VADEMECUM SOCIAL

RAGAZZE DIGITALI ER

Consulta il *vademecum social* di **Ragazze Digitali ER** per sapere come raccontare la partecipazione ai Summer Camp. Inoltre, la guida contiene utili consigli per **difendere le proprie identità digitali e i dati** e mettersi al sicuro da potenziali rischi di violazione di diritti quali l'**immagine**, la **reputazione** e la **riservatezza**.

1 Come diventare testimonial di Ragazze Digitali?

Per raccontare la propria esperienza è possibile utilizzare i contenuti di un **media kit dedicato a Ragazze Digitali ER**. Liberamente scaricabile *online*, contiene numerosi elementi grafici e immagini utilizzabili sui social per diffondere la conoscenza dei Summer Camp. **Clicca qui** per consultare il media kit. In alternativa, puoi reperire il media kit ufficiale nella sezione *'News'* del sito web: **www.digitale.regione.emilia-romagna.it/ragazze-digitali**

Quando viene pubblicata un'immagine, una foto o un video sui propri canali social (*Facebook* e *Instagram*), si possono menzionare le pagine ufficiali di *Ragazze Digitali ER* e usare l'hashtag **#RagazzeDigitaliER**.

Consigliamo di usare i tag ufficiali in particolare per la condivisione di *stories* e *reel*:

- *Facebook*: **@ragazzedigitali**
- *Instagram*: **@ragazze.digitali**

Qualora la pubblicazione di contenuti riguardanti i Summer Camp avvenisse su *Tik Tok*, suggeriamo di condividere il video anche su Instagram e menzionare il profilo ufficiale di *Ragazze Digitali ER*.

2 Proteggere i propri dati personali

La Rete mette a disposizione dei propri utenti servizi gratuiti; i gestori delle piattaforme social - come *Facebook*, *Instagram* e *Tik Tok* - chiedono però in cambio i dati personali al fine di **tracciare le ►identità digitali**[1] dei frequentatori. L'obiettivo è la **profilazione degli utenti**, cioè la raccolta ed elaborazione dei dati di chi usufruisce dei servizi *online* al fine di segmentare l'utenza in gruppi di comportamento a vantaggio delle aziende. A gestire i *social network* sono generalmente aziende che si finanziano vendendo pubblicità mirate; il loro valore di mercato dipende anche dalla loro capacità di analizzare in dettaglio il profilo, le abitudini e gli interessi dei propri iscritti, per poi rivendere le informazioni a chi ne ha bisogno.

Le interazioni che avvengono all'interno dell'ambiente digitale durante la navigazione lasciano numerose tracce di dati – e quindi informazioni – che si disperdono nella Rete, concorrendo a definire la ***digital footprint*** di ognuno, ossia la propria impronta digitale. La **dispersione dei dati personali** si manifesta sia nel corso della navigazione in Internet mediante *browser* (si pensi ai ***cookies***, tecnica utilizzata dalle applicazioni web per archiviare e recuperare informazioni relative agli utenti), sia nell'utilizzo delle piattaforme di social networking. I social network, infatti, sono "**piazze virtuali**", cioè luoghi d'incontro e scambio (fotografie, filmati, pensieri, indirizzi di amici) degli utenti *online*; essi rappresentano uno straordinario **strumento di condivisione e comunicazione**, non privo – tuttavia – di rischi per la sfera personale degli individui.

L'impressione di servirsi di uno spazio personale spinge di fatto gli utenti a esporre troppo la propria vita privata, rivelando dati e informazioni strettamente personali, azione con effetti da non sottovalutare. Le informazioni che si possono reperire *online* possono riguardare sia i **caratteri personali**, sia le **abitudini sociali** e i **gusti commerciali**. Questi due tipi di informazioni, elaborate tra loro, formano il **profilo-utente**.

La **pubblicità comportamentale**, fondata sul tracciamento delle informazioni rilasciate dagli utenti nel corso della navigazione in Internet, di per sé **non è vietata**, ma quando si inseriscono dati personali su un sito di social network si

[1] **Identità digitale** È l'insieme dei dati e delle informazioni che individuano un utente che interagisce con un sistema informatico.

perde il controllo degli stessi; i dati possono essere registrati da tutti i propri contatti e dai componenti dei gruppi cui si è aderito, rielaborati, diffusi, anche a distanza di anni. Spesso, inoltre, gli utenti più giovani non hanno a disposizione né gli strumenti necessari per capire quanto possano essere potenti le tracce digitali che lasciano, né quanto danno potrebbero causare, né tantomeno sanno quali dati vengono raccolti e da chi.

Per comprendere i rischi, occorre aver consapevolezza che tutti i dati presenti nella Rete sono in mano a **due tipologie di entità** e, più precisamente: chi riceve i dati degli utenti (ad esempio ►**Facebook**, **Tik Tok** e **Google**[2]) e chi, partendo da dati grezzi, genera informazioni (ad esempio compagnie che producono giochi o applicazioni). Questi soggetti sono di fatto aziende che cercano di estrarre quante più informazioni possibili dai dati al fine di venderle a terzi, molte volte all'insaputa dell'utente. **Questo meccanismo**, nelle mani sbagliate, **può portare anche a manipolare o polarizzare opinioni**.

Proteggere i dati personali degli utenti da utilizzi illeciti o che vadano a **violare la privacy** degli stessi è fondamentale. Il dato personale rappresenta lo strumento attraverso il quale i legislatori, nazionali e comunitari, tutelano l'insieme dei diritti collegati all'identità personale.

►**Dato personale**[3] **è qualsiasi informazione riguardante una persona fisica identificata o identificabile**, anche indirettamente, mediante informazioni

[2] **Facebook** e **Tik Tok** sono social media a scopo commerciale. Ogni volta che un utente vi accede, il sistema recupera e considera, dapprima, tutte le attività svolte (notizie cercate, foto pubblicate); successivamente, sulla base di alcuni "segnali" registrati (orario, luogo di accesso, dispositivo, tipologia di contenuto, commenti, reazioni suscitate, ecc.), l'**algoritmo** fa delle previsioni d'interesse personalizzate per ogni utente dando ad ognuna un punteggio di rilevanza: saranno queste, in base ai punti ottenuti, i contenuti mostrati prioritariamente nella "Home" dell'utente.
Anche **Google** memorizza tutto: conosce dove è stato l'utente, quello che ha cercato in Rete, ciò che ha cancellato e – sulla base di queste informazioni – ha un profilo pubblicitario di ognuno. I dati che Google ha su ogni utente sono infatti tantissimi (segnalibri, e-mail, contatti, file di Google Drive, video di YouTube, foto sul telefono, prodotti acquistati, dati del calendario, siti web creati, pagine condivise, quanti passi vengono fatti in un giorno).

[3] Il **diritto alla protezione dei dati personali** è sancito da numerose norme internazionali, dell'Unione europea e dei singoli Stati membri dell'Unione. A livello europeo, dal maggio 2018 è entrato in vigore un Regolamento, noto come **GDPR** (*General Data Protection Regulation*), che chiarisce come debbano essere trattati i dati personali degli utenti, introducendo **regole più chiare su informativa e consenso** e definendo i **limiti al trattamento automatizzato dei dati personali**; esso – inoltre – fissa norme rigorose per i **casi di violazione dei dati**.

In Italia, in materia di **diritto alla riservatezza informatica** legato alla diffusione nel web dei dati personali degli utenti, la Corte costituzionale ha affermato l'esistenza di *«un vero e proprio diritto anche al di fuori delle ipotesi espressamente previste dalla legge ordinaria»* in considerazione delle disposizioni costituzionali degli articoli 15 (riservatezza e segretezza delle comunicazioni) e 21 (tutela della libertà di pensiero e di parola). Secondo la Corte, nella disposizione costituzionale dell'articolo

supplementari; in particolare: **dati anagrafici** (nome, indirizzo e-mail, in- dirizzo di residenza, ecc.); **finanziari** (codice fiscale, conto corrente, ecc.); **identificativi** (video, foto, ecc.); **sensibili** (informazioni su opinioni politi- che, religione, ecc.); **giudiziari** (processi, denunce, ecc.).

APPROFONDIMENTO

Nel marzo 2018, un'azienda di consulenza per il marketing *online* – la **Cambridge Analytica** – è stata al centro di un grosso scandalo per l'uso scorretto di un'enorme quantità di dati prelevati da *Facebook* durante la campagna presidenziale americana del 2016, che ha visto la vittoria di **Donald Trump**. L'accusa si è basata sull'uso scorretto delle informazioni raccolte dalla società: elaborate mediante algoritmi in grado di creare **profili psicometrici degli utenti** in termini di abilità, comportamenti e caratteristiche della personalità, oltre ad essere utilizzate per creare pubblicità altamente personalizzate su gusti ed emozioni degli utenti, sono servite anche a manipolare le preferenze degli elettori a favore di Trump, grazie alla diffusione di post e notizie false contro la candidata Hillary Clinton.

Un'accusa simile è stata mossa alla stessa società in merito all'uso dei dati degli utenti per favorire l'uscita del Regno Unito dalla Unione Europea, in occasione del referendum del 2016.

15 *«trovano protezione due distinti interessi: quello inerente alla libertà e alla segretezza delle comunicazioni riconosciuto come connaturale ai diritti della personalità definiti inviolabili dall'articolo 2 della Carta costituzionale, e quello connesso all'esigenza di prevenire e reprimere reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale»*. Tale diritto ha trovato ampia tutela nella legge 675 del 1996, confluita poi nel **Codice della Privacy**.

3 Proteggersi dalle insidie dei Social

Usare i social può essere utile e divertente, ma *online* si possono celare delle insidie. In Rete, gli imbrogli più frequenti possono nascondersi nei messaggi privati (►**phishing**[4]). L'obiettivo di queste **frodi**, raggiri finalizzati al conseguimento di illeciti profitti, è **rubare dati personali** e quindi estorcere dei soldi con l'inganno.

Tra i principali rischi, anche la ►**cyberdipendenza**[5], espressione coniata dal medico Ivan Goldberg nel 1995 che descrive il **disturbo legato ad utilizzo intensivo e ossessivo del web**.

APPROFONDIMENTO

La nostra vita privata e pubblica è indubbiamente mutata con l'avvento di Internet, tanto che il numero delle famiglie italiane che possono accedere ad Internet dalla propria abitazione è in costante aumento (secondo recenti stime l'89% accede al web da casa).

L'utilizzo di Internet coincide però soprattutto con quello dei social network da parte dei giovani (*Facebook*, *Instagram*, *Tik Tok*, *YouTube* e *Twitch*). Secondo una ricerca del 2020 dell'Associazione nazionale sulle dipendenze tecnologiche, *DiTe*, **il 51% dei giovani tra i 15 e i 20 anni controlla mediamente lo smartphone 75 volte al giorno**. Non solo: il 7% lo fa fino a 110 volte. Il 79% di essi ammette di non riuscire a starne alla larga per almeno 3 ore. Il bisogno di inviare messaggi e chattare si sente anche di notte. Il 13% degli intervistati (23.000 giovani tra gli 11 e i 26 anni) trascorrono *online* **più di 10 ore al giorno**, con un costo sulla vita di relazione e sulla salute.

[4] **Phishing** È una truffa effettuata *online*, che prevede l'invio di messaggi o e-mail che imitano per aspetto o contenuto le comunicazioni ufficiali di forniture di servizi per richiedere informazioni riservate (dati finanziari, codici di accesso, ecc.).

[5] **Cyberdipendenza** Si parla di dipendenza (e non di sola abitudine) quando l'alterazione del comportamento è accompagnata da sintomi quali disturbi del sonno, aggressività, deconcentrazione, difficoltà a relazionarsi, isolamento, depressione, ansia, instabilità emotiva. La dipendenza da Internet ha varie sfumature. Una è la **nomofobia**, che indica la **paura incontrollata di essere disconnessi** e non poter, dunque, chattare con amici e parenti. La nomofobia, così come gli altri disturbi legati alla Rete, tende a minare non poco la vita di relazione; nel corso degli ultimi anni, anche in Italia è esploso il fenomeno dei *ritirati sociali*, espressione che traduce il termine giapponese **hikikomori** usato per indicare gli adolescenti che respingono il contatto con gli altri preferendo vivere isolati nelle loro camere.

Offendere un soggetto ritenuto più debole e incapace di difendersi è l'espressione caratterizzante ogni fenomeno di **bullismo** che, se attuato *online* diventa ►**cyberbullismo**[6]. Le principali categorie del cyberbullismo sono: il **flaming** (messaggi *online* violenti e volgari); le **molestie** (insulti gratuiti), la **denigrazione**, l'**esclusione**, il **doxing** (diffusione pubblica di dati personali e sensibili) e le **minacce di morte**. A queste categorie si aggiungono anche il ►***cyberstalking***[7] e il ►***revenge porn***[8].

4 Guida pratica contro le molestie online

Le molestie *online* sono in aumento. La forma di tutela più efficace è sicuramente l'**autotutela**, cioè la gestione attenta dei propri dati personali. Di seguito alcuni consigli utili:

1. **Conoscere il mezzo**. I social network sono un potente strumento per la comunicazione. È importante imparare come utilizzarli, tenendo bene gli occhi aperti per sfruttare al meglio ciò che offrono. Controllare sempre le **impostazioni della privacy** di ogni piattaforma e, se possibile, rafforzarle.

2. **Mantenere privata la propria vita**. Evitare di diffondere sui social network informazioni personali, come l'indirizzo di casa o la scuola frequentata. Parlare con i propri amici di come gestire le foto e i video in cui si è ritratti, dicendo loro di chiedere il permesso prima di postare immagini. Evitare l'**oversharing**, ovvero l'abitudine di postare e di condividere tutto ciò che capita; limitare questo atteggiamento fa calare rischi e conseguenze indesiderate.

[6] Il **cyberbullismo**, all'art. 1 comma 2 della legge n. 71 del 2017, è stato definito 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 online 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»*.

[7] **Cyberstalking** Persecuzione *online* incessante che punta a spaventare la vittima con minacce, anche di violenza fisica. Il cyberstalker, inoltre, può diffondere materiale riservato in suo possesso (fotografie sessualmente esplicite, video intimi, manoscritti personali) in Rete. Le persecuzioni possono avvenire attraverso un accesso illegale ai dispositivi elettronici delle vittime, ad esempio con invio di e-mail contenenti codici malevoli o mediante il *bluetooth*, per installare **software spyware** il cui scopo è raccogliere informazioni al fine di controllare il registro delle chiamate, la lettura dei messaggi o l'agenda.

[8] **Revenge Porn** Condivisione pubblica tramite il web di immagini intime esplicite, senza alcun consenso del protagonista delle stesse.

3. **Proteggere le comunicazioni** mediante la **crittografia**, l'**access control** e la creazione di **password complesse**, contenenti maiuscole, minuscole, numero e simboli. Le password non vanno mai rivelate.

4. **Oscurare la posizione**. Rimuovere i dati sulla posizione da immagini e video prima di pubblicare. Disattivare sempre la geolocalizzazione dalle foto e non rivelare la propria posizione nei post pubblici.

5. **Rispettare gli amici virtuali come gli amici reali**. Se si è vittime di fenomeni di cyberbullismo, non cancellare le prove di cui si dispone. Bloccare gli aggressori e, se possibile, segnalare il profilo agli amministratori del social network utilizzato. Se qualcuno o qualcosa compie un atteggiamento illecito, fare una **segnalazione ai servizi competenti**, preferibilmente facendosi affiancare da un adulto.

6. **Evitare di postare immagini personali e intime**. È importante ricordare che si può essere facilmente registrati o fotografati se si usa la webcam in modo inappropriato: un'immagine imbarazzante può essere impiegata nelle modalità più disparate.

7. **Proteggere gli altri**. Se si leggono commenti negli account personali di altri utenti, impedire che vengano pubblicati messaggi offensivi. Segnalare i trasgressori e le informazioni personali che sono state pubblicate per ferire qualcuno.

8. **Inserire periodicamente il proprio nome sui principali motori di ricerca e guardare i risultati**: se qualcosa infastidisce, è necessario cercare di eliminarlo. Chiudere un account o eliminare un profilo da un social network è una procedura a volte complessa ma fattibile.

9. **Se si naviga troppo a lungo**, spegnere il computer o il cellulare e svolgere un'altra attività.