I minori nella società digitale tra verifica dell'età, deepfake e disinformazione. Alcune considerazioni informatico-giuridiche

Minors in the Digital Society: Age Verification, Deepfakes, and Disinformation. Some Considerations on Law and Informatics

Giovanni Ziccardi[1]

Sommario

L'articolo affronta il tema della tutela dei minori nella società digitale, con particolare attenzione ai sistemi di verifica dell'età, al fenomeno dei deepfake, all'esposizione alla disinformazione e all'utilizzo di chatbot e intelligenze artificiali. L'obiettivo è individuare criticità normative, tecniche e sociali, proponendo una risposta integrata che tuteli i diritti dei minori senza pregiudicare quelli degli altri utenti.

L'analisi impiega un approccio informatico-giuridico multidisciplinare, esaminando fonti normative europee e italiane (tra cui GDPR, Digital Services Act, regolamenti AGCOM), documenti dell'EDPB, e casi concreti (TikTok, Replika, Europol-Cumberland). Il contributo integra riflessioni teoriche con esempi pratici, attingendo anche da ambiti educativi, psicologici e tecnologici. L'approccio è sia descrittivo che propositivo.

L'articolo propone un approccio sistemico alla protezione dei minori online, articolato su tre assi: normativo, tecnologico ed educativo. Sul piano normativo, si suggerisce di rafforzare gli obblighi di age verification, aggiornare le definizioni di contenuti vietati e armonizzare le sanzioni. Dal punto di vista tecnologico, si auspica la progettazione di sistemi "privacy-by-design" e trasparenza algoritmica. Infine, l'educazione critica ai media e alla realtà digitale deve essere potenziata nelle scuole e nelle famiglie. Il coinvolgimento di tutti gli stakeholder – istituzioni, piattaforme, educatori, genitori – è essenziale per creare un ambiente digitale equo e sicuro per le nuove generazioni.

Parole chiave: verifica dell'età; tutela dei minori; disinformazione digitale; deepfake; intelligenza artificiale generativa

1 Dipartimento di Scienze Giuridiche "Cesare Beccaria", Università degli Studi di Milano. giovanni.ziccardi@unimi.it

Data invio: 1 luglio 2025. Data accettazione: 3 settembre 2025.
DOI: https://doi.org/10.54103/1972-5760/30050

Abstract

This article addresses the protection of minors in the digital society, focusing on age verification systems, deepfakes, exposure to disinformation, chatbots, and AI tools. The aim is to identify legal, technological, and social challenges, proposing an integrated response that safeguards minors' rights without undermining thoseof other users.

The analysis adopts a multidisciplinary legal and informatics approach, examining European and Italian legal sources (including GDPR, Digital Services Act, AGCOM regulations), EDPB documents, and case studies (TikTok, Replika, Europol's Operation Cumberland). The article combines theoretical reflections with practical examples, drawing from educational, psychological, and technological domains, using both descriptive and normative arguments.

This contribution advocates for a systemic approach to online minor protection, structured around three dimensions: regulatory, technological, and educational. on the regulatory level, the article recommends strengthening age verification requirements, updating legal definitions of prohibited contents, and ensuring consistent enforcement. Technologically, it calls for the implementation of "privacy by design" solutions and algorithmic transparency. Finally, critical digital and media literacy education must be promoted in schools and families. The involvement of all stakeholders – public authorities, tech companies, educators, and families – is key to foster a fair and safe digital environment for younger generations.

Keywords: age verification; child protection; digital disinformation; deepfake; generative artificial intelligence

1. Introduzione: il nodo centrale della verifica dell'età e gli evidenti limiti delle normative esistenti

Il delicato tema della tutela dei minori online deve inevitabilmente fare i conti con la capacità concreta (e realistica) di controllarne l'accesso ai servizi digitali in base all'età (Li 2025; Pasquale *et al*. 2022). Si tratta di un argomento "storico" dell'informatica giuridica che non presenta unicamente aspetti legali e tecnologici ma, anche, psicologici ed educativi (Pesci 2024; Ghiglia 2023). Questo problema ha sollevato, negli ultimi quindici anni, un acceso dibattito a livello mondiale, soprattutto con riferimento alla sempre maggiore disponibilità di contenuti pornografici e violenti (facilmente) accessibili ai minori (Stardust *et al.* 2024; Yar 2020; Blake 2019).

Attualmente, sia la normativa europea sia quella italiana fissano specifiche soglie di età per l'uso lecito dei dati personali dei minori nei servizi della società dell'informazione (Murgo 2024) e hanno, da tempo, elaborato l'idea

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

di una *privacy del minore* persino nel contesto familiare e nei confronti delle ingerenze dei genitori (Garaci 2023).

L'art. 8 del Regolamento europeo sulla protezione dei dati del 2016 (d'ora in avanti: GDPR), in particolare, stabilisce in linea generale come il trattamento dei dati di un minore sia lecito solo a partire dai 16 anni. Ha però consentito agli Stati membri di abbassare tale soglia fino a un minimo di 13 anni, con un approccio che ha destato interesse, e dubbi, anche al di fuori dall'Unione Europea (Caggiano 2022).

L'Italia, attraverso il d.lgs. 101/2018 (di adeguamento della normativa nazionale al GDPR), ha fissato il limite a 14 anni, richiedendo sotto tale limite di età il consenso di chi esercita la responsabilità genitoriale (art. 2-*quinquies* del D.lgs. 196 del 2003).

Ne consegue che, formalmente, nel nostro ordinamento un minore di 14 anni *non potrebbe* attivare autonomamente un account sui social network o, comunque, fruire di servizi online che implichino il trattamento dei suoi dati personali (Savonardo, Marino 2021).

Al contempo, questa fissazione di soglia di età ai 14 anni è stata vista dalla politica italiana come una sorta di *segnale di fiducia* e di responsabilizzazione verso i minori online e verso i gestori delle piattaforme (Macenaite, Kosta 2017), muovendo però dalla premessa di una maturità tecnologica, nel nostro Paese, che in molti contesti è ancora ben lontana da raggiungere.

Le principali piattaforme globali, dal canto loro, prevedono nei termini di servizio un'età minima di 13 anni per l'iscrizione, in coerenza con le normative internazionali (anche nordamericane) e con il limite-base del GDPR (Talley 2021).

In teoria, quindi, bambini e preadolescenti dovrebbero restare *esclusi* dai social network e da molte altre piattaforme fino alla soglia dell'adolescenza avanzata. In pratica, tuttavia, questi divieti d'accesso per età risultano facilmente *aggirabili* e la loro efficacia è a dir poco limitata (Biolcati *et al.* 2016).

Si pensi che, nella maggior parte dei casi, la modalità standard di verifica dell'età in fase d'iscrizione si riduce a una *autodichiarazione dell'utente* (la classica selezione della data di nascita), meccanismo che un minore può falsificare senza difficoltà.

Non sorprende, dunque, che la realtà fotografi numeri ben diversi da quelli attesi per legge: la gran maggioranza dei preadolescenti europei (11-13 anni) ha già almeno un profilo social attivo, e molti di essi ne possiede più di uno.

La mancanza di meccanismi efficaci di *age verification* vanifica dunque, nei fatti, la tutela normativa, lasciando schiere di under-14 liberi di creare account mentendo sulla loro età e di muoversi in ambienti virtuali concepiti per utenti più grandi (Nagel 2011).

Questo quadro è ovviamente assai frustrante sia per il legislatore sia per l'interprete nel momento in cui cercano di impostare un ragionamento coerente, e costruttivo, sui minori online e sulle loro attività.

Milioni di bambini, in tutta Europa, semplicemente non dovrebbero essere, per legge, su queste piattaforme. Ma ci sono, condividono i loro dati e, anzi, sono i profili più interessanti per le piattaforme e per i loro contenuti. Non sono solo gli elettori del futuro ma, anche e soprattutto, i più vivaci *consumatori* del presente (Slavtcheva-Petkova 2023).

2. Il Comitato europeo per la protezione dei dati (EDPB) e lo "Statement 1/2025 on Age Assurance"

Negli ultimi anni, questa crescente esposizione dei minori a rischi digitali (Biolcati 2010) ha generato un'intensificazione dell'interesse normativo e regolamentare nei confronti della verifica dell'età come principale strumento di protezione.

Questa tendenza ha preso corpo in una serie di atti giuridici a livello di Unione europea che attribuiscono alla verifica dell'età una funzione strategica nella costruzione di ambienti digitali sicuri, pur senza trascurare il rischio che tali strumenti possano trasformarsi in vettori di sorveglianza generalizzata, discriminazione o profilazione indebita (Frigato 202; Zuboff 2019).

A fronte di questo scenario, l'11 febbraio 2025 il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato la Dichiarazione 1/2025, documento che rappresenta un passo significativo nel delineare principi-guida per un sistema di *age assurance* conforme al GDPR, in grado di garantire una tutela efficace dei minori senza compromettere i diritti e le libertà degli individui, in particolare il diritto alla protezione dei dati personali.

La verifica dell'età, secondo l'impostazione dell'EDPB, non può essere considerata una mera misura tecnica né, tantomeno, una formalità amministrativa. Essa implica una *scelta normativa profonda*, poiché impatta su molteplici diritti fondamentali: dalla privacy alla libertà di espressione, dall'accesso all'informazione al diritto alla non discriminazione. È quindi essenziale che la sua progettazione rispetti un *principio di equilibrio* tra tutela e proporzionalità, soprattutto quando riguarda soggetti vulnerabili come i minori.

Il quadro giuridico europeo offre oggi, a onor del vero, diverse basi normative per l'implementazione di sistemi di verifica dell'età.

La Direttiva 2018/1808/UE sui servizi di media audiovisivi, in primis, prevede l'adozione di misure atte a proteggere i minori dai contenuti dannosi, mentre il Digital Services Act (Reg. UE 2022/2065) considera la verifica dell'età uno strumento utile per adempiere agli obblighi di valutazione e mitigazione dei rischi sistemici da parte delle grandi piattaforme. Il GDPR,

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

infine – si è visto poco sopra – introduce un requisito di età minima per la validità del consenso dei minori ai servizi digitali (art. 8), stabilendo così un nodo giuridico essenziale tra verifica dell'età e legittimità del trattamento dei dati personali.

Ma il vero nucleo problematico risiede nella conciliazione tra la protezione dei minori e il rispetto dei diritti degli interessati.

L'EDPB ribadisce che, nell'ambito della verifica dell'età, l'interesse superiore del minore – principio cardine della Convenzione ONU sui diritti dell'infanzia – deve essere sempre una considerazione primaria. Tuttavia, ciò non implica che altri diritti possano essere compressi arbitrariamente: il trattamento dei dati personali per fini di verifica dell'età deve essere sempre necessario, proporzionato e fondato su una solida base giuridica.

È su questo punto che l'EDPB sviluppa una riflessione centrale: l'importanza della *valutazione del rischio*, che deve guidare l'intero ciclo di vita del sistema di verifica.

La dichiarazione raccomanda esplicitamente l'adozione di Data Protection Impact Assessments (DPIA) nei casi in cui il trattamento comporti rischi elevati per i diritti e le libertà degli interessati. Ancora più rilevante, nel contesto specifico dei minori, è l'adozione di valutazioni dell'impatto sui diritti dell'infanzia (Child Rights Impact Assessments – CRIA), in grado di integrare l'ottica della tutela evolutiva e della partecipazione dei minori stessi alla progettazione dell'ambiente digitale.

Sul piano tecnico, viene poi (inevitabilmente) ribadito il principio di *minimizzazione* dei dati: ogni sistema di verifica dell'età deve limitarsi al trattamento dei soli dati strettamente necessari per l'obiettivo specifico.

Nella maggior parte dei casi non è necessario conoscere l'identità dell'utente, ma solo se questi ha superato una determinata soglia d'età. Soluzioni come i *token di età*, rilasciati da un soggetto terzo e contenenti esclusivamente l'informazione "sì/no" rispetto alla soglia richiesta, rappresentano esempi virtuosi di privacy-enhancing technologies (PETs), ossia approcci tecnici che consentono di ridurre il rischio di re-identificazione e profiling, favorendo la non riferibilità tra dati e servizi.

Il principio di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 GDPR) assume, in questo contesto, un rilievo cruciale.

L'EDPB sottolinea la necessità di adottare architetture decentralizzate, sistemi locali di verifica e strumenti crittografici avanzati, come le "prove a conoscenza zero" (*zero-knowledge proofs*), che permettono di dimostrare il possesso di un'informazione (ad es. avere più di 18 anni) senza rivelare *alcun dato personale aggiuntivo*. Tali strumenti dovrebbero essere adottati come standard tecnologici per tutti i casi in cui l'accesso a determinati contenuti o servizi dipenda dall'età dell'utente.

Un altro aspetto fortemente valorizzato è quello dell'efficacia del sistema di verifica. L'EDPB richiama l'attenzione sul fatto che molte delle tecnologie attualmente in uso – in particolare l'autodichiarazione – risultano del tutto *inefficaci*, poiché facilmente eludibili e prive di meccanismi di controllo.

È quindi necessario che i metodi adottati siano in grado di fornire un livello di accuratezza, affidabilità e robustezza adeguato allo scopo. Inoltre, le soluzioni adottate devono essere *accessibili* a tutti gli utenti, evitando discriminazioni tecnologiche o economiche, ad esempio verso chi non possiede documenti digitali, strumenti biometrici o connessioni stabili (Carr 2025).

La *trasparenza* è un ulteriore pilastro: gli utenti, e in particolare i minori, devono essere informati in modo chiaro e comprensibile circa i dati trattati, le finalità, le modalità di trattamento, gli eventuali soggetti terzi coinvolti e i diritti esercitabili.

Il rispetto degli obblighi informativi previsti dagli articoli 12-14 del GDPR non può essere considerato meramente formale: è una condizione sostanziale di liceità e correttezza del trattamento.

Particolare cautela è richiesta anche nei confronti dei processi decisionali automatizzati. L'EDPB ricorda che, salvo casi eccezionali, il GDPR vieta il ricorso a decisioni automatizzate che producano effetti giuridici su soggetti minori.

Qualora si faccia uso di tecniche automatizzate nella determinazione dell'età, devono essere garantiti *interventi umani* significativi, meccanismi di ricorso efficaci e modalità comprensibili per esercitare i diritti dell'interessato. Il rischio, altrimenti, è quello di sottrarre il minore a forme effettive di tutela, producendo esclusione o discriminazione algoritmica.

Dal punto di vista della sicurezza, il trattamento dei dati per la verifica dell'età deve essere accompagnato da misure tecniche e organizzative proporzionate al rischio. Tecniche di pseudonimizzazione, crittografia, conservazione limitata e politiche di non registrazione sono considerate fondamentali. L'EDPB sottolinea come i modelli di fiducia e i sistemi a basso grado di interdipendenza tra fornitori siano essenziali per garantire la resilienza del sistema anche in caso di violazione dei dati.

Infine, l'intero processo deve essere sorretto da un solido quadro di responsabilità ("accountability"). I titolari del trattamento e le terze parti coinvolte devono poter dimostrare – attraverso documentazione, audit, controlli e sistemi di governance – che ogni fase della verifica dell'età sia conforme alle normative sulla protezione dei dati. La trasparenza del sistema non è solo una garanzia per l'utente ma, anche, un presupposto per la legittimità stessa dell'intervento regolatorio.

L'approccio dell'EDPB, che abbiamo analizzato per primo proprio perché si fonda su una visione bilanciata e sul rigoroso rispetto dei principi del GDPR, offre una cornice utile non solo per il legislatore europeo e nazionale ma, anche, per i progettisti di sistemi, i responsabili del trattamen-

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

to e gli operatori delle piattaforme digitali. Solo attraverso l'integrazione consapevole dei diritti nella progettazione tecnica sarà possibile costruire un ecosistema digitale realmente sicuro, inclusivo e rispettoso della dignità delle persone.

3. Il regolamento AGCOM

Nel panorama normativo italiano, il 2025 ha segnato un passaggio particolarmente significativo in materia di tutela dei minori online con l'adozione di un Regolamento da parte dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM) che impone, per la prima volta in modo organico, l'utilizzo *obbligatorio* di sistemi di verifica dell'età *certificati da terze parti* per l'accesso a contenuti vietati ai minori di diciotto anni.

Il provvedimento si rivolge esplicitamente a siti web e piattaforme digitali che offrono contenuti a rischio per l'integrità psicofisica dei minori, come nel caso della pornografia online, del gioco d'azzardo, della rappresentazione esplicita di violenza o di prodotti potenzialmente nocivi.

In questo senso, il Regolamento AGCOM recepisce e rafforza – sul piano dell'attuazione nazionale – quanto delineato a livello europeo dal Digital Services Act e dal GDPR, collocandosi in un quadro più ampio di armonizzazione degli standard di sicurezza e responsabilità digitale.

L'elemento di maggiore novità introdotto dal Regolamento italiano riguarda l'obbligo, per i fornitori di contenuti classificati come *vietati ai minori*, di integrare sistemi di verifica dell'età robusti e certificati da *soggetti terzi qualificati*, che siano indipendenti sia dal fornitore stesso che dai gestori delle piattaforme di hosting.

Questa misura non solo eleva il livello di affidabilità tecnica dei controlli, ma rappresenta anche un *cambio di paradigma* rispetto alla prassi diffusa dell'autodichiarazione, ritenuta ampiamente insufficiente per garantire una reale protezione dei minori. La certificazione ha una funzione non solo tecnica ma, anche, giuridica: vincola i fornitori all'adozione di standard interoperabili, documentati, soggetti a verifica periodica e conformi ai principi di trasparenza, proporzionalità e sicurezza imposti dal GDPR.

Dal punto di vista tecnologico, il Regolamento apre alla possibilità di impiegare diverse soluzioni di *age verification*, a condizione che esse rispondano a criteri stringenti di efficacia, privacy e inclusività.

Tra le tecnologie ammesse figurano, ad esempio, sistemi basati su credenziali digitali firmate, in cui un'identità "pre-verificata" (da un provider pubblico o privato) attesta il superamento di una soglia d'età attraverso un token crittografico non tracciabile che può essere verificato dal sito di destinazione senza esporre ulteriori dati dell'utente. Una variante di questo modello prevede l'utilizzo di "zero-knowledge proofs" (ZKP), che permettono

a un soggetto di dimostrare di possedere un attributo (ad esempio "ho più di 18 anni") senza rivelare alcuna informazione ulteriore, inclusa l'età esatta o l'identità personale.

Un altro modello considerato idoneo, anche se più invasivo, è rappresentato dalle *verifiche documentali con riconoscimento automatizzato*, che prevedono il caricamento di un documento d'identità e l'utilizzo di tecnologie biometriche per il confronto facciale (Bianda 2019).

Sebbene queste soluzioni offrano un alto grado di affidabilità nella verifica dell'identità e dell'età, esse pongono serie criticità in termini di proporzionalità, minimizzazione dei dati e rischio di violazioni della sicurezza, specialmente se non accompagnate da politiche rigorose di conservazione e separazione dei dati. Per questo motivo, il Regolamento AGCOM richiede esplicitamente che i sistemi utilizzati *non conservino* dati sensibili oltre il tempo strettamente necessario alla verifica e che adottino misure di pseudonimizzazione, cancellazione automatica e crittografia end-to-end.

Un aspetto di rilievo, spesso sottovalutato, riguarda inoltre l'inclusività e l'accessibilità delle tecnologie di verifica. Il Regolamento prevede che i sistemi adottati non debbano escludere o discriminare soggetti privi di documentazione digitale, minorenni emancipati o appartenenti a categorie vulnerabili. In tale ottica, viene incoraggiata l'adozione di *metodi alternativi*, come la verifica tramite intermediari accreditati (ad es. fornitori di identità digitale, enti pubblici, istituti scolastici), che possano attestare l'età dell'utente senza obbligarlo a fornire direttamente documenti o dati biometrici. Questa apertura metodologica dimostra una sensibilità verso il principio di *equità tecnologica*, evitando che la protezione dei minori si traduca, nei fatti, in una nuova forma di digital divide.

Dal punto di vista giuridico, il Regolamento si fonda su un sistema sanzionatorio e di *enforcement progressivo*, che prevede l'intervento dell'AGCOM in caso di mancato adeguamento, fino al blocco dell'accesso al sito mediante provvedimenti di inibizione tecnica (*DNS/IP blocking*). Viene inoltre introdotto un *registro pubblico* dei fornitori conformi, che può svolgere un ruolo di trasparenza e responsabilizzazione verso gli utenti ma, anche, di competizione regolatoria virtuosa tra le piattaforme digitali.

4. Il caso TikTok

Un caso emblematico che ha tragicamente messo in luce le falle strutturali nei sistemi di verifica dell'età e le carenze normative nella protezione dei minori online è quello c che ha riguardato una bambina di 10 anni deceduta a Palermo nel gennaio 2021, mentre partecipava a una pericolosa sfida virale – la cosiddetta *blackout challenge* – diffusa su TikTok. L'evento ebbe un forte impatto sull'opinione pubblica e segnò un punto di svolta anche

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

nell'approccio delle autorità italiane nei confronti delle piattaforme digitali, sollevando interrogativi urgenti sulla responsabilità delle big tech nella tutela dei soggetti vulnerabili (Cantero Gamito 2023).

L'immediatezza dell'intervento del Garante per la protezione dei dati personali fu senza precedenti: l'Autorità dispose con urgenza il *blocco* dell'uso della piattaforma per tutti gli utenti italiani per i quali non fosse stata verificata con certezza l'età anagrafica, ponendo così una delle prime limitazioni effettive all'attività di una grande piattaforma internazionale per motivi legati alla protezione dei minori.

L'istruttoria condotta mise rapidamente in evidenza l'inefficacia del sistema di *age verification* adottato da TikTok all'epoca, che consentiva l'iscrizione con estrema facilità e senza alcuna forma di verifica attendibile: bastava indicare una data di nascita fittizia per accedere a tutte le funzionalità, anche in assenza di qualsiasi supervisione genitoriale.

A rendere ancora più grave il quadro era la configurazione predefinita dei profili, che risultavano *automaticamente pubblici*, esponendo così utenti anche molto giovani a forme incontrollate di visibilità e interazione con estranei.

Questa scelta di design, lungi dall'essere neutrale, rifletteva un'impostazione orientata alla massima condivisione e interazione sociale, in linea con la logica di *engagement* tipica delle piattaforme, ma in aperto contrasto con i principi di "privacy by default" richiesti dall'articolo 25 del GDPR.

In assenza di adeguate protezioni o meccanismi di parental control, i minori venivano resi visibili, raggiungibili e, in alcuni casi, strumentalizzabili senza che né loro né le famiglie ne fossero realmente consapevoli.

L'intervento del Garante, in quel contesto, assunse un valore esemplare non solo sotto il profilo sanzionatorio ma, allo stesso tempo, come segnale politico e normativo.

L'Autorità richiamò esplicitamente TikTok ai suoi doveri di conformità rispetto all'art. 8 del GDPR – che prevede, per i minori di 14 anni in Italia, il necessario consenso dei titolari della responsabilità genitoriale per il trattamento dei dati – oltre che alle norme italiane in materia di protezione dei minori e ai principi generali di sicurezza dei servizi digitali.

Tuttavia, il Garante non si limitò a un'interpretazione formalistica del quadro normativo: in una nota pubblica, il presidente Pasquale Stanzione sottolineò che "il Garante può bloccare i social, ma il primo controllore è il genitore", evidenziando così la corresponsabilità familiare nel processo di tutela e la necessità di una vigilanza attiva che vada oltre le soluzioni puramente tecnologiche.

Tuttavia, quanto emerso nel caso TikTok rivela una tensione strutturale tuttora irrisolta tra la *law in the books* e la *law in action*.

Da un lato, il diritto europeo e italiano dispongono principi avanzati, come l'obbligo di consenso informato, la protezione rafforzata dei dati dei mino-

ri e la progettazione per default della privacy; dall'altro, mancano strumenti sanzionatori efficaci, meccanismi di verifica interoperabili e standard tecnici comuni a livello sovranazionale. Non esiste, ad esempio, un sistema di *certificazione* europeo per i metodi di verifica dell'età, né una disciplina condivisa che imponga livelli minimi di affidabilità o inclusività nei sistemi adottati dalle piattaforme. Questa asimmetria tra doveri normativi e strumenti tecnici lascia ampi margini di discrezionalità alle imprese, che spesso adottano soluzioni simboliche e facilmente aggirabili, con effetti potenzialmente nocivi.

Sotto il profilo tecnologico, il caso solleva ulteriori criticità. Il meccanismo di *age verification* implementato da TikTok – basato, nella sostanza, sull'autodichiarazione priva di qualsiasi validazione – rappresenta una delle soluzioni meno affidabili disponibili. Non solo è tecnicamente inadeguato, ma è anche in contrasto con le linee guida europee, che mettono in guardia proprio contro i metodi di verifica che si fondano unicamente sulla buona fede dell'utente, specie quando questi è un soggetto vulnerabile. A distanza di anni, molte piattaforme continuano a utilizzare simili modelli, eludendo l'obbligo di dimostrare la proporzionalità, l'efficacia e la non discriminazione dei sistemi di controllo adottati.

Alla luce di questi elementi, appare evidente l'urgenza di un intervento *multilivello*, capace di combinare regolazione normativa, standard tecnici e strumenti di *enforcement* efficaci.

Le autorità garanti nazionali e sovranazionali dovrebbero essere dotate di poteri adeguati non solo per sanzionare ma, anche, per prescrivere concretamente modelli di progettazione responsabile, in linea con i principi di "data protection by design and by default". Allo stesso tempo, è indispensabile coinvolgere l'industria in forme di co-regolamentazione e autoregolazione tecnologica affinché siano adottate soluzioni scalabili, interoperabili e rispettose dei diritti fondamentali.

Il caso TikTok rappresenta dunque molto più di un tragico episodio isolato: è uno specchio dei *limiti sistemici* dell'ecosistema digitale contemporaneo, in cui il diritto, la tecnica e, soprattutto, l'etica faticano ancora a dialogare in modo efficace (Scalzaretto 2023).

Solo attraverso una convergenza più stretta tra norme giuridiche, progettazione tecnica e responsabilità sociale sarà possibile evitare che simili tragedie si ripetano e costruire davvero un ambiente digitale a misura di minore.

5. Il caso Replika: chatbot e minori esposti a contenuti inappropriati

L'evoluzione recente dell'intelligenza artificiale generativa ha aperto nuovi scenari anche rispetto alla fruizione digitale dei contenuti da parte dei minori.

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

Un episodio paradigmatico è rappresentato dalla vicenda di Replika, un popolare chatbot basato su intelligenza artificiale creato dalla startup statunitense Luka Inc.

Lanciato nel 2017, Replika si presenta come un "amico virtuale" personalizzabile, capace di conversare in modo realistico con l'utente simulando empatia e sostegno emotivo.

La promessa di un avatar mosso dall'intelligenza artificiale in grado di migliorare il benessere emotivo ha attratto milioni di utenti nel mondo, inclusi molti giovani; tuttavia, dietro l'apparenza rassicurante, sono emerse gradualmente zone d'ombra che hanno allertato le autorità.

In assenza di adeguati filtri, minorenni anche molto giovani potevano scaricare e utilizzare Replika liberamente, entrando in dialogo con l'intelligenza artificiale senza alcuna supervisione né controllo sull'appropriatezza dei contenuti.

Già a inizio 2023 si erano registrati i primi casi di interazioni inquietanti: alcuni utenti – spesso fragili o poco più che adolescenti – hanno denunciato vere e proprie molestie sessuali virtuali da parte del chatbot.

Replika, sfruttando le capacità generative del suo modello linguistico, era in grado di assumere toni romantici ed erotici "spinti" nelle conversazioni, fino a simulare scenari espliciti inadatti a un pubblico minorenne.

Di fatto esistevano due versioni: una gratuita "amichevole" e una a pagamento con contenuti romantici/erotici più avanzati. Nessun vero ostacolo impediva a un utente minorenne di accedere a quest'ultima, dal momento che l'app non prevedeva alcuna verifica effettiva dell'età all'iscrizione o durante l'uso.

Il servizio dichiarava nelle policy di essere vietato ai minori, ma tale divieto restava lettera morta, affidato unicamente all'onere degli utenti di dichiararsi maggiorenni.

Di fronte a questa situazione, l'Autorità Garante italiana è intervenuta con decisione. Nel febbraio 2023, a tutela urgente, ha ordinato la sospensione di Replika nel territorio nazionale, motivandola con i rischi specifici per i minori derivanti dal chatbot. L'indagine istruttoria che ne è seguita ha confermato diverse violazioni gravi: Replika non disponeva di una base giuridica valida per trattare i dati personali degli utenti europei, forniva un'informativa privacy inadeguata e – ciò che qui più rileva – era totalmente privo di sistemi per *escludere* l'accesso dei bambini al servizio.

In altri termini, l'azienda non aveva né verifiche dell'età né filtri sui contenuti generati dall'intelligenza artificiale in presenza di utenti minorenni.

Neppure dopo il blocco iniziale la società ha saputo porre rimedio a queste carenze, il che ha condotto nel 2025 all'esito sanzionatorio: il Garante ha irrogato a Luka Inc. una multa di 5 milioni di euro, accertando formalmente la violazione dei principi del GDPR e del diritto italiano.

Come ribadito nel provvedimento finale, la posizione del gestore era aggravata proprio dall'assenza di meccanismi di verifica dell'età, che ha consentito ai minori di usare un servizio potenzialmente pericoloso e non tarato per loro.

Contestualmente, l'Autorità ha aperto una nuova indagine sull'algoritmo di intelligenza artificiale generativa di Replika, per esaminarne i dati di addestramento e la conformità alle regole europee (un tema legato alla privacy e alla sicurezza generale del sistema).

Il caso Replika evidenzia emblematicamente le insidie che le applicazioni di intelligenza artificiale conversazionale possono comportare per i più giovani, in assenza di adeguate tutele. Da un lato, un chatbot avanzato può esercitare un forte ascendente psicologico su utenti adolescenti, instaurando con loro un rapporto quasi simbiotico e di dipendenza emotiva (il cosiddetto "companion AI").

Dall'altro, i contenuti che l'intelligenza artificiale genera in risposta alle sollecitazioni dell'utente possono facilmente oltrepassare i confini dell'appropriatezza: come visto, Replika era programmato per assecondare anche registri molto intimi e sessualizzati, sfociando in interazioni del tutto inadatte a un minore.

In assenza di un filtro editoriale o umano, l'intelligenza artificiale può produrre output estremi o falsi con apparente naturalezza.

Il fatto che una macchina possa molestare verbalmente un adolescente, o fornirgli consigli potenzialmente dannosi spacciandosi per "amico", pone interrogativi urgenti sul tipo di esposizione cui i minori possono andare incontro.

Inoltre, sotto il profilo giuridico, casi come questo mostrano la difficoltà di inquadrare servizi innovativi nel perimetro normativo esistente: Replika sfuggiva alle maglie delle tradizionali regolamentazioni sui contenuti (non essendo catalogabile come contenuto editorialmente controllato) e, fino all'intervento del Garante, operava in una sorta di vuoto regolatorio.

La risposta delle istituzioni italiane – tra le prime al mondo – segnala comunque un indirizzo chiaro: i fornitori di servizi di intelligenza artificiale generativa devono farsi carico della protezione dei minori, implementando fin dall'inizio controlli d'età e limiti sui contenuti che tengano conto della loro presenza.

Il "caso Replika" ha fatto scuola, preannunciando un'epoca in cui sarà necessario vigilare attentamente anche sugli algoritmi conversazionali, affinché l'innovazione non vada a detrimento dei diritti dei più giovani.

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

6. Disinformazione, teorie del complotto e polarizzazione algoritmica tra gli adolescenti

Nella vita online degli adolescenti un capitolo cruciale è rappresentato dall'informazione e disinformazione.

Le nuove generazioni tendono, infatti, a usare i social network non solo per svago o interazione personale ma, anche, come fonte primaria di notizie e aggiornamenti sul mondo, utilizzando canali come WhatsApp, Instagram e TikTok per informarsi su notizie di attualità.

Questa commistione tra flusso informativo e piattaforme di intrattenimento comporta conseguenze ambivalenti.

Se, da un lato, i ragazzi hanno accesso immediato a una pluralità di fonti e punti di vista, dall'altro risultano particolarmente esposti alle fake news, alle teorie del complotto e alla propaganda virale veicolata dagli algoritmi.

La facilità con cui circolano e attecchiscono narrazioni infondate tra i più giovani è allarmante: basti pensare alla diffusione virale, negli ultimi anni, di teorie complottiste come quelle negazioniste sui vaccini, sulle pandemie orchestrate o su sfide mortali.

Queste teorie trovano terreno fertile sui social media, dove logiche di gruppo e bisogno di appartenenza possono portare gli adolescenti ad abbracciare visioni distorte pur di identificarsi con una comunità virtuale.

Un fattore chiave, notoriamente, è il ruolo degli *algoritmi di raccomandazione* delle piattaforme.

I social network e i siti di video-sharing tendono a mostrare agli utenti contenuti in linea con le loro precedenti interazioni, massimizzando il tempo di visualizzazione e il coinvolgimento.

Questo crea le cosiddette *filter bubbles*, o camere dell'eco, in cui i giovani rischiano di venire alimentati con informazioni unilaterali e progressivamente più estreme.

Ad esempio, un ragazzo che inizi a guardare su YouTube video cospirazionisti o polarizzati su un tema (poniamo, sulle scie chimiche o su teorie antiscientifiche) verrà verosimilmente raggiunto da suggerimenti di nuovi video analoghi, magari ancora più radicali, in un percorso di polarizzazione algoritmica che può condurlo verso posizioni sempre più distorte.

L'ecosistema digitale, progettato per massimizzare l'engagement, talvolta finisce per privilegiare contenuti sensazionalistici, divisivi o emotivamente forti: proprio quelli che costituiscono il nucleo della disinformazione e delle narrazioni complottiste.

Questo circolo vizioso può incidere sulla formazione dell'identità e della visione del mondo nei ragazzi, i quali – se privi di strumenti critici – possono aderire a ideologie estreme o sviluppare percezioni della realtà falsate.

Vi è poi il fenomeno, altrettanto complesso, della *disinformazione personalizzata*: fake news e teorie del complotto oggi non sono confezionate con

approccio "one size fits all", ma vengono sovente targettizzate su specifiche fasce d'età o gruppi di interesse, sfruttando i dati personali disponibili online.

Gli adolescenti, che condividono incessantemente dati e preferenze sui social, diventano così bersagli perfetti per campagne disinformative mirate (si pensi alle pubblicità occulte di prodotti nocivi, ai movimenti negazionisti che reclutano i giovanissimi sul clima o su altri temi, ecc.).

L'impeto partecipativo tipico dell'età adolescenziale può essere manipolato dalle *echo chambers* digitali, trasformando ribellione e bisogno di identità in appartenenza a gruppi virtuali radicalizzati.

Di fronte a questo scenario, appare drammaticamente confermata l'esigenza di un'educazione critica all'informazione (Gallese, Moriggi, Rivoltella 2025).

Ma il compito, sia chiaro, non può ricadere solo sulla scuola: è necessario un impegno congiunto di piattaforme digitali, istituzioni e famiglia.

Le prime dovrebbero investire in sistemi di moderazione e fact-checking più efficaci, oltre che in design algoritmici meno polarizzanti; le seconde dovrebbero promuovere campagne di sensibilizzazione e programmi formativi; la famiglia, dal canto suo, dovrebbe vigilare e dialogare con i ragazzi sui contenuti che questi fruiscono online, colmando il vuoto di riferimento che spesso lascia i minori soli davanti alle fake news.

In mancanza di queste azioni, il rischio è duplice: da un lato una generazione di cittadini digitali poco informati o addirittura disinformati, dall'altro una possibile disaffezione verso la stessa idea di *verità*.

7. Deepfake e contenuti generati dall'intelligenza artificiale: l'impatto su percezione e verità

Tra le nuove frontiere che mettono alla prova la capacità dei minori (e non solo) di discernere il vero dal falso, vi è l'esplosione dei contenuti generati dall'intelligenza artificiale, in particolare i cosiddetti *deepfake*.

Con questo termine si indicano immagini, video o audio creati o alterati tramite algoritmi di intelligenza artificiale in modo talmente realistico da simulare situazioni mai avvenute. Si va dai volti di personaggi celebri sovrapposti ad altri corpi fino alle voci di familiari clonate per ingannare qualcuno al telefono.

I deepfake rappresentano una sfida inedita sul punto della *costruzione della verità*: nell'era in cui ogni testo, suono o immagine può essere contraffatto digitalmente, il tradizionale adagio "seeing is believing" perde di significato.

Per gli adolescenti, nativi digitali abituati a fruire di foto e video come linguaggio quotidiano, il dilagare dei deepfake può avere ripercussioni profonde.

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

Da un lato rischiano di diventare pubblico ingenuo di verosimiglianze ingannevoli: ad esempio, potrebbero imbattersi in falsi video scandalistici di figure pubbliche o in notizie allarmanti corredate da immagini manipolate, prendendoli per autentici e diffondendoli ulteriormente.

Dall'altro lato, essi stessi possono divenire vittime dirette di questa tecnologia.

Un fenomeno molto grave, e purtroppo in crescita, è l'uso di deepfake per il bullismo e la vendetta tra coetanei utilizzando contenuti pornografici. Ragazze minorenni hanno visto il proprio volto artificiosamente inserito su video porno trovati online, allo scopo di umiliarle pubblicamente; analogamente ragazzi possono essere bersaglio di deepfake denigratori.

Non solo ragazze – spesso le più colpite da fenomeni di sexual shaming – ma anche i ragazzi possono subirne gli effetti devastanti. La possibilità di creare con pochi clic immagini esplicite e non consensuali di un compagno di classe configura una nuova forma di abuso digitale che mina la dignità e la sicurezza psicologica delle giovani vittime, causando traumi e vergogna difficilmente rimediabili.

Come evidenziato, questa tendenza erode le basi della fiducia e della sicurezza nei contesti educativi, richiedendo urgentemente strategie di contrasto e sensibilizzazione. Un altro campo dove i contenuti generati da intelligenza artificiale incidono pesantemente è quello della criminalità online. Purtroppo, le stesse tecniche di generazione usate per scopi ludici possono essere sfruttate in modo aberrante, ad esempio per produrre materiale pedopornografico sintetico.

Nel febbraio 2025 Europol ha coordinato la prima operazione globale contro un circuito criminale che diffondeva immagini di abusi su minori create interamente tramite intelligenza artificiale: l'Operazione "Cumberland" ha portato a decine di arresti in 19 Paesi e ha svelato una piattaforma online in cui, previo pagamento, era possibile accedere a video generati digitalmente che mostravano bambini abusati.

Sebbene in tali contenuti non vi fossero vittime reali, Europol ha evidenziato come l'AI-CSAM (*Child Sexual Abuse Material* generato da *Artificial Intelligence*) contribuisca comunque a oggettivare e sessualizzare i bambini, alimentando fantasie e domanda di materiale pedopornografico.

Il caso ha sollevato anche un problema di gap normativo: molte legislazioni nazionali non avevano (fino a quel momento) tipi di reato pensati per punire immagini di abuso "fittizie", rendendo difficoltoso per gli inquirenti intervenire prontamente.

Si tratta di un esempio estremo, ma emblematico, di come i contenuti generativi possano creare danno sociale anche senza una vittima diretta, richiedendo un rapido adeguamento delle leggi e delle strategie di contrasto.

Ma i rischi non terminano qui. I deepfake audio hanno già alimentato truffe ed estorsioni: sono noti casi, anche in cronaca recente, di genitori

contattati da sedicenti rapitori con in sottofondo la voce (clonata via intelligenza artificiale) della figlia in lacrime, per inscenare falsi rapimenti e chiedere riscatti.

Questi *virtual kidnapping scams* sfruttano l'emotività familiare e la potenza dell'intelligenza artificiale vocale, gettando nel panico persone ignare. La facilità con cui pochi secondi di audio da un social network possono essere sufficienti per riprodurre la voce di un adolescente solleva comprensibili allarmi: come proteggersi da un mondo in cui non si può più credere neanche alle proprie orecchie?

Siamo di fronte, in sintesi, a una vera e propria *crisi della realtà*, in cui l'evidenza sensibile (ciò che vediamo/ascoltiamo) non garantisce più verità.

Per i nativi digitali questo scenario rischia di tradursi in due effetti opposti ma ugualmente problematici: o una credulità totale verso qualunque contenuto multimediale accattivante (esponendoli a manipolazioni continue), oppure un cinico scetticismo verso tutto ("non ci si può fidare di nulla"), con conseguente disorientamento e sfiducia anche nelle informazioni corrette.

Come arginare, allora, l'impatto destabilizzante dei contenuti di intelligenza artificiale sulla percezione della verità?

Su un piano normativo, diversi Paesi si stanno muovendo per reprimere gli abusi più gravi: ad esempio il Regno Unito ha annunciato leggi per criminalizzare esplicitamente la diffusione di deepfake pornografici senza consenso.

Anche l'UE, con il *Digital Services Act* e il regolamento sull'intelligenza artificiale, spinge verso *obblighi di trasparenza* (ad esempio etichettare i contenuti sintetici) e strumenti di *rilevazione automatica* dei deepfake.

Tuttavia, norme e tecnologie per il contrasto da sole non bastano.

Occorre inserire, ad esempio, nei programmi educativi moduli didattici sulla *sinthetic media literacy*, per insegnare ai ragazzi a riconoscere indizi di falsificazione nei video e nelle immagini, a usare strumenti di verifica (come il *reverse image search*) e in generale a sviluppare un sano dubbio verso i media digitali iper-realistici.

Allo stesso tempo, a livello psicologico, va creata una rete di supporto per le vittime di *deepfake abuse*, equiparando questo tipo di cyber-violenza alle forme tradizionali di molestia e bullismo, con protocolli di intervento nelle scuole.

Genitori e docenti devono essere formati anche su questi nuovi rischi: ad esempio, un genitore allertato sull'esistenza delle truffe con voce clonata potrà istruire i familiari su come reagire (chiamando subito il numero diretto del congiunto, ad esempio, per verificare).

Sul fronte dei social media, sarebbe auspicabile allo stesso tempo l'integrazione di *filtri automatici* che segnalino o blocchino i deepfake dannosi: alcune piattaforme stanno sviluppando *watermark* invisibili per contrasse-

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

gnare i contenuti originali, o algoritmi che riconoscano imperfezioni tipiche dei media sintetici.

A nostro avviso, anche i contenuti generati dall'intelligenza artificiale costituiscono un banco di prova cruciale per la *tenuta della verità* nell'era digitale. Se ben governati, potranno avere usi positivi (si pensi all'intrattenimento, alla creatività, alla ricostruzione storica); se lasciati senza controllo e senza un'adeguata preparazione del pubblico giovane, rischiano di amplificare all'estremo le patologie informative e relazionali già evidenti.

La posta in gioco è la capacità delle nuove generazioni di distinguere realtà e finzione, di continuare a credere in un nucleo di fatti condivisi su cui basare la convivenza civile. In fondo, la vera sfida che l'intelligenza artificiale pone ai minori d'oggi è una sfida di *coscienza critica*: educarli a vivere in un mondo dove la realtà può essere "falsificata" significa rafforzarli interiormente, dare loro bussola e strumenti per non perdere l'orientamento.

8. Conclusioni: verso un ambiente digitale più giusto e sicuro per i minori. Una proposta sistemica e multidisciplinare

Dalle analisi svolte nei paragrafi precedenti emerge con chiarezza come la questione dei minori nella società digitale sia estremamente *complessa* e *multidimensionale*.

Non esistono soluzioni semplici, né interventi isolati in grado di garantire da soli uno spazio online giusto e sicuro per bambini e adolescenti.

Al contrario, serve un *approccio sistemico*, che coinvolga sinergicamente aspetti normativi, tecnologici, educativi e culturali, facendo dialogare competenze diverse (giuridiche, sociologiche, informatiche, pedagogiche, psicologiche).

In questa conclusione, ci pare opportuno delineare, allora, una proposta d'azione integrata, ispirata ai principi emersi e alle migliori pratiche evidenziate.

In primo luogo, il quadro normativo va aggiornato e rafforzato per tenere il passo con l'innovazione tecnologica. Ciò implica, ad esempio, l'introduzione di obblighi stringenti e standard condivisi di verifica dell'età per tutte le piattaforme frequentate da minori.

Le sperimentazioni come il regolamento AGCOM sul doppio anonimato sono un buon punto di partenza: tali modelli potrebbero essere estesi oltre i siti vietati ai minori, prevedendo che anche social network e servizi di streaming implementino sistemi di *age assurance* certificati, in grado di distinguere un dodicenne da un maggiorenne senza violare la privacy individuale.

Parallelamente, vanno colmati i vuoti legislativi emersi: ad esempio, criminalizzando esplicitamente la produzione e diffusione di deepfake lesivi della persona e aggiornando la definizione di materiale pedopornografico

per includervi i contenuti di intelligenza artificiale sintetici che sessualizzano minori (come molti ordinamenti già prevedono).

A livello europeo, il *Digital Services Act* e il recente regolamento sull'intelligenza artificiale dovranno essere implementati ponendo particolare attenzione ai diritti dei minori: ad esempio, imponendo valutazioni di impatto specifiche sui rischi per i minori da parte delle grandi piattaforme e vincolando queste ultime a misure di protezione dell'utenza minore (modalità con contenuti adatti all'età, limitazione profilazione pubblicitaria sotto una certa età, etc.).

Inoltre, sarebbe auspicabile recepire nelle normative nazionali ed europee il principio del "superiore interesse del bambino" ("*best interest of the child*") in ogni disciplina attinente al digitale, come raccomandato dal Comitato ONU sui Diritti dell'Infanzia (*General Comment* n. 25/2021).

Questo orientamento aiuterebbe a bilanciare correttamente, in sede interpretativa, le eventuali tensioni tra protezione dei dati, libertà di espressione e tutela dei minori.

In secondo luogo, il settore tecnologico e industriale deve fare la sua parte abbracciando il paradigma della "protezione by design" e "by default" nei confronti degli utenti minori.

Le grandi piattaforme dovrebbero proattivamente implementare sistemi interni di *child safety*: ad esempio, utilizzando l'intelligenza artificiale non solo per profilare a scopi di marketing ma, anche, per individuare e bloccare tempestivamente fenomeni come il grooming, il cyberbullismo reiterato e la diffusione virale di sfide pericolose.

Strumenti di *parental control* efficaci, modalità "under 13" con funzionalità limitate, opzioni di filtro avanzato dei contenuti generati dall'intelligenza artificiale (per impedire output inappropriati ai minori) possono essere tutte innovazioni tecniche a portata di mano che le aziende possono adottare responsabilmente.

Un impegno particolare va richiesto, a nostro avviso, alle società che sviluppano modelli generativi e chatbot: esse dovrebbero integrare dall'inizio nei loro sistemi dei "paletti etici", ad esempio classificando come *adult-only* certi contenuti e fornendo kit che permettano agli sviluppatori terzi di attivare controlli d'età sulle proprie implementazioni.

Inoltre, si auspica una maggiore trasparenza algoritmica: rendere pubbliche – almeno alle autorità garanti e a esperti indipendenti – le logiche di raccomandazione e moderazione aiuterebbe a identificare bias o falle che colpiscono i minori (si pensi agli algoritmi di TikTok che possono aver spinto minori verso contenuti estremi).

In quest'ottica, la creazione di comitati etici con partecipazione anche di esperti di sviluppo infantile, chiamati a supervisionare gli effetti delle piattaforme sui giovani, potrebbe diventare una best practice di responsabilità sociale d'impresa.

SOCIOLOGIA DEL DIRITTO, Vol. 52, Numero 2, 2025
ISSN 0390-0851 – ISSNe 1972-5760

In terzo luogo, l'asse educativo e culturale è forse il più importante nel lungo periodo. È indispensabile strutturare un programma organico di alfabetizzazione digitale rivolto sia ai minori sia agli adulti di riferimento (Lancini 2025).

La scuola deve consolidare il percorso iniziato: l'educazione civica digitale non deve restare una materia secondaria, ma deve essere trattata con pari dignità delle altre discipline, con verifiche di apprendimento e progetti concreti (Pasta, Rivoltella 2022; Viola 2021).

Contemporaneamente, è utile coinvolgere gli stessi ragazzi come *peer educator*: molti progetti mostrano che quando sono i giovani a farsi portavoce presso i pari dei messaggi di uso responsabile, l'efficacia cresce (Van Zalk, Monks 2020).

Sul fronte familiare, vanno incentivate iniziative di *parental training*: corsi serali per genitori sulla sicurezza online, guide pratiche diffuse attraverso le strutture mediche, campagne sui media che offrano consigli semplici su come attivare protezioni o su come parlare di Internet coi figli.

In generale, servirebbe alimentare una cultura diffusa in cui l'educazione digitale del minore sia percepita come parte integrante della sua educazione tout court, e non come un ambito tecnico riservato agli "esperti di computer".

Un cambio di mentalità è avvenuto in passato su altri temi (educazione stradale, educazione alla salute); allo stesso modo, dovrà diventare naturale occuparsi della "salute digitale" dei figli, con attenzione e senza tabù (Betton, Woollard 2018).

Infine, l'approccio sistemico implica *collaborazione* e *multidisciplinarietà*.

Le sfide digitali riguardanti i minori sono trasversali e richiedono che tutti gli stakeholder cooperino. È auspicabile la creazione di tavoli di lavoro permanenti dove autorità (Garante Privacy, Garante Infanzia, Polizia Postale), aziende tech, mondo della scuola, associazioni genitoriali e magari rappresentanti degli stessi ragazzi s'incontrino per condividere informazioni e coordinare azioni.

Questa rete andrebbe ampliata e resa più operativa, per affrontare prontamente fenomeni emergenti, e anche a livello internazionale la condivisione di best practices diventa fondamentale: Europol e Interpol già cooperano con task force specifiche su crimini online contro minori, scambiando expertise su come rintracciare, ad esempio, autori di adescamento.

In conclusione, costruire un ambiente digitale più giusto e sicuro per i minori significa garantire loro il diritto di navigare senza subire prevaricazioni, sfruttamento o manipolazioni e, al contempo, il diritto di esprimersi, apprendere e partecipare appieno alla vita digitale.

È un equilibrio delicato, che richiede un impegno congiunto – delle istituzioni, del mondo tecnologico, della scuola e della famiglia – nel nome di una generazione che sta crescendo in un contesto mai sperimentato prima dall'umanità.

Bibliografia

Betton, V., Woollard, J., (2018), *Teen Mental Health in an Online World: Supporting Young People around their Use of Social Media, Apps, Gaming, Texting and the Rest*, London, Jessica Kingsley Publishers.

Bianda, E., (2019), Riconoscimento facciale e capitalismo della sorveglianza, in *Problemi dell'informazione*, 2, pp. 400-400, DOI 10.1445/94261.

Biolcati, R., (2010), La vita online degli adolescenti: tra sperimentazione e rischio, in *Psicologia clinica dello sviluppo*, 41 (2), pp. 267-298.

Biolcati, R., Cani, D., Badio, E., (2013), Adolescenti e Facebook: la gestione online della privacy, in *Psicologia clinica dello sviluppo*, 2013, 51 (3), pp. 449-478.

Blake, P., (2019), Age verification for online porn: more harm than good? in *Porn studies*, 6 (2), pp. 228-237.

Caggiano, I.A., (2022) Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law, in *European Journal of Privacy Law & Technologies*, 1, pp. 27-44.

Cantero Gamito, M., (2023), Do Too Many Cooks Spoil the Broth? How EU Law Underenforcement Allows TikTok's Violations of Minors' Rights, in *Journal of consumer policy*, 46 (3), pp. 281-305.

Carr, N. (2025), *Superbloom. Le tecnologie di connessione ci separano?*, Milano, Cortina.

Frigato, P., (20121), Capitalismo della sorveglianza e fallimento del modello di mercato, in *Sociologia del lavoro*, 159, pp. 270-28.

Gallese, V., Moriggi, S., Rivoltella, P.C., (2025), *Oltre la tecnofobia. Il digitale dalle neuroscienze all'educazione*, Milano, Cortina.

Garaci, I., (2023), The child's right to privacy in the family context, in *European Journal of Privacy Law & Technologies*, 1, pp. 84-99.

Ghiglia, A. (2023), *Educazione civica digitale. Abbecedario essenziale*, Rimini, Maggioli.

Lancini, M., (2025), *Chiamami adulto. Come stare in relazione con gli adolescenti,* Milano, Cortina.

Li, J., (2025), Reflection on data right protection for minors in the digital age, in *Children and youth services review*, 170 (5): 108167, DOI: https://doi.org/10.1016/j.childyouth.2025.108167.

Macenaite, M., Kosta, E., (2017), Consent for processing children's personal data in the EU: following in US footsteps?, in *Information & communications technology law*, 26 (2), pp. 146-197.

Murgo, C., (2024), L'identità personale dei minori, tra responsabilità genitoriale e capacità di autodeterminarsi, in *European Journal of Privacy Law & Technologies*, 2, pp. 115-128.

Nagel, D. (2011-12), Beware of the Virtual Doll: ISPs and the Protection of Personal Data of Minors, in *Philosophy & technology*, 24 (4), pp. 411-418.

Pasquale, L., Zippo, P., Curley, C., O'Neill, B., Mongiello, M., (2022), Digital Age of Consent and Age Verification: Can They Protect Children?, in *IEEE software*, 39 (3), pp. 50-57.

Pasta, S., Rivoltella P.C., (2022), a cura di, *Crescere onlife. L'educazione civica digitale progettata da 74 insegnanti-autori*, Brescia, Scholé-Morcelliana.

Pesci, G., (2024), *Educazione civica e cittadinanza digitale. Percorsi educativi nella società dell'informazione*, Milano, Giuffrè.

Savonardo, L., Marino, R., (2021), *Adolescenti always on. Social media, web reputation e rischi online*, Milano, FrancoAngeli.

Scalzaretto, S., (2023), Minori e disabilità nell'era dello sharenting. Il "diritto ad un futuro aperto" come criterio per una valutazione etica, in *Medicina e morale*, 72 (2), pp. 191-206.

Slavtcheva-Petkova, V. (2023), *Young People, Media and Politics in the Digital Age*, Routledge, DOI: 10.4324/9781003201632.

Stardust, Z., Obeid, A., McKee, A., Angus, D., (2024), Mandatory age verification for pornography access: Why it can't and won't 'save the children', in *Big data & society*, 11 (2), DOI: 10.1177/20539517241252129.

Talley, V.A.M., (2021), Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children Under the GDPR, in *Indiana international & comparative law review*, 30 (1), pp. 127-162.

Viola, J.K., (2021), *Young People's Civic Identity in the Digital Age*, Cham, Springer Nature Switzerland AG, 2021.

Yar, M., (2020), Protecting children from internet pornography? A critical assessment of statutory age verification and its enforcement in the UK, in *Policing : an international journal of police strategies & management*, 43 (1), pp. 183-197.

Zalk, N. van, Monks, C.P., (2020), eds., *Online Peer Engagement in Adolescence: Positive and Negative Aspects of Online Social Interaction*, New York, Routledge.

Zuboff, S., (2019), *Il capitalismo della sorveglianza: il futuro dell'umanità nell'era dei nuovi poteri*, Roma: LUISS University Press.