

# Sicurezza dei minori online

PROTEGGERE E RESPONSABILIZZARE I MINORI  
NEL MONDO DIGITALE

RELAZIONE DEI COPRESIDENTI DEL PANEL SPECIALE

SULLA SICUREZZA DEI MINORI ONLINE

Prof. dott. Jörg M. Fegert e dott.ssa Maria Melchior



## Prefazione

Nel marzo 2026 la Presidente della Commissione europea Ursula von der Leyen ha incaricato due consiglieri speciali – il prof. dott. Jörg M. Fegert e la dott.ssa Maria Melchior – di copresiedere il panel speciale sulla sicurezza dei minori online e sulle potenziali restrizioni di accesso ai social media in base all'età. Ai copresidenti è stato affidato il compito di preparare una relazione sui risultati del panel e di fornire indicazioni sull'approccio migliore che consentirebbe all'Europa di rendere il mondo online più sicuro per i minori.

Annunciato per la prima volta nel discorso sullo stato dell'Unione 2025 dalla Presidente della Commissione, il panel ha riunito accademici di alto livello, operatori dei vari settori interessati, rappresentanti dei giovani e dei genitori e altri specialisti di svariati settori in tutta Europa per valutare gli effetti dei social media sui minori.

*"In tutto il nostro operato saremo guidati dalla necessità di dotare i genitori degli strumenti giusti e di costruire un'Europa più sicura per i nostri figli. **Perché quando si tratta della sicurezza online dei nostri figli, l'Europa pensa ai genitori, non al profitto**".*

*Ursula von der Leyen, Presidente della Commissione europea*

*Discorso sullo stato dell'Unione 2025*

Il panel speciale si è riunito tre volte e ha registrato la presenza, in ciascuna occasione, di diversi specialisti. Il primo panel speciale, riunitosi il 5 marzo 2026, ha esaminato le prove scientifiche esistenti riguardo agli effetti dei social media e, più in generale, dell'ambiente digitale sui bambini e sugli adolescenti.

Il secondo panel speciale si è riunito il 16 aprile 2026 e ha discusso la legislazione vigente e gli strumenti di cui dispone l'UE, nonché le soluzioni strategiche poste in essere a livello nazionale per affrontare la questione della sicurezza dei minori online. Il terzo panel speciale, riunitosi il 16 giugno 2026, era incentrato sulle soluzioni strategiche nazionali e sulle potenziali raccomandazioni atte a proteggere e responsabilizzare i bambini e gli adolescenti nel mondo digitale.

Principali temi discussi durante i panel:

- gli effetti positivi e negativi dell'introduzione di specifiche restrizioni basate sull'età per l'accesso ai social media e ad altri servizi digitali;
- soluzioni su misura per proteggere e responsabilizzare i minori in base alle fasce di età, al contesto socioeconomico e ai rischi specifici per età;
- la sicurezza fin dalla progettazione o per impostazione predefinita e la responsabilità dei fornitori di social media e di altri servizi digitali;

- misure educative e di sensibilizzazione per promuovere l'uso responsabile degli strumenti online tra i bambini e gli adolescenti, i genitori e coloro che si prendono cura di minori, gli insegnanti e gli educatori;
- modalità di sostegno ai genitori e agli educatori e soluzioni che diano la capacità ai bambini e agli adolescenti di sfruttare le opportunità del mondo digitale.

L'analisi e le raccomandazioni della presente relazione si basano sui contributi fondamentali di un gruppo diversificato di specialisti invitati a ciascuna riunione del panel e sull'esito di numerose riunioni supplementari con i rappresentanti degli Stati membri, in particolare quelle ospitate dalla presidenza irlandese del Consiglio dell'UE e dal Lussemburgo (riunione ministeriale D9+), con i paesi terzi (compresi Australia e Brasile) e con il Parlamento europeo e i suoi membri, in particolare l'intergruppo per i diritti dei minori, con il settore, la società civile, gruppi di riflessione e altre organizzazioni, tra cui l'OHCHR delle Nazioni Unite e il comitato europeo per la protezione dei dati (EDPB).

A seguito di tali interazioni e sulla base degli elementi raccolti, i copresidenti hanno elaborato le loro raccomandazioni. Sebbene la responsabilità delle raccomandazioni incomba esclusivamente ai copresidenti, il loro operato deve molto al contributo di altri autorevoli esperti e rappresentanti dei genitori e dei giovani, e all'apporto della Commissione europea.

L'obiettivo della relazione è orientare le azioni future che saranno proposte dalla Commissione europea e dagli Stati membri dell'UE per rafforzare la sicurezza dei minori online. Da questa valutazione analitica indipendente scaturiscono raccomandazioni e spunti di riflessione rivolti ai bambini e agli adolescenti, ai genitori e a coloro che si prendono cura di minori, agli insegnanti e agli educatori, ai fornitori di social media e di altri servizi digitali sul modo in cui proteggere meglio e responsabilizzare i minori online.

#### **Riquadro – Ambito e terminologia**

Il compito principale affidato dalla Presidente von der Leyen al panel speciale consisteva nel dibattere la sicurezza dei minori online e le potenziali restrizioni di accesso ai social media in base all'età. Sebbene l'ambito della presente relazione sia limitato a tale compito, l'evoluzione delle discussioni durante le riunioni del panel speciale e altri sviluppi politici (ad esempio l'appello dei leader del G7 a favore di uno spazio digitale più sicuro per i minori del 17 giugno 2026) evidenziano la necessità che i copresidenti definiscano la terminologia utilizzata nella presente relazione.

Fatti salvi gli atti giuridici internazionali, dell'UE o nazionali, nella presente relazione sono utilizzati i termini e le corrispondenti definizioni di seguito specificati.

- **Social media e altri servizi digitali (in breve "social media+")** – Nell'ambito della presente relazione, i termini "social media+" e "social media e altri servizi digitali" sono utilizzati per indicare in senso lato i servizi che possono essere

disponibili per i minori e presentare caratteristiche e/o contenuti inadatti all'età e/o rischiosi (ad esempio caratteristiche dannose e che creano dipendenza, tra cui lo scorrimento infinito, la riproduzione automatica, gli algoritmi di raccomandazione e le notifiche persistenti). I fornitori di social media e di altri servizi digitali includono le piattaforme online che fungono da intermediari per contenuti di terzi, come i social media o gli app store. Vi rientrano anche i sistemi di IA che presentano rischi per la sicurezza e lo sviluppo dei minori, compresi i compagni virtuali basati sull'IA, i videogiochi che espongono i minori a pratiche commerciali dannose o a contatti pericolosi e le piattaforme per la condivisione di video che consentono ai minori di accedere a contenuti inadatti alla loro età.

- **Minori, bambini e adolescenti** – Fatto salvo l'uso giuridicamente definito del termine "fanciullo" o affine (ad esempio nella Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza), la presente relazione sostiene la necessità di un approccio incentrato sullo sviluppo per proteggere i minori online, che affronti i rischi e le vulnerabilità specifici cui sono esposti in età diverse. Ai fini della presente analisi, gli autori utilizzano il termine "minori" per indicare tutti i bambini e gli adolescenti di età inferiore a 18 anni (la maggiore età). Il termine "adolescenti" si applica a tutti i minori di età compresa tra i 13 e i 18 anni. Il termine "bambini" si riferisce invece a tutti i minori di età inferiore ai 13 anni. Nella presente relazione si utilizzano i termini "diritti dei minori" per far riferimento ai diritti di tutti gli esseri umani di età inferiore ai 18 anni, quali definiti nei testi giuridici. L'espressione "sicurezza dei minori online", che figura nel mandato del panel speciale, è usato come termine generico per indicare la protezione e la responsabilizzazione dei minori nel mondo digitale.

## Prefazione: Crescere in sicurezza nel mondo dei social media+

Il rapido progresso delle tecnologie digitali ha trasformato radicalmente il modo in cui i bambini e gli adolescenti crescono e interagiscono con i loro coetanei, i genitori, gli insegnanti e il mondo che li circonda. Allo stesso tempo le attività nel mondo offline rimangono fondamentali per l'apprendimento poiché promuovono relazioni ed esperienze significative che plasmano lo sviluppo dei minori.

**Il mondo dei social media+ offre molte opportunità** di apprendimento, connessione, partecipazione e creatività ai bambini e agli adolescenti. Tuttavia i minori devono essere educati e responsabilizzati per essere in grado di cogliere queste opportunità e realizzare appieno le proprie potenzialità.

Ciononostante **gli spazi dei social media+ presentano anche una serie di rischi** per il sano sviluppo e il benessere dei minori. Tra questi rischi si ricorda l'uso eccessivo dovuto a caratteristiche che creano dipendenza, a scapito di attività favorevoli allo sviluppo, l'esposizione a contenuti dannosi e contatti online inappropriati. Tali rischi sono amplificati dall'emergere di nuove tecnologie e si rendono necessarie scelte coraggiose ma attente per proteggere i bambini e gli adolescenti online.

L'ampia diffusione dei social media e altri servizi digitali ha alimentato nei **responsabili politici e nei genitori serie preoccupazioni per le minacce cui sono esposti online i bambini e gli adolescenti**. Nonostante le critiche suscitate dalle restrizioni di accesso ai social media e ad altri servizi digitali in base all'età, **questi limiti possono rappresentare una misura precauzionale necessaria** fino a quando non sarà dimostrato che i bambini e gli adolescenti possono accedere in sicurezza agli spazi dei social media+ o non emergeranno alternative sicure.

Imporre restrizioni in base all'età non vuol dire far gravare la responsabilità principale della sicurezza online dei minori sui genitori e su coloro che si prendono cura di minori o sugli stessi bambini e adolescenti, e neppure si intende liberare da ogni obbligo i prestatori di servizi online. **I fornitori di social media e di altri servizi digitali rimangono i principali responsabili della sicurezza dei servizi che sviluppano e forniscono.**

L'onere della prova deve incombere ai fornitori, non alle autorità di regolamentazione, ai genitori e ai minori. **Fino a quando non dimostreranno che i loro servizi sono sicuri fin dalla progettazione, i fornitori di social media e di altri servizi digitali dovrebbero limitare l'accesso dei minori di età inferiore ai 13 anni nell'UE.** Oltre alle restrizioni a livello dell'UE, gli Stati membri possono introdurre ulteriori limiti di età in via precauzionale per i minori di età superiore ai 13 anni.

**Le restrizioni precauzionali in funzione dell'età sono misure immediate volte a conseguire l'obiettivo a lungo termine di garantire la sicurezza degli spazi dei social media+ per i minori mediante la promozione di un cambiamento culturale.**

Dai primi risultati registrati nei paesi che hanno introdotto divieti generalizzati di accesso ai social media in base all'età si evince che la maggior parte dei minori trova il modo di eludere il divieto. Al tempo stesso alcuni minori hanno cancellato il proprio account dai social media e altri servizi digitali rischiosi e ora hanno più tempo per attività offline (come lo sport e le interazioni sociali faccia a faccia). Ciò dimostra che un cambiamento progressivo delle norme che disciplinano l'uso, da parte dei minori, dei social media+ è possibile e deve essere riconosciuto.

**È vero, il cambiamento richiede tempo.** A titolo di esempio, perché la società cambiasse atteggiamento nei confronti del divieto per legge delle punizioni corporali nelle scuole ci è voluta più di una generazione (si pensi a Germania e Svezia). Il divieto delle punizioni corporali ha chiarito il comportamento che ci si attende dai genitori, da coloro che si prendono cura di minori, dagli insegnanti e dagli educatori e ha rafforzato il coinvolgimento degli astanti nel garantire un'educazione non violenta dei minori. Il successo di questa misura è stato dimostrato dalle tendenze positive e tramite una valutazione costante sin dalla sua introduzione.

**Anche l'efficacia delle restrizioni basate sull'età richiederebbe un cambiamento di atteggiamento da parte della società.** La valutazione continua e il monitoraggio a lungo termine possono aiutare i responsabili politici a capire se le abitudini dei minori e dei loro genitori, di coloro che si prendono cura di minori e degli educatori cambieranno nel tempo.

Crescendo nel mondo odierno dei social media+, i bambini e gli adolescenti devono essere messi in condizione di condurre una vita sana e appagante e di sfruttare le opportunità offerte dai social media e dagli altri servizi digitali. **I diritti dei minori si applicano online così come offline:** dal diritto di essere al sicuro e protetti dallo sfruttamento economico e dalla criminalità in tutte le loro forme (in particolare la violenza sessuale) al diritto di accesso alle informazioni, all'istruzione e allo svago.

*"Nel corso dei decenni siamo riusciti a rendere il mondo reale più sicuro per i minori e dobbiamo fare lo stesso nel mondo digitale. Le opportunità offerte dalla tecnologia non possono andare a scapito della sicurezza, della salute o della felicità di bambini e ragazzi."*

*Ursula von der Leyen, Presidente della Commissione europea*

**I minori hanno il diritto di crescere in un ambiente sicuro e favorevole al loro sviluppo, online così come offline.** Se è doveroso, da un lato, continuare a fornire sostegno ai minori offline, dall'altro bisogna anche riconoscere che gli ambienti online sono diventati una parte sempre più importante della vita quotidiana dei minori. È per questo motivo che la protezione deve essere garantita come impostazione predefinita in tutti i social media e negli altri servizi digitali.

I diritti dei minori devono costituire le fondamenta delle misure di sicurezza online che li riguardano. Le potenziali restrizioni basate sull'età devono rispettare pienamente i diritti dei minori ed essere proporzionate e commisurate al loro interesse superiore. I mezzi utilizzati a tal fine devono stare al passo con gli sviluppi tecnologici.

Se è vero che spetta in primo luogo ai fornitori di social media e di altri servizi digitali garantire la sicurezza dei loro servizi, in particolare per quanto riguarda i minori, **è comunque necessario un ecosistema di parti coinvolte atto a proteggere e responsabilizzare i bambini e gli adolescenti nell'ambiente dei social media+**: dalle autorità di regolamentazione che devono mettere in atto le misure necessarie, ai fornitori che offrono servizi sicuri e adeguati all'età, ai genitori, a coloro che si prendono cura di minori, agli insegnanti e agli educatori che svolgono un ruolo cruciale nel sorvegliare e orientare i minori nell'uso degli strumenti online. Poiché i minori maturano e gli ambienti dei social media+ cambiano rapidamente, **il successo dell'ecosistema dipende dalle azioni interconnesse di tutte le parti coinvolte** che condividono la stessa visione: la possibilità per bambini e adolescenti di crescere sicuri in un mondo digitale.

**Figura 1. Ecosistema per proteggere e responsabilizzare i minori online**



## Accrescere lo slancio politico per rafforzare la sicurezza dei minori online

Negli ultimi mesi è emerso chiaramente come la sicurezza dei minori online stia diventando una priorità politica in tutto il mondo. **L'introduzione, l'attuazione e la valutazione continua, da parte dell'Australia, della misura di "accesso ritardato ai social media" hanno offerto insegnamenti fondamentali al resto del mondo.** Altri paesi, come Regno Unito e Canada, hanno seguito l'esempio pianificando proposte legislative, mentre l'Indonesia ha già adottato un divieto.

**Una recente relazione suggerisce che, secondo il 92% degli europei, il rafforzamento della protezione dei minori e dei giovani online dovrebbe essere una priorità per l'UE<sup>i</sup>.**

Anche i leader europei hanno iniziato ad affrontare la questione. La dichiarazione dello Jutland<sup>ii</sup> del settembre 2025, la risoluzione del Parlamento europeo in cui si chiede un'età minima digitale a livello dell'UE<sup>iii</sup>, l'istituzione ad opera della Presidente von der Leyen del panel speciale sulla sicurezza dei minori online e le recenti conclusioni del Consiglio europeo<sup>iv</sup> sono altrettanti segnali evidenti del crescente slancio politico per l'adozione di misure concrete volte ad affrontare i rischi sempre maggiori cui sono esposti i minori online.

Nel giugno 2026, per la prima volta, il G7 – Canada, Francia, Germania, Giappone, Italia, Regno Unito, Stati Uniti d'America, e l'Unione europea – ha concordato al più alto livello politico principi comuni per la protezione dei minori dai servizi digitali che presentano rischi<sup>v</sup>.

**Diversi Stati membri dell'UE stanno inoltre legiferando per stabilire un'età minima di accesso ai social media e ad altri servizi digitali** che possono rivelarsi dannosi per bambini e adolescenti. Ad esempio, in Francia la proposta in esame fissa il limite di età a 15 anni sulla scorta di una lista nera di servizi soggetti a restrizioni. La Grecia sta valutando di fissare a 15 anni il limite per accedere a servizi di social network online. In Danimarca si discute di un limite per i minori di età inferiore ai 16 anni, con la possibilità di abbassare l'età con il consenso dei genitori. La proposta svedese fissa il limite nell'anno in cui il minore compie 15 anni ed esonera diversi tipi di servizi. Molti altri paesi, da Portogallo e Spagna a Germania e Polonia, stanno valutando la possibilità di legiferare in materia.

In tale contesto la frammentazione del mercato unico europeo dei servizi digitali rappresenta un rischio tangibile e, in considerazione di ciò, molti Stati membri chiedono che la questione sia affrontata a livello dell'UE. È opportuno riconoscere che gli Stati membri hanno contesti culturali e nazionali diversi per quanto riguarda l'istruzione, l'alfabetizzazione digitale e la protezione dei minori. La frammentazione potrebbe far sì che i minori godano di livelli di protezione diversi attraverso l'UE. Ciò potrebbe comportare anche difficoltà pratiche per le autorità di regolamentazione incaricate di far rispettare le norme e costi di conformità più elevati per i prestatori.

Ne potrebbero derivare effetti a catena sullo sviluppo di social media e altri servizi digitali più sicuri e sull'efficacia delle leggi in materia di sicurezza online.

L'UE ha già preso provvedimenti concreti per la protezione dei minori. Le recenti decisioni adottate dalla Commissione europea hanno solo sottolineato la necessità di fronteggiare con elementi concreti le minacce cui sono esposti i bambini e gli adolescenti online. Ne sono un chiaro esempio le constatazioni preliminari nei confronti di Meta e TikTok per il presunto mancato rispetto degli elevati standard di protezione dei minori online stabiliti dal regolamento sui servizi digitali e per la mancanza di meccanismi facilmente accessibili per la segnalazione di contenuti pedopornografici. Inoltre le recenti decisioni fondamentali dei giudici statunitensi hanno segnato una svolta epocale nel dibattito sulla responsabilità delle piattaforme.

## Breve cronistoria della protezione dei minori online

Le iniziative volte a proteggere i bambini e gli adolescenti online risalgono alle origini di internet e sono il retaggio di un periodo antecedente ai social media, agli smartphone e all'IA. Le basi delle norme odierne per la protezione dei minori online sono state poste negli anni 1990 e nei primi anni 2000 con leggi concepite per consentire ai servizi e alle imprese di operare e scambiare informazioni a livello transfrontaliero. Tali norme, benché non siano state immaginate al solo scopo di proteggere i bambini e gli adolescenti online, hanno stabilito molti dei principi che continuano a costituire le fondamenta della legislazione vigente in tre settori.

In primo luogo, la regolamentazione dei media e dei servizi digitali nel mercato interno ha introdotto in tutta l'Europa norme comuni per i servizi televisivi, tra cui garanzie contro i contenuti che potrebbero essere dannosi per i minori. Il primo quadro armonizzato per i servizi online o "della società dell'informazione" (nell'ambito della direttiva sul commercio elettronico) ha contribuito a sostenere lo sviluppo di servizi online transfrontalieri all'interno dell'UE.

Il secondo settore è rappresentato dalla disciplina della protezione dei dati e della vita privata, a partire dalle norme comuni per la raccolta e l'uso delle informazioni personali in tutti gli Stati membri previste dalla direttiva sulla protezione dei dati del 1995.

In terzo luogo e da ultimo, la tutela dei consumatori. Mediante le norme comuni dell'UE si contrastano le pratiche commerciali ingannevoli e aggressive e si riconosce la necessità di offrire una protezione supplementare ai consumatori vulnerabili, principio importante nell'ambiente digitale nel quale rientra l'esposizione di bambini e adolescenti a pratiche commerciali che possono influenzarli in maniera diversa dagli adulti.

Con la progressiva e sempre più profonda integrazione delle tecnologie digitali nella vita quotidiana, l'UE ha continuato ad aggiornare tali quadri giuridici per rispondere alle nuove sfide. Il regolamento generale sulla protezione dei dati (GDPR) ha introdotto forme specifiche di tutela per salvaguardare i dati personali e il consenso online dei minori. La direttiva sui servizi di media audiovisivi è stata estesa a nuove

forme di contenuti audiovisivi e piattaforme per la condivisione di video. Infine il regolamento sui servizi digitali ha stabilito norme per i servizi intermediari online, anche allo scopo specifico di proteggere i minori.

**Quest'evoluzione riflette una tendenza più ampia: le tecnologie digitali non rientrano più perfettamente in un'unica categoria normativa o giuridica.** I social media e gli altri servizi digitali combinano elementi dei media, della comunicazione, del commercio e dell'elaborazione dei dati, spesso all'interno di una stessa piattaforma. Ne consegue che un approccio efficace alla protezione dei minori online deve essere olistico e avvalersi di strumenti appartenenti a diversi ambiti del diritto dell'UE, tra cui la regolamentazione delle piattaforme, la protezione dei dati, la tutela dei consumatori e la regolamentazione dei media audiovisivi.

Con lo sviluppo e la diffusione incalzanti dell'IA, i rischi per i minori online aumentano in misura esponenziale. A ciò si aggiunge la continua evoluzione dei social media e degli altri servizi digitali nel catturare e tenere agganciati gli utenti in quella che oggi si definisce "economia dell'attenzione". È più che mai necessario che le autorità di regolamentazione intervengano per rafforzare la protezione dei minori e consentire loro di navigare in sicurezza nel mondo dei social media+.

## Prove dei rischi e delle possibilità per i minori online

Il rapido progresso tecnologico ha offerto ai minori possibilità straordinarie per interagire con i coetanei, esprimere la propria creatività e accedere a conoscenze e servizi di assistenza. Tuttavia i minori non sono adulti e l'ambiente dei social media+ li espone a diversi rischi per la salute fisica e mentale e per lo sviluppo nelle diverse fasce d'età. Svolgono un ruolo determinante anche fattori socioeconomici e personali, quali il contesto familiare e il genere, come pure la progettazione dei social media e di altri servizi digitali.

**Per orientare azioni adeguate di protezione e responsabilizzazione dei minori online è fondamentale disporre di prove solide che associno i rischi e i danni all'uso dei social media e di altri servizi digitali.** Le caratteristiche, le funzionalità o i formati specifici applicati nei social media+ possono nuocere in modo diverso, a seconda del contesto sociale e di quello personale del bambino o dell'adolescente. I minori appartenenti a gruppi razziali, etnici e religiosi minoritari, membri della comunità LGBTQ+, caratterizzati da bisogni educativi speciali o affetti da problemi di salute mentale preesistenti possono essere particolarmente vulnerabili ai danni online. Questa vulnerabilità è naturalmente amplificata dai social media e da altri servizi digitali caratterizzati da contenuti o progettazioni dannosi, manipolativi o che creano dipendenza. All'evoluzione di tali caratteristiche dovrebbe affiancarsi quella della ricerca e dell'acquisizione di prove.

**I rischi per la salute fisica e mentale che i social media e altri servizi digitali pongono per i minori sono considerevoli.** Sul piano del benessere fisico, il tempo eccessivo trascorso davanti allo schermo sostituisce il gioco all'aperto e lo sport e può

incidere sulla salute, sulla forma fisica e sulla qualità del sonno. I minori che utilizzano social media+ e dispositivi sin dalla giovane età trascurano l'esplorazione pratica e l'interazione sociale diretta, il che può comprometterne lo sviluppo socioemotivo e renderli suscettibili di problemi di salute mentale. Anche l'uso prolungato dei dispositivi può essere fonte di problemi, come disturbi muscoloscheletrici e affaticamento oculare da esposizione allo schermo.

I rischi per la salute mentale nei minori che utilizzano i social media e altri servizi digitali sono significativi. I rischi dell'ambiente dei social media+ che nuocciono in modo diretto alla salute mentale dei minori si intersecano con il potenziale di acuire eventuali disturbi psichici preesistenti, tra cui depressione e ansia. Anche in questo caso l'esposizione ai rischi per bambini e adolescenti è determinata da fattori sociali e personali.

In linea generale l'elevato utilizzo dei social media e di altri servizi digitali tra i bambini e gli adolescenti è associato a disturbi del sonno e della concentrazione come pure all'aumento dei tassi di depressione e ansia. Le caratteristiche di progettazione che creano dipendenza amplificano tali effetti promuovendo controlli compulsivi, la FOMO ("fear of missing out", ovvero la paura di essere tagliati fuori) e un maggiore confronto sociale, che per i minori possono tradursi nell'erosione dell'autostima e in un aumento dello stress. I sistemi algoritmici di amplificazione e raccomandazione possono accrescere la disinformazione e l'incitamento all'odio. A pagarne il prezzo maggiore sono soprattutto i gruppi vulnerabili online.

**I rischi che i minori siano esposti a contenuti criminali e illegali online sono considerevoli.** Sia gli adulti che i minori utilizzano i social media e altri servizi digitali, come le piattaforme di gaming, per interagire con bambini e adolescenti. Tra i rischi figurano l'esposizione ad abusi sessuali su minori (materiale pedopornografico), l'adescamento, il bullismo online, la radicalizzazione e l'istigazione a commettere atti illegali, violenti o terroristici. L'uso diffuso degli strumenti di IA pone una grave minaccia per i bambini e gli adolescenti a causa della produzione di materiale pedopornografico sintetico (ad esempio i deepfake). Questi abusi incidono in modo drastico sullo sviluppo e sulla salute psicofisica dei minori e, nei casi più gravi, possono costare loro la vita.

**I fornitori di social media e di altri servizi digitali rimangono i principali responsabili della sicurezza dei minori che usufruiscono dei loro servizi.** Inoltre i genitori e coloro che si prendono cura di minori svolgono un ruolo importante nel monitorare il tempo che bambini e adolescenti trascorrono online, guidandoli a gestire insieme i rischi cui sono esposti negli ambienti dei social media+. Garantire attività offline e interazioni in presenza adeguate è fondamentale per ogni fascia d'età.

Nonostante i numerosi potenziali pericoli, **il mondo dei social media+ offre un ampio ventaglio di possibilità ai bambini e agli adolescenti.** In un mondo in cui i minori interagiscono online in modo sicuro e vantano solide competenze digitali, l'uso dei social media e di altri servizi digitali può favorire il benessere e la connessione

sociale, come anche creare reti di sostegno tra pari, possibilità di espressione personale, impegno civico e apprendimento autonomo. Iniziative mirate sulle competenze digitali, come la strategia dell'UE per un'internet migliore per i ragazzi, i centri per un'internet più sicura e l'integrazione dell'alfabetizzazione mediatica nei programmi di istruzione e formazione nazionali, si sono rivelate efficaci nell'affinare il pensiero critico, rafforzare la resilienza alla disinformazione e migliorare la capacità di navigazione sicura fra i minori.

**I social media e altri servizi digitali "sicuri fin dalla progettazione" potrebbero contribuire alla responsabilizzazione e alla partecipazione online dei bambini e degli adolescenti** sostenendo l'acquisizione di competenze digitali e l'alfabetizzazione mediatica. Grazie a un'educazione digitale adeguata all'età, impartita dalle scuole con il sostegno dei genitori e di coloro che si prendono cura di bambini o adolescenti, i minori potrebbero disporre degli strumenti necessari per cogliere le possibilità offerte dalla dimensione online e gestirne i possibili rischi e pericoli.

### Necessità di far fronte ai rischi specifici per età

Man mano che i minori crescono e acquisiscono maggiore indipendenza, la capacità dei genitori di supervisionarne le attività online diminuisce. Aumenta, invece, il ruolo dell'influenza dei coetanei. Durante l'adolescenza, verso il compimento della maggiore età, i minori diventano sempre più autonomi nella navigazione online e maggiormente in grado di comprendere e gestire i rischi cui vanno incontro. Va da sé: le esigenze di un bambino di 3 anni e quelle di un adolescente di 16 sono differenti. Ciò sottolinea **l'importanza di un approccio alla sicurezza dei minori online attento allo sviluppo**, come quello applicato nella presente relazione, **che operi una distinzione tra le varie fasce di età**.

I bambini **al di sotto dei 3 anni**, in quanto utenti passivi, corrono principalmente rischi relazionali e di "tecnoferenza"<sup>1</sup>. La fonte dei rischi risiede soprattutto nel sostituire l'interazione diretta con il tempo trascorso davanti allo schermo, cui coloro che si prendono cura di bambini ricorrono per "calmare" o distrarre i più piccoli. Ciò può incidere sulla soglia dell'attenzione, sull'acquisizione del linguaggio e sullo sviluppo socioemotivo del bambino.

I bambini **tra i 3 e i 5 anni** d'età, che esordiscono come utenti indipendenti pur sotto supervisione, sono sempre più vulnerabili ai rischi posti dagli ambienti online e connessi a una maggiore esposizione allo schermo. I social media e altri servizi digitali ottimizzati per la gratificazione immediata, la ricompensa ripetitiva e la continua stimolazione esterna sono fundamentalmente inadatti alle capacità ancora in fase evolutiva dei bambini e possono nuocere al loro sviluppo a lungo termine.

---

<sup>1</sup> Interruzione delle interazioni tra genitori e figli per via della tecnologia.

**Tra i 6 e i 9 anni** l'uso dei social media e di altri servizi digitali da parte dei bambini si espande in modo significativo. I riscontri esterni provenienti dall'ambiente online (come i "mi piace", i punteggi e le classifiche) si intrecciano con l'autostima emergente basata sullo sviluppo delle competenze nel mondo reale, il che può amplificare l'ansia da prestazione e il confronto tra pari, aumentando la vulnerabilità al bullismo online, all'incitamento all'odio e alle molestie da parte dei coetanei.

**Tra i 10 e i 12 anni d'età** l'accesso dei bambini agli spazi dei social media+ diviene un presupposto essenziale per la partecipazione sociale. In questa fascia d'età le loro sensibilità evolutive convergono in modo quanto mai acuto con l'effetto amplificatorio generato dalle piattaforme. I sistemi algoritmici di raccomandazione accentuano il confronto sociale e l'esposizione a contenuti dannosi o illegali (tra cui materiale pedopornografico, propaganda di stampo estremista e disinformazione) e a modelli di progettazione che creano dipendenza, con conseguente aggravarsi dei sintomi di depressione e ansia. Una recente ricerca prospettica suggerisce che l'acquisto del primo smartphone a 12 anni (anziché a 13) potrebbe essere legato a un rischio maggiore di sviluppare depressione e altri problemi di salute mentale a un anno di distanza<sup>vi</sup>. Da questo esempio si evince che, in linea generale, i minori sono particolarmente vulnerabili al di sotto dei 13 anni.

**Tra i 13 e i 15 anni** gli adolescenti passano da un uso controllato dei social media e di altri servizi digitali a un uso via via più autonomo. In questa fase le forme tradizionali di supervisione da parte di coloro che si prendono cura di minori e degli educatori scolastici perdono progressivamente efficacia. I rischi sono sempre più plasmati dalle strutture dei social media e altri servizi digitali, piuttosto che dal comportamento del singolo. Una sfida fondamentale consiste nella gestione dei sistemi algoritmici, che strutturano l'esposizione e influenzano il comportamento con un livello di trasparenza limitato.

Il passaggio all'autonomia è una tappa naturale della crescita nel mondo odierno, online così come offline. Pertanto l'obiettivo non è frenare gli adolescenti nel percorso verso l'autonomia, ma piuttosto limitarne l'esposizione ai danni in una fase dello sviluppo di massima vulnerabilità. Una protezione efficace richiede un approccio orientato allo sviluppo e multilivello, che combini regolamentazione dei social media e di altri servizi digitali, interventi educativi e sostegno all'autoregolamentazione e all'uso critico dei media.

Infine, **tra i 16 e i 18 anni** gli adolescenti vivono una fase di consolidamento della propria identità, accompagnata da una crescente autonomia. Lo sviluppo delle capacità consente loro di comprendere e gestire meglio i rischi della dimensione online. Tuttavia il loro sviluppo neurobiologico è lungi dall'essere compiuto e l'uso dei social media e di altri servizi digitali aggrava i rischi di dipendenza, ansia e problemi di salute mentale. In questa fascia d'età gli adolescenti devono acquisire le competenze necessarie (ad esempio il pensiero critico e la capacità di valutazione)

per navigare con successo e in sicurezza nel mondo digitale e sbloccarne appieno il potenziale.

## Sei principi guida per proteggere e responsabilizzare i minori online

La compresenza di rischi e possibilità per bambini e adolescenti nell'ambiente dei social media+ richiede la definizione di un quadro strategico globale di protezione e responsabilizzazione dei minori nella dimensione online. I seguenti **sei principi guida elaborati dai copresidenti hanno orientato i lavori del panel speciale** e si riflettono nella struttura della presente relazione. Le misure dovrebbero poggiare su prove e analisi solide delle sfide e delle possibilità che i minori incontrano online. Garantire un'attuazione e una valutazione efficaci sarà fondamentale per ottenere risultati.

- **Principio 1. Approccio evolutivo (cfr. capitolo 1)**

**Occorre garantire una regolamentazione adeguata all'età e orientamenti differenziati.** Lo sviluppo per fasi di bambini e adolescenti richiede la progettazione e l'attuazione di misure di protezione che trattino rischi specifici per fascia d'età. Ove possibile, tali misure dovrebbero tenere conto del contesto personale e sociale dei minori, che può aggravarne l'esposizione ai rischi.

- **Principio 2. Uguaglianza e diversità (cfr. capitolo 2)**

È importante riconoscere le disuguaglianze in termini di rischi ed esposizione ai danni online per le diverse fasce d'età e i diversi gruppi socioeconomici. Il genere, la sessualità, il contesto razziale, etnico e religioso, i bisogni educativi speciali e i problemi di salute mentale preesistenti sono tutti fattori che determinano la vulnerabilità dei minori ai danni online. Influenzano anche le risorse e le capacità di cui dispongono i genitori e coloro che si prendono cura di minori per sostenere i bambini e gli adolescenti nel percorso verso l'autonomia.

- **Principio 3. Protezione dei minori (cfr. capitolo 3)**

I bambini e gli adolescenti devono poter beneficiare di spazi sicuri sui social media+. La progettazione dei social media e degli altri servizi digitali dovrebbe prevedere la protezione dei minori dai contenuti dannosi, dalle caratteristiche che creano dipendenza, dalla negligenza digitale<sup>2</sup> e dai reati commessi online (ad esempio gli abusi sessuali). I minori dovrebbero poter segnalare facilmente eventuali caratteristiche o contenuti dannosi. I fornitori dovrebbero dare la priorità a tali segnalazioni e rimuovere prontamente le caratteristiche o i contenuti dannosi.

- **Principio 4. Responsabilità dei servizi digitali e diritti dei consumatori (cfr. capitolo 3)**

---

<sup>2</sup> Reiterata incapacità della persona che si prende cura del minore di assicurare un'attenzione, una reattività, una supervisione o una protezione adeguate alla fase di sviluppo, in quanto le tecnologie digitali interferiscono con le funzioni essenziali di assistenza, le sostituiscono o le intralciano.

La responsabilità del fatto che i social media e gli altri servizi digitali garantiscano un accesso e un utilizzo sicuro ai minori deve ricadere principalmente sui fornitori. Si tratta di incentivare misure di "sicurezza fin dalla progettazione" per i servizi digitali e di applicare rapidamente una regolamentazione basata sui contenuti. Ai fornitori di social media e di altri servizi digitali dovrebbe incombere l'onere di dimostrare che le caratteristiche dei loro servizi non sono dannose, prima che bambini e adolescenti vi possano accedere.

- **Principio 5. Responsabilizzazione ed educazione mediatica (cfr. capitolo 4)**

I genitori, coloro che si prendono cura di minori, gli insegnanti e gli educatori dovrebbero essere messi in condizione di sostenere i bambini e gli adolescenti nella transizione graduale verso una navigazione online sicura e autonoma. Si dovrebbero offrire sufficienti opportunità (ad esempio di alfabetizzazione digitale e mediatica) e infrastrutture adeguate che permettano ai genitori di riflettere sul loro operato e di guidare i minori nelle interazioni online. Le misure devono essere adattate ai ruoli di coloro che si prendono cura di minori e degli educatori, che evolvono man mano che i bambini e gli adolescenti maturano.

- **Principio 6. Diritti e partecipazione dei minori (cfr. capitolo 4)**

Occorre salvaguardare il diritto dei minori a una partecipazione, un'interazione e una cocreazione sicure, online così come offline. Le misure di protezione dei minori dovrebbero sempre essere fondate sui loro diritti, quali intesi ai sensi dei pertinenti quadri normativi internazionali<sup>3</sup>. I limiti d'età devono rispettare i diritti dei minori online ed essere proporzionati, limitati nel tempo e commisurati al loro interesse superiore. Ciò sottolinea anche la necessità di sostenere finanziariamente e promuovere attività offline per i minori di tutte le età.

---

<sup>3</sup> In particolare la Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza e le osservazioni generali del Comitato sui diritti dell'infanzia e dell'adolescenza, la Carta dei diritti fondamentali dell'Unione europea e la strategia dell'UE sui diritti dei minori.

*Consiglieri speciali della Presidente e copresidenti del panel speciale sulla sicurezza dei minori online*

*Prof. dott. Jörg M. Fegert*



**Prof. dott. Jörg M. Fegert**

Direttore sanitario del dipartimento di Psichiatria, psicosomatica e psicoterapia infantili e adolescenziali presso l'Ospedale universitario di Ulm

*Dott.ssa Maria Melchior*



**Dott.ssa Maria Melchior**

Direttrice di ricerca presso l'Istituto nazionale francese per la sanità e la ricerca medica (INSERM)

# Proteggere e responsabilizzare i minori online

## SICUREZZA DEI MINORI ONLINE

### ANALISI DELLA SITUAZIONE

---

#### APPROCCIO EVOLUTIVO

Garantire una regolamentazione adeguata all'età e orientamenti differenziati

#### UGUAGLIANZA E DIVERSITÀ

Riconoscere le disuguaglianze in termini di rischi, esposizione e danni online in tutti i gruppi

#### PROTEZIONE DEI MINORI

Protezione da contenuti dannosi, progettazioni che creano dipendenza, negligenza digitale e reati (ad es. abusi sessuali, bullismo)

#### RESPONSABILITÀ DEI SERVIZI DIGITALI E DIRITTI DEI CONSUMATORI

Applicare misure di sicurezza fin dalla progettazione e una regolamentazione basata sui contenuti

#### RESPONSABILIZZAZIONE ED EDUCAZIONE MEDIATICA

Consentire ai genitori e a coloro che si prendono cura di minori di sostenere le competenze digitali e l'alfabetizzazione mediatica di bambini e adolescenti per un uso responsabile

#### DIRITTI E PARTECIPAZIONE DEI MINORI

Salvaguardare il diritto a una partecipazione e a una cocreazione sicure online

---

### MISURE

### VALUTAZIONE

## Raccomandazioni chiave per proteggere e responsabilizzare i minori online

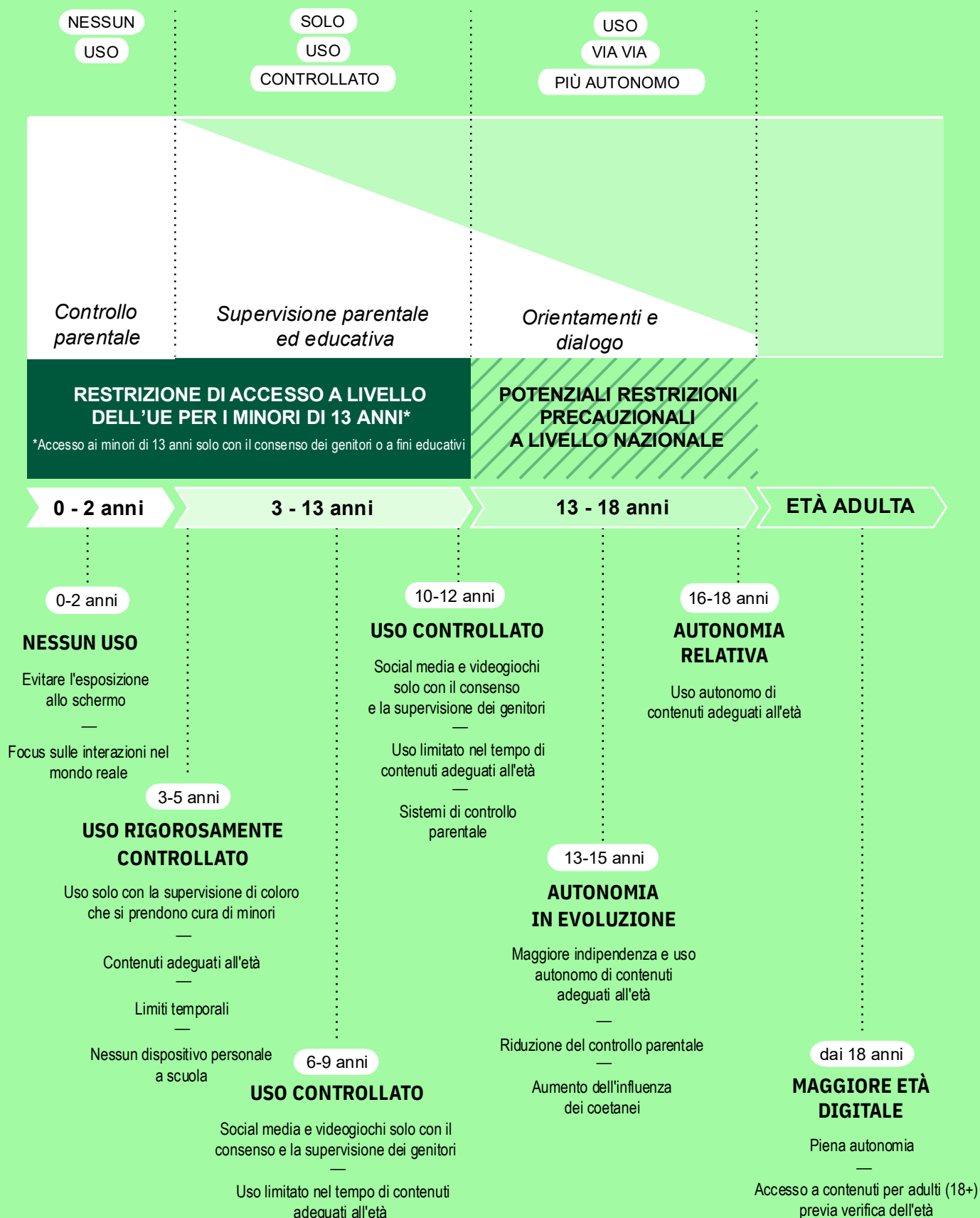
L'obiettivo generale delle raccomandazioni della presente relazione, che si fondano su un approccio attento allo sviluppo e rispecchiano i sei principi guida, è trovare un equilibrio tra la necessità di proteggere i bambini e gli adolescenti online e il loro diritto di partecipare al mondo dei social media+ e di coglierne le possibilità.

### Raccomandazioni sull'uso adeguato all'età dei social media e di altri servizi digitali

- 1. Da 0 a 2 anni: evitare gli schermi e i social media+.** Evitare l'esposizione prolungata allo schermo nella prima infanzia non significa divieto assoluto; significa riconoscere le esigenze evolutive dei bambini in termini di attaccamento, sviluppo sensoriale e apprendimento precoce del linguaggio. I genitori e coloro che si prendono cura dei bambini in questa fascia di età dovrebbero prediligere le interazioni faccia a faccia e, nel proprio rapporto col mondo digitale, optare per un uso consapevole dei dispositivi così da offrire un modello di riferimento positivo ed evitare la "tecnoferenza". L'approccio è in linea con le raccomandazioni dell'Organizzazione mondiale della sanità di evitare nel bambino perturbazioni dello sviluppo neurobiologico e cognitivo e dell'attaccamento emotivo così come l'insorgenza di disturbi fisici (ad esempio, problemi alla vista).
- 2. Da 3 a 12 anni: uso controllato dei social media+ e dei dispositivi adeguati all'età.** I bambini non dovrebbero essere autorizzati a utilizzare dispositivi per la navigazione internet senza supervisione. Le scuole dovrebbero prevedere strutture per un uso controllato e limitato dei dispositivi a fini educativi, sostenendo l'alfabetizzazione digitale e mediatica, la resilienza emotiva e la riflessione critica sui rischi. I genitori e coloro che si prendono cura di bambini in questa fascia di età dovrebbero supervisionare e sostenere il passaggio graduale all'autonomia digitale attraverso social media e altri servizi digitali adeguati all'età. Dovrebbero inoltre affrontare periodicamente con i bambini il tema dei potenziali benefici e rischi delle interazioni online. Coloro che si prendono cura di bambini in questa fascia di età e gli educatori dovrebbero continuare a incoraggiare i bambini a partecipare ad attività offline.
- 3. Da 13 a 18 anni: evoluzione dell'uso autonomo dei social media+ adeguati all'età.** Dai 13 ai 18 anni gli adolescenti dovrebbero avere accesso solo a social media adeguati all'età e "sicuri per impostazione predefinita" come pure ad altri servizi digitali che hanno introdotto proattivamente funzioni di sicurezza essenziali (ad esempio, limiti allo scorrimento infinito e ai sistemi di raccomandazione). Fino a quando non saranno sviluppati questi social media e altri servizi digitali "sicuri per impostazione predefinita", il controllo e la supervisione parentali individuali e adeguati all'età resteranno cruciali. Le autorità di regolamentazione potrebbero valutare l'introduzione di ulteriori misure precauzionali. Nonostante gli adolescenti

di età superiore ai 16 anni acquisiscano via via una maggiore autonomia digitale, i rischi connessi all'esposizione a contenuti dannosi online permangono. Per tale ragione è importante che i genitori e coloro che si prendono cura di adolescenti proseguano il dialogo con i minori sulle loro esperienze online. Gli adolescenti dovrebbero godere di un accesso privilegiato ai servizi di sostegno e ai sistemi di reclamo, beneficiando nel contempo di reti di sostegno tra pari che promuovano l'uso responsabile dei social media e degli altri servizi digitali.

# Uso dei social media+ adeguato all'età da parte dei minori



## Raccomandazioni per proteggere bambini e adolescenti online

- **Proporre una restrizione di accesso ai social media e ad altri servizi digitali armonizzata a livello dell'UE per i minori di 13 anni**

Serve una restrizione di accesso ai social media e ad altri servizi digitali, compresi gli assistenti IA, armonizzata a livello dell'UE per i minori di 13 anni. In questo modo si agevolerebbe l'applicazione di metodi di garanzia dell'età proporzionati e rispettosi dei diritti e si incoraggerebbe l'introduzione di obblighi di sicurezza fin dalla progettazione per i fornitori di social media e altri servizi digitali. Fino ai 13 anni i bambini dovrebbero poter accedere ad ambienti di social media+ consoni alla loro età, con limiti di tempo e soltanto con l'autorizzazione e la supervisione dei genitori o in contesti didattici, mentre dai 13 anni in su gli adolescenti dovrebbero iniziare a usare social media e altri servizi digitali sicuri e adatti all'età in modo via via più autonomo.

Una disciplina armonizzata a livello dell'UE che fissi a 13 anni l'età minima contribuirebbe al buon funzionamento del mercato unico garantendo ai fornitori un quadro unico di conformità. Faciliterebbe inoltre l'applicazione delle norme e la vigilanza da parte delle autorità di regolamentazione a livello sia nazionale che dell'Unione e assicurerebbe lo stesso livello di protezione online a tutti i minori nell'UE, a prescindere dal contesto socioeconomico, culturale e nazionale.

- **Introdurre sistemi efficaci di garanzia dell'età per verificare questo dato, rendendo possibili approcci che puntino alla sicurezza fin dalla progettazione e siano calibrati in funzione dell'età per proteggere e responsabilizzare i minori online**

I metodi di garanzia dell'età (verifica o stima) devono essere proporzionati e rispettare requisiti minimi, in particolare per quanto riguarda i diritti fondamentali degli utenti, tra cui i diritti dei minori e le relative misure di salvaguardia. Qualsiasi metodo utilizzato per accertare l'età dovrebbe aderire ai massimi standard di protezione dei dati e della vita privata e non dovrebbe comportare il trattamento di documenti di identità e dati biometrici ai fini della stima dell'età. Si dovrebbero applicare norme tecniche quali la dimostrazione a conoscenza zero (*zero-knowledge proof*) affinché né la piattaforma tenuta a valutare l'età né il prestatore di servizi di verifica dell'età ricevano informazioni che possano portare al tracciamento o all'identificazione dell'utente.

I metodi di garanzia dell'età dovrebbero permettere di determinare con precisione l'età o le fasce d'età richieste ed essere attendibili e facili da usare nella pratica in condizioni reali. Dovrebbero anche essere solidi, così da evitare l'elusione e le minacce alla cibersecurity, inclusivi, non discriminatori e disponibili in egual misura a tutti coloro che ne hanno bisogno. I fornitori di social media e altri servizi

digitali devono ottemperare all'obbligo di impedire che i minori siano esposti a servizi rischiosi o abbiano a che fare con utenti che si fingono bambini o adolescenti.

- **Ampliare e armonizzare le norme sulle funzioni di sicurezza essenziali nella progettazione dei social media e degli altri servizi digitali**

I social media e gli altri servizi digitali dovrebbero prevedere chiare garanzie di sicurezza fin dalla progettazione e adeguatezza all'età (ad esempio possibili limiti allo scorrimento infinito, alla riproduzione automatica, alle notifiche push e ai motori di raccomandazioni personalizzate problematiche). Per contrastare la progettazione studiata per creare dipendenza, i contatti non richiesti e i fenomeni dei "percorsi oscuri" (*dark pattern*) e dei "vortici di contenuti" (*rabbit hole*), le impostazioni predefinite di protezione dovrebbero formare parte integrante dei social media e degli altri servizi digitali. Ampliare e armonizzare le norme sulle funzioni di sicurezza essenziali apporterebbe certezza e uniformità all'intero ecosistema dei social media+. Dato il rapido sviluppo delle tecnologie è auspicabile che queste norme siano adattabili, in modo da tenere il passo con le nuove caratteristiche di progettazione deleterie.

- **Trasferire ai fornitori di social media e altri servizi digitali l'onere di dimostrare che i loro prodotti e servizi sono sicuri per i minori**

Fino a quando i fornitori di social media e altri servizi digitali non avranno introdotto funzioni di sicurezza essenziali nella progettazione, dovrebbero applicarsi restrizioni specifiche in funzione dell'età, e finché non avranno dimostrato di aver predisposto funzioni sicure e adatte all'età, conformandosi alle misure dell'UE e nazionali, non dovrebbero poter raggiungere il pubblico minorenni. Quando esiste una versione "sicura per impostazione predefinita", le funzioni non consone all'età (ossia quelle per adulti) dovrebbero essere attivate solo una volta ottenute garanzie effettive dell'età.

- **Rafforzare le capacità di applicazione delle norme e valutazione**

Vista la molteplicità di norme che oggi disciplinano la sicurezza dei minori online (regolamento sui servizi digitali, regolamento generale sulla protezione dei dati, regolamento sull'IA, eccetera), le autorità di vigilanza dovrebbero intensificare la cooperazione e lo scambio di informazioni fra i diversi quadri giuridici. Si tratta di un aspetto chiave per evitare incongruenze e garantire che il contesto giuridico sia radicato nella tutela dei diritti fondamentali e sia coerente, prevedibile ed efficace. La Commissione europea dovrebbe vagliare meccanismi che consentano una cooperazione agevole tra autorità di vigilanza per fare leva sulle strutture esistenti di applicazione delle norme. Occorre inoltre valutare se le autorità di regolamentazione responsabili dell'applicazione delle norme e della valutazione

necessitano di risorse supplementari e interventi di ristrutturazione. È opportuno prendere in considerazione azioni volte a rafforzare il ruolo della società civile nell'applicazione delle norme e il suo contributo all'aumento della capacità in tal senso, anche attraverso le strutture che già esistono. Le norme dovrebbero essere applicate all'insegna della complementarità, evitando azioni contrastanti.

- **Adottare rapidamente misure per assoggettare i fornitori di social media e altri servizi digitali a chiari obblighi di prevenire, individuare, segnalare e fermare gli abusi sessuali online sui minori, anche nelle comunicazioni interpersonali**

Bisogna colmare quanto prima le attuali lacune in materia di sicurezza dei minori dovute allo scadere del regolamento provvisorio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori; i legislatori dell'UE dovrebbero adottare con celerità la proposta di regolamento a lungo termine che lo sostituisce. Oltre l'80% delle indagini sugli abusi sessuali su minori prende avvio da segnalazioni dei fornitori di social media e altri servizi digitali: spesso i minori hanno troppa paura per denunciare e l'unico modo di fermare gli abusi è individuare il materiale pedopornografico, anche nelle comunicazioni interpersonali.

- **Gli Stati membri possono introdurre ulteriori restrizioni precauzionali di accesso ai social media e ad altri servizi digitali a partire dai 13 anni**

Le eventuali ulteriori restrizioni precauzionali di accesso dovrebbero essere complementari alla restrizione a livello dell'UE che preclude l'accesso ai social media e ad altri servizi digitali ai minori di 13 anni. Gli adolescenti possono accedere solo ad ambienti di social media+ sicuri in termini di contenuti e progettazione, adatti alla loro età e concepiti tenendo conto dei loro diritti e delle loro esigenze. Gli Stati membri, che hanno contesti storici e nazionali diversi, potrebbero voler optare per una soglia di età superiore ai 13 anni. Ogni restrizione precauzionale supplementare dell'accesso a livello nazionale dovrebbe essere oggetto di valutazione continua ed eventualmente di riesame quando i social media e gli altri servizi digitali saranno sicuri per impostazione predefinita per bambini e adolescenti.

- **Rafforzare l'applicazione delle norme in materia di accesso ai dati e controllo dei dati da parte dei ricercatori**

In linea di principio l'atto delegato adottato a luglio 2025 in applicazione dell'articolo 40 del regolamento sui servizi digitali ha aperto ai ricercatori abilitati una nuova possibilità di accedere ai dati delle piattaforme online che possono risultare utili per la ricerca che contribuisce al rilevamento, all'identificazione e alla

comprensione dei rischi sistemici nonché alla valutazione delle misure di attenuazione del rischio che promuovono la sicurezza dei minori online.

Perché la possibilità si concreti è necessario che i fornitori di social media e altri servizi digitali si conformino alle norme e che le autorità di regolamentazione le facciano effettivamente rispettare. I risultati dipendono inoltre dalla gamma di servizi coperti e dalla qualità e continuità dei dati forniti. La Commissione dovrebbe valutare l'efficacia operativa delle prescrizioni dell'articolo 40 in materia di accesso ai dati e controllo dei dati dopo le prime esperienze dei ricercatori a norma dell'atto delegato. Si tratta di un passaggio fondamentale per garantire che le piattaforme online diano seguito alle richieste di accesso ai dati a scopi di conformità, valutazione dei rischi e ricerca.

Gli obblighi relativi all'accesso ai dati non sono solo uno degli strumenti fondamentali di trasparenza offerti dal regolamento sui servizi digitali, bensì anche una delle più ampie responsabilità di attenuazione del rischio che incombono ai fornitori di social media e altri servizi digitali. Anche le piattaforme di dimensioni minori dovrebbero essere incoraggiate a consentire l'accesso dei ricercatori ai dati, considerati i rischi che esse pongono per i minori e il ruolo del controllo indipendente nell'affrontarli. L'uso dei principi guida FAIR<sup>4</sup> per la gestione etica dei dati scientifici dovrebbe essere la norma in sede di attuazione dell'articolo 40.

## Raccomandazioni per responsabilizzare bambini e adolescenti online

- **Creare più possibilità per i minori di contribuire a plasmare attivamente e in sicurezza l'ambiente dei social media+**

Bambini e adolescenti dovrebbero avere possibilità concrete di plasmare attivamente la legislazione, le politiche e le iniziative didattiche che ne promuovono la sicurezza e responsabilizzazione online. Dovrebbe essere ampliato il ricorso a strumenti partecipativi rivolti ai minori e ai giovani per contribuire ai lavori in tal senso: più nello specifico, i minori dovrebbero essere coinvolti nell'elaborazione di politiche, programmi di formazione, valutazioni e orientamenti sul tema della sicurezza. Le misure dovrebbero essere monitorate e valutate su base continuativa per analizzarne gli effetti sulla sicurezza e sui diritti dei minori.

I processi di partecipazione dovrebbero prevedere che i minori ricevano informazioni chiare, capiscano come saranno usati i loro contributi e abbiano un riscontro sui risultati raggiunti. Ci si dovrebbe adoperare in particolar modo per includere minori appartenenti a gruppi svantaggiati, emarginati e vulnerabili.

---

<sup>4</sup> Introdotti nel 2016 in un articolo pubblicato nella rivista *Scientific Data*, i principi guida FAIR per la gestione etica dei dati scientifici mirano a migliorare l'infrastruttura a sostegno del riutilizzo dei dati accademici rafforzando la capacità delle macchine e degli esseri umani di trovare e usare i dati. Cfr. Wilkinson, M.D., et al. (2016), "[The FAIR Guiding Principles for scientific data management and stewardship](#)", *Scientific Data* 3.

Tutte le attività partecipative che coinvolgono minori dovrebbero essere accompagnate dalle opportune misure di salvaguardia.

- **Consolidare i meccanismi di reclamo e i diritti dei consumatori a beneficio di bambini e adolescenti**

Le segnalazioni e i reclami di bambini e adolescenti dovrebbero avere la priorità nelle procedure di moderazione dei contenuti messe in atto dai fornitori di social media e altri servizi digitali. Gli obblighi dei fornitori a norma dei quadri vigenti dovrebbero essere rafforzati per finanziare adeguatamente le linee dirette di assistenza e i meccanismi di reclamo, che devono essere adeguati all'età, di facile utilizzo, accessibili, rispettosi della vita privata ed efficaci.

- **Incrementare al massimo la diffusione delle iniziative di educazione e alfabetizzazione digitali per minori, genitori e altri che si prendono cura di minori, insegnanti ed educatori**

L'educazione e l'alfabetizzazione digitali dovrebbero essere integrate a tutti i livelli di istruzione in quanto competenza fondamentale per minori, genitori e insegnanti. Il benessere digitale dovrebbe diventare parte integrante dell'educazione digitale per tutti.

L'educazione digitale dovrebbe dare ai bambini e agli adolescenti gli strumenti per valutare criticamente le informazioni e le fonti online e riconoscere le tecniche manipolative, tra cui disinformazione, deepfake e pubblicità mirata. Dovrebbe anche aiutare minori, genitori e insegnanti a capire come vengono creati e condivisi i contenuti digitali e come gli algoritmi determinano quello che gli utenti vedono e vivono nel mondo dei social media+.

Un'educazione strutturata alla sicurezza online dovrebbe sviluppare competenze pratiche di protezione dei dati personali, gestione delle impostazioni di riservatezza, mantenimento di identità digitali sicure e individuazione dei rischi sui social media, in particolare negli ambienti di messaggistica e gaming. Dovrebbe essere un processo graduale, che inizia dalle pratiche basilari di sicurezza per poi giungere alla comprensione di aspetti più complessi quali le tracce digitali, il consenso e i rischi delle piattaforme. Si dovrebbe coltivare un uso sano dello schermo mediante orientamenti sulla moderazione, sulla gestione dell'attenzione e sul modo in cui riconoscere abitudini di utilizzo eccessivo o dannoso.

- **Creare più opportunità e infrastrutture adeguate a sostegno delle attività offline**

Gli Stati membri e le autorità locali dovrebbero preservare e ampliare l'accesso a prezzi accessibili ad attività sportive e artistiche, associazioni giovanili, biblioteche

e spazi comunitari, così da incoraggiare una sana partecipazione alla vita offline e proporre ai minori alternative allettanti all'uso eccessivo dello schermo. Le iniziative in tal senso dovrebbero comprendere investimenti in ambienti sicuri, inclusivi e adatti all'età, in cui i minori possano incontrarsi, apprendere, giocare e costruire relazioni positive all'interno della propria comunità.

- **Promuovere l'elaborazione in comune di orientamenti rivolti ai genitori**

In collaborazione con le associazioni dei genitori, l'UE e gli Stati membri dovrebbero promuovere l'elaborazione di orientamenti contenenti consigli chiari e accessibili che consentano ai genitori di minori e a coloro che si prendono cura di minori di aiutarli a muoversi negli ambienti dei social media+ in modo sicuro, responsabile e partecipativo. Gli orientamenti dovrebbero dare indicazioni pratiche su tematiche fondamentali quali la sicurezza e la tutela della vita privata online, il benessere digitale, l'uso etico e responsabile e l'accesso al sostegno.

- **Garantire finanziamenti pubblici sufficienti e norme comuni per le organizzazioni della società civile e la consulenza tra pari**

L'UE e gli Stati membri dovrebbero garantire che i centri per un'internet più sicura e le organizzazioni comparabili della società civile continuino a ricevere risorse finanziarie sufficienti e che il loro operato si basi su norme comuni elaborate da esperti. Questo è essenziale perché proseguano e potenzino le loro attività, comprese quelle di sensibilizzazione e formazione e i servizi di sostegno. I finanziamenti pubblici sono cruciali per garantire indipendenza e coesione.

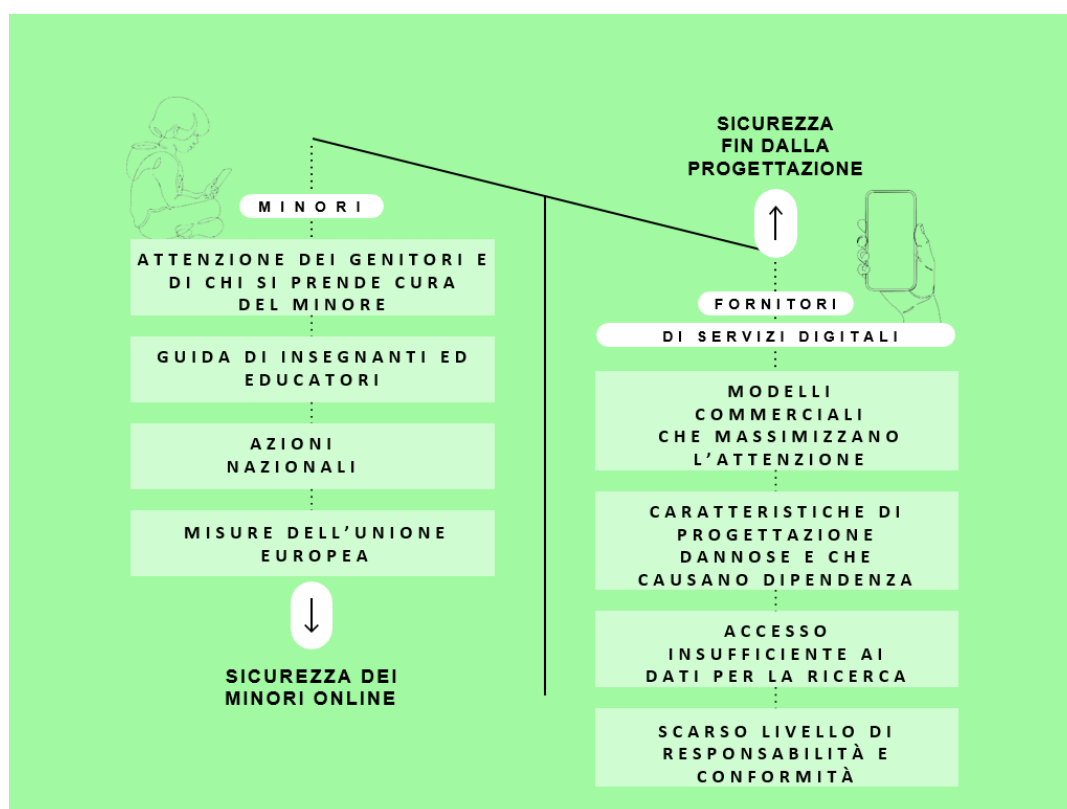
I fondi dovrebbero anche favorire l'ulteriore sviluppo della consulenza tra pari, delle linee dirette di assistenza e di emergenza, delle risorse didattiche, delle campagne di sensibilizzazione e delle attività di rafforzamento delle capacità. Investimenti supplementari dovrebbero essere destinati ad aumentare la visibilità, l'accessibilità e la diffusione di tali diversi strumenti, anche tra i minori vulnerabili, e a sostenere iniziative che promuovano ambienti dei social media+ più sicuri.

- **Mettere a disposizione finanziamenti a lungo termine per la ricerca longitudinale europea su larga scala e continuare a sostenere gli studi di controllo randomizzati**

Esempi come quello dello studio statunitense sullo sviluppo cognitivo del cervello in adolescenza (Adolescent Brain Cognitive Development – ABCD)<sup>5</sup> potrebbero servire da ispirazione per la ricerca longitudinale europea su larga scala relativa alla sicurezza dei minori online. Per un approccio imperniato sullo sviluppo e sulla neurobiologia è importante disporre di prove longitudinali europee su larga scala (riguardanti un periodo di dieci anni o più) che aiutino a colmare le lacune nei risultati, per lo più correlazionali, cui si è pervenuti nel contesto europeo in relazione all'impatto dell'uso dei social media e di altri servizi digitali sullo sviluppo e sulla salute psicofisica dei minori e sulla loro esposizione ai pericoli online.

Gli studi di controllo randomizzati sono un altro elemento cruciale per rafforzare la base di conoscenze funzionali alle politiche. I finanziamenti alla ricerca dovrebbero sostenere esplicitamente prospettive evolutive e psicopatologiche nello studio delle vulnerabilità dei minori ai rischi online, che sono influenzate da fattori sociali e personali nel corso dell'infanzia e dell'adolescenza.

**Figura 2. Bilanciare l'ecosistema: sicurezza fin dalla progettazione negli ambienti dei social media+**



<sup>5</sup> Lo studio ABCD, il più grande studio a lungo termine sullo sviluppo cerebrale e la salute dei minori negli Stati Uniti, sta seguendo oltre 11 000 bambini dall'età di 9-10 anni, durante l'adolescenza e fino alla giovane età adulta. I dati raccolti permetteranno di definire standard di riferimento per lo sviluppo cerebrale in adolescenza ed esaminare l'influenza di sesso, genere, igiene del sonno, attività fisica e tempo trascorso davanti allo schermo sullo sviluppo degli adolescenti. I risultati aiuteranno anche a comprendere l'insorgere di problemi di salute mentale durante l'adolescenza e la loro relazione con l'abuso di sostanze.

# Sicurezza online

## CONSIGLI PER BAMBINI E RAGAZZI



**Conosci i tuoi diritti:** ricorda che la sicurezza e il rispetto online sono un tuo diritto.



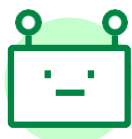
**Sii cortese:** i social e il gaming dovrebbero essere un'esperienza positiva per tutti. Tratta gli altri con lo stesso rispetto che vorresti ricevere.



**Pensa prima di postare:** foto, video e commenti possono rimanere online per sempre. Non condividere niente di cui potresti pentirti tra qualche anno.



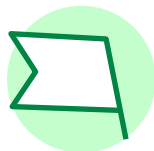
**Proteggi le tue informazioni personali:** non condividere online dettagli personali come nome e cognome, indirizzo, scuola, numero di telefono, password o posizione in tempo reale.



**Ricorda che l'IA è uno strumento, non una persona in carne e ossa:** può commettere errori e generare informazioni, immagini, video, voci e messaggi falsi.



**Verifica prima di fidarti o ricondividere:** non tutto quello che vedi online è vero. Chiediti sempre se le informazioni sono veritiere, soprattutto storie, video o messaggi sorprendenti, e controlla fonti attendibili prima di ricondividere.



**Riconosci i pericoli:** fermati un attimo a riflettere quando ricevi strane richieste da "amici di amici", offerte troppo allettanti per essere vere o messaggi che cercano di spingerti a prendere una decisione.



**Non accettare foto o richieste di chat da sconosciuti:** se hai dubbi sull'età o sull'identità di qualcuno, chiedi a un adulto di controllare chi sia (o rispondi che mamma/papà è lì con te e vedi qual è la reazione).



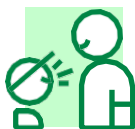
**Sfrutta le impostazioni di riservatezza e sicurezza:** mantieni privati i tuoi account, usa password robuste e, se sono disponibili, attiva sempre le funzioni di sicurezza aggiuntive.



**Non condividere immagini private:** non condividere mai foto o video intimi, anche se qualcuno ti mette pressione (soprattutto se hai meno di 18 anni). Una volta condivisi sono fuori dal tuo controllo.



**Blocca, segnala e salva le prove:** sei vittima di bullismo, truffe o minacce online, o qualcuno ti mette a disagio? Segnala, blocca e salva le schermate o i messaggi.



**Confidati con un adulto di fiducia se qualcosa ti turba:** non è una sciocchezza e non finirai nei guai per aver chiesto aiuto.



**Contribuisci a rendere la rete un posto più sicuro:** impara come funzionano le app, i giochi, i siti web, gli algoritmi e l'IA e aiuta anche gli altri a rimanere al sicuro.



**Fatti sentire:** scendi in campo e contribuisci a plasmare il futuro del mondo digitale.



# Sicurezza online

## CONSIGLI PER I GENITORI E PER CHI SI OCCUPA DI MINORI



**Aiuta bambini e ragazzi a coltivare abitudini sane davanti allo schermo.** Metti dei paletti: schermi vietati fino ai 2 anni e limiti di tempo consoni all'età per i bambini fino a 10-12 anni, sempre sotto la tua supervisione. Per gli adolescenti tra i 13 e i 18 anni si dovrebbero comunque discutere delle limitazioni, così che abbiano il tempo di studiare e vedere gli amici di persona.



**Verifica che le app e i giochi siano adeguati all'età** di chi li usa.



I bambini (fino a 12 anni) dovrebbero **usare console e device solo in presenza di un adulto.**



**I device non dovrebbero essere ammessi in bagno, in camera o a tavola.**



**Presta attenzione al tono delle conversazioni** online e durante le sessioni di gaming. Stai all'erta e riconosci i campanelli d'allarme.



**Prevedi di trascorrere del tempo online insieme:** chiedi ai bambini o ragazzi di guardare insieme i loro contenuti preferiti.



**Non criticare le "cose loro":** aiutali a sviluppare il senso critico (ti farai anche un'idea di che cosa propone loro l'algoritmo).



**Se online succede qualcosa che li preoccupa, incoraggiali a parlatene:** rassicurali che li aiuterai senza biasimarli, punirli o sequestrare il device.



**Continua a dialogare** sulla sicurezza online man mano che crescono, anche dai 16 ai 18 anni e oltre.



**Evita lo "sharenting":** rifletti bene prima di condividere online foto o video che ritraggono bambini o adolescenti. Possono essere usati in molti modi da estranei e dall'IA.



**Dai il buon esempio:** non stare incollato allo schermo quando sei con i tuoi figli o coi bambini o ragazzi di cui ti occupi. Dedica loro l'attenzione che meritano e non perderti momenti e conversazioni preziosi.



# Rassegna delle raccomandazioni dei copresidenti per capitolo

## Capitolo 1: un approccio evolutivo alla sicurezza dei minori online

1. Progettare e attuare misure di protezione dei minori online adeguate all'età.
2. Garantire spazi online sicuri per i minori.
3. Responsabilizzare i minori e le loro reti di sostegno.
4. (Fino ai 2 anni) Sensibilizzare chi si prende cura dei bambini riguardo all'importanza evolutiva dell'interazione umana diretta fin dalla prima infanzia.
5. (Fino ai 2 anni) Evitare l'uso di social media e altri servizi digitali e ridurre al minimo l'esposizione agli schermi, in particolare per i bambini al di sotto dei 3 anni.
6. (Fino ai 2 anni) Limitare la divulgazione dei dati dei bambini attraverso i profili social.
7. (Dai 3 ai 12 anni) Garantire che i bambini usino la rete in modo strutturato e controllato.
8. (Dai 3 ai 12 anni) Offrire ai bambini e alle loro reti di sostegno un'educazione di qualità sui temi del digitale e del benessere.
9. (Dai 13 ai 18 anni) Garantire che gli adolescenti usino la rete in modo via via più autonomo.

## Capitolo 2: dati concreti sui rischi cui sono esposti i minori online

10. Muovere dalle evidenze nei settori poco studiati per rafforzare l'elaborazione di politiche fondate su dati concreti.
11. I social media e gli altri servizi digitali dovrebbero coinvolgere attivamente esperti indipendenti del mondo accademico nella progettazione di strategie e strumenti di attenuazione del rischio.
12. Mettere a disposizione finanziamenti a lungo termine per la ricerca longitudinale europea su larga scala e continuare a sostenere gli studi di controllo randomizzati.
13. Investire in infrastrutture europee di ricerca sicure e condivise per consentire l'accesso in sicurezza ai dati dei minori.
14. Rafforzare l'applicazione delle norme in materia di accesso ai dati e controllo dei dati da parte dei ricercatori.

### **Capitolo 3: proteggere i minori in un ambiente dei social media+ in rapida evoluzione**

15. Proporre una restrizione di accesso ai social media e ad altri servizi digitali armonizzata a livello dell'UE per i minori di 13 anni.
16. Introdurre sistemi efficaci di garanzia dell'età per verificare questo dato, rendendo possibili approcci che puntino alla sicurezza fin dalla progettazione e siano calibrati in funzione dell'età per proteggere e responsabilizzare i minori online.
17. Ampliare e armonizzare le norme sulle funzioni di sicurezza essenziali nella progettazione dei social media e degli altri servizi digitali.
18. Trasferire ai fornitori di social media e altri servizi digitali l'onere di dimostrare che i loro prodotti e servizi sono sicuri per i minori.
19. Rafforzare le capacità di applicazione delle norme e valutazione.
20. Adottare rapidamente misure per assoggettare i fornitori di social media e altri servizi digitali a chiari obblighi di prevenire, individuare, segnalare e fermare gli abusi sessuali online sui minori, anche nelle comunicazioni interpersonali.
21. Gli Stati membri possono introdurre ulteriori restrizioni precauzionali di accesso ai social media e ad altri servizi digitali a partire dai 13 anni.
22. Rafforzare le politiche di tutela dei consumatori per proteggere i minori online.
23. Monitorare e valutare su base continuativa gli effetti delle misure attuate.
24. Quando trattano i dati dei minori ai sensi del regolamento generale sulla protezione dei dati, i social media e gli altri servizi digitali dovrebbero far sì che l'interesse superiore del minore sia una considerazione preminente.
25. Garantire l'effettiva attuazione della direttiva sulla responsabilità per danno da prodotti difettosi.

### **Capitolo 4: responsabilizzare i minori perché possano navigare in sicurezza nel mondo digitale**

26. Creare più possibilità per i minori di contribuire a plasmare attivamente e in sicurezza l'ambiente dei social media+.
27. Rafforzare i meccanismi di reclamo e i diritti dei consumatori a beneficio di bambini e adolescenti.
28. Finanziare e promuovere la creazione e l'uso di social media e altri servizi digitali basati sui valori dell'UE in cui i minori possano interagire in modo sicuro coi coetanei.
29. Incrementare al massimo la diffusione delle iniziative di educazione e alfabetizzazione digitali per minori, genitori e altri che si prendono cura di minori, insegnanti ed educatori.

30. Creare più opportunità e infrastrutture adeguate a sostegno delle attività offline.
31. Promuovere l'elaborazione in comune di orientamenti rivolti ai genitori.
32. Garantire che i genitori e coloro che si prendono cura di minori possano sempre contare su strumenti di controllo e supervisione aggiornati e allo stato dell'arte.
33. Garantire finanziamenti pubblici sufficienti e norme comuni per le organizzazioni della società civile e la consulenza tra pari.
34. Mettere il sistema sanitario nelle condizioni di diagnosticare e trattare le dipendenze e altri disturbi mentali connessi all'uso dei social media e di altri servizi digitali.
35. Sostenere l'inclusione dell'alfabetizzazione digitale e mediatica nella formazione degli insegnanti e coinvolgere i genitori.
36. Promuovere l'alfabetizzazione in materia di IA come parte integrante dell'educazione digitale.
37. Le scuole dovrebbero offrire opportunità strutturate per migliorare la salute mentale e il benessere digitale.
38. Le risposte incentrate sull'istruzione dovrebbero prestare particolare attenzione ai gruppi vulnerabili.
39. Investire in infrastrutture didattiche digitali sicure, precauzionali, solide e affidabili.

## Note finali – Prefazione

---

<sup>i</sup> Commissione europea (2026). [Digital decade – Eurobarometer report \(febbraio - marzo 2026\)](#).

<sup>ii</sup> Presidenza danese, Consiglio dell'Unione europea (2026). [Dichiarazione dello Jutland sulla costruzione di un mondo online sicuro per i minori](#).

<sup>iii</sup> Parlamento europeo (2025). [Protezione dei minori online – Risoluzione del Parlamento europeo del 26 novembre 2025 sulla protezione dei minori online \(2025/2060\(INI\)\)](#).

<sup>iv</sup> Consiglio europeo (2026). [Conclusioni del Consiglio europeo](#), 19 marzo 2026.

<sup>v</sup> G7 (2026). [Leaders' call on a safer digital space for minors](#).

<sup>vi</sup> Children's Hospital of Philadelphia (2026), [Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study](#), consultato il 12 luglio 2026.