FONDO per la REPUBBLICA DIGITALE

IFEL ISTITUTO PER LA FINANZA E L'ECONOMIA LOCALE DELLA CAMPANIA

DISPENSA DIDATTICA

TEMA B
SICUREZZA E USO CONSAPEVOLE DEI SERVIZI DIGITALI
CYBERBULLISMO ED ESCLUSIONE SOCIALE

Digita Facile Campania

"DIGITA FACILE CAMPANIA" Bando "DRITTI AL PUNTO" è un progetto selezionato e sostenuto dal Fondo per la Repubblica Digitale Impresa sociale

Presentazione della dispensa

Questa dispensa accompagna il percorso formativo dedicato al tema Cyberbullismo ed Esclusione Sociale, sviluppato nell'ambito del progetto Digita Facile Campania. Si rivolge a chiunque voglia comprendere più a fondo un fenomeno che attraversa ogni fascia d'età, ogni ambiente sociale e ogni angolo della rete: il cyberbullismo e, più in generale, le dinamiche di aggressione, esclusione e violenza che si producono negli spazi digitali. Il percorso è articolato in cinque moduli. Il primo introduce le caratteristiche del cyberbullismo, distinguendolo dal bullismo tradizionale e illustrando i reati digitali correlati e i meccanismi psicologici che li alimentano. Il secondo analizza i ruoli degli attori coinvolti — vittima, bullo, spettatori — con particolare attenzione al potere trasformativo di chi assiste. Il terzo propone strumenti concreti per un uso etico della rete: la netiquette, la gestione della privacy, la difesa dal phishing e il pensiero critico come antidoto ai bias cognitivi. Il quarto fornisce un protocollo operativo per rispondere concretamente a episodi di cyberbullismo, con indicazioni sugli strumenti tecnologici di protezione e sul quadro normativo vigente. Il quinto, infine, pone al centro la cultura dell'inclusione e la responsabilità collettiva, con un toolkit di regole d'oro per un uso quotidiano consapevole della rete.

Questo non è un tema da affrontare con distacco accademico. È una questione che riguarda la vita reale di persone reali: adolescenti che abbandonano la scuola, adulti che perdono il lavoro a causa di contenuti diffusi senza consenso, anziani raggirati da truffe digitali. Comprendere questi fenomeni è il primo passo per contrastarli — come individui, come genitori, come educatori, come cittadini.

La rete non è un mondo parallelo: è il nostro mondo

Il digitale come spazio di vita, non solo di svago

Uno degli equivoci più pericolosi riguardo alla vita online è quello di considerarla una dimensione separata, parallela, meno reale della vita di tutti i giorni. "È solo internet" è la frase con cui si tende a minimizzare insulti, umiliazioni e violenze che avvengono attraverso schermi e tastiere. Ma questa distinzione è falsa, e le sue conseguenze possono essere devastanti. Le parole scritte in una chat, le foto condivise senza consenso, i commenti pubblicati sotto un post: questi atti producono effetti reali su persone reali. La vergogna, la paura, l'isolamento, la depressione che derivano da una campagna di cyberbullismo sono altrettanto reali quanto quelli prodotti da una violenza fisica. In alcuni casi, sono anche più duraturi, perché il contenuto digitale può restare accessibile per anni, rivivendo il danno ogni volta che viene trovato o ricondiviso.

Il digitale come estensione della responsabilità

Riconoscere che la rete non è un mondo separato significa anche riconoscere che le regole della convivenza civile — il rispetto, l'empatia, il consenso, la responsabilità per le proprie azioni — non si sospendono quando si entra online. Chi pubblica un contenuto offensivo, chi condivide una foto privata senza consenso, chi si unisce a una campagna di odio contro una persona reale sta compiendo atti con

conseguenze reali, legalmente perseguibili e moralmente inaccettabili. Questa dispensa non intende soltanto informare sui rischi della rete: intende contribuire a costruire una cultura digitale in cui la responsabilità, l'empatia e il rispetto siano valori praticati online con la stessa naturalezza con cui si praticano, o si dovrebbero praticare, nella vita quotidiana.

MODULO 1

Cos'è il cyberbullismo: caratteristiche, reati e meccanismi psicologici

Obiettivi del modulo

Al termine di questo modulo saprai distinguere il cyberbullismo dal bullismo tradizionale attraverso le sue caratteristiche specifiche di pervasività, anonimato, risonanza pubblica e permanenza. Conoscerai i principali reati digitali correlati (revenge porn, cyberstalking, dissing) e le relative conseguenze legali. Saprai riconoscere le forme più comuni di aggressione online e comprenderai i meccanismi psicologici che trasformano un utente comune in un aggressore.

Dal bullismo al cyberbullismo: cosa cambia

Il bullismo esiste da sempre: è una forma di aggressione sistematica e intenzionale nei confronti di una persona più debole o percepita come tale. Il cyberbullismo ne è la versione digitale, ma non si tratta soltanto di un trasferimento dello stesso fenomeno su un nuovo mezzo. Le caratteristiche specifiche della rete trasformano profondamente la natura e la portata del fenomeno, rendendolo in molti casi più grave e più difficile da gestire rispetto alla sua versione tradizionale.

Nel bullismo tradizionale, l'aggressione è limitata nello spazio e nel tempo: avviene a scuola, in un quartiere, in un contesto definito. Quando la vittima torna a casa, ha almeno un momento di respiro. Nel cyberbullismo, questa distinzione scompare: lo smartphone è con la vittima ventiquattro ore su ventiquattro, sette giorni su sette. L'aggressione può raggiungerla a qualsiasi ora, in qualsiasi luogo. È questa la caratteristica che i ricercatori definiscono pervasività: l'impossibilità di sfuggire all'aggressore rifugiandosi in uno spazio fisico separato.

La seconda caratteristica distintiva è l'anonimato. Online è relativamente facile creare profili falsi, usare nickname, nascondere la propria identità. Questo abbassa enormemente la soglia di inibizione: molte persone scrivono online cose che non direbbero mai di persona, protette dalla sensazione — spesso illusoria — di essere invisibili. L'anonimato non protegge però dal punto di vista legale: le autorità competenti sono in grado di risalire all'identità reale di chi compie reati digitali.

La risonanza pubblica è la terza caratteristica. Un atto di bullismo tradizionale ha tipicamente un numero limitato di testimoni. Un contenuto offensivo pubblicato online può essere visto, condiviso e amplificato da migliaia di persone in pochissimo tempo. La dimensione pubblica del danno moltiplicato è spesso ciò che rende il cyberbullismo particolarmente devastante per la vittima.

La permanenza è forse la caratteristica più insidiosa. Il web ha una memoria lunghissima: un contenuto una volta pubblicato è estremamente difficile da eliminare completamente. Può essere salvato,

ricondiviso, riemerso anni dopo. Per la vittima, questo significa che l'umiliazione non è circoscritta a un momento specifico ma può rivivere indefinitamente, ogni volta che qualcuno trova quel contenuto.

Quando il comportamento online diventa reato

Molti comportamenti che si manifestano online non sono semplici mancanze di educazione o "ragazzate": sono reati penalmente perseguibili. Conoscerli è fondamentale sia per proteggersi sia per non commettere atti di cui non si comprendono le conseguenze legali.

Il revenge porn — tecnicamente definito dalla legge italiana come "diffusione illecita di immagini o video sessualmente espliciti" — è la condivisione senza consenso di immagini o video intimi di una persona. Dalla legge 69 del 2019, è un reato specifico punito con la reclusione da uno a sei anni e con la multa. Non è necessario che il contenuto sia stato originariamente prodotto senza consenso: anche condividere immagini che erano state condivise privatamente e volontariamente costituisce reato, se avviene senza l'autorizzazione della persona ritratta.

Il cyberstalking è la persecuzione sistematica attraverso mezzi digitali: messaggi ripetuti e indesiderati, monitoraggio dei profili social, minacce, pubblicazione di informazioni private. È perseguibile penalmente come atto persecutorio ai sensi dell'articolo 612-bis del Codice Penale, con pene che possono arrivare fino a sei anni di reclusione in caso di aggravanti.

Il dissing è la divulgazione pubblica di informazioni riservate, umilianti o dannose riguardanti una persona, con l'intento di danneggiarla agli occhi degli altri. Può assumere la forma di diffamazione aggravata quando avviene attraverso strumenti informatici, un reato previsto dall'articolo 595 del Codice Penale con l'aggravante dell'articolo 595, terzo comma.

Le forme di aggressione online: riconoscerle per contrastarle

Le aggressioni online assumono forme diverse, non sempre immediatamente riconoscibili come tali. Conoscerle aiuta a identificarle quando si verificano, a non perpetrarle inconsapevolmente e a sapere come rispondere.

Il trolling è la pratica di provocare deliberatamente altre persone online con commenti offensivi, fuori luogo o contraddittori, con l'unico scopo di generare reazioni emotive negative. Non ha mai un obiettivo costruttivo: è aggressione mascherata da opinione. La risposta più efficace al trolling è il non rispondere: privare il troll della reazione emotiva che cerca è l'unico modo per disinnescarlo.

L'hate speech — discorso d'odio — è qualsiasi forma di comunicazione che incita all'odio, alla discriminazione o alla violenza contro persone o gruppi in base alla loro identità: etnia, religione, genere, orientamento sessuale, disabilità. È vietato dalla legge italiana e dalle politiche di quasi tutte le piattaforme digitali. È importante distinguerlo dalla critica, anche dura: l'hate speech non è una opinione, è un atto di aggressione verso una categoria di persone.

Il body shaming è la pratica di criticare, deridere o umiliare una persona per il suo aspetto fisico. Sebbene possa sembrare meno grave di altri tipi di aggressione, può avere conseguenze psicologiche

molto serie, soprattutto negli adolescenti, e contribuisce a una cultura tossica che associa il valore delle persone al loro aspetto esteriore.

Il furto d'identità e il catfishing sono fenomeni diversi ma correlati. Nel primo caso, qualcuno usa l'identità di un'altra persona (il suo nome, le sue foto, i suoi dati) per impersonarla online, spesso per danneggiarla. Nel secondo, qualcuno costruisce un'identità falsa per instaurare relazioni ingannevoli, spesso a scopo manipolativo o truffaldino.

I meccanismi psicologici: perché le persone diventano aggressive online

Comprendere perché le persone si comportano online in modi che non adotterebbero mai nella vita di tutti i giorni è fondamentale per affrontare il problema alla radice. Due meccanismi psicologici giocano un ruolo centrale.

L'effetto di disinibizione descrive il fenomeno per cui la mancanza di contatto visivo diretto — non vedere la faccia dell'altra persona, non sentire la sua voce, non percepire le sue reazioni emotive — riduce significativamente i freni inibitori naturali che regolano i comportamenti sociali. Nella comunicazione faccia a faccia, l'empatia è attivata automaticamente dalla percezione delle emozioni altrui: vediamo qualcuno soffrire e sentiamo una risposta interna che ci frena dall'infliggere ulteriore sofferenza. Online, questa retroazione emotiva è assente, e il comportamento aggressivo diventa più facile da mettere in atto.

I bias cognitivi — in particolare il bias di conferma e il bias di ostilità — sono un ulteriore fattore che contribuisce alle aggressioni online. Il bias di conferma porta a cercare e a interpretare le informazioni in modo da confermare le proprie opinioni preesistenti, rifiutando quelle contraddittorie. Il bias di ostilità porta a interpretare azioni o parole ambigue come intenzionalmente ostili: un commento neutro viene letto come un attacco, un emoji viene interpretato come sarcasmo. Questi meccanismi, amplificati dalla rapidità della comunicazione digitale e dall'assenza di contesto non verbale, producono conflitti che possono degenerare rapidamente.

> Condividere o mettere "like" a un atto di cyberbullismo significa diventarne complici. La complicità online non è moralmente neutrale e può avere conseguenze legali, specialmente per i minori che raggiungono l'età penalmente rilevante.

MODULO 2

Gli attori, i fattori di rischio e le conseguenze

Obiettivi del modulo

Al termine di questo modulo saprai analizzare i ruoli degli attori coinvolti in una dinamica di cyberbullismo: la vittima, il bullo e, con particolare attenzione, gli spettatori. Conoscerai i principali fattori di rischio individuali e ambientali che rendono alcune persone più vulnerabili. Saprai riconoscere i segnali di allarme che indicano che qualcuno potrebbe essere vittima di cyberbullismo e comprenderai la natura delle conseguenze fisiche, comportamentali e psicopatologiche che il fenomeno può produrre.

Gli attori: molto più di bullo e vittima

L'analisi del cyberbullismo che si ferma alla coppia bullo-vittima è incompleta e fuorviante. La realtà è più complessa e coinvolge un terzo protagonista spesso trascurato ma forse il più importante: gli spettatori.

La vittima è la persona che subisce sistematicamente e intenzionalmente le aggressioni digitali. Spesso si sente sola, incompresa e senza via d'uscita. Uno degli aspetti più dolorosi del cyberbullismo è la sensazione che nessuno intervenga, che chi assiste preferisca guardare senza prendere posizione. La permanenza dei contenuti online e la difficoltà di sfuggire all'aggressione amplificano la sofferenza e il senso di impotenza.

Il cyberbullo è la persona che attua le aggressioni. Non sempre si tratta di un individuo caratterizzato da cattiveria o da problemi psicologici gravi: spesso è qualcuno che non ha piena consapevolezza delle conseguenze delle proprie azioni, che agisce per cercare approvazione nel gruppo, che usa l'aggressione come strumento per affermare un dominio sociale, o che è a sua volta vittima di dinamiche negative in altri contesti. Comprendere le motivazioni del bullo non significa giustificarlo, ma è necessario per costruire interventi efficaci.

Il potere degli spettatori: da testimoni a protagonisti

Gli spettatori sono le persone che assistono alle aggressioni digitali: chi vede il post offensivo, chi legge i commenti, chi riceve lo screenshot. Sono la maggioranza silenziosa che, con il suo comportamento — attivo o passivo — determina in modo cruciale l'evoluzione della situazione.

Lo spettatore attivo è chi interviene amplificando l'aggressione: condivide i contenuti, aggiunge commenti offensivi, mette like, si unisce alla campagna di scherno. Anche se non è l'iniziatore dell'aggressione, contribuisce attivamente ad essa e ne è corresponsabile sul piano morale e, in certi casi, legale.

Lo spettatore passivo è chi assiste senza fare nulla: vede ma tace, legge ma non commenta, è consapevole ma non interviene. Spesso il silenzio è motivato dalla paura di diventare a propria volta vittima, dal desiderio di non complicarsi la vita, o dalla sensazione che il problema non riguardi direttamente se

stessi. Ma il silenzio dello spettatore ha un effetto concreto: dice al bullo che il suo comportamento è accettato, o almeno tollerato, e dice alla vittima che è sola.

L'alleato è lo spettatore che sceglie di intervenire in difesa della vittima. Non necessariamente con confronti diretti con il bullo — che potrebbero essere controproducenti — ma supportando la vittima privatamente, segnalando i contenuti alle piattaforme, coinvolgendo adulti di riferimento o semplicemente facendo sentire alla vittima che non è sola. Il potere dell'alleato è spesso sottovalutato: anche un singolo gesto di sostegno può fare una differenza enorme nella vita di chi subisce.

> La ricerca mostra che il cyberbullismo tende a cessare o a ridursi significativamente quando un numero sufficiente di spettatori si trasforma in alleati. Il cyberbullo smette quando smette di ricevere il rinforzo del gruppo. La decisione di non essere spettatore passivo è una delle più potenti che si possa prendere online.

I fattori di rischio

Non tutti sono ugualmente esposti al rischio di diventare vittime di cyberbullismo. Esistono fattori individuali e ambientali che aumentano la vulnerabilità, e conoscerli permette di intervenire in modo più mirato.

A livello individuale, i fattori di rischio includono una bassa autostima e una scarsa sicurezza in sé stessi, difficoltà nelle relazioni sociali, esperienze pregresse di vittimizzazione (chi è già stato vittima di bullismo tende a esserlo anche online) e una scarsa familiarità con le dinamiche digitali che rende difficile riconoscere e rispondere alle aggressioni. Anche le caratteristiche che rendono una persona diversa dalla norma percepita: l'aspetto fisico, l'orientamento sessuale, la provenienza, le difficoltà di apprendimento possono aumentare il rischio di essere presi di mira.

A livello ambientale, i fattori di rischio includono una scarsa supervisione e comunicazione in famiglia riguardo all'uso del digitale, un contesto scolastico o comunitario che tollera o minimizza le dinamiche di aggressione, e la mancanza di educazione digitale formale. Quest'ultimo fattore è di particolare importanza: chi non conosce le implicazioni legali e psicologiche dei propri comportamenti online, chi non sa come segnalare un contenuto offensivo, chi non conosce i propri diritti in quanto vittima è significativamente più vulnerabile.

Le conseguenze: il peso invisibile

Le conseguenze del cyberbullismo sono reali, profonde e spesso durature. Non si tratta di reazioni esagerate o di fragilità individuale: sono risposte psicologiche e fisiche documentate e studiate dalla ricerca scientifica, che possono manifestarsi con intensità diversa a seconda della gravità e della durata dell'aggressione.

I segnali comportamentali che possono indicare che qualcuno sta subendo cyberbullismo includono il ritiro sociale, il cambiamento improvviso nelle abitudini di uso del telefono o del computer, l'evitamento di eventi sociali, il calo del rendimento scolastico o lavorativo, la perdita di interesse per attività precedentemente piacevoli. Spesso la vittima inizia a evitare di usare i dispositivi digitali o, al contrario, non riesce a staccarsi da essi, in preda a un'ansia di controllo costante di ciò che viene detto di lei online.

I sintomi fisici possono includere disturbi del sonno, mal di testa, dolori addominali, stanchezza cronica. Questi sintomi sono la risposta del corpo a uno stato di stress prolungato: il cyberbullismo, per la sua natura pervasiva, mantiene la vittima in uno stato di allerta continua che ha conseguenze fisiche concrete.

L'impatto psicopatologico può essere molto grave: ansia, depressione, disturbi post-traumatici da stress, nei casi più gravi pensieri suicidari. La permanenza dei contenuti digitali amplifica questo impatto: a differenza di un'aggressione fisica che si esaurisce in un momento, il cyberbullismo può essere rivissuto ogni volta che si accede alla rete, ogni volta che qualcuno trova quel contenuto e lo ricondivide.

Segnale d'allarme: Un cambiamento brusco e inspiegabile nelle abitudini digitali o nel comportamento sociale di una persona (soprattutto di un giovane) è spesso il primo segnale che qualcosa non va. Prendersene cura, chiedere come sta e offrire ascolto senza giudicare può fare una differenza cruciale.

MODULO 3

Uso etico della rete: netiquette, privacy e pensiero critico

Obiettivi del modulo

Al termine di questo modulo conoscerai i principi fondamentali della netiquette e dell'impronta digitale, comprenderai il concetto di consenso nel contesto digitale e saprai come gestire attivamente la tua privacy online. Conoscerai le principali tecniche di phishing e saprai come difenderti. Avrai strumenti concreti per sviluppare il pensiero critico come antidoto ai bias cognitivi che alimentano le aggressioni online.

La netiquette: il galateo della rete

La netiquette — contrazione di network etiquette — è l'insieme delle norme di comportamento che regolano la comunicazione online. Non è un codice scritto con forza di legge, ma una serie di convenzioni condivise che permettono la convivenza civile negli spazi digitali. La sua regola fondamentale è semplice e potente: comportati online come vorresti essere trattato, e come ti comporteresti in un contesto pubblico reale.

Alcune norme di netiquette sono particolarmente rilevanti nel contesto di questa dispensa. Non condividere mai contenuti di altri (foto, messaggi privati, informazioni personali)senza il loro esplicito consenso. Non pubblicare informazioni su situazioni, luoghi o persone senza aver chiesto il permesso. Non usare un tono aggressivo, sarcastico o denigratorio nei commenti: la critica può essere diretta e onesta senza essere offensiva. Non alimentare le discussioni aggressive con la propria partecipazione: il silenzio attivo, ossia scegliere deliberatamente di non amplificare, è spesso la risposta più efficace.

L'impronta digitale: cosa lasci di te online

Ogni azione che compiamo online lascia una traccia: i commenti che pubblichiamo, le foto che carichiamo, i like che mettiamo, le ricerche che facciamo, i siti che visitiamo. L'insieme di queste tracce costituisce la nostra impronta digitale, una sorta di curriculum informale che ci precede e che ci segue in ogni contesto in cui qualcuno voglia cercarci.

La metafora del muro è utile per comprendere la portata di questo concetto: se tutto ciò che scrivi oggi restasse scolpito su un muro della tua città per i prossimi cinquant'anni, saresti fiero di averlo firmato? Molti comportamenti online che sembrano effimeri come un commento scritto di getto o una foto condivisa in un momento di rabbia, possono riemergere anni dopo con conseguenze che non si erano previste. I selezionatori del lavoro cercano i candidati online. I partner controllano i profili social. Le istituzioni possono richiedere l'accesso a contenuti digitali in caso di procedimenti legali. L'impronta digitale non è un concetto astratto: è parte della propria reputazione nel mondo reale.

La cultura del consenso

Il consenso è il principio fondamentale che regola l'uso etico dei contenuti che riguardano altre persone. Prima di condividere una foto in cui c'è qualcun altro, bisogna chiedere il permesso a quella persona. Prima di pubblicare informazioni su qualcuno, bisogna assicurarsi di averne il consenso. Prima di taggare qualcuno in un post, bisogna verificare che sia a proprio agio con quella visibilità.

Il consenso deve essere libero, informato e specifico: qualcuno che ha acconsentito a essere fotografato non ha necessariamente acconsentito a che quella foto venga pubblicata sui social network. Qualcuno che ha condiviso con te privatamente un'informazione non ha acconsentito a che tu la condivida con altri. Il consenso non è una burocrazia: è il rispetto fondamentale per l'autonomia e la dignità dell'altro.

Privacy e sicurezza: proteggersi attivamente

La gestione della privacy online non è una questione di paranoia: è una competenza fondamentale di cittadinanza digitale. Le piattaforme social raccolgono enormi quantità di dati sui propri utenti, e la configurazione predefinita tende a massimizzare la visibilità e la condivisione dei dati, non a proteggere la privacy. Chi non configura attivamente le impostazioni di privacy dei propri profili sta, di fatto, concedendo a chiunque l'accesso alle proprie informazioni personali. La configurazione attiva della privacy comprende alcune pratiche essenziali: controllare regolarmente le impostazioni di privacy di ogni account social, verificando chi può vedere i propri contenuti, chi può taggare la propria persona, chi può trovare il profilo tramite ricerca; usare password forti con non meno di dodici caratteri, con combinazione di lettere maiuscole e minuscole, numeri e simboli e diverse per ogni account; attivare l'autenticazione a due fattori, che richiede una seconda verifica — tipicamente un codice inviato al telefono — per accedere all'account anche se qualcuno conosce la password.

La difesa dal phishing è altrettanto importante. Il phishing è una tecnica truffaldina che cerca di ottenere dati personali, password o informazioni finanziarie fingendosi un'entità affidabile: una banca, un servizio online, un ente pubblico. Si manifesta tipicamente attraverso email o messaggi che sembrano provenire da fonti legittime e che contengono link a siti che imitano quelli originali. Riconoscerlo richiede attenzione: controllare il mittente reale dell'email, verificare l'URL del sito prima di inserire dati, non cliccare su link ricevuti in messaggi non attesi, non fornire mai password o dati bancari in risposta a richieste via email.

Il pensiero critico: l'antivirus contro i bias

Il pensiero critico è la capacità di valutare le informazioni e le situazioni con metodo e consapevolezza, resistendo alle reazioni impulsive e alle distorsioni cognitive. Nell'ecosistema digitale, dove le informazioni si moltiplicano a velocità vertiginosa e dove i meccanismi di raccomandazione delle piattaforme tendono a rafforzare le posizioni già possedute, il pensiero critico è la difesa più efficace contro la disinformazione, i bias e le reazioni aggressive. La tecnica Wait and Think — aspetta e rifletti — è uno strumento semplice ma potente. Prima di rispondere a un commento che sembra offensivo, prima di condividere un contenuto che provoca indignazione, prima di reagire a ciò che sembra un attacco: aspetta. Prenditi trenta secondi, un minuto, un'ora. Chiedi ad almeno una persona di cui ti fidi

cosa ne pensa. La maggior parte delle reazioni aggressive online nasce da reazioni impulsive che, con un minimo di tempo e riflessione, non verrebbero mai messe in atto.

La Peer Education (l'educazione tra pari) è una delle strategie più efficaci per diffondere questi strumenti nelle comunità. Chi impara a riconoscere i propri bias cognitivi, a praticare il pensiero critico, a distinguere fatti da opinioni e a gestire le reazioni emotive online ha una responsabilità: condividere questi strumenti con chi gli sta vicino. La cultura digitale responsabile non si costruisce attraverso decreti dall'alto: si costruisce attraverso le relazioni, le conversazioni, gli esempi.

MODULO 4

Come rispondere: protocollo S.O.S., strumenti e quadro legale

Obiettivi del modulo

Al termine di questo modulo conoscerai il protocollo da adottare in caso di cyberbullismo: conservazione delle prove, non reazione, segnalazione istituzionale. Saprai utilizzare gli strumenti tecnologici di protezione disponibili, tra cui parental control, software di monitoraggio e strumenti delle piattaforme. Conoscerai il quadro normativo italiano, con particolare riguardo alla Legge 71/2017 e le principali responsabilità penali derivanti dai reati digitali.

Il protocollo S.O.S.: cosa fare quando succede

Quando si è vittima di cyberbullismo, o quando si è testimoni di un episodio che riguarda qualcuno vicino, sapere cosa fare concretamente fa una differenza enorme. Il protocollo S.O.S. (Salva, Osserva, Segnala) è uno schema operativo semplice che aiuta a non cedere al panico e a prendere le misure giuste.

La prima azione è non rispondere e non reagire. Qualsiasi risposta emotiva all'aggressore come insulti, minacce, difese appassionate, alimenta il conflitto, dà al bullo la soddisfazione della reazione e può essere usata contro di noi. La tentazione di rispondere è comprensibile, ma resistere è la scelta più efficace. Bloccare l'aggressore è la misura tecnica immediata da adottare.

La seconda azione è conservare le prove. Prima di eliminare qualsiasi contenuto, è fondamentale fare screenshot di tutto: i messaggi offensivi, i post, i commenti, le date e gli orari, i nomi dei profili coinvolti. Le prove digitali sono essenziali per qualsiasi procedimento legale o segnalazione istituzionale. Senza prove documentate, la parola della vittima è più difficile da sostenere davanti alle autorità.

La terza azione è la segnalazione istituzionale. Le piattaforme digitali hanno tutte strumenti di segnalazione dei contenuti offensivi: usarli è importante, anche se i tempi di risposta possono essere lunghi. Per i reati più gravi, è necessario rivolgersi alla Polizia Postale, che è l'organo specializzato nella gestione dei reati informatici. Il Garante per la Protezione dei Dati Personali ha poteri specifici per richiedere la rimozione di contenuti entro 48 ore: in caso di contenuti che violano la privacy (es. immagini diffuse senza consenso) è un'autorità fondamentale a cui rivolgersi.

Non aspettare che le cose si risolvano da sole. Il cyberbullismo, senza intervento, tende ad aggravarsi nel tempo. Agire prima segnalando, cercando supporto e coinvolgendo adulti di riferimento, è sempre meglio che aspettare.

Gli strumenti tecnologici di protezione

La tecnologia che può essere usata per fare del male può anche essere usata per proteggerci. Esistono strumenti specifici progettati per ridurre i rischi online, particolarmente utili nel contesto della tutela dei minori ma non esclusivi di quella fascia d'età.

Il parental control è un insieme di funzionalità software che permette di limitare l'accesso a determinati contenuti, di monitorare l'uso del dispositivo, di impostare limiti di tempo e di gestire le app installate. È disponibile come funzionalità nativa nei principali sistemi operativi (iOS, Android, Windows, macOS) e come applicazione dedicata. Non è uno strumento di sorveglianza invasiva: usato in modo trasparente, come parte di una conversazione aperta su sicurezza digitale, è un supporto prezioso per i genitori che vogliono proteggere i propri figli mantenendo un dialogo.

Le piattaforme digitali offrono anche strumenti specifici di protezione: la possibilità di bloccare utenti, di segnalare contenuti, di limitare chi può commentare i propri post o inviare messaggi privati, di filtrare i commenti con parole chiave specifiche. Usare attivamente questi strumenti è parte di una gestione responsabile della propria presenza online.

Il quadro normativo: la Legge 71/2017 e i reati digitali

L'Italia ha una legge specifica sul cyberbullismo: la Legge 71 del 29 maggio 2017, nota come Legge Mancini. È la prima legge italiana dedicata specificamente al fenomeno e ha introdotto strumenti importanti per la tutela dei minori e per la prevenzione e il contrasto del cyberbullismo nelle scuole.

La legge prevede che le scuole nominino un referente per le politiche di prevenzione e contrasto del cyberbullismo, con l'obbligo di attivare procedure di intervento in caso di episodi segnalati. Il preside/dirigente scolastico ha poteri e responsabilità specifiche: deve essere informato di qualsiasi episodio di cyberbullismo che riguardi la comunità scolastica e deve intervenire adottando le misure necessarie.

La legge prevede anche uno strumento specifico per i minori: la possibilità di chiedere al Garante per la Protezione dei Dati Personali l'oscuramento, la rimozione o il blocco di contenuti che ritengono essere atti di cyberbullismo, senza necessariamente avviare un procedimento penale. Il Garante è tenuto a rispondere entro 48 ore.

Per quanto riguarda le responsabilità penali, è importante sapere che in Italia la responsabilità penale inizia a 14 anni. Un minore di 14 anni non è penalmente imputabile, ma chi esercita la responsabilità genitoriale può essere chiamato a rispondere civilmente del danno. Tra i 14 e i 18 anni, i minori sono penalmente imputabili ma con trattamento differenziato rispetto agli adulti. Sopra i 18 anni, si risponde pienamente delle proprie azioni digitali.

I principali reati digitali perseguibili includono: la minaccia, articolo 612 del Codice Penale, fino a un anno di reclusione; la diffamazione aggravata tramite strumenti informatici, articolo 595, terzo comma, fino a tre anni di reclusione; la sostituzione di persona, articolo 494, fino a un anno; gli atti persecutori o cyberstalking, articolo 612-bis, da uno a sei anni, con aggravante in caso di uso di strumenti informatici; la diffusione illecita di immagini intime, legge 69 del 2019, da uno a sei anni.

Da sapere: Se sei vittima di un reato digitale, puoi presentare denuncia presso qualsiasi commissariato di Polizia o stazione dei Carabinieri. La Polizia Postale ha anche uno sportello online sul sito commissariatodips.it per le segnalazioni di reati informatici.

MODULO 5

La cultura dell'inclusione: da spettatori ad alleati

Obiettivi del modulo

Al termine di questo modulo avrai sviluppato una comprensione più profonda del concetto di empatia digitale e della responsabilità collettiva nel contrasto al cyberbullismo. Saprai come passare da spettatore passivo ad alleato proattivo. Avrai un toolkit operativo che include le regole d'oro per un uso quotidiano consapevole della rete e che puoi applicare immediatamente e condividere con chi ti sta vicino.

L'empatia digitale: vedersi nell'altro

L'empatia è la capacità di comprendere e condividere i sentimenti di un'altra persona, di mettersi nei suoi panni. Nell'ambiente digitale, questa capacità è sistematicamente erosa dall'assenza di contatto fisico, dalla velocità della comunicazione e dall'effetto di disinibizione che riduce la percezione della realtà emotiva dell'altro. Coltivare l'empatia digitale significa lavorare deliberatamente contro questa erosione.

Un esercizio pratico di empatia digitale è chiedersi, prima di pubblicare qualsiasi contenuto che riguardi un'altra persona: come mi sentirei se questo fosse pubblicato su di me? Se la risposta è che mi sentirei a disagio, ferito, umiliato, o se non posso sapere come si sentirebbe quella persona, magari perché non l'ho mai chiesto, allora è il momento di fermarsi.

L'empatia digitale non riguarda soltanto il non fare del male: riguarda anche il fare del bene attivamente. Riconoscere il contributo di qualcuno in una discussione online, esprimere sostegno a qualcuno che si trova in difficoltà, segnalare un contenuto offensivo perché si tiene alla dignità della persona che coinvolge: questi sono atti di empatia digitale che costruiscono comunità online migliori.

La responsabilità collettiva: il cyberbullismo si vince con la cultura

Il cyberbullismo non è un problema che può essere risolto soltanto dalla legge, dai filtri tecnologici o dagli adulti di riferimento. È un problema culturale che richiede una risposta culturale. Le norme legislative sono necessarie ma non sufficienti: una norma senza una cultura che la sostenga non cambia i comportamenti reali.

La responsabilità collettiva significa che tutti (non solo le vittime e non solo i bulli) hanno un ruolo nella costruzione di spazi digitali più sicuri e più rispettosi. Chi sceglie di non condividere contenuti offensivi contribuisce. Chi segnala un post problematico contribuisce. Chi supporta una persona che sta subendo un'aggressione contribuisce. Chi parla apertamente di questi temi con i propri figli, i propri studenti, i propri colleghi contribuisce. La transizione dall'esclusione sociale all'inclusione digitale non avviene automaticamente: è il risultato di scelte quotidiane, individuali e collettive, che sommandosi producono un cambiamento culturale reale. Ogni persona che legge questa dispensa e decide di applicare i principi che contiene è parte di questo cambiamento.

Il toolkit: le cinque regole d'oro

Al termine di questo percorso, è utile avere un promemoria operativo — un toolkit — che sintetizzi i principi fondamentali in regole concrete e applicabili ogni giorno. Queste regole d'oro non sostituiscono la complessità di ciò che si è discusso: la sintetizzano in azioni immediate.

1. Pensa prima di postare. Ogni contenuto che pubblichi è potenzialmente permanente e pubblico. Chiediti: se questo restasse online per sempre, sarei a mio agio? Se la risposta è no, non pubblicarlo.

2. Il consenso è sacro. Non condividere mai contenuti che riguardano altre persone senza il loro esplicito permesso. Questo vale per le foto, per le informazioni personali, per i messaggi privati. Il consenso non è una formalità: è rispetto.

3. Le parole hanno un peso. Anche online, anche in forma anonima, anche in una chat privata. Le parole che scrivi raggiungono persone reali con emozioni reali. Usa il tono che useresti guardando negli occhi la persona a cui ti stai rivolgendo.

4. Non restare in silenzio. Se sei testimone di un'aggressione online, non girare la testa. Segnala il contenuto, supporta la vittima, coinvolgi adulti di riferimento. Il silenzio degli spettatori è il carburante del cyberbullismo.

5. Proteggi i tuoi dati. Configura attivamente le impostazioni di privacy dei tuoi account. Usa password forti e diverse. Non condividere informazioni sensibili in risposta a richieste non verificate. La tua sicurezza online dipende in gran parte dalle tue scelte.

Queste regole non sono restrizioni alla libertà online: sono le fondamenta di una libertà digitale più autentica. Chi usa la rete con responsabilità e rispetto può fruire di tutti i suoi

benefici senza le conseguenze legali, reputazionali, relazionali che derivano dai comportamenti irresponsabili.

Il ruolo degli adulti: genitori, educatori e comunità

Perché il dialogo è più efficace del controllo

Uno degli errori più comuni che gli adulti commettono nel tentativo di proteggere i giovani dal cyberbullismo è quello di affidarsi esclusivamente al controllo: sottrarre i dispositivi, installare filtri senza spiegarne il motivo, vietare l'accesso ai social network. Queste misure, adottate senza una comunicazione aperta e senza un lavoro educativo di accompagnamento, producono quasi sempre l'effetto contrario: il giovane impara a nascondere la propria vita digitale, e il problema si sposta in uno spazio in cui l'adulto non ha più alcuna visibilità.

La ricerca è chiara su questo punto: i giovani che affrontano meglio le situazioni difficili online sono quelli che hanno la certezza di poter parlare con un adulto di riferimento senza essere giudicati, puniti o privati del telefono. Questo non significa che i genitori e gli educatori debbano approvare qualsiasi comportamento: significa che devono costruire una relazione di fiducia sufficiente perché il giovane scelga di chiedere aiuto anziché affrontare da solo una situazione che lo sopraffà.

Il dialogo preventivo, parlare di questi temi prima che accada qualcosa, è molto più efficace di quello reattivo. Un genitore che discute apertamente con i propri figli di cosa fare se si riceve un messaggio offensivo, di come riconoscere il phishing, di quali contenuti non condividere: questo genitore sta costruendo un'armatura culturale che nessun software di parental control potrà mai replicare.

Come parlare di cyberbullismo con i giovani

Non esiste uno script perfetto per questa conversazione, ma esistono alcune linee guida che la rendono più efficace. La prima è partire dall'ascolto, non dalla norma: prima di spiegare cosa si deve o non si deve fare, chiedere cosa sa già il giovane di questi temi, cosa ha visto, cosa gli è capitato. Ascoltare senza interrompere, senza giudicare, senza reagire con allarme eccessivo: questi atteggiamenti creano lo spazio psicologico in cui la comunicazione diventa possibile.

La seconda linea guida è usare esempi concreti, non astratti. Non "il cyberbullismo fa male" ma "hai mai visto qualcuno essere trattato male in un gruppo WhatsApp? Come ti sei sentito? Cosa hai fatto?". I casi concreti, inclusi quelli che compaiono nelle notizie, sono strumenti educativi potenti se usati senza sensazionalismo e con un focus sull'analisi critica della situazione.

La terza linea guida è chiarire che chiedere aiuto non significa perdere il telefono. Questa è spesso la ragione principale per cui i giovani non parlano con gli adulti quando subiscono cyberbullismo: hanno paura che la reazione immediata dell'adulto sia quella di togliere il dispositivo, che per loro è anche lo strumento di connessione con gli amici, il mezzo di espressione, lo spazio di autonomia. Esplicitare che l'obiettivo è aiutare, non punire, è il primo passo per abbattere questa barriera.

Il ruolo della scuola: oltre la Legge 71/2017

La scuola ha un ruolo unico nel contrasto al cyberbullismo: è il luogo in cui la maggior parte delle dinamiche di gruppo tra adolescenti si forma e si manifesta, e in cui è possibile raggiungere tutti i giovani con un intervento sistematico ed educativo. La Legge 71/2017 ha formalizzato questo ruolo con obblighi specifici, ma l'efficacia dell'intervento scolastico va molto oltre l'adempimento normativo. I programmi di educazione digitale che funzionano non sono quelli che si limitano a elencare i rischi della rete: sono quelli che mettono al centro le competenze, il pensiero critico, la gestione delle emozioni, la capacità di riconoscere i propri bias e che usano metodologie attive come il role playing, la peer education e la discussione di casi reali. La dispensa che stai leggendo è concepita esattamente in quest'ottica: non come un testo da memorizzare ma come uno strumento per attivare riflessioni e cambiamenti di comportamento.

Il referente scolastico per il cyberbullismo (figura prevista dalla Legge 71/2017) ha un ruolo di coordinamento che va oltre la gestione degli episodi critici: include la promozione di una cultura digitale responsabile all'interno della comunità scolastica, il raccordo con le famiglie e le istituzioni esterne, e la formazione continua dei docenti su questi temi. Una scuola che forma adulti digitalmente consapevoli forma, indirettamente, famiglie e comunità più capaci di affrontare questi fenomeni.

La comunità come rete di protezione

Il cyberbullismo non è soltanto un problema che riguarda i giovani e le scuole. Coinvolge adulti — mobbing digitale, revenge porn tra ex partner, stalking online — e anziani — truffe, manipolazione, isolamento digitale. Una risposta culturale efficace deve coinvolgere l'intera comunità, non solo le fasce d'età più giovani.

Le biblioteche, i centri anziani, le associazioni di quartiere, le parrocchie, le organizzazioni di volontariato: sono tutti luoghi in cui si può fare educazione digitale e promuovere una cultura del rispetto online. Iniziative come il progetto Digita Facile Campania dimostrano che la formazione digitale rivolta agli adulti e agli anziani produce risultati concreti in termini di autonomia, sicurezza e qualità della vita. Una comunità digitalmente consapevole è una comunità più resiliente di fronte ai rischi della rete.

Per i genitori: Se tuo figlio segnalasse di essere vittima di cyberbullismo, la prima risposta dovrebbe essere gratitudine per la fiducia dimostrata e ascolto attivo. Solo dopo, insieme, si valutano le azioni da intraprendere. Non togliere il telefono come prima reazione: è il modo più rapido per perdere la comunicazione.

Imparare dai casi: scenari e riflessioni

Uno degli strumenti più efficaci per comprendere davvero un fenomeno è confrontarsi con situazioni concrete. I seguenti scenari, costruiti a partire da tipologie reali di episodi di cyberbullismo, sono pensati per attivare la riflessione e per applicare i concetti discussi in questa dispensa a situazioni riconoscibili.

Scenario 1: il gruppo di classe

Giulia, 15 anni, viene esclusa dal gruppo WhatsApp della classe senza spiegazioni. I suoi compagni creano un gruppo parallelo in cui condividono screenshot di sue conversazioni private, aggiungendo commenti ironici sul suo aspetto e sul suo modo di parlare. Giulia lo scopre per caso attraverso un'amica. Nei giorni successivi, i commenti ironici si trasferiscono anche sui social network, sempre più pubblici. Giulia inizia a non voler andare a scuola.

Questo scenario illustra alcune caratteristiche tipiche del cyberbullismo tra adolescenti: la dimensione di gruppo, che amplifica la portata dell'aggressione; la transizione dal privato al pubblico, che ne aumenta la gravità; e il legame con la vita offline, che rende impossibile per la vittima separare le due sfere. In questo caso, cosa avrebbe potuto fare l'amica che ha scoperto la situazione? Come dovrebbe reagire un genitore informato? Cosa prevede la scuola in questo caso?

Scenario 2: l'ex partner

Marco, 23 anni, termina una relazione. L'ex partner, in risposta, pubblica sui social network screenshot di messaggi privati, commentandoli in modo da screditarlo agli occhi degli amici comuni. Successivamente, crea un profilo falso con il nome di Marco e inizia a inviare messaggi offensivi ai suoi contatti. Marco si trova a dover spiegare a tutti che non è lui il mittente di quei messaggi.

Questo scenario combina due reati distinti: la diffamazione (la pubblicazione dei messaggi con commenti offensivi) e la sostituzione di persona (il profilo falso). Illustra come il cyberbullismo non riguardi soltanto i giovanissimi e come possa avere conseguenze concrete e immediate sulla vita reale, nelle relazioni sociali e professionali. Quali sono le prime azioni che Marco dovrebbe intraprendere? A quali autorità può rivolgersi?

Scenario 3: lo spettatore

Lucia, 17 anni, fa parte di un gruppo online in cui alcuni ragazzi iniziano a prendere in giro sistematicamente un compagno di scuola, condividendo foto modificate in modo ridicolo e inventando storie false sul suo conto. Lucia non conosce molto bene il compagno preso di mira, ma si rende conto che le cose stanno peggiorando. Non vuole essere coinvolta, ma sente che il silenzio la rende complice.

Questo scenario esplora il dilemma dello spettatore passivo: la tensione tra il desiderio di non complicarsi la vita e la consapevolezza che il silenzio ha un costo morale. Lucia non deve necessariamente confrontarsi direttamente con i ragazzi che stanno facendo del male: può segnalare il contenuto alla piattaforma, può contattare privatamente il compagno per fargli sapere che non è solo, può parlare con un adulto di riferimento. Anche il gesto più piccolo può fare la differenza.

Scenario 4: l'adulto e la truffa digitale

Antonio, 68 anni, riceve un'email che sembra provenire dalla sua banca, con il logo ufficiale e un tono formale. L'email lo informa di un'anomalia sul conto e lo invita a cliccare su un link per verificare i propri dati. Antonio clicca, inserisce le credenziali e si ritrova con il conto svuotato in poche ore. Quando lo racconta ai figli, si sente rispondere che "doveva stare più attento".

Questo scenario illustra due fenomeni distinti ma correlati: il phishing sofisticato, che non è più facilmente riconoscibile come in passato, e la tendenza a colpevolizzare le vittime di truffe digitali. Antonio non è caduto in una truffa per stupidità: è caduto in una truffa perché era ben costruita e perché non aveva ricevuto una formazione adeguata su come riconoscerla. La risposta giusta non è il rimprovero: è il supporto immediato, come contattare la banca, sporgere denuncia e la formazione preventiva per evitare che accada di nuovo.

I casi reali ci ricordano che il cyberbullismo e le aggressioni digitali non sono fenomeni astratti. Dietro ogni scenario c'è una persona reale con una vita reale che viene danneggiata. Tenere questa consapevolezza viva è il fondamento di qualsiasi cultura digitale responsabile.

Riepilogo dei concetti fondamentali

Questo percorso formativo ha affrontato il cyberbullismo e l'esclusione sociale digitale nella loro complessità: non come un problema di tecnologia ma come un problema umano, culturale e sociale che richiede risposte a più livelli. Il cyberbullismo si distingue dal bullismo tradizionale per quattro caratteristiche che lo rendono spesso più grave: la pervasività, non conosce orari né confini fisici; l'anonimato, che abbassa le difese psicologiche dell'aggressore ; la risonanza pubblica, che moltiplica il danno; la permanenza, che lo rende difficile da archiviare. Molti comportamenti online non sono semplici mancanze di educazione ma reati penalmente perseguibili: revenge porn, cyberstalking, diffamazione aggravata, sostituzione di persona.

Comprendere gli attori del cyberbullismo significa andare oltre la coppia bullo-vittima. Gli spettatori sono i protagonisti più numerosi e, collettivamente, i più potenti: la loro scelta di essere attivi, passivi o alleati determina in misura cruciale l'evoluzione della situazione. Il cyberbullo smette quando smette di ricevere il rinforzo del gruppo. La decisione di trasformarsi da spettatore in alleato è una delle più importanti che si possa prendere online.

Un uso etico della rete richiede tre pilastri: la netiquette, comportarsi online come ci si comporterebbe in un contesto pubblico reale; il consenso, non condividere mai contenuti altrui senza permesso; il pensiero critico, resistere alle reazioni impulsive e ai bias cognitivi che alimentano i conflitti. La gestione attiva della propria privacy e la difesa dal phishing completano il quadro delle competenze di sicurezza digitale.

Quando si è vittime o testimoni di cyberbullismo, sapere come agire fa la differenza: non rispondere all'aggressore, conservare le prove con screenshot, segnalare alle piattaforme, alla Polizia Postale e al Garante per la Protezione dei Dati. La Legge 71/2017 offre strumenti specifici per i minori; il Codice Penale prevede sanzioni precise per i reati digitali a partire dai 14 anni.

La lotta al cyberbullismo si vince con la cultura. L'empatia digitale, la responsabilità collettiva, la scelta quotidiana di non essere spettatori passivi: sono questi gli ingredienti di una rete migliore. Ogni persona che applica le cinque regole d'oro (pensare prima di postare, rispettare il consenso, pesare le parole, non restare in silenzio, proteggere i propri dati) contribuisce a costruire spazi digitali più sicuri e più degni per tutti.

> Il web non dimentica. Ma tu puoi scegliere cosa lasciare su quel muro. Ogni giorno, ogni post, ogni commento è una scelta. Scegli bene.

Test di autovalutazione

Indica la risposta corretta per ciascuna domanda. Le risposte si trovano in fondo alla sezione.

1. Come agisce l'effetto di disinibizione sull'aggressore online? a) Lo rende più timido e riservato. b) Riduce i freni inibitori e l'empatia perché la mancanza di contatto visivo "anestetizza" la percezione delle emozioni altrui. c) Rallenta la velocità di scrittura.

2. Interpretare negativamente le intenzioni di qualcuno sulla base di un messaggio ambiguo è un esempio di: a) Bias di conferma. b) Bias di ostilità. c) Effetto tunnel.

3. La Legge 71/2017 cosa prevede per le scuole? a) L'obbligo di sequestrare i telefoni. b) La nomina di un referente e procedure di prevenzione e intervento. c) L'installazione di telecamere.

4. Perché l'impronta digitale è rischiosa? a) Perché rovina lo smartphone. b) Perché incide sulla reputazione futura in modo difficile da controllare. c) Perché rallenta il wi-fi.

5. Qual è lo scopo principale della bias mitigation? a) Usare il pensiero critico per evitare reazioni aggressive alimentate da pregiudizi cognitivi. b) Bloccare i profili falsi. c) Migliorare la grafica dei post.

6. Qual è la prima azione da compiere se si riceve una minaccia online? a) Rispondere con tono fermo. b) Fare uno screenshot e non rispondere. c) Eliminare l'account.

7. Qual è la differenza tra spettatore attivo e alleato? a) Lo spettatore attivo aiuta il bullo; l'alleato aiuta la vittima. b) Sono sinonimi. c) L'alleato è un complice del bullo.

> **Risposte:** 1-b / 2-b / 3-b / 4-b / 5-a / 6-b / 7-a

Glossario essenziale

Alleato: lo spettatore che sceglie di intervenire attivamente in difesa della vittima di cyberbullismo, supportandola e segnalando i contenuti offensivi.

Anonimato (online): la possibilità di agire online nascondendo la propria identità reale. Riduce i freni inibitori ma non protegge dalle conseguenze legali.

Bias cognitivo: distorsione sistematica nel modo in cui si elaborano le informazioni e si prendono decisioni. Il bias di conferma e il bias di ostilità sono particolarmente rilevanti nel contesto delle aggressioni online.

Body shaming: pratica di criticare, deridere o umiliare una persona per il suo aspetto fisico, online o offline.

Catfishing: costruzione di un'identità falsa online per instaurare relazioni ingannevoli con altri utenti.

Cyberbullismo: forma di bullismo perpetrata attraverso dispositivi digitali e piattaforme online. Si distingue dal bullismo tradizionale per pervasività, anonimato, risonanza pubblica e permanenza.

Cyberstalking: persecuzione sistematica attraverso mezzi digitali — messaggi ripetuti, minacce, monitoraggio dei profili social. È perseguibile come atto persecutorio ai sensi dell'art. 612-bis del Codice Penale.

Disinibizione (effetto): fenomeno psicologico per cui la mancanza di contatto visivo online riduce i freni inibitori e la percezione delle emozioni altrui, facilitando comportamenti aggressivi.

Dissing: divulgazione pubblica di informazioni riservate o umilianti riguardanti una persona con l'intento di danneggiarla. Può configurarsi come diffamazione aggravata.

Empatia digitale: la capacità di riconoscere e rispettare le emozioni altrui negli spazi digitali, nonostante l'assenza di contatto fisico diretto.

Garante per la Protezione dei Dati Personali: autorità italiana che tutela la privacy dei cittadini. Ha poteri specifici per richiedere la rimozione di contenuti digitali lesivi entro 48 ore.

Hate speech: discorso d'odio che incita alla discriminazione, all'ostilità o alla violenza verso persone o gruppi in base alla loro identità. Vietato dalla legge italiana e dalle politiche delle piattaforme digitali.

Impronta digitale: l'insieme delle tracce lasciate online dalle proprie attività digitali: post, commenti, like, ricerche, interazioni. Costituisce un curriculum informale che può influenzare la reputazione reale.

Legge 71/2017: prima legge italiana specificamente dedicata al contrasto del cyberbullismo. Prevede strumenti di tutela per i minori, obblighi per le scuole e procedure di intervento istituzionale.

Netiquette: insieme di norme di comportamento che regolano la comunicazione civile negli spazi digitali. Deriva dall'unione di network ed etiquette.

Peer Education: educazione tra pari: strategia formativa in cui persone con caratteristiche simili si trasmettono competenze e comportamenti, risultando spesso più efficace della comunicazione verticale adulto-giovane.

Permanenza (del contenuto digitale): caratteristica del web per cui i contenuti pubblicati sono difficili da eliminare completamente e possono riemerge anche a distanza di anni.

Phishing: tecnica truffaldina che finge di provenire da fonti affidabili per ottenere dati personali, password o informazioni finanziarie.

Polizia Postale: organo specializzato nella gestione dei reati informatici in Italia. È il riferimento principale per le denunce di cyberbullismo e reati digitali.

Revenge porn: diffusione illecita di immagini o video sessualmente espliciti senza il consenso della persona ritratta. È reato specifico in Italia dalla Legge 69/2019, punito con la reclusione da uno a sei anni.

Trolling: pratica di provocare deliberatamente altri utenti online con commenti offensivi o fuori luogo, con l'unico scopo di generare reazioni emotive negative.

Risorse e contatti utili

In caso di episodi di cyberbullismo o per ulteriori informazioni, è possibile rivolgersi alle seguenti risorse.

Polizia Postale: commissariatodips.it — sportello online per segnalare reati informatici e consultare informazioni su truffe e sicurezza digitale.

Garante per la Protezione dei Dati Personali: gpdp.it/cyberbullismo — per richiedere la rimozione di contenuti lesivi della privacy e ottenere informazioni sui propri diritti digitali.

Telefono Azzurro: 19696 — servizio di ascolto e supporto per bambini e adolescenti in difficoltà, operativo tutti i giorni.

Parole O_Stili: paroleostili.it — progetto culturale che promuove un uso responsabile e rispettoso delle parole online.

Note finali

Questa dispensa è un materiale didattico prodotto nell'ambito del progetto Digita Facile Campania, promosso dalla Fondazione IFEL Campania e selezionato e sostenuto dal Fondo per la Repubblica Digitale – Impresa sociale, nell'ambito del bando "Dritti al Punto", in collaborazione con il Dipartimento per la Trasformazione Digitale. Il progetto si rivolge a cittadine e cittadini delle aree interne della Campania con l'obiettivo di rafforzare le competenze digitali nelle fasce di popolazione più esposte al rischio di esclusione, promuovendone l'autonomia e l'inclusione. Il percorso formativo si ispira al quadro europeo DigComp 2.2 e include tre macro-aree tematiche: Accesso ai Servizi Essenziali, Sicurezza e Uso Consapevole dei Servizi Digitali, Lavoro e Sviluppo Produttivo. Per ulteriori informazioni sul progetto e per conoscere il calendario dei prossimi corsi, visita la pagina dedicata su ifelcampania.it/eventi.