Accanto all'illusione dell'anonimato ne esiste quindi un'altra: **l'illusione della scomparsa**. Possiamo pensare che cancellando una fotografia, un messaggio o un commento tutto torni esattamente come prima. La realtà è più complessa.

Con l'espressione **impronta digitale** possiamo indicare l'insieme delle informazioni e delle tracce prodotte dalla nostra presenza e dalle nostre attività online. Alcune vengono create consapevolmente, altre sono generate automaticamente dal funzionamento dei servizi digitali.

Si può distinguere, a scopo didattico, tra:

a) **Impronta attiva**: comprende le informazioni che scegliamo direttamente di pubblicare o condividere, come fotografie, video, post, commenti, recensioni, informazioni inserite in un profilo o contenuti inviati attraverso una piattaforma.

b) **Impronta passiva**: comprende dati che possono essere prodotti mentre utilizziamo dispositivi e servizi, come identificativi online, indirizzi IP, dati relativi all'utilizzo di un servizio, localizzazione quando attiva o informazioni raccolte attraverso tecnologie di tracciamento.

Il Regolamento generale europeo sulla protezione dei dati (GDPR) ricorda proprio che una persona può essere identificabile anche attraverso elementi come dati relativi all'ubicazione e identificativi online. Il considerando 30 osserva inoltre che dispositivi, applicazioni e protocolli possono associare alle persone identificativi che, combinati con altre informazioni, possono lasciare tracce utilizzabili per creare profili e identificare gli utenti.

Questo non significa che qualsiasi nostra azione rimarrà necessariamente disponibile per sempre. Esistono strumenti di cancellazione, tutele giuridiche e, in determinate condizioni, il **diritto alla cancellazione dei dati**, spesso chiamato "diritto all'oblio", previsto dall'articolo 17 del GDPR. Tale diritto non è però assoluto e deve essere bilanciato con altri diritti e obblighi.

Soprattutto, cancellare il contenuto originale non significa poter controllare tutte le copie eventualmente create da altri. Una fotografia può essere salvata, uno screenshot può essere condiviso in un'altra chat, un video può essere ripubblicato su una piattaforma diversa. Il Garante per la protezione dei dati personali ricorda proprio che immagini e informazioni pubblicate online possono uscire dal nostro controllo e contribuire alla costruzione dell'immagine e della reputazione digitale di una persona.

4. Reputazione digitale e dati personali

Le tracce che lasciamo contribuiscono a formare la nostra **reputazione digitale**, ossia l'immagine che gli altri possono costruirsi di noi attraverso le informazioni disponibili online.

Questa immagine non dipende soltanto da quello che scegliamo consapevolmente di raccontare. Può essere formata anche da fotografie pubblicate da amici, tag, commenti scritti anni prima, discussioni nelle quali siamo stati coinvolti, recensioni, articoli, video o contenuti ripubblicati da altre persone.

La reputazione digitale non deve però essere interpretata soltanto in senso negativo, come qualcosa da cui difendersi. Anche online possiamo costruire nel tempo un'identità positiva attraverso progetti, capacità, passioni, comportamenti rispettosi, attività creative e partecipazione alla vita della comunità. L'obiettivo non dovrebbe quindi essere "non lasciare tracce", cosa sempre più difficile in una società digitale, ma **imparare a comprenderle e gestirle consapevolmente**.

Il Garante privacy sottolinea proprio come ciò che avviene sui social possa produrre effetti nella vita quotidiana e nei rapporti con gli altri, esponendo gli utenti, in caso di uso improprio dei dati, anche a furti

d'identità e danni alla reputazione. Nella guida *Social Privacy* aggiornata nel 2025 invita quindi gli utenti a interrogarsi, prima di pubblicare informazioni o immagini, anche su come potrebbero essere percepite a distanza di tempo.

Costruire una reputazione digitale sana richiede quindi alcuni comportamenti di base: conoscere e utilizzare le impostazioni di privacy; riflettere prima di pubblicare dati personali propri o di altre persone; chiedere il consenso prima di condividere fotografie che riguardano altri; proteggere account e credenziali; verificare periodicamente ciò che abbiamo reso pubblico; evitare di partecipare alla diffusione di umiliazioni o aggressioni.

Una domanda particolarmente utile può essere: **“Sarei tranquillo se questo contenuto fosse visto tra alcuni anni da una persona che oggi non conosco?”**. Non perché ogni comportamento online debba essere costruito pensando a un futuro datore di lavoro o a un giudizio esterno, ma perché questa domanda ci ricorda che il pubblico potenziale di ciò che condividiamo può essere diverso da quello che immaginiamo nel momento della pubblicazione.

La reputazione, inoltre, non riguarda soltanto il singolo. Quando partecipiamo a un gruppo, una classe, una squadra, una comunità o un'organizzazione, le nostre azioni contribuiscono anche all'immagine collettiva di quello spazio. Una chat scolastica piena di insulti comunica qualcosa non soltanto su chi scrive quei messaggi, ma anche sulle norme sociali che il gruppo accetta o rifiuta.

Il passaggio fondamentale è quindi comprendere che **online e offline non sono due vite completamente separate**. Dietro un account esistono persone reali e ciò che facciamo attraverso quello stesso account può produrre conseguenze reali. La distanza dello schermo non elimina la responsabilità, così come la possibilità di cancellare un contenuto non garantisce che ogni sua traccia scompaia.

Sviluppare empatia digitale significa imparare a vedere la persona dietro lo schermo. Costruire una buona reputazione digitale significa invece imparare a vedere il futuro possibile delle tracce che lasciamo oggi.

Riferimenti bibliografici e normativi

Suler, J. (2004). *The Online Disinhibition Effect*. *CyberPsychology & Behavior*, 7(3), 321-326.

Council of Europe (2022). *Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech*.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio – *General Data Protection Regulation (GDPR)*.

Legge 29 maggio 2017, n. 71, *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*, come modificata dalla Legge 17 maggio 2024, n. 70.

Garante per la protezione dei dati personali (2025). *Social Privacy – Come tutelarsi nell'epoca dei social media*.

Traccia per l'attività in classe

Attività 1: Dietro lo schermo. Analizzare aggressività e responsabilità nella cronaca

Scopo di questa attività è stimolare gli allievi a riconoscere come anonimato percepito, distanza emotiva e caratteristiche della comunicazione digitale possano intervenire nei comportamenti aggressivi online, e a riflettere sulle conseguenze che tali azioni possono avere per tutte le persone coinvolte.

Il docente individua nelle sezioni di cronaca di uno o più quotidiani un articolo relativo a un caso di uso distorto della Rete: cyberbullismo, diffusione non autorizzata di immagini, campagne di insulti, profili falsi, attacchi d'odio o altri episodi analoghi. È preferibile utilizzare articoli che permettano di ricostruire non soltanto l'episodio, ma anche le conseguenze scolastiche, sociali o giuridiche. Nel caso siano coinvolti minori, si dovrà prestare particolare attenzione a utilizzare soltanto informazioni già adeguatamente anonimizzate dalla testata.

Gli studenti, lavorando in coppia, analizzano il caso compilando il modulo seguente.

Analisi di un caso di aggressività e responsabilità online

Descrizione

Caso analizzato (breve descrizione):

- 1. Fonte e quotidiano utilizzato**
- 2. Comportamento online al centro della vicenda**
- 3. Soggetti coinvolti**
- 4. Possibili elementi di anonimato o pseudonimato**
- 5. Possibili elementi di invisibilità o distanza emotiva**
- 6. Presenza di comunicazione asincrona**
- 7. Elementi riconducibili alla disinibizione online**
- 8. Il caso può essere definito cyberbullismo? Perché?**
- 9. Sono presenti elementi riconducibili allo hate speech? Perché?**
- 10. Conseguenze per la persona o le persone colpite**
- 11. Conseguenze sociali, scolastiche o giuridiche per chi ha agito**
- 12. Quali tracce digitali hanno permesso di ricostruire l'accaduto?**
- 13. Come sarebbe cambiato il comportamento se le persone si fossero trovate faccia a faccia?**
- 14. Quali comportamenti alternativi avrebbero potuto evitare o interrompere il conflitto?**

Una volta compilati i moduli, le coppie presentano il proprio caso alla classe. Il dibattito dovrà concentrarsi in particolare sulla distanza tra **percezione di impunità e conseguenze effettive**: chi ha agito riteneva che il comportamento online fosse meno grave? L'anonimato era reale oppure soltanto percepito? Quali effetti sono rimasti anche dopo l'eventuale cancellazione dei contenuti?

In una seconda sessione, gli studenti possono confrontare il modo in cui due testate differenti raccontano lo stesso caso, osservando quali aspetti vengono messi maggiormente in evidenza: il comportamento dell'autore, il danno subito dalla vittima, le responsabilità delle piattaforme, le conseguenze legali o le possibili strategie educative.

Attività 2: L'impronta che lasciamo

Scopo di questa attività è aiutare gli allievi a comprendere come differenti azioni online possano produrre tracce e contribuire alla costruzione della reputazione digitale di una persona.

Il docente prepara un **profilo digitale immaginario**, evitando quindi di utilizzare direttamente i profili personali degli studenti. Il profilo potrà contenere, ad esempio, fotografie pubblicate, commenti, like, partecipazione a gruppi, un vecchio nickname, una recensione, una fotografia pubblicata da un amico, informazioni relative alla localizzazione o altri elementi simili.

Agli studenti, organizzati in coppia, viene chiesto di analizzare ciascuna traccia e di valutarne possibili conseguenze presenti e future.

Analisi dell'impronta e della reputazione digitale

Descrizione

Profilo digitale analizzato:

1. Tracce pubblicate consapevolmente dall'utente
2. Tracce prodotte o pubblicate da altre persone
3. Possibili tracce generate automaticamente dai servizi utilizzati
4. Dati personali presenti
5. Pubblico a cui il contenuto era inizialmente destinato
6. Chi potrebbe potenzialmente vederlo in futuro?
7. Il contenuto può essere copiato, inoltrato o fotografato?
8. Quale immagine della persona contribuisce a costruire?
9. Può avere effetti sulla reputazione di altre persone?
10. Sono presenti possibili rischi per la privacy?
11. Quali precauzioni sarebbe stato utile adottare prima della pubblicazione?

12. Quali azioni si possono tentare dopo la pubblicazione per ridurre la diffusione?

13. La persona sarebbe probabilmente tranquilla nel ritrovare questo contenuto online tra cinque anni?

Una volta completata l'analisi, le coppie presentano alla classe gli elementi che ritengono maggiormente significativi. Quindi, il docente guida una discussione sulla differenza tra ciò che **possiamo controllare direttamente** e ciò che, una volta condiviso, può uscire dal nostro controllo.

In una seconda sessione di lavoro la classe può costruire collettivamente un breve **“Patto per la reputazione e l'empatia digitale”**, individuando alcune regole da applicare non soltanto ai propri profili personali, ma anche alle chat e agli spazi digitali condivisi dalla classe. Le regole dovrebbero riguardare sia la tutela di sé stessi — dati personali, privacy, reputazione — sia la responsabilità verso gli altri, ad esempio evitando di pubblicare immagini senza consenso, non contribuendo alla diffusione di contenuti umilianti e intervenendo quando un comportamento online rischia di danneggiare.