Protezione dei minori online, il nodo che il dibattito ignora

Verifica dell'età, potere delle piattaforme e i limiti di una critica che si ferma alla sorveglianza. L'UE prova a suggerire delle soluzioni per una tutela necessaria dentro un web dominato dagli interessi delle grandi aziende.

Verso Zero

Pubblicato il 18.04.2026: https://centroriformastato.it/protezione-dei-minori-online-il-nodo-che-il-dibattito-ignora/

Il dibattito contemporaneo sui sistemi digitali di verifica dell'età sconta un limite ricorrente: tende a ridursi a una contrapposizione tra "protezione dei minori" e "libertà della rete", senza quasi mai entrare nel merito delle architetture tecniche, delle alternative regolatorie e soprattutto dei rapporti di potere economico che strutturano davvero l'ambiente digitale. Il problema viene così sistematicamente spostato dal terreno materiale delle infrastrutture e dei modelli di business, cioè dal luogo in cui si esercita realmente il potere economico nell'ambiente digitale, al piano teorico – per certi versi più "comodo" – della sola interferenza esterna (di questi meccanismi digitali di controllo) sul soggetto individuale.

È precisamente questo il limite che si cerca di mettere a fuoco: scambiare la libertà formale dell'utente isolato per emancipazione reale, mentre si lascia intatto il dominio sostanziale esercitato dalle piattaforme e dai loro gestori nel cyberspazio. Si critica, cioè, il possibile controllo pubblico o regolatorio introdotto con sistemi digitali di verifica dell'età diretti alla tutela dei minori, ma si naturalizza il controllo privato già esistente, incorporato nelle architetture delle piattaforme, negli algoritmi, nei meccanismi di cattura dell'attenzione e nella subordinazione dell'esperienza online alla produzione di profitto.

L’esposizione dei minori a certi meccanismi digitali è reale e quotidiana. Proprio per questo serve una lettura politica che rimetta ordine nella discussione: non per negare i rischi della sorveglianza, ma per collocarli all’interno del problema più ampio dei rapporti di potere e delle infrastrutture che oggi plasmano Internet.

Di cosa parliamo quando parliamo di verifica dell'età online

La verifica dell'età online è il problema, tecnico, giuridico e politico, di accertare che chi accede ad un determinato servizio digitale abbia l'età richiesta per farlo. Per decenni, l'accesso a qualsiasi servizio si è basato sull’autodichiarazione: un clic su "ho più di 18 anni", una data di nascita inventata ed il gioco era fatto. Il risultato è stato che i minori sono stati esposti senza filtro o cautela alcuna a un ambiente digitale progettato per massimizzare il coinvolgimento e l'estrazione di dati di chiunque vi acceda, indipendentemente dall'età. Secondo la Commissione europea, il 97% dei giovani nell'UE usa Internet quotidianamente e più di uno su dieci mostra segni di comportamento problematico nell'uso delle piattaforme.

La pressione politica per intervenire è oggi fortissima: Australia, Francia, Spagna, Regno Unito e diversi altri paesi hanno introdotto o stanno introducendo restrizioni all'accesso dei minori ai social network. In Italia sono in discussione proposte di legge bipartisan.

Il Parlamento europeo ha votato una risoluzione che propone un'età minima di 16 anni. Ma il nodo resta invariato: come si verifica l'età senza schedare gli utenti di Internet? Le alternative più intrusive richiedono documenti d'identità o dati biometrici, creando banche dati vulnerabili. L'Unione Europea sta lavorando a un approccio diverso: un sistema che genera un token contenente solo l'attestazione della maggiore età, con l'obiettivo di integrare prove crittografiche a conoscenza zero (zero-knowledge proofs) come spiegato nell'ultima sezione. La fase di test è in corso in cinque paesi.

È questa soluzione, le sue architetture, le sue implicazioni politiche e i rapporti di potere economico che la circondano, l'oggetto di questo articolo.

Le critiche al sistema di verifica dell'età europeo e il loro limite

Negli ultimi mesi sono circolati interventi critici rispetto ai sistemi digitali di verifica dell'età e in particolare a quello europeo. Vale la pena confrontarsi con i più seri, perché colgono problemi reali, anche quando le conclusioni cui pervengono non consentono di individuare delle soluzioni soddisfacenti.

Un primo filone critico sostiene che la protezione dei minori non debba trasformarsi in un sistema di controllo dell'accesso. Il problema, si argomenta, non sarebbe tanto "chi entra" (cioè accede a determinati contenuti digitali) quanto "cosa accade una volta entrati": recommendation systems, dark patterns – cioè quelle tecniche di progettazione delle interfacce studiate per manipolare le scelte dell'utente, spingendolo verso azioni che non avrebbe compiuto spontaneamente: accettare condizioni sfavorevoli, cedere dati personali, restare connesso più a lungo, effettuare acquisti non voluti –, design compulsivo, modelli di business costruiti sull'estrazione dell'attenzione. Un secondo filone, più sofisticato, sostiene che i sistemi digitali di verifica dell'età stiano progressivamente re-architettando il web verso un modello in cui l'identità diventa parte dell'infrastruttura stessa e l'accesso alla rete non è più neutro ma mediato da nuovi livelli di verifica. Questo è il caso, ad esempio, degli articoli di Horkan e Dyne pubblicati a marzo 2026, che rappresentano bene questi due approcci critici.

Entrambe le posizioni colgono un aspetto importante: il tema non riguarda solo la tutela dei minori, ma il futuro dell'architettura di Internet. Organizzazioni come la Electronic Frontier Foundation (EFF) hanno sollevato preoccupazioni concrete sul rischio che la soluzione europea escluda rifugiati, persone senza documenti o senza fissa dimora (si veda in particolare la seconda parte della loro serie sulla verifica dell'età in Europa: https://www.eff.org/deeplinks/2025/04/age-verification-european-union-mini-id-wallet). EDRi ha sostenuto che la soluzione proposta dalla Commissione non offre garanzie di privacy sufficienti e che la verifica dell'età nel suo complesso è una forma di esclusione, non di emancipazione dei soggetti che intende proteggere (https://edri.org/our-work/why-age-verification-misses-the-mark-and-puts-everyone-at-risk/). Il Chaos Computer Club ha chiesto al Governo tedesco di rifiutare ogni forma di sorveglianza di massa e di ridurre la dipendenza dai giganti tecnologici.

Vale la pena soffermarsi sulla critica di EFF riguardo all'esclusione dei gruppi marginalizzati, perché è quella che più facilmente viene accolta

senza esame. L'argomento è che il *blueprint* (cioè le specifiche tecniche della soluzione europea), richiedendo un documento d'identità per l'attivazione, taglierebbe fuori rifugiati, persone senza fissa dimora e minori non accompagnati, poiché – appunto – sprovvisti di documenti. È una preoccupazione legittima, ma che presenta due debolezze significative.

In primo luogo, l'argomento confonde il perimetro attuale della soluzione europea con un'applicazione generalizzata che allo stato non esiste. La proposta europea si concentra per il momento sull'accesso a contenuti riservati agli adulti. In questo ambito, il requisito di un documento non è diverso da quanto già richiesto offline per comprare alcolici, entrare in un casinò o accedere a una slot machine. EFF non ha mai sostenuto che la richiesta di un documento per acquistare alcolici sia discriminatoria verso i rifugiati.

In secondo luogo, e questo è il punto decisivo, la critica EFF non offre alcuna soluzione alternativa concreta. La posizione dell'organizzazione, esplicitata nella terza parte della sua serie sulla verifica dell'età in Europa (https://www.eff.org/deeplinks/2025/05/keeping-people-safe-online-fundamental-rights-protective-alternatives-age-checks), è che la verifica dell'età non andrebbe fatta affatto. Questo, tuttavia, non può essere considerato un argomento a favore dell'inclusione dei rifugiati: è piuttosto un argomento a sostegno dell'abolizione dei sistemi digitali di verifica dell'età che utilizza i rifugiati come leva retorica. Se la preoccupazione fosse davvero l'accessibilità per i gruppi marginalizzati, la risposta coerente dovrebbe essere quella di chiedere percorsi di utilizzo più inclusivi, non l'eliminazione di qualsiasi protezione tout court. Proporre l'inazione strutturale in nome dell'inclusione, mentre le piattaforme continuano a esporre i minori, inclusi quelli più vulnerabili e appartenenti a gruppi marginalizzati, ad un ecosistema predatorio, non è una posizione inclusiva. È una rinuncia politica travestita da principio.

Le critiche sollevate sono serie, dunque meritano risposte altrettanto serie. Tuttavia, il loro limite comune emerge quando si passa all'analisi politica: finiscono per trattare la libertà quasi esclusivamente come assenza di ostacoli immediati. La libertà predicata consisterebbe in un "*accesso senza checkpoint, senza verifiche, senza mediazioni*". È una concezione intuitiva, persino seducente. Ma confonde la libertà formale di entrare in uno spazio con la libertà sostanziale di non essere dominati al suo interno. E soprattutto, difendendo l'"apertura" della rete senza interrogarsi sulla

proprietà delle infrastrutture, sulla concentrazione dei mercati digitali e sul ruolo delle piattaforme nel governare visibilità e attenzione, si finisce per opporsi ai nuovi livelli di controllo pubblico lasciando intatto il potere economico che già struttura lo spazio digitale.

Lo stesso limite si manifesta, in forma più sottile, anche nella richiesta, avanzata ad esempio dal Chaos Computer Club, di ridurre la dipendenza dai giganti tecnologici. La critica consisterebbe, in questo caso, nel fatto che qualsiasi meccanismo di verifica dell'età si fonda su *mobile device* messi a disposizione proprio da quei giganti tecnologici. È una richiesta legittima e necessaria, ma che rischia di restare altrettanto astratta se non viene ancorata a un'analisi dei rapporti di forza economici che producono quella dipendenza.

Chiedere meno dipendenza dalle grandi piattaforme senza interrogarsi su cosa rende strutturalmente inevitabile quella dipendenza equivale a criticare un effetto senza toccare la causa.

In questo quadro, la richiesta di "non dipendere dalle piattaforme" resta insufficiente se si limita a invocare soluzioni tecniche alternative, decentralizzazione, *open source*, interoperabilità, senza affrontare la struttura economica che riproduce la concentrazione. Un protocollo aperto in un mercato monopolistico verrà o assorbito o marginalizzato. Una soluzione *open source* senza una politica industriale che ne sostenga l'adozione resterà un esperimento di nicchia. La decentralizzazione tecnica, da sola, non produce decentralizzazione del potere economico: può anzi mascherarla, offrendo un'illusione di autonomia mentre le dinamiche di valorizzazione restano intatte. L'utente digitale è formalmente libero di scegliere la propria piattaforma, ma materialmente vincolato a infrastrutture che controllano l'accesso, la visibilità e le condizioni stesse dell'interazione sociale.

Il problema, quindi, non è solo tecnico ma politico-economico. Una critica che si fermi alla richiesta di indipendenza tecnologica senza mettere in discussione i rapporti di proprietà, i meccanismi di estrazione del valore e la struttura oligopolistica dei mercati digitali riproduce, paradossalmente, lo stesso schema che denuncia: propone soluzioni individuali o di comunità a problemi generati da rapporti di forza sistemici. È la stessa logica della privatizzazione della responsabilità, applicata questa volta non per trasferire responsabilità sociali dalla sfera pubblica alla famiglia o alla scuola, ma alla comunità tecnica o al movimento per il software libero.

Il nodo che il dibattito elude

Un Internet senza sistemi digitali di verifica dell'età non è affatto un Internet senza controllo. È semplicemente un Internet in cui il controllo è già operativo, ma in forma privata, opaca e diffusa. Non si esercita all'ingresso, ma dopo l'ingresso. Non si presenta come un gate visibile, ma come una trama continua di incentivi, catture, gerarchie di visibilità e meccanismi di dipendenza.

Il controllo passa per le architetture proprietarie delle piattaforme, per i ranking algoritmici, per i sistemi di raccomandazione, per il design persuasivo, per la profilazione comportamentale. Passa soprattutto per un modello economico preciso: l'attenzione come materia prima da estrarre, organizzare e monetizzare. Se i minori sono particolarmente vulnerabili, non è per un accidente: l'ambiente in cui si muovono è strutturato per sfruttare vulnerabilità cognitive, emotive e relazionali.

C'è però un punto che va precisato, perché la formulazione ormai corrente dell'"economia dell'attenzione" rischia di oscurare la reale natura del problema. In termini rigorosi, la materia prima delle piattaforme non è l'attenzione: è il comportamento umano ridotto a dato. L'attenzione è il meccanismo di cattura, non l'oggetto della valorizzazione. Ciò che viene estratto, organizzato e venduto è l'attività sociale degli utenti, le loro interazioni, preferenze, relazioni, ritmi quotidiani, che vengono trasformati in profili predittivi commerciabili. La differenza non è accademica. Cambia completamente il tipo di intervento necessario: se il problema fosse l'attenzione, basterebbe limitare il tempo di esposizione; se il problema è la trasformazione sistematica del comportamento in merce, la soluzione richiede un intervento sulla struttura stessa dell'estrazione e della proprietà dei dati.

Le piattaforme, inoltre, non si limitano a vendere un servizio in un mercato competitivo. Occupano una posizione strutturalmente analoga a quella del proprietario fondiario nell'economia classica: estraggono rendita non perché producano valore in proporzione ai loro profitti, ma perché controllano l'accesso a un'infrastruttura diventata condizione necessaria della partecipazione sociale, economica e persino politica. Chi vuole comunicare, informarsi, vendere, organizzarsi, cercare lavoro o semplicemente esistere nello spazio pubblico contemporaneo deve passare attraverso infrastrutture proprietarie che impongono le proprie condizioni. È una rendita di

posizione, non un profitto da innovazione. E come ogni rendita, più una piattaforma diventa infrastruttura indispensabile, più il suo potere di estrazione cresce indipendentemente dalla qualità del servizio offerto.

Questo spiega perché la semplice regolazione dei comportamenti delle piattaforme (come ad es. limitare i *dark patterns*, rendere trasparenti gli algoritmi, vietare la pubblicità comportamentale verso i minori, etc.), è necessaria ma strutturalmente fragile. La rendita infrastrutturale genera le risorse economiche e il potere lobbistico per erodere, aggirare o catturare qualsiasi regolazione, esattamente come è avvenuto con la regolazione finanziaria dopo il 2008. Il che non è un argomento contro la regolazione, ma un argomento per non illudersi che la regolazione sia sufficiente.

Chi dice "*il problema non è l'accesso, ma ciò che avviene dentro le piattaforme*" predica una verità importante, ma la semplice asserzione risulta insufficiente se non ne trae una conseguenza strutturale. Se il danno è prodotto da modelli di business estrattivi e da architetture manipolative, il problema non può essere risolto scaricando l'adozione di adeguate misure di tutela sulla famiglia, sulla scuola o sul singolo utente. Le famiglie dovrebbero essere in grado di compensare ciò che le piattaforme progettano. Gli insegnanti dovrebbero riuscire ad arginare ciò che i mercati incentivano. I singoli utenti dovrebbero difendersi "privatamente" da infrastrutture costruite per neutralizzare la loro capacità di scelta. È il passaggio ideologico classico: il problema è sistemico, ma la responsabilità viene trasferita dalla sfera pubblica a quella privata.

Il rischio reale: controllo privato e sorveglianza pubblica

Sarebbe però un errore speculare liquidare frettolosamente ogni critica ai sistemi digitali di verifica dell'età. Il rischio che la tutela dei minori venga usata come cavallo di Troia per normalizzare nuove forme di tracciamento è reale. Le architetture contano. Gli standard contano. I livelli dello *stack* in cui una soluzione viene collocata contano. E contano gli attori che ne controllano l'implementazione.

EFF ed EDRi hanno ragione quando insistono su questi punti. Il Chaos Computer Club ha ragione quando chiede che queste infrastrutture non alimentino nuove dipendenze dai giganti tecnologici. Queste critiche

diventano problematiche solo quando si fermano qui, perché denunciare il rischio della sorveglianza pubblica senza affrontare il dominio privato già esistente significa proporre una libertà puramente nominale.

Il nodo non può essere ridotto alla domanda “sistemi digitali di verifica dell'età sì o no?”. La vera domanda è: quale tipo di verifica, con quale minimizzazione dei dati, sotto quale governance, con quali limiti funzionali e con quali effetti sulla struttura del mercato? Il rischio è duplice: da un lato, lasciare i minori esposti a un ecosistema predatorio in nome di una libertà astratta; dall’altro, costruire infrastrutture intrusive che trasformino il controllo dell’età in un sistema generale di tracciamento.

Da dove partire: quattro elementi per una proposta adeguata

Una posizione politica adeguata sul punto dovrebbe sapersi sottrarre a questa falsa alternativa. Si tratta di affrontare il problema sotto una prospettiva completamente diversa: la verifica dell’età, quando necessaria, deve essere ridotta a una prova minimale e non trasformarsi mai in identificazione della persona. Il sistema deve “dire il meno possibile”: non chi sei, non dove vai, non cosa fai, ma solo se superi una certa soglia di età. Questa prova non deve essere riusabile come identità generale e non deve generare tracciabilità tra servizi diversi.

La protezione dei minori non può diventare la via surrettizia per imporre meccanismi generalizzati di tracciamento.

Ma la minimizzazione tecnica, da sola, non basta. Anche la migliore soluzione privacy-preserving sarebbe insufficiente se venisse usata come alibi per non intervenire sul vero motore economico del problema. Verificare l’età senza toccare recommendation systems, dark patterns e monetizzazione dell’attenzione significa aggiungere una barriera all’ingresso senza trasformare l’ambiente che produce il danno.

Per questo una proposta adeguata deve tenere insieme almeno quattro elementi.

Primo: una verifica dell’età strettamente minimizzata, non identificante, non tracciabile e interoperabile, progettata come prova di soglia e non come credenziale generale.

Secondo: una regolazione più aggressiva delle piattaforme, che contempli obblighi di *safety by design*, limiti ai *dark patterns*, trasparenza sui sistemi di raccomandazione, vincoli più forti alla profilazione e alla pubblicità comportamentale verso i minori.

Terzo: una governance che impedisca sia la centralizzazione pubblica indiscriminata sia la privatizzazione oligopolistica di questa infrastruttura. La verifica dell'età non deve diventare né un registro generalizzato né una nuova rendita infrastrutturale per Big Tech, *browser vendor*, *app store* o grandi intermediari dell'identità.

Quarto: il rifiuto della privatizzazione della responsabilità sociale. Famiglia e scuola hanno un ruolo importante, ma non possono essere l'ultima diga chiamata a contenere problemi prodotti su larga scala da apparati industriali. La protezione dei minori deve tornare a essere una responsabilità collettiva, sostenuta da regole pubbliche e da una politica regolatoria capace di incidere sui modelli di business.

Questi quattro elementi operano tutti dentro il quadro esistente dei rapporti di proprietà. Non mettono in discussione la proprietà privata delle infrastrutture digitali, né la legittimità dell'estrazione di rendita da parte delle piattaforme, né la struttura monopolistica del mercato in quanto tale. È una proposta riformista, e conviene dirlo apertamente. Interviene sugli effetti senza modificare i rapporti di proprietà che li producono.

La domanda che resta sullo sfondo, e a cui questo articolo non pretende di rispondere, è allora se sia possibile proteggere davvero i minori senza intervenire sulla struttura proprietaria delle piattaforme, o se qualsiasi regolazione, per quanto sofisticata, verrà progressivamente erosa dai soggetti che si propone di regolare. Non porre questa domanda significherebbe cadere nello stesso errore che l'articolo contesta: trattare i rapporti di potere economico come un dato naturale anziché come il terreno su cui si gioca il conflitto. Porla esplicitamente, riconoscendo che i quattro elementi sopra individuati devono essere compresenti in un intervento necessario ma che potrebbe non essere sufficiente, è l'unico modo per tenere aperto l'orizzonte politico senza rinunciare all'efficacia dell'azione concreta nel presente.

La proposta europea: un inizio nella direzione giusta

La Commissione europea ha pubblicato il 14 luglio 2025 le specifiche e il codice *open source* che implementa una soluzione per la verifica dell'età. La soluzione è *open source*, *privacy-preserving* e interoperabile con i futuri EUDI Wallets. Cinque paesi, Danimarca, Francia, Grecia, Italia e Spagna, partecipano alla fase pilota. La seconda versione ha introdotto l'attivazione tramite passaporto e carta d'identità. La soluzione consente all'utente di provare di avere più di 18 anni senza rivelare altre informazioni personali, con processi di emissione e presentazione gestiti da entità separate.

La Commissione collega esplicitamente il *blueprint* alle linee guida DSA sulla protezione dei minori, pubblicate anch'esse nel luglio 2025. Queste linee guida affrontano *addictive design*, controllo delle raccomandazioni, account privati di default, limiti ai *dark patterns* e a pratiche commerciali manipolative verso i minori. Non si tratta quindi di una soluzione per la verifica dell'età isolata, ma di un pacchetto regolatorio che tiene insieme verifica dell'età e trasformazione dell'ambiente digitale, esattamente secondo l'approccio che questo articolo sostiene.

Con una avvertenza già esplicitata: questo pacchetto opera dentro un campo di forze in cui i soggetti regolati dispongono delle risorse economiche e del potere lobbistico per eroderne progressivamente l'efficacia. Il che non è un argomento per rinunciare alla regolazione, ma per non trattarla come un risultato acquisito: è un terreno di conflitto permanente, non una soluzione stabile.

Sarebbe tuttavia poco serio trattare l'iniziativa della Commissione come un atto puramente protettivo, senza interrogarsi sulle ragioni strutturali che l'hanno resa possibile. Il *blueprint* per sistemi digitali di verifica dell'età non nasce nel vuoto: nasce all'interno della strategia europea di costruzione dell'EUDI Wallet, che a sua volta risponde all'esigenza geopolitica dell'UE di dotarsi di un'infrastruttura di identità digitale non dipendente dalle grandi piattaforme.

La verifica dell'età è, tra i possibili casi d'uso dell'identità digitale europea, quello politicamente più "spendibile", la protezione dei minori genera consenso trasversale e riduce le resistenze all'adozione di una nuova infrastruttura. Questo non significa che la tutela dei minori sia un pretesto. Significa che è anche il veicolo attraverso cui si legittima e si accelera un progetto infrastrutturale più ampio, con le proprie logiche di potere e di competizione tra blocchi economici. Riconoscere questa doppia natura non

indebolisce la proposta: la rende più lucida. Chi lavora su queste architetture deve essere consapevole di operare dentro un campo di forze che eccede la tutela dei minori, e deve vigilare affinché la protezione dei minori resti il fine reale e non diventi la giustificazione residuale di un'infrastruttura che si espande per ragioni proprie.

Bisogna però essere onesti sui limiti. Le linee guida DSA non sono vincolanti: costituiscono un *benchmark* per la valutazione della conformità, ma non impongono obblighi diretti. L'adozione effettiva dipende dagli Stati membri e dalla volontà politica dei Digital Services Coordinators nazionali. La soluzione europea non è definitiva.

È però un inizio rilevante. Ed è per questo che appare centrale che il dibattito intorno a questa soluzione abbandoni gli slogan sulla "fine dell'Internet aperto" e si concentri su una critica più seria del potere economico che governa lo spazio digitale e, allo stesso tempo, offra contributi tecnici e politici capaci di migliorare le soluzioni concretamente implementate.

Se il confronto pubblico resta fermo alla denuncia astratta della sorveglianza non si andrà molto lontano. Se invece prova a misurarsi con architetture, standard, governance e rapporti di forza, può ancora aiutare a costruire una protezione reale dei minori senza normalizzare il tracciamento.

Protecting Minors Online, the Knot the Debate Ignores

Age verification, platform power, and the limits of a critique that stops at surveillance. The EU attempts to suggest solutions for the necessary protections within a web dominated by the interests of Big Tech.

Verso Zero

Pubblicato il 18.04.2026:

The contemporary debate on digital age verification systems suffers from a recurring limitation: it tends to reduce itself to an opposition between “protecting minors” and “freedom of the internet”, almost never engaging with the merits of the technical architectures, the regulatory alternatives, and above all the relations of economic power that actually structure the digital environment. The problem is thereby systematically displaced from the material terrain of infrastructures and business model – that is, from the place where economic power is actually exercised in the digital environment – to the theoretical plane, in some ways more “comfortable”, of mere external interference (by these digital control mechanisms) on the individual subject.

This is precisely the limit we seek to bring into focus: mistaking the formal freedom of the isolated user for real emancipation, while leaving intact the substantive dominance exercised by platforms and their operators in cyberspace. What is criticised, in other words, is the potential public or regulatory control introduced through digital age verification systems aimed at protecting minors, while the private control already in place is naturalised – control embedded in the architectures of platforms, in algorithms, in attention-capture mechanisms, and in the subordination of online experience to the production of profit.

The exposure of minors to certain digital mechanisms is real and daily. For precisely this reason, a political reading is needed to bring the discussion back into order: not to deny the risks of surveillance, but to situate them within the broader problem of the power relations and infrastructures that shape today's internet.

What we are talking about when we talk about online age verification

Online age verification is the problem – technical, legal, and political – of ascertaining that whoever accesses a given digital service has the required age to do so. For decades, access to any service has relied on self-declaration: a click on "I am over 18", a made-up date of birth, and the trick was done. The result has been that minors have been exposed without any filter or caution whatsoever to a digital environment designed to maximise engagement and data extraction from anyone who accesses it, regardless of age. According to the European Commission, 97% of young people in the EU use the internet daily and more than one in ten show signs of problematic behaviour in their use of platforms.

The political pressure to intervene is today extremely strong: Australia, France, Spain, the United Kingdom, and several other countries have introduced or are introducing restrictions on minors' access to social networks. In Italy, bipartisan legislative proposals are under discussion.

The European Parliament has voted a resolution proposing a minimum age of 16. But the knot remains unchanged: how do you verify age without registering the users of the internet? The more intrusive alternatives require identity documents or biometric data, creating vulnerable databases. The European Union is working on a different approach: a system that generates a token containing only the attestation of majority age, with the goal of integrating zero-knowledge cryptographic proofs as explained in the final section. The testing phase is underway in five countries.

It is this solution – its architectures, its political implications, and the relations of economic power surrounding it – that is the subject of this article.

The criticisms of the European age verification system and their limits

In recent months, critical interventions have circulated regarding digital age verification systems, and in particular the European one. It is worth engaging with the most serious of these, because they identify real problems – even when the conclusions they reach do not allow for the identification of satisfactory solutions.

A first line of critique argues that protecting minors must not turn into an access-control system. The problem, it is argued, would not be so much "who enters" (that is, who accesses certain digital content) as "what happens once inside": recommendation systems, dark patterns – that is, those interface design techniques devised to manipulate the user's choices, pushing them toward actions they would not have taken spontaneously: accepting unfavourable terms, giving up personal data, staying connected longer, making unwanted purchases – compulsive design, business models built on the extraction of attention. A second line, more sophisticated, argues that digital age verification systems are progressively re-architecting the web toward a model in which identity becomes part of the infrastructure itself and access to the network is no longer neutral but mediated by new layers of verification. This is the case, for example, with articles by Horkan and Dyne published in March 2026, which well represent these two critical approaches.

Both positions capture an important aspect: the issue concerns not only the protection of minors, but the future of the architecture of the internet. Organisations such as the Electronic Frontier Foundation (EFF) have raised concrete concerns about the risk that the European solution will exclude refugees, undocumented persons, or people without a fixed address (see in particular the second part of their series on age verification in Europe: https://www.eff.org/deeplinks/2025/04/age-verification-european-union-mini-id-wallet). EDRi has argued that the solution proposed by the Commission does not offer sufficient privacy guarantees and that age verification as a whole is a form of exclusion, not of emancipation for the subjects it intends to protect (https://edri.org/our-work/why-age-verification-misses-the-mark-and-puts-everyone-at-risk/). The Chaos Computer Club has asked the German government to reject any form of mass surveillance and to reduce dependence on the tech giants.

It is worth dwelling on the EFF's critique regarding the exclusion of marginalised groups, because it is the one most readily accepted without scrutiny. The argument is that the blueprint (that is, the technical

specifications of the European solution), by requiring an identity document for activation, would cut out refugees, homeless people, and unaccompanied minors since – precisely – they lack documents. It is a legitimate concern, but one that has two significant weaknesses.

In the first place, the argument conflates the current scope of the European solution with a generalised application that currently does not exist. The European proposal focuses for the moment on access to adult-only content. In this domain, the requirement of a document is no different from what is already required offline to buy alcohol, enter a casino, or access a slot machine. EFF has never argued that requiring a document to buy alcohol is discriminatory toward refugees.

In the second place – and this is the decisive point – the EFF critique offers no concrete alternative solution. The organisation's position, spelled out in the third part of its series on age verification in Europe (https://www.eff.org/deeplinks/2025/05/keeping-people-safe-online-fundamental-rights-protective-alternatives-age-checks), is that age verification should not be done at all. This, however, cannot be considered an argument in favour of the inclusion of refugees: it is rather an argument in support of abolishing digital age verification systems that uses refugees as rhetorical leverage. If the concern were truly accessibility for marginalised groups, the coherent response would be to call for more inclusive usage pathways, not the elimination of any protection tout court. Proposing structural inaction in the name of inclusion, while platforms continue to expose minors – including the most vulnerable and those belonging to marginalised groups – to a predatory ecosystem, is not an inclusive position. It is a political renunciation disguised as principle.

The criticisms raised are serious, and therefore deserve equally serious responses. Nevertheless, their common limit emerges once one moves to political analysis: they end up treating freedom almost exclusively as the absence of immediate obstacles. The freedom advocated would consist in *"access without checkpoints, without verifications, without mediations"*. It is an intuitive, even seductive conception. But it conflates the formal freedom to enter a space with the substantive freedom of not being dominated within it. And above all, by defending the "openness" of the network without questioning the ownership of the infrastructures, the concentration of digital markets, and the role of platforms in governing visibility and attention, one

ends up opposing new layers of public control while leaving intact the economic power that already structures the digital space.

The same limit manifests itself, in a more subtle form, also in the call – advanced for example by the Chaos Computer Club – to reduce dependence on the tech giants. The critique consists, in this case, in the fact that any age verification mechanism rests on *mobile devices* provided by those very tech giants. It is a legitimate and necessary demand, but one that risks remaining just as abstract if it is not anchored to an analysis of the economic power relations that produce that dependence.

Demanding less dependence on the large platforms without questioning what makes that dependence structurally inevitable amounts to criticising an effect without touching the cause.

In this framework, the call for "non-dependence on platforms" remains insufficient if it limits itself to invoking alternative technical solutions – decentralisation, *open source*, interoperability – without addressing the economic structure that reproduces concentration. An open protocol in a monopolistic market will either be absorbed or marginalised. An *open-source* solution without an industrial policy supporting its adoption will remain a niche experiment. Technical decentralisation, on its own, does not produce decentralisation of economic power: it may indeed mask it, offering an illusion of autonomy while the dynamics of valorisation remain intact. The digital user is formally free to choose their platform, but materially bound to infrastructures that control access, visibility, and the very conditions of social interaction.

The problem, therefore, is not merely technical but political-economic. A critique that stops at the call for technological independence without questioning property relations, value-extraction mechanisms, and the oligopolistic structure of digital markets paradoxically reproduces the very pattern it denounces: it proposes individual or community-based solutions to problems generated by systemic power relations. It is the same logic of the privatisation of responsibility, applied this time not to transfer social responsibilities from the public sphere to the family or the school, but to the technical community or the free-software movement.

The knot the debate eludes

An internet without digital age verification systems is by no means an internet without control. It is simply an internet in which control is already operating, but in private, opaque, and diffuse form. It is not exercised at the entrance, but after the entrance. It does not present itself as a visible gate, but as a continuous weave of incentives, captures, hierarchies of visibility, and mechanisms of dependence.

Control passes through the proprietary architectures of platforms, through algorithmic rankings, through recommendation systems, through persuasive design, through behavioural profiling. Above all, it passes through a precise economic model: attention as raw material to be extracted, organised, and monetised. If minors are particularly vulnerable, this is not by accident: the environment in which they move is structured to exploit cognitive, emotional, and relational vulnerabilities.

There is, however, a point that needs to be clarified, because the now current formulation of the “attention economy” risks obscuring the real nature of the problem. In rigorous terms, the raw material of platforms is not attention: it is human behaviour reduced to data. Attention is the capture mechanism, not the object of valorisation. What is extracted, organised, and sold is the social activity of users – their interactions, preferences, relationships, daily rhythms – transformed into commercialisable predictive profiles. The difference is not academic. It completely changes the kind of intervention required: if the problem were attention, it would suffice to limit exposure time; if the problem is the systematic transformation of behaviour into commodity, the solution requires intervention on the very structure of extraction and ownership of data.

Platforms, moreover, do not merely sell a service in a competitive market. They occupy a position structurally analogous to that of the landowner in classical economics: they extract rent not because they produce value in proportion to their profits, but because they control access to an infrastructure that has become a necessary condition of social, economic, and even political participation. Those who wish to communicate, inform themselves, sell, organise, look for a job, or simply exist in the contemporary public space must pass through proprietary infrastructures

that impose their own conditions. It is a positional rent, not an innovation profit. And like any rent, the more a platform becomes an indispensable infrastructure, the more its extractive power grows independently of the quality of the service offered.

This explains why the mere regulation of platform behaviour (such as limiting dark patterns, making algorithms transparent, banning behavioural advertising to minors, etc.) is necessary but structurally fragile. Infrastructural rent generates the economic resources and lobbying power to erode, circumvent, or capture any regulation – exactly as happened with financial regulation after 2008. Which is not an argument against regulation, but an argument for not deluding oneself that regulation is sufficient.

Those who say "*the problem is not access, but what happens inside the platforms*" preach an important truth, but the mere assertion is insufficient if no structural consequence is drawn from it. If the harm is produced by extractive business models and manipulative architectures, the problem cannot be solved by offloading the adoption of adequate protective measures onto the family, the school, or the individual user. Families would have to be able to compensate for what platforms design. Teachers would have to manage to stem what markets incentivise. Individual users would have to defend themselves "privately" against infrastructures built to neutralise their capacity to choose. It is the classic ideological move: the problem is systemic, but responsibility is transferred from the public to the private sphere.

The real risk: private control and public surveillance

It would however be a mirror-image error to hastily dismiss every criticism of digital age verification systems. The risk that the protection of minors may be used as a Trojan horse to normalise new forms of tracking is real. Architectures matter. Standards matter. The layers of the stack in which a solution is placed matter. And the actors who control its implementation matter.

EFF and EDRi are right when they insist on these points. The Chaos Computer Club is right when it asks that these infrastructures not fuel new dependencies on the tech giants. These criticisms become problematic only when they stop there, because denouncing the risk of public surveillance

without addressing the already-existing private dominance means proposing a purely nominal freedom.

The knot cannot be reduced to the question “digital age verification systems yes or no?” The real question is: what kind of verification, with what data minimisation, under what governance, with what functional limits, and with what effects on the structure of the market? The risk is twofold: on the one hand, leaving minors exposed to a predatory ecosystem in the name of an abstract freedom; on the other, building intrusive infrastructures that turn age control into a general tracking system.

Where to start: four elements for an adequate proposal

An adequate political position on the point should know how to escape this false alternative. The matter is to approach the problem from a completely different perspective: age verification, when necessary, must be reduced to a minimal proof and must never turn into identification of the person. The system must “say as little as possible”: not who you are, not where you go, not what you do, but only whether you exceed a certain age threshold. This proof must not be reusable as a general identity and must not generate traceability across different services.

The protection of minors cannot become the surreptitious route to impose generalised tracking mechanisms.

But technical minimisation, on its own, is not enough. Even the best privacy-preserving solution would be insufficient if it were used as an alibi for not intervening on the real economic engine of the problem. Verifying age without touching recommendation systems, dark patterns, and the monetisation of attention means adding a barrier at the entrance without transforming the environment that produces the harm.

For this reason, an adequate proposal must hold together at least four elements.

First: an age verification strictly minimised, non-identifying, non-traceable and interoperable, designed as a threshold proof and not as a general credential.

Second: a more aggressive regulation of platforms, contemplating safety-by-design obligations, limits on dark patterns, transparency on

recommendation systems, and stronger constraints on profiling and behavioural advertising toward minors.

Third: a governance that prevents both indiscriminate public centralisation and oligopolistic privatisation of this infrastructure. Age verification must become neither a generalised registry nor a new infrastructural rent for big tech, browser vendors, app stores, or large identity intermediaries.

Fourth: the refusal of the privatisation of social responsibility. Family and school play an important role, but cannot be the last dam called upon to contain problems produced on a large scale by industrial apparatuses. The protection of minors must return to being a collective responsibility, sustained by public rules and by a regulatory policy capable of affecting business models.

These four elements all operate within the existing framework of property relations. They do not call into question the private ownership of digital infrastructures, nor the legitimacy of rent extraction by platforms, nor the monopolistic structure of the market as such. It is a reformist proposal, and it is best to say so openly. It intervenes on the effects without modifying the property relations that produce them.

The question that remains in the background – and which this article does not claim to answer – is therefore whether it is possible to really protect minors without intervening on the proprietary structure of platforms, or whether any regulation, however sophisticated, will be progressively eroded by the subjects it sets out to regulate. Not to pose this question would be to fall into the same error the article contests: treating relations of economic power as a natural given rather than as the terrain on which the conflict is played out. Posing it explicitly, while recognising that the four elements identified above must be co-present in an intervention that is necessary but might not be sufficient, is the only way to keep the political horizon open without renouncing the effectiveness of concrete action in the present.

The European proposal: a beginning in the right direction

On 14 July 2025, the European Commission published the specifications and the open-source code implementing a solution for age verification. The solution is open source, privacy-preserving, and interoperable with the

future EUDI Wallets. Five countries – Denmark, France, Greece, Italy, and Spain – are participating in the pilot phase. The second version introduced activation via passport and identity card. The solution allows the user to prove being over 18 without revealing any other personal information, with issuance and presentation processes managed by separate entities.

The Commission explicitly links the *blueprint* to the DSA guidelines on the protection of minors, also published in July 2025. These guidelines address addictive design, control of recommendations, private accounts by default, limits on dark patterns, and manipulative commercial practices toward minors. It is therefore not an isolated age-verification solution, but a regulatory package that holds together age verification and the transformation of the digital environment, exactly in line with the approach this article advocates.

With a caveat already made explicit: this package operates within a field of forces in which the regulated subjects possess the economic resources and lobbying power to progressively erode its effectiveness. Which is not an argument for giving up on regulation, but for not treating it as an acquired result: it is a terrain of permanent conflict, not a stable solution.

It would nevertheless be unserious to treat the Commission's initiative as a purely protective act, without questioning the structural reasons that made it possible. The *blueprint* for digital age verification systems does not arise in a vacuum: it is born within the European strategy of constructing the EUDI Wallet, which in turn responds to the EU's geopolitical need to equip itself with a digital identity infrastructure not dependent on the large platforms.

Age verification is, among the possible use cases of European digital identity, the one politically most "spendable": the protection of minors generates cross-cutting consensus and reduces resistance to the adoption of a new infrastructure. This does not mean that the protection of minors is a pretext. It means that it is also the vehicle through which a broader infrastructural project is legitimised and accelerated, with its own logics of power and competition between economic blocs. Recognising this dual nature does not weaken the proposal: it makes it more lucid. Those who work on these architectures must be aware of operating within a field of forces that exceeds the protection of minors, and must be vigilant so that the

protection of minors remains the real goal and does not become the residual justification of an infrastructure expanding for reasons of its own.

One must, however, be honest about the limits. The DSA guidelines are not binding: they constitute a benchmark for compliance assessment, but impose no direct obligations. Actual adoption depends on the Member States and on the political will of the national Digital Services Coordinators. The European solution is not definitive.

It is, however, a relevant beginning. And it is for this reason that it appears central that the debate around this solution should abandon the slogans about the “end of the open internet” and concentrate on a more serious critique of the economic power governing the digital space and, at the same time, offer technical and political contributions capable of improving the solutions concretely implemented.

If public debate remains stuck at the abstract denunciation of surveillance, it will not go very far. If, on the other hand, it tries to grapple with architectures, standards, governance, and power relations, it can still help to build a real protection of minors without normalising tracking.