

SPORTELLLO DEL CONSUMATORE

PILLOLE DI TUTELA

Tutela dei dati personali dei minori nel mondo digitale.
Esperienze online: rischi per i minori.
Silvia Galimberti, avvocato Movimento Consumatori Torino



**BENVENUTI
NEL "FAR
WEST"
DIGITALE
DEI NOSTRI
FIGLI**



**Quando diamo uno
smartphone in mano a un
bambino, lo stiamo
spingendo in un mercato
globale dove la merce più
preziosa sono proprio i
suoi dati: cosa guarda,
cosa gli piace, quanto
tempo si ferma su una
foto o su un contenuto,
quali sono le sue fragilità**

Protezione dei dati personali dei minori online

In Europa:

**GDPR - Regolamento Generale
sulla Protezione dei Dati**
(Regolamento UE/2016/679)

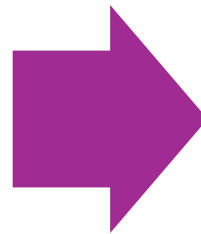
In Italia:

Codice Privacy (D. Lgs. 30 giugno
2003 196/2003 e successive
modifiche e integrazioni)

EUROPA

SOGLIA DEI 16 ANNI

Secondo la normativa europea, un minore può iscriversi a un social network o a un'app e accettare in autonomia l'informativa sulla privacy solo a partire dai 16 anni



ITALIA

SOGLIA DEI 14 ANNI

Il GDPR permette agli Stati membri di abbassare questa soglia (fino ai 13 anni) e in Italia la legge fissa a 14 anni il limite in cui il ragazzo/a può esprimere autonomamente il consenso per i servizi digitali

SCELTA FORTEMENTE
CRITICATA DAL
GARANTE PER
L'INFANZIA
E L'ADOLESCENZA

PERCHÉ?

- Mancanza di una reale consapevolezza digitale
- Esposizione a rischi psicologici e sociali precoci
- Disomogeneità e disparità di tutela



Il Garante per
l'Infanzia sostiene
che l'innalzamento a
16 anni debba andare
di pari passo con
sistemi tecnologici di
verifica dell'età
adeguati

Il Garante chiede che
i social applichino
controlli severi (come
una sorta di SPID o
sistemi di intelligenza
artificiale per il
riconoscimento
dell'età)



26 agosto 2026

Transazione storica tra
META

(multinazionale che
controlla facebook e
instagram)

e 48 Stati americani

Quali sono i maggiori rischi per i minori che utilizzano strumenti connessi alla Rete?

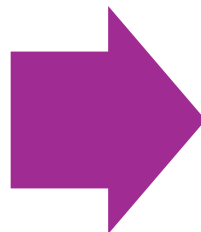
- 
- 1) Rivelare a sconosciuti informazioni su dove abita o dove va a scuola, sui percorsi che compie di solito, sulle sue abitudini
 - 2) Diffondere i dati contenuti nel dispositivo utilizzato (ad esempio: foto, rubrica dei contatti)
 - 3) Consentire a cybercriminali di accedere a dati poi utilizzabili per scopi illeciti (ad esempio: i riferimenti della carta di credito dei genitori)

4) Fare involontariamente acquisti online o scaricare contenuti, come app e programmi, a pagamento

5) 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)

6) Partecipare ad azioni di cyberbullismo, oppure esserne vittima

E SOTTO I 14 ANNI?



Per qualsiasi trattamento di dati personali, iscrizione a piattaforme o pubblicazione di foto, è obbligatorio il **consenso dei genitori**



SUGGERIMENTI DEL GARANTE PRIVACY

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)



Leggere con attenzione l'informativa sul trattamento dei dati personali, che deve essere sempre presente (sul sito, nella app) e deve essere completa di tutte le informazioni previste dalla normativa



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



Utilizzare programmi di controllo parentale

Altra normativa degna di nota
in tema di tutela dei minori
anche sotto il profilo della privacy:
DIGITAL SERVICES ACT – DSA
Regolamento UE 2022/2065

Novembre 2022: Il regolamento è entrato ufficialmente in vigore, avviando un'introduzione graduale.

Agosto 2023: È diventato vincolante per le grandissime piattaforme e motori di ricerca (VLOSE) come Google, TikTok, Meta, X.

Febbraio 2024: L'applicazione è stata estesa alla totalità delle piattaforme e dei servizi intermediari digitali che operano nell'UE

Il regolamento obbliga le piattaforme a rispettare, in materia di tutela dei minori, il seguente principio fondamentale:

I fornitori di piattaforme online accessibili ai minori adottano misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio (art. 28, co. 1)

CIÒ COSA SIGNIFICA IN CONCRETO?

Obbligo di individuazione e valutazione dei possibili rischi online per i bambini e i giovani che utilizzano i loro servizi

Valutazione di qualsiasi effetto negativo, attuale o prevedibile, in relazione alla protezione dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona

Adozione di misure di attenuazione dei rischi a tutela dei diritti dei minori, compresi strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi

Obbligo di rendere pubbliche le informazioni sulle proprie pubblicità in modo che chiunque, compresi i ricercatori, possano analizzare i possibili rischi

Se hanno la ragionevole
certezza che l'utente sia
un minore, le piattaforme
non possono mostrare
alcuna pubblicità basata
sulla profilazione

(ATTENZIONE PERÒ:
NON VIENE VIETATA LA
PUBBLICITÀ IN
ASSOLUTO)

PERCHÈ È IMPORTANTE RIDURRE IL PIÙ POSSIBILE
L'ESPOSIZIONE DEI MINORI ALLE PIATTAFORME, AI
SOCIAL MEDIA E AI FLUSSI PUBBLICITARI?

Per ridurre il rischio che si crei una **dipendenza psicologica e un'abitudine d'uso** difficilissima da scardinare



Perché, una volta compiuti i 18 anni, quel minore diventerà un utente "profilabile" al 100%, con un valore commerciale immenso, e sarà, per allora, già completamente fidelizzato



Perché molte piattaforme integrano sistemi di micro-transazioni (acquisto di monete virtuali, filtri speciali, abbonamenti a canali o elementi estetici nei videogiochi e nei social). Più tempo un minore passa all'interno dell'applicazione, più è alta la probabilità statistica che ceda alla tentazione di effettuare un acquisto o di spingere i genitori a farlo

Ci sono, inoltre, specifici rischi connessi alla sovraesposizione



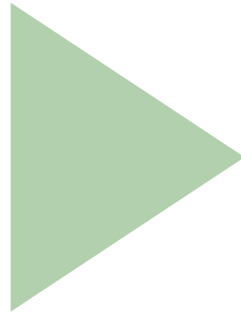
La riduzione del sonno (*Vamping*): Il minore passa le ore notturne sui social, riducendo le ore di riposo.

La sedentarietà: Il tempo online sottrae spazio all'attività fisica e al gioco all'aperto.

L'isolamento sociale: Le interazioni digitali sostituiscono i rapporti reali con amici e familiari.

Il calo del rendimento scolastico: Difficoltà di concentrazione dovute al continuo stimolo visivo dei video brevi e delle pubblicità.

Lo scopo del
Regolamento è proprio
quello di disinnescare i
meccanismi di
dipendenza
psicologica e i rischi
sistemici delle
piattaforme e dei
social



- 1) Spegnere i «motori
della dipendenza»
- 2) Disinnescare le
"Tane del Coniglio"
(*Rabbit Holes*)
- 3) Vietare i *Dark
Patterns* manipolatori

01

Stop al Volo Continuo

(Autoplay): I video successivi o i contenuti multimediali non possono partire in automatico nei profili dei minori. La riproduzione deve fermarsi finché il ragazzo non compie un'azione volontaria

02

Interruzione dello scorrimento infinito (*Infinite Scroll*)

Gli algoritmi devono inserire dei blocchi o dei messaggi di avviso ben visibili (es. *"Hai guardato video per 30 minuti, che ne dici di fare una pausa?"*) per spezzare lo stato di trance da scorrimento

03

Notifiche push silenziate di default:

Durante le ore scolastiche e quelle notturne, le applicazioni non possono inviare notifiche push che stimolino la curiosità del minore (es. *"Vedi cosa ha pubblicato il tuo amico"*) per evitare di farlo rientrare continuamente nell'app.

01

Se un minore mostra interesse per un video triste o legato a standard estetici irrealistici, l'algoritmo **ha il divieto di proporgli a ripetizione contenuti identici**, che rischierebbero di amplificare ansia, depressione o disturbi alimentari

02

Le piattaforme devono garantire la **diversificazione del feed**: l'algoritmo deve inserire forzatamente contenuti neutri, positivi o educativi per interrompere la spirale negativa.

01

Nessun senso di colpa

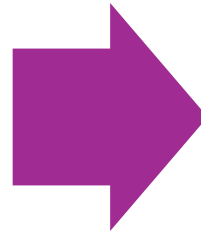
digitale: Se un minore decide di attivare un limite di tempo o di chiudere l'app, la piattaforma non può mostrargli messaggi manipolatori (es. *"Se te ne vai, ti perderai i video dei tuoi amici!"*) o icone tristi per farlo sentire in colpa

02

Facilità di disattivazione:

Attivare le opzioni di protezione della privacy, limitare il tempo di utilizzo o disconnettersi deve essere facile tanto quanto iscriversi (un solo clic, senza passaggi nascosti nei menu)

**SISTEMA
SANZIONATORIO**
(coordinato tra AGCOM
e Commissione
europea)



- 1) Sanzioni pecuniarie (fino al 6% fatturato annuo)
- 2) Penalità di mora giornaliera (fino al 5% del fatturato medio giornaliero)
- 3) Sospensione del servizio (in caso di violazioni reiterate che mettono a rischio l'utente)



Aprile 2026 :
la Commissione Europea ha emesso un pesante **rilievo preliminare di violazione** contro Meta. L'accusa formale è di **non aver protetto i minori di 13 anni**, permettendo loro l'accesso e non mitigando i rischi per la salute mentale legati al design degli algoritmi (creazione di dipendenza e "tane del coniglio"). Questo procedimento sta progredendo verso una potenziale sanzione miliardaria se Meta non adeguerà i suoi sistemi di verifica dell'età.



La Camera di Commercio di Torino, in collaborazione con il proprio Laboratorio chimico e il Dipartimento di giurisprudenza dell'Università degli studi di Torino e con il supporto delle Associazioni dei consumatori, iscritte all'albo della Regione Piemonte, sostiene i cittadini attraverso il progetto «Sportello del Consumatore»: un punto informativo dedicato alla conoscenza dei propri diritti, alla verifica della conformità e sicurezza dei prodotti e all'approfondimento della normativa in materia di sicurezza alimentare.

GRAZIE PER L'ATTENZIONE!