GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# SOCIAL PRIVACY

## COME TUTELARSI NELL'ERA DEI SOCIAL MEDIA

# INDICE


PREMESSA ..... 3
DA FACEBOOK A TIKTOK ..... 4
MINORI E PROTEZIONE DATI ..... 6
L'ATTIVITÀ DEL GARANTE ..... 7
UN BREVE DIZIONARIO ..... 9
AVVISI AI NAVIGANTI ..... 11
15 CONSIGLI ..... 16
TI SEI MAI CHIESTO? ..... 24
PILLOLE DI PROTEZIONE DATI ..... 28

# PREMESSA

La tecnologia e il mondo delle reti sociali sono in costante evoluzione e il Garante per la protezione dei dati personali ne segue con attenzione gli sviluppi, allo scopo di tutelare i diritti e le libertà di giovani e adulti.
I social network sono il luogo in cui non esistono barriere tra la vita digitale e quella reale: quello che succede online ha sempre più spesso impatto fuori da Internet, nel quotidiano e nei rapporti con gli altri.
I social offrono vantaggi significativi e immediati: semplificano i contatti, rendono possibili scambi di informazioni con un numero enorme di persone, permettono di esprimere idee, passioni o talenti, ma amplificano allo stesso tempo i rischi di un utilizzo improprio o fraudolento dei dati personali degli utenti, esponendoli a furti di identità, a veri e propri abusi, a danni della reputazione, a informazioni non verificate o vere e proprie fake news.
Proprio con l'obiettivo di aumentare la consapevolezza dei giovani, e degli adulti, e offrire loro ulteriori spunti di riflessione e strumenti di tutela, il Garante ha aggiornato questa guida ai social media, pubblicata nel 2009 e rinnovata nel 2016, mantenendo la struttura agile che ne ha favorito in questi anni la diffusione e il facile utilizzo.

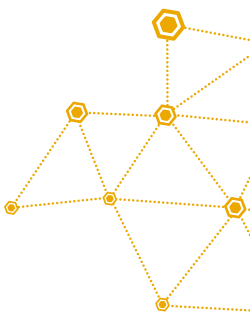
# DA FACEBOOK A TIKTOK

I social media sono “piazze digitali” in cui via Internet ci si ritrova condividendo con altri informazioni, fotografie, filmati, pensieri, indirizzi, conoscenze e tanto altro.
Facebook nasce in ambito universitario, come una bacheca telematica tra colleghi di corso che non si volevano “perdere di vista” e che desideravano ritrovarsi e scambiare informazioni, una volta entrati nel mondo del lavoro.
L’esigenza di condivisione ha trovato una risposta nella nascita di altre piattaforme, come quelle che permettono di comunicare con testi brevi (Twitter, ora X) o di esprimersi attraverso la pubblicazione di foto (Instagram) e video (sempre Instagram, poi Snapchat e TikTok), o di fare rete in ambito professionale (LinkedIn). Altre, come YouTube, si sono evolute, arrivando a proporre veri e propri palinsesti tv online, altre ancora appartengono già all’archeologia (MySpace).
Insieme alle modalità di espressione, i social network si stanno ormai distinguendo anche per i target, cioè il pubblico a cui si rivolgono: è infatti sempre più probabile, ad esempio, che su Facebook ci si ritrovino i genitori o i nonni, mentre i più giovani interagiscono coi loro coetanei su Instagram o TikTok.
Sebbene non si tratti di piattaforme, anche le app di messaggistica, che ci permettono di essere sempre in contatto e di scambiarci file, immagini e video, come WhatsApp o Telegram, sono considerati social media.

Ma com'è che queste piattaforme gratuite sono tra le aziende più ricche del mondo? I social si finanziano vendendo pubblicità mirate. Il valore di queste imprese è legato proprio alla capacità di analizzare nel dettaglio i profili degli utenti: le loro abitudini, gli interessi, la rete di contatti, le interazioni con i contenuti pubblicati dagli altri utenti etc..
In poche parole, i loro dati personali.
Tutto ciò al fine di prevedere i nostri comportamenti, le nostre scelte, i nostri prossimi acquisti.
Queste informazioni vengono poi vendute a chi sceglie di utilizzare i social per promuovere la propria attività, lanciare offerte commerciali, sostenere campagne di diverso genere, influenzare le opinioni degli utenti.
Sui social, e sul web in generale, dietro a un servizio gratuito si nasconde l'utilizzo e, talvolta, lo sfruttamento dei nostri dati.

# MINORI E PROTEZIONE DATI

Insieme a straordinarie opportunità di crescita e conoscenza, la rete presenta pericoli che si amplificano in misura esponenziale quanto più piccoli e tendenzialmente immaturi sono gli utenti delle piattaforme. Queste insidie vengono accresciute dalla scarsa consapevolezza che i minori hanno delle conseguenze di ogni loro “click”, ma anche dagli effetti che un uso improprio della loro immagine o l’esposizione a determinati contenuti può avere sulla formazione della personalità. È per questo che la normativa privacy accorda ai minori una tutela rafforzata. Il Regolamento europeo sulla protezione dati (GDPR) stabilisce infatti che il trattamento dei dati dei giovani con un'età inferiore ai 16 anni, nell’ambito dell’offerta di servizi della società dell’informazione, sia lecito soltanto se il consenso è prestato o autorizzato dai genitori o da chi esercita la responsabilità genitoriale. Ma il GDPR permette a ogni Stato membro dell’Unione di stabilire un'età inferiore per accedere ai servizi e agli strumenti offerti dalla rete, purché non sia inferiore ai 13 anni.
In Italia questo limite è stato fissato dalla legge a 14 anni.
La normativa prevede inoltre che le informazioni da fornire ai più giovani per spiegare se e come vengono trattati i dati personali siano scritte con un linguaggio particolarmente chiaro e semplice, conciso, facilmente accessibile e comprensibile, in modo che il minore sia realmente consapevole dell’utilizzo dei suoi dati.



# L'ATTIVITÀ DEL GARANTE

Il Garante per la protezione dei dati personali è un'Autorità indipendente, istituita per assicurare la tutela dei diritti e delle libertà fondamentali nel trattamento dei dati personali e il rispetto della dignità degli individui.
Il Garante attribuisce una rilevanza centrale alla tutela dei **minori** e attraverso provvedimenti, eventi e iniziative dedicate e la realizzazione di contenuti informativi, promuove un uso responsabile di Internet e delle nuove tecnologie. In questi ultimi anni l'Autorità ha rivolto un'attenzione particolare verso le piattaforme social.
L'attività del Garante si è concentrata in un primo momento sull'obiettivo di sensibilizzarle rispetto all'esigenza di adottare sistemi efficaci per la verifica dell'età, in modo da evitare l'indebito accesso dei più piccoli a 'giochi' troppo più grandi di loro, in pericolosa solitudine. Nel 2021, il Garante ha così ottenuto da TikTok l'eliminazione di oltre mezzo milione di profili di minori con meno di 13 anni, a seguito del provvedimento di blocco temporaneo della piattaforma.
La sempre più capillare diffusione dell'Intelligenza artificiale generativa ha poi indotto il Garante a monitorare i sistemi di verifica dell'età degli utenti utilizzati da alcuni social media di più recente creazione. È stato bloccato il sistema di intelligenza artificiale Replika, la cui carenza di sistemi adeguati di verifica dell'età era ancora più grave in ragione dei contenuti offerti agli utenti, molti dei quali

inadatti ai minori (compresi, in particolare, quelli sessualmente espliciti). Sono state poi prese alcune importanti misure nei confronti di ChatGPT, affinché si mettesse in regola con la normativa europea sulla privacy, e si dotasse, anch'essa, di sistemi adeguati di verifica dell'età.
Inoltre, il Garante rappresenta anche e soprattutto un presidio essenziale per ragazze e ragazzi vittime di un uso violento degli strumenti digitali.
È infatti possibile rivolgersi all'Autorità per la rimozione di contenuti relativi a episodi di cyberbullismo e revenge porn.

**REVENGE PORN**
Nel caso in cui tu abbia un fondato timore che immagini a contenuto sessualmente esplicito possano essere diffuse senza il tuo consenso è possibile presentare una segnalazione al Garante Privacy:
**www.gpdp.it/revengeporn**

**CYBERBULLISMO**
I minori possono chiedere l'oscuramento, la rimozione o il blocco di contenuti, a loro riferiti e diffusi per via telematica, che ritengono essere atti di cyberbullismo, rivolgendosi al Garante Privacy:
**www.gpdp.it/cyberbullismo**

# UN BREVE DIZIONARIO

**Challenge (Sfide social)**
Azioni sconsiderate che giovani e adolescenti compiono per il brivido del rischio e condividono sui social.

**Cyberbullismo**
Con il termine «cyberbullismo» si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali realizzati, per via telematica, a danno di minori.

**Deepfake**
I deepfake sono foto, video e audio creati mediante software di intelligenza artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

**Deep nude**
Si tratta di una particolare tipologia di deepfake, in cui persone ignare possono essere rappresentate nude, in situazioni compromettenti o addirittura in contesti pornografici, grazie all'utilizzo di specifici software. Questi contenuti si prestano inoltre alla pratica del **revenge porn**.

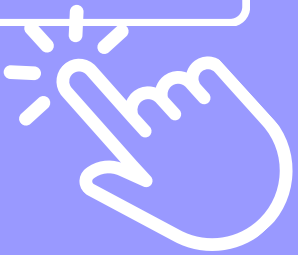
**Grooming**
Adescamento di un minore in Internet tramite tecniche di manipolazione psicologica volte a superarne le resistenze e a ottenerne la fiducia per abusarne sessualmente.

**Revenge porn**
Il revenge porn, consiste nell'invio, consegna, cessione, pubblicazione o diffusione di immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, da parte di chi li ha realizzati o sottratti e senza il consenso della persona cui si riferiscono.
Tale diffusione avviene di solito a scopo vendicativo, per denigrare pubblicamente, ricattare, bullizzare o molestare. Si tratta di una pratica che può avere effetti drammatici a livello psicologico, sociale e anche materiale sulla vita delle persone che ne sono vittime.

**Sexting**
Scambio di immagini di nudo, che a volte coinvolge anche soggetti minori.

**Sharenting**
Condivisione online costante da parte dei genitori di contenuti che riguardano i propri figli. Lo sharenting è un fenomeno all'attenzione del Garante per i rischi che comporta sull'identità digitale del minore e sulla formazione della sua personalità.

# AVVISI AI NAVIGANTI



## Vita digitale e vita reale

Vita online e vita offline si sovrappongono molto spesso. Quello che scriviamo e le immagini che pubblichiamo sui social hanno quasi sempre un riflesso diretto sulla nostra vita di tutti i giorni e nei rapporti con amici, familiari, compagni di classe, colleghi di lavoro. Ed è bene ricordare che l'effetto può non essere necessariamente immediato, ma ritardato nel tempo.

## Non è un Far West

Il web è spesso raccontato come un luogo senza regole dove ogni utente può dire o fare quello che vuole. In realtà, le regole ci sono e sono le stesse di civile convivenza, così come le norme che tutelano, ad esempio, dalla diffamazione, dalla violazione della tua dignità, dall'uso improprio dei dati personali, valgono nella vita reale come sui social network, in chat o sui blog.
Non esistono zone franche dalle leggi e dal buon senso.

## Per sempre o quasi

Quando inseriamo i nostri dati personali su un sito di social network, ne perdiamo il controllo. I dati possono essere registrati da tutti i nostri contatti e dai componenti dei gruppi di cui facciamo parte, rielaborati, diffusi, anche a distanza di anni.

## Il mito dell'anonimato

Non è poi così difficile risalire all'identità di coloro che pubblicano contenuti con l'intento di danneggiare l'immagine o la reputazione di un'altra persona. L'anonimato in rete può essere usato per necessità, ma mai per commettere reati: in questo caso le autorità competenti hanno molti strumenti per intervenire e scoprire il "colpevole".

## Non sono io!

Attenzione ai falsi profili. Basta la foto, il nome e qualche informazione sulla nostra vita per impadronirsi on line della nostra identità. Sono già molti i casi di attori, politici, personaggi pubblici, ma anche di gente comune, che hanno trovato su social network e blog la propria identità gestita da altri.

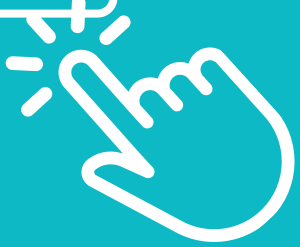
## Giocare e farsi male

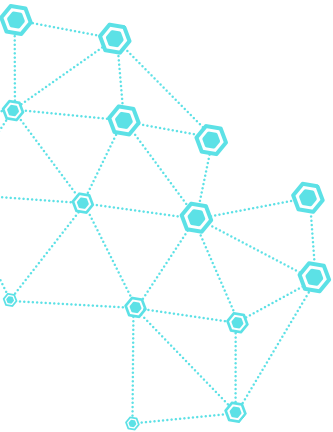
Molti giovani, ma non soltanto loro, pensano che l'adozione di alcuni piccoli stratagemmi, come l'invio di messaggi che si "autodistruggono" dopo la lettura, possano metterli al riparo dai rischi di un uso inappropriato del materiale che viene così condiviso. Questa falsa sicurezza può spingerci a scambiare, senza pensarci troppo, messaggi sessualmente espliciti **(sexting)**, insulti gratuiti o semplicemente inopportuni. Tutto quello che è condiviso, però, può sempre essere in qualche maniera salvato e riutilizzato.
Se stiamo giocando, attenzione a non farci male.

## Disattivazione o cancellazione?

Alcune piattaforme permettono di prendersi una pausa dai social disattivando l'account, o di allontanarsi definitivamente cancellando il proprio profilo.
Ogni piattaforma prevede percorsi specifici per procedere alla disattivazione o alla cancellazione degli account personali, ma è bene ricordare che determinate informazioni o contenuti potrebbero restare memorizzate nei loro sistemi informatici persino dopo la cancellazione del profilo. Per cui, leggiamo bene cosa prevedono le condizioni d'uso che si sono sottoposte al momento dell'iscrizione al servizio, e quali sono le garanzie offerte in tema di privacy.

# 15 CONSIGLI





## 1. Occhio alle impostazioni

Gli account sui social media dei minori tra i 14 e i 18 anni dovrebbero essere impostati automaticamente su "privato": in questo modo solo i nostri amici possono vedere cosa ci piace, quello che postiamo e i contenuti che condividiamo. Se, invece, il profilo social è impostato su "pubblico", chiunque può sapere ciò che facciamo. Meglio riflettere attentamente sulle eventuali conseguenze prima di disattivare i controlli sulla privacy.
Anzi, controlliamo periodicamente le impostazioni privacy del profilo: chi ci può contattare, chi può leggere quello che scriviamo, chi può inserire commenti alle nostre pagine, che diritti hanno gli utenti dei gruppi ai quali apparteniamo.
Limitiamo al massimo la disponibilità di informazioni, soprattutto per quanto riguarda la reperibilità dei dati da parte dei motori di ricerca.
Controlliamo quali diritti di accesso concediamo alle app installate sui nostri smartphone o tablet affinché non possano utilizzare dati personali (contatti, telefonate, foto...) senza il nostro consenso.

## 2. Pensaci bene

Qualunque siano le impostazioni che scegliamo, ricordiamo sempre che un contenuto, una volta pubblicato online, sarà difficile da rimuovere definitivamente dalla rete. Prima di pubblicare, chiediamoci se quelle parole, quella foto o quel video sono davvero ciò che vogliamo sia visto da tutti negli anni a venire.

## 3. Quindi, non fare agli altri...

Trattiamo i dati degli altri come tratteremmo i nostri. Se un amico o un conoscente ci chiede di cancellare una loro foto o un video, eliminiamola. Un giorno potremmo essere noi ad aver bisogno del suo aiuto.

## 4. Attenzione al "check-in"

Condividere la propria posizione online può essere rischioso.
Se non è proprio necessario segnalarsi in un posto, disattiviamo le impostazioni di localizzazione e rinunciamo a fare il check-in social.

## 5. A te la scelta

Alcune app e piattaforme utilizzano espedienti per indurci a fornire più informazioni di quelle effettivamente necessarie. Per esempio, ingrandiscono il pulsante che vogliono sia cliccato (o lo creano di un colore sgargiante), mentre "nascondono" quello che indica la scelta più utile per noi, rimpicciolendolo o non mettendolo in evidenza. Facciamo attenzione a questi trucchi (si chiama "design ingannevole"), mettiamo da parte la fretta e prendiamoci il tempo necessario a comprendere le conseguenze di un clic. Scegliamo l'opzione che ci fa sentire a nostro agio e non la scorciatoia.

## 6. Leggi l'informativa e i termini e le condizioni di utilizzo. O almeno provaci!

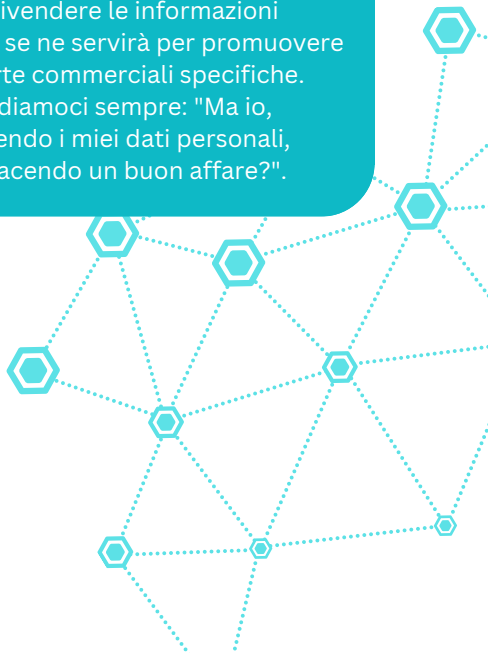
Le aziende sono obbligate a informarci su cosa faranno dei nostri dati personali. Quando sono rivolte ai minori, queste informazioni devono essere scritte con un linguaggio particolarmente chiaro e semplice, conciso ed esaustivo; devono essere facili da trovare e comprensibili.
E, in caso di dubbi, facciamoci sempre aiutare da un genitore o da un adulto fidato.

## 7. Sicuro di “accettare tutto”?

La prossima volta che compare sullo schermo un avviso privacy o un banner cookie, diamo un’occhiata alle impostazioni e non clicchiamo subito su "accetta tutto". I cookie sono piccoli file che i siti da noi navigati rilasciano sui nostri dispositivi, sia per consentire un miglior funzionamento dei siti, sia per tenere traccia dei nostri comportamenti a fini pubblicitari. Per legge, siti e app devono offrire la scelta di rifiutare i cookie non necessari o essenziali. Ci vuole qualche secondo in più, ma in questo modo possiamo scegliere di non condividere più informazioni di quante pensiamo e vogliamo.

## 8. I miei dati valgono

I servizi "gratuiti" non sono quasi mai davvero gratuiti. Grazie ai dati personali che condividiamo online, le aziende guadagnano con la pubblicità. Il loro valore è legato alla capacità di analizzare il profilo degli utenti (abitudini, interessi, interazioni, contatti) per rivendere le informazioni a chi se ne servirà per promuovere offerte commerciali specifiche. Chiediamoci sempre: "Ma io, fornendo i miei dati personali, sto facendo un buon affare?".



## 9. Sei tu ad avere il controllo

Abbiamo tutti dei diritti quando si tratta dei nostri dati personali. Possiamo esercitarli presso le piattaforme online o le aziende, che sono tenute ad ascoltarci. Abbiamo diritto di chiedere una copia dei nostri dati in loro possesso o di cancellare i nostri profili social. Se non ci rispondono o la loro risposta non è soddisfacente, possiamo rivolgerci al Garante privacy.

## 10. I genitori sono qui apposta

Le aziende sono obbligate a informarci su cosa faranno dei nostri dati personali. Quando sono rivolte ai minori, queste informazioni devono essere scritte con un linguaggio particolarmente chiaro e semplice, conciso ed esaustivo; devono essere facili da trovare e comprensibili.
E, in caso di dubbi, facciamoci sempre aiutare da un genitore o da un adulto fidato.

## 11. Facciamo pulizia!

Se non utilizziamo più un profilo social, perché non ci interessa più o perché ci siamo trasferiti su un'altra piattaforma, chiudiamolo. Potrebbe essere violato e utilizzato per accedere agli altri nostri account, soprattutto se abbiamo impostato password deboli o facili da decifrare.

## 12. Non ci sono password per tutte le stagioni

Scegliamo password sufficientemente lunghe e complesse. Configuriamo l'autenticazione a due fattori, laddove possibile, per rendere la vita ancora più difficile ai malintenzionati.
È buona norma non basare le password su elementi ovvi che qualcuno potrebbe indovinare, come il nome del nostro gatto o quello della serie preferita.
Se possibile, impariamo a utilizzare un gestore di password, un sistema fatto apposta per aiutarci e a ricordarsele al posto nostro.

## 13. Se quel messaggio suona strano

Anche nel mondo digitale, non bisogna dare retta agli sconosciuti. E occhio anche ai messaggi sospetti che arrivano da amici e conoscenti: potrebbero essere una truffa di qualche tipo o contenere virus. Ricordiamoci di non aprirli, di non cliccare sui link o gli allegati e cancelliamo tutto. Nel dubbio che sia un messaggio affidabile, chiediamo conferma all'amico: se è sicuro, non esiterà a inviarcelo di nuovo.

## 14. Il Wi-Fi? Solo protetto

È importante fare molta attenzione quando ci si connette a un hotspot Wi-Fi pubblico. Infatti, se la rete Wi-Fi pubblica non è sufficientemente protetta, può nascondere insidie inaspettate: un pirata informatico che utilizza la stessa rete potrebbe provare a penetrare i nostri dispositivi e rubare i dati.
Per proteggersi, è sempre bene verificare che la connessione al sito web sia cifrata e che l'identità del sito sia autentica: ciò può essere fatto cliccando sull'apposita icona che compare generalmente alla sinistra dell'indirizzo stesso.

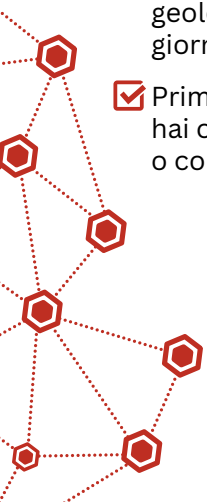
## 15. Teniamoci aggiornati

Non c'è peggior nemico del "Ricordamelo più tardi". Gli aggiornamenti di app e programmi contengono spesso importanti protezioni contro i virus e le truffe più recenti. Quando compare l'avviso di sicurezza, installiamo gli aggiornamenti prima possibile.

TI SEI MAI CHIESTO?

# SEI UN MINORE?

- ☑ Se sapessi che il vicino di casa o il tuo professore possono accedere al tuo profilo e al tuo diario online, scriveresti le stesse cose e nella stessa forma?
- ☑ Sei sicuro che le foto e le informazioni che pubblichi ti piaceranno anche tra qualche anno?
- ☑ Prima di postare la “foto ridicola” di un amico, ti sei chiesto se a te farebbe piacere trovarti nella stessa situazione?
- ☑ I membri dei gruppi ai quali sei iscritto possono leggere le informazioni riservate che posti sul tuo profilo?
- ☑ Vuoi veramente far sapere a chiunque dove ti trovi (si chiama geolocalizzazione) e chi stai incontrando in ogni momento della giornata?
- ☑ Prima di inviare, anche per gioco, un video sexy a un’altra persona, hai considerato che potrebbe essere condiviso con i suoi amici o con degli sconosciuti?



# SEI UN GENITORE?

- Tuo figlio o tua figlia sanno che non devono toccare il fornello acceso, li hai educati ad attraversare la strada e a “non accettare caramelle dagli sconosciuti”, ma hai insegnato loro a riconoscere i segnali di pericolo della rete?

- Hai ragionato con tuo figlio o con tua figlia su come difendersi dalle aggressioni di potenziali provocatori o molestatori online? Gli hai suggerito di non raccontare a tutti, anche a sconosciuti, particolari della vita privata e di quella degli amici?

- Hai mai provato a navigare insieme a tuoi figli? Hai chiesto loro di mostrarti come usano Internet e i social a cui sono iscritti?

- Provi mai a farti spiegare dai tuoi figli quali sono gli argomenti di discussione più interessanti sui social in quel momento?

- Conosci i vantaggi e gli svantaggi di comparire su un social network con la propria identità riconoscibile o in forma anonima? E ne hai discusso con i tuoi figli?

- Sei sicuro che sia così opportuno postare sui social foto dei tuoi figli fin dai primi giorni e per tutta la loro adolescenza? Ti sei mai chiesto come e da chi potrebbero essere usate quelle immagini? Sei sicuro che i tuoi figli un giorno saranno d’accordo ad avere momenti della loro vita online disponibili per chiunque?

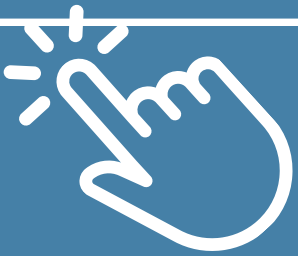
# SEI UN UTENTE CONSAPEVOLE?

- ☑ Da quanto tempo non verifichi le impostazioni privacy dei tuoi profili social?
- ☑ Hai controllato l'uso che le piattaforme social possono fare di contenuti, immagini e video che hai postato?
- ☑ Prima di installare una nuova app, hai verificato a quali dei tuoi dati personali il programma ti chiede di accedere? E per quale motivo?
- ☑ Il gruppo di persone con cui interagisci online corrisponde al target professionale che ti sei prefissato di raggiungere?
- ☑ Hai valutato se stai condividendo informazioni con qualcuno che può danneggiarti?
- ☑ Quando offri un servizio a un cliente, chiedi di essere retribuito per il tuo lavoro. Ti sei mai domandato come "paghi" un social network?

## E SE STAI CERCANDO UN LAVORO?

- Sai che le società di selezione del personale cercano informazioni sui candidati utilizzando i motori di ricerca o consultando i loro profili?
- Ti sei chiesto se un certo post o una foto sconveniente che hai pubblicato potrà danneggiarti nella ricerca del lavoro?

# PILLOLE DI PROTEZIONE DATI



## A COSA SI APPLICA LA NORMATIVA SULLA PROTEZIONE DEI DATI PERSONALI?

La normativa sulla protezione dei dati copre la maggior parte delle situazioni in cui le informazioni relative a qualcuno (“i dati personali" di una persona fisica, cioè “l’interessato") vengono utilizzate per un qualche scopo ("trattate") da un'altra persona o da un’organizzazione (il "titolare del trattamento").
La legge che si applica alla maggior parte dei tipi di trattamento di dati personali è il "Regolamento generale (UE) sulla protezione dei dati" (GDPR). Il GDPR è valido in Italia e in tutto lo Spazio economico europeo (SEE), mentre ulteriori norme sono stabilite a livello nazionale dal Codice per la protezione dei dati personali (dlgs 196/2003), noto anche come Codice della privacy.
Il GDPR non si applica al trattamento dei dati personali effettuato da parte di un individuo per finalità "puramente personali o domestiche", cioè senza alcun collegamento con un'attività professionale o commerciale. L’utilizzo della rubrica telefonica o dei propri contatti e-mail rientra ad esempio tra le attività personali.

Approfondiamo qualche concetto. Per dati personali si intendono tutte le informazioni relative a una persona fisica, quando questa è identificata, cioè quando è chiaro di chi si tratta, o quando potrebbe essere identificata, quando cioè si può conoscere la sua identità attraverso il contesto o l’utilizzo di ulteriori informazioni (questa persona è detta “interessato”).

**Alcuni esempi**

- “Marco gioca a calcio nella squadra del quartiere” **->** La persona è identificata.
- “La sorella di Marco gioca a calcio nella squadra del quartiere” **->** La persona è identificabile, perché sappiamo che è sorella di Marco e che gioca a calcio nella squadra del quartiere.

Sono dati personali, per esempio, il nome, la data di nascita, l'indirizzo e-mail, il numero di telefono, l'indirizzo di casa, le caratteristiche fisiche o i dati relativi alla posizione geografica di una persona in un determinato momento.
Ma i dati personali possono anche essere informazioni sull'aspetto di una persona, come una foto o registrazioni audio o video.
Esistono poi alcuni tipi di dati personali molto delicati:
le "categorie particolari di dati". Si tratta dei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale; i dati genetici;
i dati biometrici trattati per identificare in modo univoco una persona;
i dati relativi alla salute; i dati relativi alla vita sessuale o all'orientamento sessuale di una persona.
Le categorie particolari di dati sono soggette a una protezione aggiuntiva e il loro trattamento è generalmente vietato, tranne nei casi in cui siano soddisfatti requisiti specifici (come il consenso esplicito dell’interessato).

Abbiamo detto che la legge sulla protezione dei dati regola le situazioni in cui i dati personali vengono "trattati". Ma cosa intendiamo esattamente per “trattamento”?

> Il trattamento è sostanzialmente l'utilizzo che si fa dei dati personali, per esempio: la raccolta, l'archiviazione, il recupero, la consultazione, la divulgazione o la condivisione con altri, la modifica, la cancellazione o la distruzione.
> Come detto, se il trattamento viene effettuato per finalità puramente personali o domestiche, la legge sulla protezione dei dati non si applica.

## CHI È IL TITOLARE DEL TRATTAMENTO E CHE DOVERI HA?

Il titolare del trattamento è la persona, azienda o ente che decide come e perché trattare i dati personali dell'interessato.
Il titolare del trattamento ha una serie di obblighi e deve rispettare i principi di protezione dei dati, affinché i dati personali siano trattati:

- in modo lecito, corretto e trasparente;
- per finalità specifiche;
- limitatamente a quanto necessario;
- mantenendoli esatti e aggiornati;
- per un periodo non superiore a quello necessario;
- proteggendoli da trattamenti non autorizzati o illeciti, da perdita, distruzione o danneggiamento accidentali.

I titolari devono inoltre essere in grado di dimostrare in ogni momento il rispetto di questi principi (“responsabilizzazione”).
Inoltre, in base al principio di trasparenza, i titolari del trattamento devono fornire alcune informazioni agli interessati quando raccolgono i loro dati personali: identità e dati di contatto del titolare; dati di contatto del suo "responsabile della protezione dei dati" (RPD), se ne ha designato uno; le finalità e la "base giuridica" del trattamento; con chi saranno condivisi i dati; per quanto tempo saranno conservati i dati; i diritti dell'interessato e il diritto di fare reclamo al Garante per la protezione dei dati personali.

> Le informazioni fornite agli interessati devono essere trasparenti, comprensibili e facilmente accessibili, espresse con un linguaggio chiaro e semplice.

Le informazioni devono essere fornite per iscritto o con altri mezzi, compresi, se del caso, quelli elettronici.

## COSA SIGNIFICA BASE GIURIDICA DEL TRATTAMENTO?

Il trattamento è lecito se rispetta uno dei presupposti previsti dal Regolamento, le cosiddette “basi giuridiche”, che sono:

- il consenso;
- l’esecuzione di un contratto;
- l'adempimento di un obbligo legale a cui è sottoposto il titolare;
- la tutela di interessi vitali dell’interessato;
- l’esecuzione di un compito di interesse pubblico;
- il legittimo interesse del titolare (ma solo se il titolare dimostra
- che questo interesse prevale sui diritti dell'interessato).

Non esiste una gerarchia tra le basi giuridiche, né un'opzione preferenziale: i trattamenti di dati personali devono essere basati sulla base giuridica più appropriata nelle circostanze specifiche di quel trattamento.

Il "consenso" non è l'unica base giuridica per il trattamento dei dati personali e in molti casi neanche la più appropriata, ma è sicuramente la più nota.
Quando si utilizza il consenso, vi sono una serie di requisiti da rispettare, affinché costituisca una base giuridica valida per il trattamento: deve essere specifico, informato e inequivocabile e deve essere dato liberamente. In certi casi, se si trattano categorie particolari di dati, la legge prevede che il consenso sia “esplicito”, quindi deve risultare con certezza che l’interessato abbia dato il proprio consenso. Deve inoltre essere possibile ritirare il consenso dopo che è stato concesso; una volta ritirato, i dati personali non possono più essere trattati su tale base.

È responsabilità del titolare identificare la base giuridica del trattamento dei dati personali che effettua. Questa informazione devono essere fornite agli interessati, come parte del principio di trasparenza.

## QUALI SONO I DIRITTI DEGLI INTERESSATI E COME POSSONO ESERCITARLI?

Il Regolamento assegna all'interessato una serie di diritti:

- il diritto di essere informato se, come e perché i suoi dati vengono trattati;
- il diritto di accedere ai dati e di ottenerne una copia;
- il diritto di ottenere la rettifica o l'integrazione dei suoi dati se inesatti o incompleti;
- il diritto di ottenere la cancellazione o l'eliminazione dei dati;
- il diritto di limitare o circoscrivere l'utilizzo dei dati;
- il diritto alla portabilità dei dati;
- il diritto di opporsi al trattamento dei suoi dati;
- il diritto di non essere sottoposto a decisioni automatizzate senza il coinvolgimento di un operatore umano, qualora ciò abbia un impatto significativo sull'interessato.

È importante notare che questi diritti non sono assoluti e sono soggetti a una serie di limitazioni e restrizioni. Alcuni diritti si applicano a tutte le attività di trattamento, mentre altri diritti si applicano solo in determinate circostanze.

Se desiderate esercitare i vostri diritti in qualità di interessati, il primo passo consiste nell'individuare il titolare del trattamento dei dati e nel presentare una richiesta in tal senso.
Se il titolare del trattamento non risponde o non vi consente di esercitare i vostri diritti, potete rivolgervi al Garante per la privacy:
☞ **www.gpdp.it/i-miei-diritti.**

GPDP

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Piazza Venezia 11
00187 Roma
tel. +39 06 696771
e-mail: protocollo@gpdp.it
www.gpdp.it

**Per informazioni presso l'Autorità:**
Ufficio relazioni con il pubblico
Orario di ricevimento telefonico: lunedì - venerdì ore 10.00 - 12.30
Orario di ricevimento in sede (previo appuntamento): lunedì - venerdi ore 10-12,30
tel. +39 06 69677 2917
e-mail: urp@gpdp.it

**Pubblicazione a cura del Servizio relazioni esterne e media**
**Novembre 2025**