

Per proteggere i minori dobbiamo controllare tutti?

La Francia ha provato a vietare i social network ai minori di quindici anni. Prima il confronto con Bruxelles ha portato il Parlamento a eliminare quasi tutti i meccanismi nazionali pensati per far rispettare il divieto, poi il Consiglio costituzionale lo ha censurato. Il caso mostra quanto sia difficile proteggere i ragazzi senza estendere il controllo a tutti.

Enrico Capiro | 16 agosto 2026



Vietare ai minori di quindici anni l'accesso ai social network sembra una risposta semplice a un problema che semplice non è. Se alcune piattaforme possono esporre bambini e adolescenti a contenuti nocivi, cyberbullismo, contatti indesiderati, uso compulsivo e meccanismi progettati per trattenerli online il più a lungo possibile, la soluzione più immediata appare quasi intuitiva. Se quell'ambiente è pericoloso, impediamo loro di entrarci.

È ciò che ha provato a fare la Francia. Il 21 luglio 2026 il Parlamento ha approvato definitivamente un testo che avrebbe vietato ai minori di quindici anni l'accesso ai servizi di social network online a partire dal 1° settembre, prevedendo altri quattro mesi per gli account già esistenti. Il 14 agosto il Consiglio costituzionale francese, il

Conseil constitutionnel, ha però dichiarato incostituzionale proprio l'articolo che introduceva quel divieto.

Per capire davvero la decisione bisogna però aggiungere un passaggio che rischia di perdersi nella formula semplice del divieto. Il testo arrivato davanti al Consiglio costituzionale era già molto diverso da quello discusso nei mesi precedenti. La Francia aveva notificato il progetto alla Commissione europea il 9 aprile 2026 e, l'8 luglio, la Commissione aveva emesso un parere circostanziato nell'ambito della procedura europea prevista per le regole tecniche nazionali. Quel confronto aveva reso evidente il problema di sovrapporre nuovi obblighi francesi alle regole europee già applicabili alle piattaforme.

Quando deputati e senatori hanno trovato il compromesso finale nella commissione mista del 20 luglio, hanno quindi eliminato la lista di piattaforme da vietare, il meccanismo di autorizzazione parentale previsto per altri servizi e le specifiche prerogative nazionali attribuite all'Arcom, l'autorità francese di regolazione della comunicazione audiovisiva e digitale. Il divieto è rimasto a carico dei minori, senza sanzioni nei loro confronti, mentre per le piattaforme l'applicazione della disciplina avrebbe fatto affidamento in larga misura sul quadro europeo. Lo stesso Senato descriveva ormai il testo come essenzialmente simbolico e di portata normativa limitata.

Questo non significa che la norma fosse inesistente. Fissava ancora un divieto generale, un ambito di applicazione e una data di entrata in vigore. Ma non conteneva più una propria architettura nazionale capace di trasformare quel divieto in un blocco operativo imposto direttamente alle piattaforme. È una distinzione importante, perché il paradosso che emerge dalla decisione non consiste nel fatto che la Francia avesse già costruito un sistema di verifica generalizzata dell'età. Consiste nel fatto che qualunque divieto fondato sull'età, se vuole diventare realmente efficace, deve prima risolvere il problema di sapere chi ha l'età per entrare e chi no.

Il Consiglio costituzionale non ha cancellato l'intero testo e, soprattutto, non ha stabilito che bambini e adolescenti debbano poter utilizzare qualsiasi piattaforma senza limiti. La decisione n. 2026-911 DC riconosce pienamente il problema e la legittimità dell'intervento pubblico, ma mette in discussione il modo in cui si è scelto di intervenire. È una distinzione che sposta la discussione dal terreno molto semplice del vietare o non vietare a una domanda più difficile, perché quando vogliamo proteggere qualcuno dai rischi della tecnologia dobbiamo anche chiederci quali libertà siamo disposti a limitare e quali conseguenze siamo pronti ad accettare per rendere quella protezione realmente efficace.

Proteggere i minori è legittimo, ma non basta che lo sia lo scopo

Il Consiglio costituzionale parte da un punto sul quale non c'è ambiguità. Proteggere i minori dai rischi connessi all'uso dei social network è un obiettivo costituzionalmente legittimo e può giustificare anche limitazioni alla loro libertà di accesso a determinati servizi online. Nella decisione vengono richiamati l'interesse superiore del minore e l'esigenza di prevenire lesioni all'ordine pubblico, quindi il problema non riguarda il fatto che lo Stato possa intervenire, ma il modo in cui quell'intervento viene costruito.

La libertà di espressione e di comunicazione è protetta in Francia dall'articolo 11 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789 e può certamente subire limitazioni, ma queste devono essere necessarie, adeguate e proporzionate. Fuori dal linguaggio giuridico significa che una buona ragione, da sola, non basta per comprimere una libertà. Bisogna verificare che la restrizione sia davvero adatta a ridurre il rischio, che non vada oltre ciò che serve e che il sacrificio imposto agli altri diritti sia giustificato dal risultato che ci aspettiamo di ottenere.

Il rischio non era emerso soltanto dopo il voto finale. Già nel gennaio 2026 il Conseil d'État, chiamato a esprimere un parere sulla proposta originaria, aveva osservato che un'interdizione generale e assoluta poteva raggiungere nello stesso modo servizi di cui erano documentati effetti dannosi e servizi per i quali rischi analoghi non risultavano dimostrati. Aveva inoltre segnalato l'assenza di una modulazione legata all'età e alla maturità del minore e lo spazio troppo ridotto lasciato alla responsabilità dei genitori.

Il testo definitivo aveva introdotto alcune eccezioni. Restavano fuori le enciclopedie online, i repertori educativi o scientifici e le piattaforme dedicate allo sviluppo e alla condivisione di software libero o di progetti digitali educativi in modalità aperta. Non era quindi un divieto letteralmente privo di distinzioni, ma per il Consiglio costituzionale quelle esclusioni non bastavano. La proibizione continuava a trattare nello stesso modo servizi molto diversi per funzionalità, contenuti, rischi e misure di protezione e poteva raggiungere anche piattaforme rispetto alle quali non erano stati dimostrati pericoli per la salute e la sicurezza dei minori comparabili a quelli che avevano spinto il legislatore a intervenire.

Anche i minori venivano considerati come una categoria sostanzialmente uniforme. La norma non lasciava ai titolari della responsabilità genitoriale la possibilità di rimuovere o modulare il divieto in relazione al proprio figlio e non consentiva di tenere conto dell'età concreta e del grado di maturità del minore. Questo non significa che qualsiasi soglia anagrafica sia illegittima, né che ogni ragazzo debba essere valutato individualmente prima di applicare una regola. Significa piuttosto che, quando limitiamo una libertà fondamentale, non possiamo dare per scontato

che piattaforme diverse, rischi diversi e situazioni diverse possano essere governati sempre con la stessa misura soltanto perché la finalità perseguita è importante.

Una finalità può quindi essere pienamente legittima senza che lo sia, per ciò solo, anche il mezzo scelto per realizzarla. Ed è quando la decisione passa dalla libertà di comunicazione alla vita privata che questa distinzione diventa ancora più interessante.

Per escludere i minori dobbiamo sapere chi è minorenne

Qui serve distinguere con precisione due piani. Il testo francese definitivo non imponeva più alle piattaforme uno specifico sistema nazionale di verifica dell'età e non aveva costruito un'infrastruttura tecnica per far rispettare il divieto. Ma un divieto fondato sull'età, se vuole diventare effettivo, contiene una difficoltà che viene prima della tecnologia. Per impedire l'accesso a chi ha meno di quindici anni dobbiamo essere in grado di distinguerlo da chi ne ha sedici, venticinque o sessanta e, prima di avere effettuato questa verifica, non sappiamo ancora a quale di queste categorie appartenga la persona che sta cercando di entrare.

È proprio questo passaggio logico che il Consiglio costituzionale porta alle sue conseguenze. Al paragrafo 20 della decisione osserva che la proibizione implica che ogni persona, anche maggiorenne, debba essere in grado di provare la propria età prima di accedere al servizio. Una regola apparentemente destinata a una fascia circoscritta della popolazione finisce così, nel momento in cui la si vuole rendere applicabile, per modificare le condizioni di accesso alla piattaforma per tutti.

È qui che la protezione dei minori incontra il diritto al rispetto della vita privata, che la giurisprudenza costituzionale francese ricava dalla libertà garantita dall'articolo 2 della Dichiarazione del 1789. Il legislatore non aveva definito in modo sufficientemente preciso le condizioni e i limiti entro i quali l'età avrebbe dovuto essere dimostrata, né le garanzie destinate a proteggere la vita privata degli utenti. Il problema non era quindi che la legge avesse già imposto a tutti di identificarsi, ma che un divieto destinato a richiedere una prova dell'età fosse stato approvato senza disciplinare adeguatamente il modo in cui quella prova avrebbe dovuto funzionare.

Il problema diventa molto concreto appena immaginiamo il passaggio dalla regola sulla carta alla sua applicazione. Se milioni di persone devono dimostrare una caratteristica personale prima di utilizzare un servizio, dobbiamo stabilire chi effettua la verifica, quali informazioni può conoscere, se può conservarle, se può riutilizzarle e se controlli compiuti in servizi o momenti diversi possono essere collegati tra loro. Sono domande che riguardano l'efficacia del divieto e, nello stesso tempo, il livello di sorveglianza che siamo disposti a introdurre per renderlo efficace.

A questo punto emerge il paradosso che rende il caso francese molto più interessante di una semplice discussione sul limite dei quindici anni. Un divieto facile da aggirare rischia di incidere poco sui comportamenti, ma quanto più vogliamo renderlo difficile da aggirare, tanto più abbiamo bisogno di un sistema affidabile capace di distinguere chi può accedere da chi non può farlo. Il problema del proibizionismo tecnologico non è quindi soltanto che un adolescente possa mentire sulla data di nascita, utilizzare l'account di un adulto o trovare un'altra strada per superare il blocco, perché la questione più profonda riguarda il prezzo che tutti gli utenti devono pagare affinché quel blocco funzioni davvero.

Verificare l'età non significa necessariamente sapere chi siamo

Da questo ragionamento sarebbe però sbagliato ricavare che qualsiasi verifica dell'età comporti necessariamente l'identificazione della persona. Esistono metodi molto diversi per stabilire l'età o la fascia di età di un utente, dalla semplice dichiarazione alla stima fino a sistemi che utilizzano informazioni o credenziali affidabili per accertare il superamento di una soglia, e non tutti richiedono che la piattaforma conosca l'identità di chi si trova dall'altra parte dello schermo.

Se per entrare in un servizio occorre soltanto sapere se abbiamo più di quindici anni, la piattaforma non ha necessariamente bisogno di conoscere il nostro nome, la data di nascita completa, l'indirizzo o gli estremi di un documento. Può essere sufficiente che un sistema affidabile confermi una sola informazione, cioè che la soglia richiesta è stata superata.

L'Unione europea sta lavorando proprio in questa direzione. Il 29 aprile 2026 la Commissione europea ha adottato la raccomandazione (UE) 2026/1035, un atto non vincolante che invita gli Stati membri ad accelerare la diffusione di una soluzione comune di verifica dell'età. Il modello europeo è pensato per consentire all'utente di dimostrare di avere superato una determinata soglia senza comunicare alla piattaforma l'età esatta, l'identità o altri dettagli personali non necessari.

La questione non è lontana dal lettore italiano. L'Italia è tra i sette Stati con cui la Commissione sta lavorando più da vicino per portare questa soluzione ai cittadini, insieme a Cipro, Danimarca, Francia, Grecia, Irlanda e Spagna. La discussione aperta dalla decisione francese riguarda quindi un'infrastruttura che l'Europa sta già cercando di rendere concretamente disponibile.

Questo cambia molto i termini del problema, perché l'alternativa non è tra un Internet nel quale nessuno verifica nulla e un Internet nel quale dobbiamo consegnare il documento d'identità a ogni piattaforma che utilizziamo. Possiamo costruire soluzioni molto meno invasive, ma la domanda non scompare. Se la verifica dell'età diventa progressivamente una condizione ordinaria per entrare in un

numero crescente di servizi digitali, dobbiamo comunque decidere come vogliamo che funzioni questa infrastruttura, chi possa gestirla, quali dati possa conoscere e in quale misura una verifica possa essere collegata alle altre attività della stessa persona.

Sapere solo ciò che serve sapere

Anche le regole europee sulla protezione dei dati personali non vietano affatto la verifica dell'età. Chiedono però che la soluzione scelta sia realmente necessaria rispetto al rischio da affrontare e che le informazioni utilizzate siano limitate a quelle che servono per raggiungere quello scopo.

Il Comitato europeo per la protezione dei dati lo ha spiegato nella dichiarazione sulla garanzia dell'età adottata nel febbraio 2025. La verifica dovrebbe essere progettata in modo proporzionato al rischio e, tra più misure ugualmente efficaci, andrebbe scelta quella meno invasiva. Soprattutto, il sistema non dovrebbe trasformarsi in un'occasione per attribuire ai fornitori di servizi nuovi strumenti con cui identificare, localizzare, costruire profili delle persone o seguirne il comportamento online. Il Comitato osserva inoltre che trattamenti di questo tipo possono presentare rischi elevati per i diritti e le libertà degli interessati e, quando ricorrono le condizioni previste dal regolamento europeo sulla protezione dei dati, richiedere una valutazione d'impatto preventiva.

La logica si comprende meglio con un esempio molto semplice. Se tutto ciò che un servizio ha bisogno di sapere è se una persona abbia compiuto quindici anni, comunicare anche il suo nome, la fotografia, l'indirizzo e la data di nascita completa significa mettere a disposizione informazioni che non servono allo scopo. Il principio europeo di minimizzazione dei dati chiede esattamente il contrario, cioè che si conosca soltanto ciò che è realmente necessario per svolgere quella funzione.

Applicato alla verifica dell'età, questo principio conduce a un'idea importante. Dimostrare una caratteristica non dovrebbe significare automaticamente dover rivelare la propria identità. La protezione della vita privata non diventa così un argomento per escludere qualsiasi controllo dell'età, ma un criterio per decidere quanto sia legittimo conoscere di una persona per ottenere il risultato che riteniamo necessario.

Il fatto che un divieto possa essere aggirato non significa che sia inutile

Rimane una questione che non possiamo evitare se vogliamo discutere seriamente di proibizionismo tecnologico. Una regola non diventa inutile soltanto perché può essere violata, perché accade continuamente anche fuori dal mondo digitale e

nessuno pretenderebbe di valutare l'utilità di un divieto chiedendosi semplicemente se esista almeno una persona capace di aggirarlo.

Per questo l'argomento secondo cui i ragazzi troveranno comunque qualche espediente, preso da solo, è troppo debole. Il fatto che un sistema possa essere eluso non ci dice quante persone riusciranno a farlo, quanto diventerà difficile accedere, quanti rinunceranno e quale effetto complessivo produrrà la regola.

L'esperienza australiana è utile proprio perché rende il quadro meno semplice. Dal 10 dicembre 2025 le piattaforme soggette alla disciplina devono adottare misure ragionevoli per impedire ai minori di sedici anni di mantenere account. A metà dicembre le piattaforme avevano rimosso o limitato l'accesso a circa 4,7 milioni di account e, all'inizio di marzo, oltre 300.000 account ulteriori erano stati impediti nell'accesso. Ma l'autorità australiana eSafety ha precisato che si tratta di account, non di persone, che uno stesso utente può averne più di uno e che una parte di quei profili poteva non essere attivamente utilizzata. eSafety ha inoltre ricordato che la conformità non si misura soltanto dal numero di account rimasti o rimossi, ma richiede di verificare i sistemi e i processi adottati dalle piattaforme per compiere le misure ragionevoli richieste dalla legge.

A giugno è arrivato un dato di natura diversa. Uno studio osservazionale pubblicato sul British Medical Journal ha seguito 408 adolescenti australiani a circa tre mesi dall'entrata in vigore della disciplina. Più dell'85 per cento degli under sedici intervistati dichiarava ancora di utilizzare piattaforme soggette alla legge. L'uso quotidiano risultava sostanzialmente stabile tra i dodici e i tredici anni e diminuiva tra i quattordici e i quindici, dal 78 al 69 per cento, ma l'analisi non ha trovato prove sufficienti di una riduzione sostanziale immediata dell'uso attribuibile alla soglia dei sedici anni.

Nemmeno questo studio chiude il dibattito. È una valutazione precoce, condotta a soli tre mesi dall'avvio della misura, su un campione limitato e attraverso dati riferiti dagli stessi partecipanti. Non dimostra che la legge australiana sia inutile, ma impedisce di trasformare il numero degli account rimossi nella prova che i comportamenti dei ragazzi siano cambiati nella stessa proporzione.

Nel frattempo eSafety ha individuato problemi molto concreti nell'applicazione. In alcuni casi ragazzi che avevano già dichiarato di avere meno di sedici anni sono stati invitati a tentare comunque una verifica; in altri è stato possibile ripetere più volte lo stesso metodo fino a ottenere un esito da sedicenne. A marzo l'autorità ha avviato indagini su Facebook, Instagram, Snapchat, TikTok e YouTube e, a fine maggio, dichiarava che gli accertamenti erano ancora in corso e che non era stata ancora raggiunta una conclusione definitiva sulla conformità delle piattaforme.

Le due cose possono quindi essere vere insieme. Una soglia anagrafica può costringere le piattaforme a intervenire, rimuovere un numero molto elevato di account e rendere più difficile l'accesso, mentre allo stesso tempo molti minori continuano a utilizzare i servizi e i sistemi di verifica mostrano margini di errore o di elusione. La domanda utile non è se il divieto sia perfettamente impermeabile, ma se i benefici ottenuti giustifichino i controlli necessari per produrli e se esistano strumenti diversi, o complementari, capaci di proteggere i minori intervenendo più vicino alla fonte del rischio.

Forse il problema non è soltanto chi entra, ma ciò che trova una volta dentro

Se un social network è pericoloso per un ragazzo di quattordici anni, vale infatti la pena chiedersi che cosa lo renda pericoloso. In alcuni casi il problema può essere il contenuto al quale il minore riesce ad accedere, ma in altri dipende anche dal modo in cui il servizio funziona, da quali contenuti decide di mostrare e in quale ordine, dalla pressione esercitata dalle notifiche, dalla possibilità di continuare a scorrere senza incontrare mai una fine o dalla facilità con cui uno sconosciuto può entrare in contatto con un ragazzo.

Nel gennaio 2026 l'Agenzia nazionale francese per la sicurezza sanitaria, l'ANSES, ha pubblicato un'ampia valutazione scientifica sugli effetti dei social network sulla salute degli adolescenti. Il lavoro analizza oltre un migliaio di studi e individua numerosi possibili rischi, in particolare per la salute mentale, richiamando l'attenzione sul modo in cui molte piattaforme sono progettate per catturare e mantenere l'attenzione e sul fatto che alcune caratteristiche dell'adolescenza possono aumentare la vulnerabilità a questi meccanismi.

Questa fonte va però letta con la stessa prudenza che chiediamo alle leggi. Per l'analisi dei legami tra uso dei social network ed effetti sulla salute, il corpus principale degli articoli originali selezionati comprendeva lavori pubblicati tra il 1° gennaio 2011 e il 24 maggio 2021, anche se gli esperti lo hanno integrato con studi precedenti e con dati successivi al 2021 per alcuni confronti e verifiche. L'Agenzia precisa inoltre che, per la propria missione, ha descritto i diversi usi dei social network ma non ha cercato di valutarne gli eventuali effetti positivi. Non significa che le conclusioni debbano essere accantonate, ma che non possiamo trasformare una valutazione scientifica complessa nella formula secondo cui ogni social network, in ogni condizione e per ogni adolescente, produce lo stesso danno.

La parte più interessante riguarda proprio le soluzioni proposte. L'ANSES raccomanda di intervenire prioritariamente alla fonte degli utilizzi dannosi, facendo in modo che i minori possano accedere a servizi progettati e configurati per

proteggerne la salute. Tra le misure richiamate ci sono la limitazione delle interfacce manipolative, il contrasto all'amplificazione di contenuti dannosi e una maggiore regolazione delle funzionalità costruite per aumentare, mantenere o prolungare l'utilizzo della piattaforma.

A questo punto la prospettiva cambia. Se una parte del rischio dipende dal modo in cui il servizio è stato costruito, non siamo costretti a intervenire soltanto sulla persona che cerca di accedervi. Possiamo certamente impedire a un quattordicenne di entrare in determinati ambienti quando ciò sia necessario, ma possiamo anche chiedere alla piattaforma di non offrirgli proprio le caratteristiche che aumentano concretamente il pericolo.

Pensiamo agli algoritmi che decidono quali contenuti mostrarci e in quale ordine. Se il loro funzionamento tende a spingere progressivamente un adolescente verso sequenze ripetitive di contenuti dannosi o a trattenere la sua attenzione il più a lungo possibile, possiamo intervenire su quel funzionamento. Lo stesso vale per le notifiche continue, la riproduzione automatica, i meccanismi che premiano l'uso quotidiano senza interruzioni o le impostazioni che espongono automaticamente un profilo minorile al contatto con persone sconosciute.

In un modello regoliamo soprattutto chi può entrare, mentre nell'altro cominciamo a regolare anche l'ambiente nel quale quella persona entra. La differenza è sostanziale perché cambia il soggetto sul quale facciamo ricadere una parte della responsabilità.

L'Europa prova a spostare una parte della responsabilità sulle piattaforme

È almeno in parte questa la logica del regolamento europeo sui servizi digitali, il Digital Services Act. Nel proprio ambito di applicazione, l'articolo 28 impone alle piattaforme online accessibili ai minori di adottare misure adeguate e proporzionate per garantire un elevato livello di tutela della loro vita privata, di sicurezza e di protezione. Lo stesso articolo precisa però che il rispetto di questi obblighi non costringe i fornitori a trattare dati personali ulteriori per valutare se il destinatario del servizio sia minorenne.

Gli orientamenti pubblicati dalla Commissione europea nel luglio 2025 rendono questa impostazione molto concreta. Non sono norme vincolanti e seguirli non garantisce automaticamente la conformità, ma la Commissione li utilizza come punto di riferimento per valutare il rispetto dell'articolo 28 e possono orientare anche l'azione delle autorità nazionali.

Tra le misure indicate ci sono profili dei minori privati per impostazione predefinita, strumenti che consentano di bloccare facilmente altri utenti, modifiche ai sistemi che

selezionano i contenuti per ridurre il rischio di essere trascinati in sequenze ripetitive di materiale dannoso e la disattivazione predefinita di alcune funzioni che possono favorire un uso eccessivo, come la riproduzione automatica, le notifiche continue, le ricevute di lettura e i meccanismi che premiano la continuità quotidiana dell'utilizzo. La Commissione chiede anche di contrastare caratteristiche progettate soprattutto per spingere l'utente a restare coinvolto il più a lungo possibile.

Gli stessi orientamenti non escludono affatto la verifica dell'età. La considerano appropriata in determinati contesti, soprattutto quando l'accesso è riservato agli adulti o quando una norma stabilisce una soglia minima, ma chiedono che i sistemi siano accurati, affidabili, robusti, non eccessivamente invasivi e non discriminatori. L'approccio europeo non obbliga quindi a scegliere tra verificare l'età e intervenire sul funzionamento delle piattaforme, perché le due strategie possono essere combinate quando il rischio lo richiede.

È probabilmente questa la differenza più importante rispetto a una logica puramente proibizionista. Il divieto concentra l'attenzione soprattutto sulla porta di ingresso, mentre una regolazione basata sul rischio prova a guardare anche a ciò che accade una volta che quella porta è stata superata.

Le soluzioni semplici hanno una grande forza politica

È facile capire perché una proibizione generalizzata possa esercitare una forte attrazione. “Niente social prima dei quindici anni” è un messaggio immediato, comprensibile in pochi secondi e capace di trasmettere l'impressione che il problema sia stato affrontato con una regola chiara.

È molto più difficile spiegare che occorre modificare i sistemi che scelgono i contenuti, limitare alcune tecniche progettate per trattenere l'attenzione, rendere privati per impostazione predefinita gli account dei minori, ridurre la quantità di dati trattati, progettare sistemi di verifica dell'età rispettosi della vita privata e differenziare le misure in base ai rischi effettivamente presenti. Ma la facilità con cui una norma può essere raccontata non dice molto sulla sua capacità di governare un fenomeno complesso.

Nel mondo digitale questo limite diventa particolarmente evidente, perché tecnologie e comportamenti cambiano rapidamente. Un ragazzo escluso da una piattaforma può cercare di rientrare, utilizzare l'account di un'altra persona o spostarsi su un servizio diverso. Non possiamo sapere in anticipo quanto questi fenomeni peseranno e sarebbe altrettanto sbagliato utilizzarli per concludere che ogni limite di età sia inutile, ma dobbiamo considerarli quando valutiamo se una misura funzioni davvero.

Una regola, soprattutto nel digitale, non dovrebbe essere giudicata soltanto per quello che vieta sulla carta, ma anche per i comportamenti che produce nella realtà. Una buona regolazione dovrebbe quindi chiedersi quale rischio vogliamo ridurre, quanto sia efficace la misura scelta, quali nuove conseguenze produca e quanto dobbiamo comprimere altri diritti per farla funzionare.

La vicenda francese aggiunge un avvertimento ulteriore. Nel tentativo di costruire una risposta semplice, il Parlamento è arrivato al voto finale con un divieto che il confronto con il diritto europeo aveva già privato di gran parte dei meccanismi nazionali pensati per renderlo operativo. Poche settimane dopo, il controllo costituzionale ha censurato proprio quella regola generale perché la conciliazione tra protezione dei minori, libertà di comunicazione e vita privata non era stata costruita in modo proporzionato. La semplicità dello slogan non è riuscita a diventare semplicità della regolazione.

La domanda è dove vogliamo mettere il controllo

La decisione francese non sostiene che i ragazzi debbano essere lasciati soli davanti ai social network, non afferma che qualsiasi limite di età sia incompatibile con la libertà di comunicazione e non esclude che l'età possa essere verificata quando necessario. Dice qualcosa di più esigente. Quando decidiamo di limitare una libertà fondamentale, la bontà dello scopo non ci esonera dal dimostrare che il mezzo scelto sia adeguato, necessario e proporzionato e che non produca una compressione eccessiva degli altri diritti.

A quel punto la domanda diventa meno rassicurante del semplice sì o no al divieto. Dove vogliamo collocare il controllo? Possiamo concentrarlo soprattutto all'ingresso, costruendo sistemi sempre più affidabili per impedire ai minori di superare una soglia. Oppure possiamo spostarne una parte maggiore sull'ambiente digitale, intervenendo sui sistemi di raccomandazione, sulle interfacce persuasive, sui contenuti amplificati e sulle funzionalità che prolungano l'uso. Le due strategie possono convivere, ma non hanno lo stesso impatto sui diritti e non distribuiscono nello stesso modo responsabilità e costi.

Possiamo immaginare sistemi capaci di dimostrare il superamento di una soglia di età senza comunicare l'identità della persona, distinguere tra servizi che presentano rischi molto diversi e chiedere a chi progetta le piattaforme di assumersi una parte maggiore della responsabilità per l'ambiente che crea. Possiamo anche continuare a investire nell'educazione digitale dei ragazzi e degli adulti che li accompagnano, perché nessun sistema tecnico potrà sostituire completamente la capacità di comprendere gli strumenti che utilizziamo, riconoscerne i rischi e imparare a governarli.

Educazione, progettazione responsabile, verifica dell'età e limiti di accesso non sono necessariamente alternative tra loro. Il punto è scegliere e combinare questi strumenti in funzione del rischio, senza trasformare il controllo dell'utente nella risposta automatica a problemi che, almeno in parte, nascono dal modo in cui le piattaforme sono progettate.

La decisione del Consiglio costituzionale francese non chiude quindi il dibattito sul rapporto tra minori e social network e forse il suo merito più grande è proprio quello di costringerci a formulare meglio la domanda. Non soltanto a quale età sia giusto entrare in un social network, ma quale social network siamo disposti a offrire a chi ha quattordici anni e quanto controllo sugli altri utenti siamo disposti ad accettare per impedirgli di accedere a ciò che non siamo riusciti a rendere sufficientemente sicuro.

Fonti e riferimenti

Fonti primarie e riferimenti utilizzati per la ricostruzione e l'analisi.

Conseil constitutionnel. Décision n° 2026-911 DC du 14 août 2026, Loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, ECLI FR:CC:2026:2026.911.DC, in particolare parr. 6-23 e dispositivo. [Fonte ufficiale](#)

Conseil d'État. Avis sur une proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, 8 gennaio 2026, in particolare parr. 18-28. [Fonte ufficiale](#)

Assemblée nationale. Texte adopté n° 339, 21 luglio 2026, Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, testo definitivo, in particolare art. 1. [Fonte ufficiale](#)

Sénat. Commission mixte paritaire del 20 luglio 2026, resoconto dei lavori e comunicato sull'accordo relativo all'età minima di accesso ai social network. [Fonte ufficiale](#)

Commissione europea, TRIS. Notifica 2026/0185/FR, ricevuta il 9 aprile 2026; parere circostanziato della Commissione, messaggio TRIS/(2026) 1828 dell'8 luglio 2026; termine dello standstill prorogato al 10 agosto 2026. [Fonte ufficiale](#)

Unione europea. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali, in particolare art. 28 e, per le piattaforme e i motori di ricerca di dimensioni molto grandi, artt. 34, 35 e 37. [Fonte ufficiale](#)

Commissione europea. Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065, 14 luglio 2025. [Fonte ufficiale](#)

Comitato europeo per la protezione dei dati. Statement 1/2025 on Age Assurance, adottata l'11 febbraio 2025, versione 1.2, in particolare i principi sulla proporzionalità, minimizzazione e scelta della misura meno invasiva. [Fonte ufficiale](#)

Commissione europea. Raccomandazione (UE) 2026/1035 del 29 aprile 2026 relativa all'istituzione di un quadro comune per le tecnologie di verifica dell'età a livello dell'UE; documentazione sulla EU Age Verification Solution. [Fonte ufficiale](#)

ANSES. Avis relatif aux effets de l'usage des réseaux sociaux numériques sur la santé des adolescents, 16 dicembre 2025, e Usages des réseaux sociaux numériques et santé des adolescents, rapport d'expertise collective, ottobre 2025, autosaisine n° 2019-SA-0152; documenti pubblicati online il 13 gennaio 2026. [Fonte ufficiale](#)

Australian eSafety Commissioner. Platforms restrict access to 4.7 million under-16 accounts across Australia, 16 gennaio 2026. [Fonte ufficiale](#)

Australian eSafety Commissioner. Social Media Minimum Age: Compliance Update, marzo 2026, in particolare Key points, account removals, compliance observations e ongoing investigations. [Fonte ufficiale](#)

Australian eSafety Commissioner. Senate Estimates Opening Statement, 27 maggio 2026, sullo stato delle indagini relative alla Social Media Minimum Age. [Fonte ufficiale](#)

Barnes C. et al.. Assessing early effects of Australia's Social Media Minimum Age Act on adolescents' social media use: observational study, BMJ 2026;393:e363695, pubblicato il 24 giugno 2026, doi:10.1136/bmj-2026-363695. [Studio peer-reviewed](#)