



# GPDP

**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

## Dating online e protezione dei dati

# Quando insegui Cupido online, fai attenzione alla privacy! Dating online e protezione dei dati

**Vuoi usare o già usi siti o applicazioni per cercare la tua “anima gemella” online? Hai pensato alla tua privacy?**

**Sei consapevole che, per quanto utili, i servizi di dating on line possono raccogliere, trattare ed eventualmente diffondere varie informazioni che ti riguardano, anche di carattere molto sensibile? Parliamo ad esempio delle tue abitudini sociali, di alcuni aspetti molto privati del tuo vissuto emotivo e caratteriale, dei tuoi orientamenti sessuali, della tua rete di relazioni e della natura di tali relazioni, compresi, quindi, eventuali tradimenti...**

**Ecco allora le accortezze che è bene considerare se vuoi proteggere la tua riservatezza e i tuoi dati personali quando usi strumenti per il dating online.**

- **Leggi sempre con grande attenzione l’informativa sul trattamento dei dati personali.** In particolare, cerca di capire quanti e quali dati verranno raccolti, chi tratterà i tuoi dati personali e con quali finalità, per quanto tempo verranno conservati i dati personali che ti riguardano e se possono essere condivisi con terze parti per finalità commerciali o di altro tipo.
- **Al momento dell’iscrizione, fornisci solo i dati indispensabili per fruire del servizio.** Controlla le impostazioni privacy ed eventualmente disattiva ogni strumento di raccolta di informazioni non essenziali per utilizzare il servizio. Laddove possibile e nel caso non sia indispensabile, **limita o blocca la possibilità che la app di dating acceda alla memoria o ad alcune funzionalità (microfono, camera, ecc.) del tuo smartphone.** Disattiva l’accesso ai dati di **geolocalizzazione** del tuo smartphone se non è assolutamente necessario per fruire del servizio.
- **Evita in generale di fornire troppe informazioni, specie se queste riguardano aspetti molto privati** (pensieri, emozioni, stato di salute, abitudini sessuali, relazioni intime, ecc.),

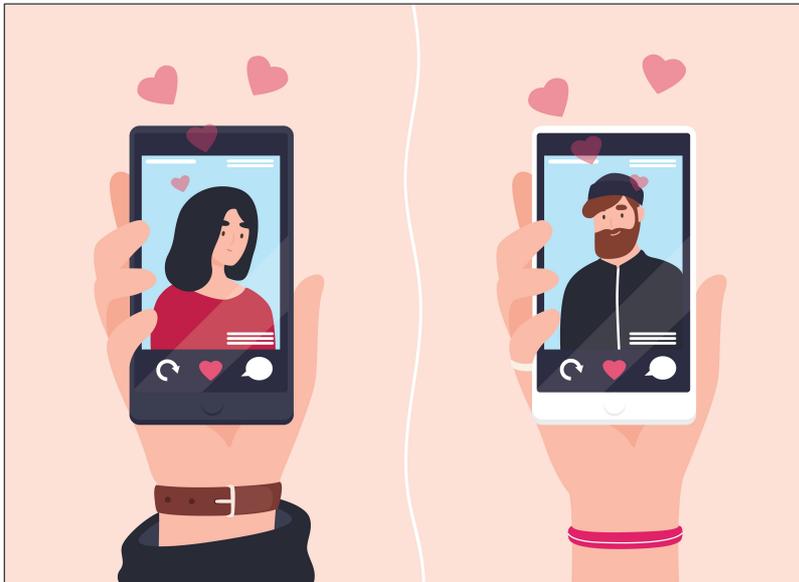
perché potrebbero essere utilizzate per scopi di profilazione e con finalità che potrebbero non essere trasparenti. I rischi che dati riguardanti aspetti così personali siano utilizzati per scopi non chiari (o addirittura illeciti) diventano più elevati se, come capita ormai spesso, il servizio di dating online integra sistemi di intelligenza artificiale, il cui funzionamento può non rispondere ai comuni parametri etici e può addirittura situarsi in "zone grigie", ancora non completamente regolamentate dalla legge.

Laddove possibile, e nel caso non sia indispensabile per accedere a determinate funzioni, limita o blocca la possibilità che l'app o il sito di dating online acceda alla memoria o ad alcune funzionalità (microfono, camera, ecc.) del dispositivo.

Disattiva l'accesso ai dati di geolocalizzazione del tuo dispositivo se non è assolutamente necessario per fruire del servizio.

• **Considera la possibilità di interagire inizialmente con gli altri utenti tramite un nick name o pseudonimo** e di iscriverti non utilizzando la tua e-mail abituale, ma creandone una ad hoc, che magari non contenga riferimenti al tuo nome e cognome. In questo modo, sarai più protetto in caso di eventuali diffusioni - anche involontarie o accidentali - di dati che ti riguardano e potrai anche assicurarti di non poter essere rintracciato "fuori" dai servizi di dating online da utenti con cui non vuoi interagire.

Per le stesse ragioni – e anche per evitare che la app o il sito di dating abbiano eventualmente accesso a ulteriori informazioni che ti riguardano - anche se può sembrare più facile e rapido, **evita di iscriverti tramite l'accesso ai tuoi profili social o ad altri servizi online** (motori di ricerca, repository musicali, ecc.).



- **Rifletti sulla pubblicazione della tua foto nel profilo.** Vuoi davvero essere facilmente riconoscibile da tutti? Sai che scaricando e inserendo la tua foto in un motore di ricerca è possibile accedere a numerose informazioni che ti riguardano? Laddove possibile, decidi eventualmente di rendere la foto del tuo profilo accessibile **solo** agli utenti che autorizzi o a quelli con cui accetti di interagire.

**Valuta con attenzione se è opportuno caricare foto o video personali sulla app o sul sito di dating e, ancora di più, se è sicuro condividerle in privato: una volta pubblicate o diffuse ne perderai il controllo.** Ricorda che diffondere immagini personali, specie quelle con contenuto sessuale più o meno esplicito, espone al rischio di cadere vittima di fenomeni molto pericolosi, come la **sextortion** (il ricatto sessuale online), il **revenge porn** (cioè la diffusione di immagini compromettenti a scopo di diffamazione e vendetta) o il **deep nude** (la creazione di video falsi in cui soggetti con il tuo viso compiono atti sessuali espliciti).

In particolare è sempre bene:

- verificare che nell'informativa siano ben illustrati dal fornitore dei servizi di dating online tutti i possibili utilizzi delle immagini che si mettono a disposizione;
- ricordare che i volti sono collegati a dati di natura molto delicata - come i dati biometrici ad esempio - che potrebbero anche essere utilizzati da malintenzionati per finalità illecite (basti pensare, ad esempio, al fatto che i dati biometrici del volto sono già oggi utilizzati come password per l'accesso agli smartphone, ecc.) o ceduti a terzi per finalità ignote.
- In generale, è bene **evitare di memorizzare su siti o app dati come le coordinate di accesso di carte di credito e sistemi di pagamento.** Vale ovviamente anche per i servizi di dating online.
- **Non fornire a sconosciuti informazioni troppo personali e cerca sempre di essere prudente.** Ad esempio, alcuni utenti con cui interagisci potrebbero fare **screenshot** delle conversazioni, mantenendo accesso alle informazioni che comunichi loro anche nel caso tu decida di cancellare la chat: pondera quindi sempre con attenzione quello che scrivi e che riveli di te. Un rischio molto insidioso e in forte crescita è il cosiddetto **catfishing**. Il termine descrive un'attività malevola basata sulla simulazione di una falsa identità, che in alcuni casi può essere finalizzata a raccogliere informazioni e dati utilizzati poi per ricattare o molestare gli altri utenti, o addirittura per realizzare truffe e attività illecite. Quando si usano piattaforme di dating online si può avere una maggiore voglia di esporsi ed entrare in confidenza, e quindi purtroppo può diventare più facilmente vittima di questi fenomeni.

- **Se possibile, cancella periodicamente i dati raccolti dal sito o dalla app.** Nel caso in cui decidessi di non usare più il servizio di dating online, disattiva l'account personale e informati su come ottenere la cancellazione di tutti i dati ad esso collegati.
- Per utilizzare servizi ed app di dating online con maggiore sicurezza, puoi adottare alcune semplici accortezze di base, sempre valide nell'utilizzo di strumenti tecnologici, come impostare **password** di accesso complesse e sicure, ricordandoti di cambiarle spesso, e aggiornare periodicamente le app alle **nuove versioni**, che contengono di solito anche miglioramenti sul fronte della sicurezza. Se prevista dal servizio, attiva una autenticazione di accesso a più fattori. Per approfondire il tema: [www.gdpd.it/temi/cybersecurity](http://www.gdpd.it/temi/cybersecurity)
- **E' importante evitare che i minori utilizzino app o siti per il dating**, perché non sono a loro dedicati, ma soprattutto perché, in generale, i più giovani sono maggiormente esposti al rischio di finire vittime di malintenzionati o di diffondere inconsapevolmente dati sensibili, informazioni sul conto bancario o la carta di credito, ecc.. Si ricorda, a tal proposito, che in Italia il Codice privacy stabilisce inoltre che **solo a partire dai 14 anni** un minore può esprimere autonomamente il consenso al trattamento dei propri dati personali, anche da parte di servizi digitali. Per i minori di 14 anni è infatti necessario il consenso di chi esercita la responsabilità genitoriale. **Se i servizi di dating sono utilizzati su un dispositivo** (smartphone, tablet, pc) **usato da tutta la famiglia**, è bene impostare limitazioni d'uso o profili con impostazioni d'uso limitate, in modo che certe applicazioni **non siano accessibili ai minori**.