DECALOGO
PER UN USO CONSAPEVOLE DEI SOCIAL

CNF Consiglio Nazionale Forense — FAI Fondazione dell'Avvocatura Italiana — IL DUBBIO

1 LOCALIZZAZIONE E METADATI

Quando le impostazioni di geolocalizzazione sono attive, vengono sempre registrate tutte le informazioni precise sul luogo in cui viene scattata una foto. Questi dati possono essere accessibili se i metadati non vengono eliminati prima di pubblicare l'immagine online. Nel mondo digitale, la localizzazione e i metadati rappresentano due aspetti fondamentali della gestione delle informazioni. La loro raccolta, conservazione e utilizzo sollevano importanti questioni legali, soprattutto in materia di privacy, sicurezza e responsabilità. La localizzazione si riferisce alla raccolta e all'uso di dati relativi alla posizione geografica di un individuo o di un dispositivo che può avvenire attraverso:

- GPS (Global Positioning System);
- Reti Wi-Fi e indirizzi IP;
- Torri di telecomunicazione (triangolazione cellulare);
- Sensori Bluetooth e RFID.

Rischi:

- Uso improprio dei dati da parte di terzi (furto di identità e pericolo che le foto finiscano sui siti pornografici) Adescamento online Cyberbullismo Frodi
- Profilazione eccessiva da parte di aziende.

Ogni immagine può rimanere online per sempre e finire nelle mani sbagliate.

I metadati sono informazioni strutturate che descrivono altre informazioni, spesso utilizzate per catalogare, gestire o analizzare contenuti digitali. Esempi comuni includono:

- Metadati di file: data di creazione, autore, dispositivo utilizzato;
- Metadati delle comunicazioni: orario, destinatario, posizione di una chiamata o di un messaggio;
- Metadati web: indirizzi IP, cookie, preferenze utente.

Rischi:

- Tracciamento non autorizzato delle attività online;
- Possibile utilizzo in procedimenti giudiziari (es. prove digitali);
- Responsabilità per conservazione e protezione dei dati.

2 CONFINI PERSONALI E ACCORDO

Alcuni genitori sono disposti a condividere molte informazioni sui propri figli online, mentre altri preferiscono non condividere nulla. Ogni famiglia è diversa, ed è per questo che è fondamentale stabilire confini personali e comunicarli agli altri.

Suggerimento: Questo può essere integrato negli accordi tra i genitori, su nostro suggerimento.

Modalità: inserire negli accordi una clausola del seguente tenore "Le parti concordano che la privacy e la sicurezza dei propri figli costituiscono per entrambi aspetti di massima importanza. Pertanto, si impegnano a non pubblicare, condividere o divulgare immagini, video o informazioni personali dei figli sui social media o su altre piattaforme online senza il consenso reciproco e quello dei figli in grado di discernimento. Qualora una delle parti desideri condividere contenuti che includono i figli, dovrà informare l'altra parte e ottenere il consenso scritto prima della pubblicazione. In caso di disaccordo, le parti si impegnano a discutere la questione in modo costruttivo e a trovare una soluzione che rispetti il benessere dei figli, comunque impegnandosi a non pubblicare nulla in difetto di accordo..
Laddove le parti intendessero aprire di comune accordo un account social ai figli minori che questo sia privato e monitorato dai genitori".

3 CONTROLLO PERSONALE

I genitori potrebbero essere agevolati da una check list al fine di comprendere se sia opportuno o meno pubblicare online fotografie e/o informazioni riguardo ai propri figli.

Occorre riflettere su: a) Le motivazioni che portano a voler condividere un contenuto (fermarsi e riflettere!); b) Come potrebbero sentirsi gli altri (incluso il bambino) se l'informazione diventasse pubblica; c) Se è stato ottenuto il permesso per la pubblicazione; d) Se sono state prese sufficienti precauzioni per garantire la sicurezza del bambino.

Suggerimento: collegare questa idea al concetto di confini personali, spiegando che è un valido consiglio per i genitori.

4 PERMESSO E RISPETTO

I bambini ci osservano e ci prendono ad esempio. Diventa quindi essenziale che i genitori utilizzino i social media con rispetto posto che tale modalità diviene una lezione preziosa per bambini e ragazzi.

Suggerimento: gli avvocati possono sensibilizzare i genitori, dentro e fuori dal conflitto familiare, sull'importanza di mantenere un approccio pacato e rispettoso anche negli scambi che avvengono sui social.

5 PIATTAFORME DI CONDIVISIONE PRIVATA

Una volta che le fotografie vengono condivise online, controllare chi può accedere a quelle immagini o come vengono utilizzate diventa impossibile. Esistono tuttavia piattaforme di condivisione privata, come Google Foto o Storypark, che potrebbero costituire una buona alternativa per alcune famiglie.

Suggerimento: consigliare queste opzioni come alternativa sicura alla condivisione pubblica.

6 CONDIVISIONE ANONIMA

I genitori condividono informazioni online per vari motivi. Prima di pubblicare qualsiasi contenuto, può essere utile considerare se le informazioni sensibili possano essere condivise in forma anonima per proteggere la privacy del bambino.

Suggerimento: includere questa raccomandazione nel discorso generale sulla protezione dei dati personali.

7 PREFERENZA PER I SOCIAL MEDIA

A volte, persone diverse dai genitori condividono immagini o informazioni sui bambini online.
Questo può diventare complicato se le parti hanno opinioni diverse su cosa sia appropriato condividere.

Suggerimento: stabilire confini personali, avere strategie per gestire post non autorizzati e verificare sempre con gli altri genitori prima di pubblicare contenuti che riguardano i loro figli.

8 IMPOSTAZIONI SULLA PRIVACY

Le piattaforme social evolvono continuamente. Gli esperti raccomandano di rivedere regolarmente le impostazioni sulla privacy degli account e di aggiornarle quando necessario.

Suggerimento: è fondamentale insegnare ai genitori come navigare tra queste impostazioni per proteggere le informazioni personali.

Modalità: impostare profilo privato e protetto

9 ALERT

I genitori possono sentirsi ansiosi riguardo al tipo di informazioni disponibili online sui propri figli. Creare un messaggio di allerta che invii una notifica ogni volta che il nome del figlio viene menzionato sul web può offrire maggiore tranquillità.

Modalità: impostare idoneo Alert nel telefonino

10 SUPPORTO

Ottenere aiuto immediato può essere complicato. I social media generalmente rimuovono solo immagini che violano i loro termini di servizio. La polizia può intervenire solo in caso di reato e la Polizia Ufficio del Commissario per la sicurezza online può agire solo in alcune situazioni di cyberbullismo. Attivare sempre il parental control che permette il monitoraggio e l'eventuale blocco a determinati siti/social.

Suggerimento: il miglior approccio rimane stabilire confini personali chiari e comunicarli fermamente agli altri.

Modalità: fare riferimento al sito del Garante privacy che prevede tutte le modalità di segnalazione.

- Leggere sempre con attenzione le informative privacy;
- Impostare i profili come privato; usare password forti;
- Evitare wi fi pubblici;
- Aggiornare sempre i software di sicurezza;
- Disattivare la localizzazione quando non necessaria;
- Controllare i permessi delle app sullo smartphone;
- Leggere accuratamente le informazioni ed il contratto al momento di scaricare una app;
- Usare vpn e strumenti di protezione per ridurre la raccolta di metadati.

MODALITÀ SUI SOCIAL

FACEBOOK

1. **Disattivare la localizzazione:**
- Vai su Impostazioni e privacy > Impostazioni > Posizione.
- Disattiva l'opzione Servizi di localizzazione.

2. **Limitare i dati sensibili:**
- Accedi a Impostazioni sulla privacy e seleziona chi può vedere i post e le informazioni personali.
- Rimuovi eventuali informazioni sensibili dal profilo (es. indirizzo, numero di telefono).

INSTAGRAM

Una volta che le fotografie vengono condivise online, controllare chi può accedere a quelle immagini o come vengono utilizzate diventa impossibile. Esistono tuttavia piattaforme di condivisione privata, come Google Foto o Storypark, che potrebbero costituire una buona alternativa per alcune famiglie.

Suggerimento: consigliare queste opzioni come alternativa sicura alla condivisione pubblica.

X

1. **Disattivare la localizzazione:**
- Vai su Impostazioni e privacy>Privacy e sicurezza > Informazioni sulla posizione.
- Disattiva l'opzione Aggiungi posizione ai Tweet.

2. **Limitare i dati sensibili**: - Controlla chi può vedere i tuoi Tweet e disattiva la geolocalizzazione nei post.

TIKTOK

1. **Disattivare la localizzazione**:
- Vai su Impostazioni > Privacy>Autorizzazioni app e disattiva l'accesso alla posizione.

2. **Proteggere i dati:**
- Imposta l'account come privato e limita chi può inviarti messaggi o commentare i tuoi video.

CONSIGLI GENERALI

Disattivare il GPS del dispositivo:
Vai su Impostazioni>Posizione e disattiva il GPS per tutte le app non necessarie.

ATTIVARE PARENTAL CONTROL