Febbraio 2021

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

MINORI E NUOVE TECNOLOGIE

Consigli ai «GRANDI» per un utilizzo sicuro da parte dei «PICCOLI»

Strumenti come smartphone, tablet, computer, assistenti digitali, console per videogiochi e smart TV offrono opportunità di divertimento, ma anche di apprendimento e di educazione.

Questi dispositivi possono però nascondere alcune **insidie** e qualche pericolo se utilizzati da minori senza la supervisione di un adulto.

E' bene allora essere informati e provare a riflettere su quali accortezze è possibile mettere in campo per garantire un uso **consapevole** e soprattutto **sicuro** da parte dei più piccoli.

LE «INSIDIE» DELLA RETE

Un minore che utilizza strumenti connessi alla Rete potrebbe**, anche involontariamente**:

rivelare a sconosciuti informazioni su dove abita o dove va a scuola, sui percorsi che compie di solito, sulle sue abitudini;

diffondere i dati contenuti nel dispositivo utilizzato (ad esempio: foto, rubrica dei contatti);

fare involontariamente **acquisti online** o scaricare contenuti, come app e programmi**, a pagamento**;

consentire a **cybercriminali** di accedere a dati poi utilizzabili per scopi illeciti (ad esempio: i riferimenti della carta di credito dei genitori);

essere esposto alla **visione di materiali pornografici o violenti**, o essere vittima di fenomeni come il **sexting** (cioè, l'invio e la ricezione di messaggi sessualmente espliciti);

entrare in contatto con eventuali **malintenzionati**;

partecipare ad azioni di **cyberbullismo**, oppure esserne vittima.

MINORI «ACCOMPAGNATI»

E' buona abitudine **non lasciare che i più piccoli utilizzino le nuove tecnologie da soli** e spiegare loro quali rischi possono correre e cosa è meglio evitare di fare, **controllando che non siano entrati in contatto con sconosciuti** che potrebbero anche avere cattive intenzioni.

PER UNA NAVIGAZIONE SICURA

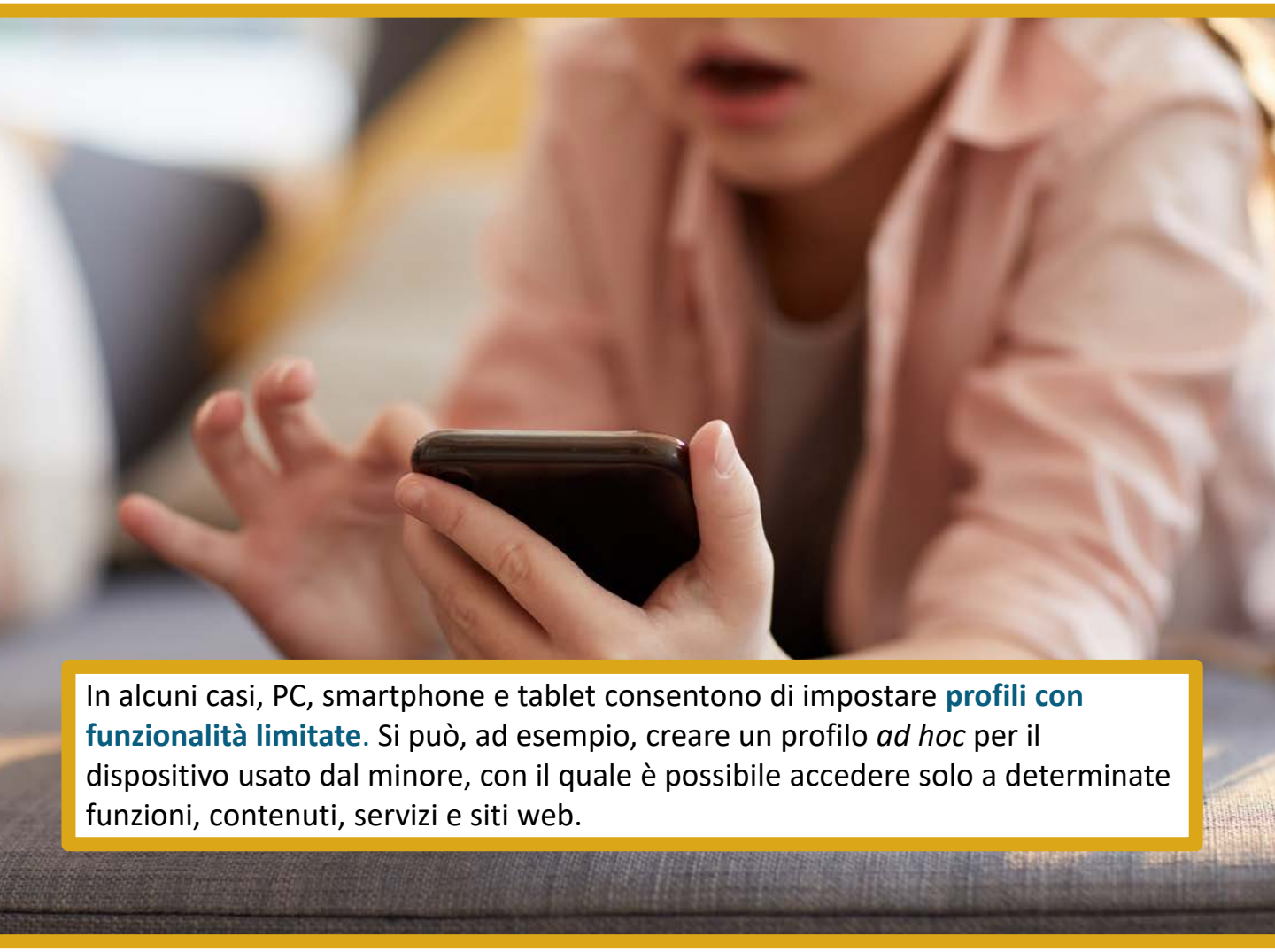
Meglio regolare su **livelli di adeguata sicurezza le impostazioni privacy dei dispositivi e di eventuali servizi utilizzati dai minori** (sistemi di messaggistica, download di app, acquisti online) e **leggere con attenzione l'informativa sul trattamento dei dati personali**, che deve essere sempre presente (nella confezione del prodotto, sul sito, nella app), completa di tutte le informazioni previste dalla normativa e scritta in un linguaggio chiaro e comprensibile.

Si può anche decidere di **bloccare** del tutto l'uso di determinati social network o servizi di messaggistica da parte del minore.

Al tale proposito, è bene ricordare che **alcune piattaforme non consentono l'iscrizione sotto una certa soglia di età.**

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. Prima di questa età è infatti necessario il consenso di chi esercita la responsabilità genitoriale.

Per quanto riguarda la navigazione sul web, è utile sapere che molti browser (i programmi utilizzati per navigare sul web) consentono di **impostare blocchi e filtri**, che possono essere utilizzati ad esempio per impedire che il minore veda determinati siti, scarichi contenuti potenzialmente dannosi o possa ricercare determinate parole associate a temi e argomenti non idonei.



In alcuni casi, PC, smartphone e tablet consentono di impostare **profili con funzionalità limitate**. Si può, ad esempio, creare un profilo *ad hoc* per il dispositivo usato dal minore, con il quale è possibile accedere solo a determinate funzioni, contenuti, servizi e siti web.

I **programmi di controllo parentale** permettono di monitorare l'uso di un dispositivo elettronico da parte di un minore. In particolare, consentono di:

- **impostare blocchi e filtri per determinate funzioni** (es: download di software) e pagine web (es: pornografia, acquisti online);
- **creare liste di parole che il minore non può ricercare e trovare sui motori di ricerca;**
- **offrire informazioni sull'uso che il minore fa del dispositivo** (es: siti visitati, chiamate, messaggi inviati);
- **limitare l'uso del dispositivo** solo ad alcune ore del giorno e per un tempo definito;
- **attivare servizi di geolocalizzazione per rintracciare il dispositivo** (e quindi eventualmente anche il minore che lo sta usando, in caso di emergenza).

Alcuni PC, smartphone, tablet offrono di default sistemi di parental control con funzionalità di base, mentre in altri casi è possibile attivare il parental control installando apposite app. In questo ultimo caso, è sempre bene **leggere con attenzione l'informativa sul trattamento dei dati personali** per comprendere quali e quanti dati tratta la app, per quali finalità ed eventualmente a chi possono essere trasmessi.

LE FOTO DEI BAMBINI ONLINE

Occorre sempre ricordare che le immagini dei minori pubblicate on line potrebbero finire anche nelle mani di malintenzionati. Meglio quindi non lasciare che i più piccoli possano pubblicarle online da soli.

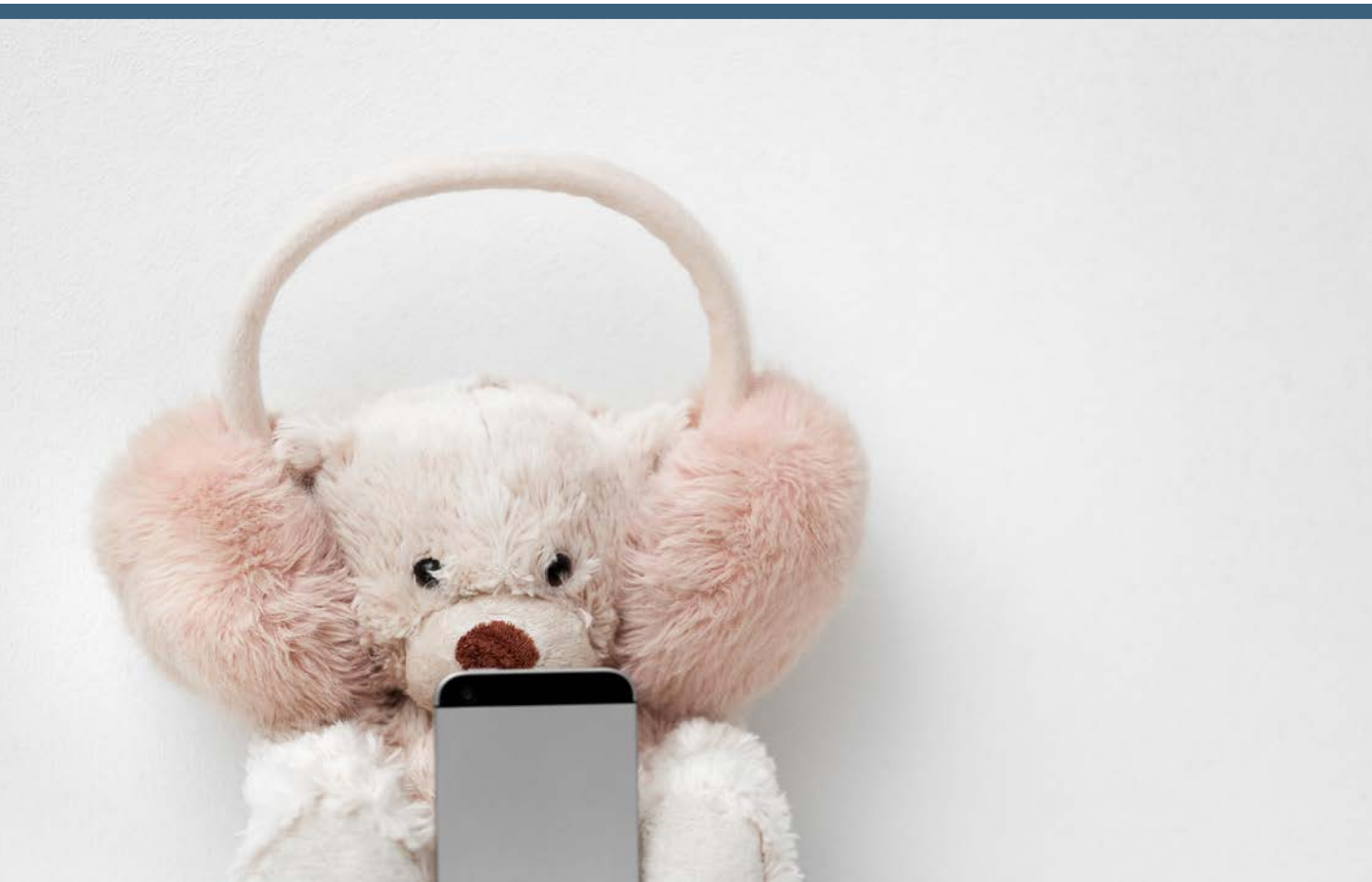
Ma è bene che anche gli adulti evitino di "postare" foto di minori.

Se proprio non si vuole fare a meno di pubblicare immagini i cui ci sono bambini, utilizzare in quel caso almeno alcune **accortezze**, come:

- **rendere irriconoscibile il viso del minore** (ad esempio, utilizzando programmi di grafica per "pixellare" i volti, disponibili anche gratuitamente online);

- **coprire semplicemente i volti con una "faccina" emoticon**;

- **limitare le impostazioni di visibilità** delle immagini sui social network solo alle persone che si conoscono.



PRIVACY BY DEFAULT E BY DESIGN

Il Regolamento UE/2016/679 in materia di protezione dati prevede che i sistemi elettronici siano prodotti e configurati per ridurre al minimo la raccolta e il trattamento di dati personali (privacy by design e privacy by default). Importante ricordare anche il principio di minimizzazione dei dati, richiamato all'art. 5, par. 1, lett. c) del Regolamento.

Occorre inoltre che siano rispettati alcuni principi fondamentali, come quello di trasparenza riguardo il trattamento dei dati e i diritti riconosciuti dal Regolamento Ue alle persone fisiche.

Tali regole e principi debbono essere conosciuti e rispettati dai produttori di dispositivi digitali e dai fornitori di servizi di comunicazione ed eventualmente certificati.

PER INFORMAZIONI E TUTELA

Nei casi in cui ci siano dubbi sull'effettivo rispetto delle norme o sul corretto uso dei propri dati personali, ci si può rivolgere al Garante per la protezione dei dati personali.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Attenzione quando pubblichi immagini online

Pubblica immagini di altre persone solo con il loro consenso

Potrebbero non voler apparire online o sentirsi in imbarazzo. Inserisci nelle immagini tag con i nomi di altre persone solo se sei sicuro che queste siano d'accordo

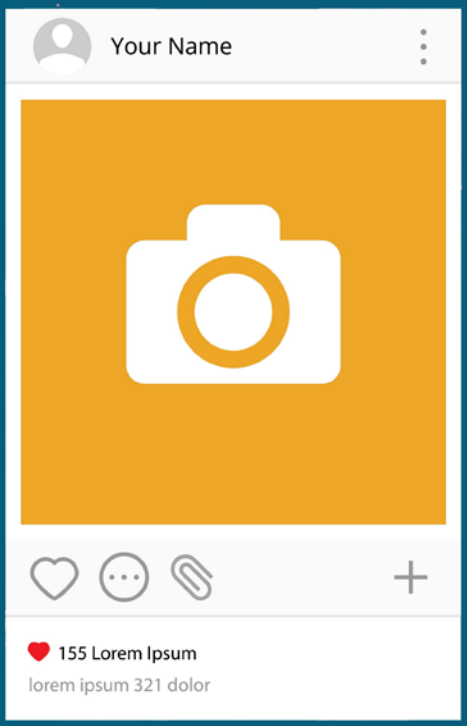
Rifletti bene prima di postare online foto o filmati

Potrebbe poi essere molto difficile eliminarli, soprattutto se qualcuno li ha copiati, condivisi, o diffusi su altri siti o social network

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Controlla chi può vedere le tue immagini

I principali social network consentono di scegliere se foto e immagini che pubblichi saranno visibili a tutti o solo a liste di persone scelte da te



Controlla i tag con il tuo nome associati a foto e filmati

Alcuni social network consentono eventualmente di applicare scelte come:
1) bloccare l'inserimento di tag con il tuo nome nelle immagini postate da altre persone
2) autorizzare solo alcune persone a taggare le immagini con il tuo nome
3) ricevere un messaggio di avviso se qualcuno collega il tuo nome ad un'immagine, in modo che tu possa approvare o rifiutare il tag

Molte app richiedono l'accesso alle foto o ai filmati che conservi su smartphone o tablet

Prima di autorizzare l'accesso, cerca di capire a quale scopo potrebbero essere utilizzate o diffuse le tue immagini

La scheda ha finalità meramente divulgative e sarà aggiornata in base agli sviluppi tecnologici e normativi

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Fatti smart! Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet (anno 2013)

Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet

Non ci pensiamo quasi mai, forse. Smartphone e tablet ci accompagnano ovunque e custodiscono parti importanti e spesso delicate delle nostre vite, sotto forma di foto, filmati, messaggi e dati telematici. E noi stiamo sempre attenti a proteggere adeguatamente queste informazioni con piccole ma utili precauzioni?

In un video-tutorial il Garante per la protezione dei dati personali offre alcune utili indicazioni per tutelare la nostra privacy quando utilizziamo smartphone e tablet.

Attenzione ai dati conservati su smartphone e tablet

Non conservare su smartphone e tablet informazioni troppo personali che potrebbero essere smarrite o rubate, o perfino clonate o attaccate da pirati elettronici. Non si dovrebbero mai conservare, ad esempio, password personali, codici di accesso e dati bancari in chiaro.

Ricorda, poi, che smartphone e tablet venduti, regalati o buttati possono contenere ancora dati privati. Se te ne liberi, quindi, **cerca di adottare alcune piccole precauzioni di sicurezza** come:

- ripristinare le impostazioni di fabbrica

- rimuovere la scheda SIM e la scheda di memoria
- eliminare tutti i backup contenuti nella memoria.

Proteggi i tuoi dati

Se vuoi evitare che qualcuno legga di nascosto le tue e-mail e i tuoi sms o che usi a tua insaputa il tuo smartphone o il tuo tablet, usa alcune precauzioni.

Imposta sempre un codice PIN abbastanza complicato, evitando, ad esempio, di usare il tuo nome e cognome, la data di nascita, il nome dei figli o quello del gatto di casa, o comunque altre parole che ti renderebbero in qualche modo riconoscibile.

Magari imposta anche un **codice di blocco**, quello che si attiva automaticamente quando il cellulare è acceso ma non viene utilizzato per un po´ di tempo. E anche in questo caso, evita codici un po´ troppo facili da scoprire.

Alcuni sistemi operativi consentono anche di impostare password di sicurezza che bloccano completamente l´accesso ai dati personali. Per farlo, basta collegare smartphone e tablet con il pc e utilizzare il software per la gestione del prodotto.

Conserva con cura il codice IMEI, che trovi sulla scatola del prodotto che acquisti e che in caso di furto o smarrimento puoi utilizzare per bloccare a distanza l´accesso al tuo smartphone o tablet.

Quando navighi su smarthone e tablet

Se ti connetti a Internet e ai social network via smartphone e tablet, **verifica le impostazioni privacy e leggi le condizioni d´uso dei servizi**.

Per navigare sul web, inoltre, **installa sempre - se disponibile - software di sicurezza anti-virus informatici o contro le intrusioni da parte di pirati telematici e ladri d´identità digitali**.

Quando usi connessioni wi-fi gratuite, ad esempio nei locali pubblici, **verifica che la navigazione sia protetta con protocolli di scambio dati criptati** e che l´autenticazione ai siti che eventualmente vengono visitati utilizzi il **protocollo Https**. In caso contrario, se si utilizzano credenziali di accesso a siti e servizi come la posta elettronica o l´home banking, il rischio che non ci siano adeguate garanzie di sicurezza per i propri dati è reale.

APP-rova di privacy

Se scarichi delle applicazioni, **evita le fonti sconosciute e utilizza sempre i market ufficiali**, a meno che tu non sia in grado di valutare autonomamente l´affidabilità della fonte - ad esempio leggendo i commenti eventualmente lasciati dagli altri utenti - per comprendere se ci sono eventuali rischi o problematiche.

Una volta installata un´applicazione, verifica se richiede **l´accesso a contenuti presenti sul tuo smartphone o sul tuo tablet** (ad esempio, le tuo foto o i contatti in rubrica) e leggi con attenzione le **condizioni d´uso del servizio**, soprattutto per evitare di dover pagare servizi non richiesti o di vedere esposte oltremisura informazioni di carattere personale (ad esempio: foto, video, contatti, ecc.).

Occhio allo spam

Smartphone e tablet sono terreno di caccia per lo spam.

Attenzione ai link presenti in e-mail, sms e messaggistica istantanea, perché, in alcuni casi, cliccandoli, potresti inconsapevolmente accettare di ricevere comunicazioni indesiderate, divenendo bersaglio di messaggi pubblicitari non richiesti da cui, poi, può anche essere abbastanza difficile liberarsi.

Vuoi sempre far sapere dove sei?

Smartphone e tablet hanno **funzioni di geolocalizzazione**, ma sei tu a decidere se, quando e chi può conoscere la tua posizione.

Per **disabilitare la geolocalizzazione**, puoi disattivare - controllando le impostazioni dello smartphone o tablet - il GPS o la connessione wi-fi quando non usi questi servizi o altri ad essi collegati.

E´ bene, inoltre, controllare anche le **impostazioni di geolocalizzazione dei servizi di social network** che eventualmente utilizzi su smartphone o tablet. La scelta finale di far sapere o meno dove sei, in fin dei conti, è sempre la tua.