390

9 settembre 2026

ISTITUTO BRUNO LEONI
IDEE PER IL LIBERO MERCATO

IBL Focus

Age verification e deroga ePrivacy

Normalizzazione della sorveglianza preventiva in Italia e in Europa

Di Claudia Giulia Ferrauto

1. Introduzione

Il dibattito sulla protezione dei minori online ha assunto, tra il 2025 e il 2026, una dimensione operativa e istituzionale di crescente portata. In Italia, il Decreto Caivano e le successive delibere dell'Autorità per le garanzie nelle comunicazioni (AGCOM) hanno introdotto obblighi di verifica dell'età per l'accesso a contenuti per adulti (pornografici). Nel frattempo, a livello europeo, il Parlamento ha approvato, il 9 luglio 2026, la proroga della deroga, temporanea negli intenti iniziali, alla direttiva ePrivacy, consentendo alle piattaforme online di proseguire, su base volontaria - senza alcuna possibilità di opposizione lato utente - la scansione delle comunicazioni non cifrate alla ricerca di materiale di abuso sessuale su minori (CSAM)[1].

Queste misure, sebbene viaggino in modalità formalmente distinte, condividono un presupposto comune critico e potenzialmente destabilizzante: l'idea che il giusto obiettivo della tutela dei minori giustifichi l'introduzione di meccanismi preventivi, massivi e infrastrutturali di identificazione e/o di monitoraggio di contenuti e di chi ne fruisce, coinvolgendo indistintamente tutta la popolazione, ossia milioni di cittadini incensurati e nell'assenza di specifici mandati da parte dell'autorità giudiziaria. Il presente contributo analizza il caso italiano dell'age verification - con particolare attenzione al ruolo di SPID, CIE e IT Wallet - collocandolo nel contesto della deroga ePrivacy, al fine di evidenziare come sia in corso una spinta univoca e preoccupante che rischia di erodere la tutela al diritto di riservatezza delle comunicazioni private e dell'autonomia personale di milioni di cittadini.

2. Dal Decreto Caivano al voto del 9 luglio 2026

L'articolo 13-bis del Decreto Caivano ha imposto ai gestori di siti e piattaforme che diffondono contenuti pornografici accessibili dall'Italia l'obbligo di verificare la maggiore età degli utenti. La delibera AGCOM n. 96/25/CONS dell'8 aprile 2025 ha definito le modalità tecniche di attuazione, prevedendo un sistema di "doppio anonimato" basato su certificati terzi che rilasciano attestati (token) di conferma della maggiore età. I termini di adeguamento erano scaglionati: novembre 2025 per i soggetti (siti e piat-

Claudia Giulia Ferrauto è analista indipendente in comunicazione e tecnologia, ha collaborato con *Il Foglio* e *Il Sole 24 Ore*. Autrice di "Intelligenza Artificiale: cos'è davvero" (Bollati Boringhieri).

1 CSAM: Child Sexual Abuse Material (materiale di abuso sessuale su minori).

taforme) stabiliti in Italia e febbraio 2026 per quelli stabiliti in altri Stati membri.

Nel medesimo arco temporale, il dibattito europeo sulla proroga della deroga ePrivacy -scaduta il 3 aprile 2026 - è giunto a maturazione. Il 9 luglio 2026, nonostante una maggioranza semplice di voti in Parlamento europeo contraria alla proroga, questa è comunque passata grazie all'espediente della procedura d'urgenza e resterà in vigore fino al 3 aprile 2028 Tale procedura prevede la necessità di una maggioranza qualificata (assoluta) per bloccare la proposta della Commissione. La deroga approvata in queste modalità consente quindi legalmente ai fornitori di servizi di comunicazione elettronica di scandagliare le comunicazioni degli utenti al fine di poter, eventualmente, anche rilevare materiale CSAM in tutte le comunicazioni non cifrate (e-mail, messaggistica istantanea social non criptata eccetera), escludendo esplicitamente i sistemi che adottano l'end-to-end encryption (quali Whatsapp, Signal, Telegram).

La convergenza temporale tra l'operatività dell'age verification italiana e il voto sulla deroga ePrivacy fa acquisire a questi provvedimenti un orizzonte unitario di carattere fortemente critico. Entrambe le iniziative si inseriscono infatti in un quadro più ampio di politiche europee e nazionali che privilegiano strumenti preventivi di controllo e sorveglianza di massa, rispetto a interventi mirati e giurisdizionalmente autorizzati.

3. L'age verification italiana: architettura normativa e tecnica

Il sistema italiano di verifica dell'età, cui oggi tutta la popolazione dovrebbe fare riferimento per avere accesso a contenuti per adulti, si fonda sul principio di minimizzazione dei dati e sul modello del "doppio anonimato": un soggetto terzo certificato emette una prova dell'età che conferma unicamente la maggiore età dell'utente, senza trasmettere l'identità completa al sito destinatario. Queste prove possono essere generate tramite SPID, CIE o soluzioni basate su IT Wallet nell'App IO.

Sebbene questo approccio di verifica nasca oggi come strumento limitato all'accesso alla pornografia, il modello è stato rapidamente invocato per l'utilizzo diffuso in altri ambiti (accesso ai social media, o ad altri contenuti leciti di varia natura), sempre in coerenza con lo stendardo aulico di adempiere così alle obbligazioni di tutela dei minori previste dal Digital Services Act. Tuttavia l'architettura prescelta crea, di fatto, un sistema di gatekeeper obbligatori tra l'utente e l'accesso a contenuti leciti, spostando il baricentro dalla responsabilità genitoriale e personale, dalle indagini mirate, verso una verifica preventiva e una supervisione paternalistica collettiva generalizzata.

4. SPID, CIE e IT Wallet: l'infrastruttura di autenticazione e i suoi rischi strutturali

Un punto nodale - trascurato dal dibattito pubblico - risiede nella natura delle infrastrutture di autenticazione. L'autenticazione avviene attraverso canali preposti: l'utilizzo della Carta d'Identità Elettronica (CIE), che collega direttamente l'utente a database statali centralizzati, e dove, anche in presenza del "doppio anonimato" a valle, i log relativi alle richieste di token "18+" possono conservare traccia del fatto che un soggetto chiaramente identificato (nome, cognome, codice fiscale) ha richiesto accesso (nel tal orario, del tal giorno) a una determinata categoria di conte-

nuti adulti. Poiché al momento tale categoria afferisce esclusivamente a contenuti sessuali espliciti e per legge l'ambito sessuale rappresenta un ambito specifico di legittima tutela, va sottolineato che la conservazione di tali log può rappresentare un elemento discriminante. Nonostante questo, il metadato temporale e categoriale rimane disponibile a livello di infrastruttura pubblica centralizzata o delegata, secondo il mezzo scelto per l'autenticazione.

Un altro sistema di accesso e verifica infatti è offerto dal Sistema Pubblico di Identità Digitale (SPID), gestito da Identity Provider privati in concorrenza tra loro, che distribuisce i log d'accesso, riducendo il rischio di controllo centralizzato, esponendo tuttavia i gestori a responsabilità elevate in caso di data breach e comunque non elimina la registrazione e la possibile conservazione della richiesta di attestato. Ci sono poi le soluzioni basate su IT Wallet e token on-device, nate per migliorare la privacy (locale), ma anche queste non cancellano la traccia a monte.

Il rischio strutturale è chiaro: lo Stato e i soggetti gestori sanno - o possono sapere - che un determinato cittadino, identificato in modo distinto e univoco, ha richiesto accesso a contenuti di una certa natura. Questo rischio riguarda tutta la popolazione e coinvolge quindi anche figure professionali e istituzionali particolarmente esposte: politici, attivisti, avvocati, giornalisti. Questa conoscenza, oggi limitata alla pornografia e dedicata alla tutela dei minori, sarà però potenzialmente estensibile ad altre categorie di contenuti o servizi. Si tratta di un'infrastruttura di identificazione preventiva che sopravvive alla singola normativa, creando le condizioni per il function creep[2], cioè l'espansione dell'utilizzo ben al di là degli obiettivi inizialmente dichiarati.

In termini tecnici, le tracce residue si dividono in due tipi principali. A monte, presso l'Identity Provider o il soggetto certificatore, permane un metadato che collega un soggetto identificato alla richiesta di una prova di maggiore età in un determinato momento; le tempistiche di conservazione di tali log dipendono dalle policy dei gestori e dalle norme sulla conservazione dei dati di autenticazione. A valle, il token presentato sul sito può essere monouso o a breve validità (spesso legato alla sessione o a scadenza dopo periodi di inattività), ma può comunque restare memorizzato sul dispositivo dell'utente o nell'app/wallet, lasciando tracce tecniche residue. Il sistema di "doppio anonimato", così efficace nella sua dicitura nominale, riduce significativamente l'esposizione al fornitore di contenuti, ma non elimina del tutto la possibilità di ricostruzione a livello dell'infrastruttura di autenticazione[3].

5. Criticità giuridiche e tensioni con i principi dell'Unione Europea

Le misure sollevano questioni di compatibilità con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE e con i principi di necessità, proporzionalità e minimizzazione previsti dal GDPR. La giurisprudenza della Corte di giustizia ha più volte

2 Function creep: espansione progressiva e non prevista dell'uso di una tecnologia o infrastruttura oltre il fine originario.

3 Nel sistema del doppio anonimato, l'attestato trasferito al sito finale contiene unicamente la conferma della maggiore età, senza dati identificativi; resta tuttavia la traccia a livello di infrastruttura di autenticazione.

censurato forme di sorveglianza generalizzata e indiscriminata[4]. Il doppio anonimato, che rappresenta un tentativo di bilanciamento, non elimina né le criticità del metadato, né la natura di sostituzione preventiva e generalizzata della responsabilità genitoriale, che nella sua applicazione concreta - indirizzata alla tutela dei minori impedendo loro di accedere a contenuti pornografici dai device dati loro dalle famiglie - va a costituire di fatto un sistema di controllo di massa.

Si configura quindi una forma di sorveglianza e supervisione della popolazione generale in totale assenza di sospetto individuale, in tensione con la presunzione di non colpevolezza. Il Garante per la protezione dei dati personali ha espresso pareri cauti, sottolineando la necessità di ulteriori garanzie[5].

6. La deroga ePrivacy e la proroga di Chat Control: la dimensione europea della stessa logica

La proroga della deroga ePrivacy varata con la procedura d'urgenza lo scorso 9 luglio 2026 opera secondo una logica analoga all'age verification, seppur muovendosi in modo diverso e distinto. La misura prevede un sistema di scansione di dati di massa che – seppur formalmente volontaria per le piattaforme – crea incentivi e fragilità strutturali che possono non solo renderla prassi diffusa, ma creare un substrato di normalità legislativa che si muove in contraddizione dei diritti civili e individuali. Le comunicazioni non cifrate - quali ad esempio le e-mail, o i messaggi su piattaforme che non adottano end-to-end encryption – diventano permeabili a controlli sistematici eseguiti silenziosamente e senza che gli utenti possano avere alcuna certezza personale, da vari fornitori, poiché essi sono autorizzati - e qui risiede una delle preoccupazioni principali - dal quadro normativo europeo.

Inoltre, non esiste un obbligo generalizzato e standardizzato di informare individualmente ogni utente in modo chiaro e preventivo sulla scansione volontaria che viene messa in atto massivamente. Le piattaforme restano soggette agli obblighi di trasparenza del GDPR e dell'ePrivacy, ma la natura volontaria della misura e l'assenza di un diritto di opposizione efficace segnano in modo evidente una crepa e lasciano ampi margini di opacità.

Una conseguenza rilevante, che pare sottovalutata, è che milioni di liberi cittadini, professionisti, enti e studi legali o commercialisti che utilizzano quotidianamente servizi delle maggiori piattaforme non dispongono di strumenti concreti per opporsi o, in alcuni casi, neppure per essere informati della sorveglianza a cui sono soggetti. E anche qualora venissero correttamente avvertiti, la stragrande maggioranza non migrerebbe all'improvviso verso soluzioni alternative, sia per ragioni di praticità sia, e soprattutto, per l'impossibilità tecnica di proteggere le comunicazioni pregresse già archiviate su quei sistemi.

A chi sostiene che basterebbe una comunicazione più trasparente, o che permane la possibilità del singolo di migrare verso altri canali di comunicazione, va chiarito che questo non risolverebbe interamente il problema: le eventuali comunicazioni

4 Corte di giustizia dell'Unione europea, sentenza Schrems II (C-311/18) e sentenza La Quadrature du Net e a. (C-511/18 e ss.).

5 Garante per la protezione dei dati personali, parere reso in occasione dell'adozione della delibera AGCOM n. 96/25/CONS.

storiche restano comunque disponibili per scansioni massive e non motivate da alcun sospetto individuale. La misura, presentata come volontaria e temporanea, ha carattere potenzialmente massivo e sproporzionato, in quanto priva i cittadini di strumenti effettivi di difesa della propria riservatezza e, nell'ambito della volontarietà, consente alle piattaforme di sorvegliare milioni di persone e le loro comunicazioni senza alcun dovere di lasciare traccia verificabile del loro operato.

7. Il filo comune: dalla protezione mirata alla sorveglianza preventiva generalizzata

Il filo conduttore che unisce l'age verification e la deroga ePrivacy è il passaggio da un modello di intervento mirato - quello legale basato su indagini giudiziarie, cooperazione internazionale (MLAT, Europol, Interpol) e responsabilità genitoriale - a uno di controllo preventivo e generalizzato affidato a società terze. In entrambi i casi - pur nelle loro diverse specificità - la tutela dei minori è il vessillo invocato per giustificare l'introduzione di infrastrutture che trattano l'intera popolazione di milioni di utenti come una massa di individui che rappresentano una potenziale fonte di pericolo.

Questo spostamento d'orizzonte concettuale produce conseguenze strutturali: creazione di gatekeeper obbligatori, accumulo di metadati sensibili, rischio di function creep e indebolimento dei principi di proporzionalità e di autonomia individuale. L'obbligo di sottoporre l'accesso a contenuti leciti o le proprie comunicazioni non cifrate a meccanismi di verifica o di scansione costituisce, in sostanza, un'interferenza massiva e generalizzata nella vita privata dei cittadini, realizzata con strumenti del tutto sproporzionati.

Il problema non è tanto, in sé, l'age verification limitata all'accesso a contenuti pornografici. Il problema è che questa misura appare destinata a fungere da un primo passo verso forme più ampie di sorveglianza diffusa. Un cavallo di Troia. Non a caso si è già paventata l'idea, a livello politico e istituzionale, di un'estensione all'accesso ai social media e, più in generale, a interi pezzi dell'ecosistema digitale.

In un Paese come l'Italia, caratterizzato peraltro da un bassissimo tasso di natalità e da una esigua minoranza di minori rispetto alla popolazione complessiva, la domanda di proporzionalità si fa particolarmente stringente. I dispositivi digitali sono, nella stragrande maggioranza dei casi, forniti e controllabili dai genitori o da chi ne fa le veci. Se questi ultimi non esercitano (o non sono messi nelle condizioni di esercitare) una effettiva responsabilità genitoriale, la risposta istituzionale non può e non deve consistere nel sottoporre l'intera popolazione adulta a un sistema di verifica preventiva generalizzata. Si tratta di uno spostamento di paradigma che rischia di trasformare la tutela di una minoranza in un'infrastruttura di controllo massivo e sproporzionato, applicabile a tutti.

8. Il caso della Francia: da primo Stato europeo per l'adozione dell'age verification, al dietrofront grazie allla bocciatura della Consiglio Costituzionale.

Un esempio concreto e recente viene dalla Francia. Alla fine del 2025, il paese si era orientato ad adottare la verifica dell'età per accedere alle piattaforme online; poi, nel luglio 2026, ha imposto la verifica a tutta la popolazione per consentire l'accesso ai social network, con il dichiarato obiettivo di proteggere i minori un-

der-15. Ma poi, il 14 agosto 2026, Consiglio Costituzionale francese ha bocciato l'intero progetto, considerandolo generico e sproporzionato. Infatti, non solo limitava la libertà di espressione, ma avrebbe costretto gli adulti a dimostrare l'età senza garanzie sufficienti sulla privacy. Il Consiglio Costituzionale ha sottolineato che l'interdizione non teneva conto dell'età precisa, della maturità o della situazione familiare dei ragazzi, e secondo i giudici questo limita eccessivamente la libertà di espressione e di comunicazione. Allo stesso tempo, la Corte ha individuato un problema di privacy, in quanto, per far rispettare il divieto, tutti, anche gli adulti, avrebbero dovuto dimostrare la propria età, ma la legge non prevedeva regole chiare e garanzie sufficienti su come gestire questi dati, violando così il diritto alla privacy. Il Consiglio ha riconosciuto che proteggere i minori è un obiettivo legittimo, ma la misura si presenta troppo ampia e non bilanciata ed è quindi stata considerata una limitazione eccessiva delle libertà fondamentali[6].

9. Limiti pratici e conseguenze sistemiche

Infine, nessuna tecnologia di age verification è immune da comportamenti elusivi o bypass (prestito di credenziali di amici di età maggiore, uso di VPN, condivisione di dispositivi di terzi già autorizzati). I report internazionali, tra cui quelli dell'eSafety Commissioner australiano[7], documentano l'inefficacia relativa di tali sistemi. Allo stesso modo, la scansione volontaria delle comunicazioni non cifrate non intercetta i contenuti protetti da end-to-end encryption e può inoltre generare una mole di falsi positivi, con la conseguenza ulteriore di drenare energia alle forze dell'ordine senza motivo.

Le conseguenze sistemiche sono più rilevanti dei limiti tecnici: le infrastrutture di identificazione e di monitoraggio sopravvivono infatti alle singole normative, con incentivi alla centralizzazione dei dati e normalizzazione di un modello di sorveglianza preventiva che si discosta e mina le basi della tradizione giuridica liberale.

10. Proposte alternative

Le alternative più coerenti con i principi di proporzionalità e di tutela dei diritti fondamentali includono mezzi più efficienti, rispettosi, solidi e meno invasivi della sfera privata: l'educazione digitale strutturata e evidence-based nelle scuole e nelle famiglie; strumenti di parental control efficaci e compatibili con la riservatezza dei dati personali; indagini mirate autorizzate dall'autorità giudiziaria; rafforzamento

6 La Francia e le evoluzioni sull'age verification: 31 dicembre 2025 - France targets Australia-style social media ban for children next year" - https://www.theguardian.com/world/2025/dec/31/france-plans-social-media-ban-for-under-15s-from-september-2026. Luglio 2026 - La Francia approva la disciplina che impone la verifica dell'età a tutta la popolazione per l'accesso ai social media (https://www.theguardian.com/world/2026/jul/21/france-ban-social-media-access-under-15s). 14 agosto 2026 - Il Consiglio Costituzionale francese boccia la legge giudicata sproporzionata e lesiva della libertà di espressione. La stessa sentenza blocca anche l'obbligo di verifica dell'età per tutti gli utenti, inclusi i maggiorenni, per tutelare la vita privata e evitare misure generali eccessive.Communiqué de presse ufficiale: https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2026-911-dc-du-14-aout-2026-communique-de-presse

7 eSafety Commissioner (Australia), report e analisi sull'efficacia dei sistemi di age assurance.

della cooperazione internazionale esistente; sviluppo di tecnologie privacy-preserving per attestazioni di età senza trasmissione di dati identificativi.

Se l'obiettivo è proteggere i minori, assoggettare l'intera popolazione a controlli generalizzati, creando infrastrutture riutilizzabili per scopi diversi da quelli originari, non è una misura proporzionata.

11. Conclusioni

L'age verification italiana e la proroga della deroga ePrivacy del luglio 2026 illustrano un fenomeno ricorrente: la scusante nobile della tutela dei minori si traduce, all'atto pratico, in una deresponsabilizzazione di ruolo delle figure genitoriali, e in un'espansione significativa di meccanismi di identificazione e di monitoraggio istituzionale che coinvolge indistintamente milioni di persone. Le infrastrutture basate su SPID, CIE e IT Wallet, così come la possibilità di scansione volontaria delle comunicazioni non cifrate, creano tutte le condizioni necessarie a garantire un clima di sorveglianza preventiva generalizzata. Questo, a sua volta, pone rischi di profilazione, function creep e, più in generale, di indurre le persone a non mettere in atto comportamenti di per sé leciti (come scrivere un messaggio scherzoso a un amico o visitare un sito per adulti) per timore di essere schedati e doverne, un giorno, rispondere o anche solo di doversene giustificare.

Un cambio di paradigma è necessario: responsabilità genitoriale, strumenti mirati e cooperazione giudiziaria, anziché soluzioni preventive e generalizzate. È possibile tutelare i minori senza compromettere le libertà fondamentali tutelando la natura libera e aperta dell'ambiente digitale. In conclusione, l'introduzione dei sistemi di age verification e l'instabilità delle altre proroghe normative ripropongono l'eterno, falso dilemma tra sicurezza e libertà. Come ammoniva Stefano Rodotà, le esigenze di sicurezza pubblica non possono mai ridurre la privacy a forme incompatibili con una società democratica. Sacrificare i diritti fondamentali sull'altare di un controllo preventivo e generalizzato non rende la società più sicura, ma solo meno libera. La vera sfida regolatoria, dunque, non è rincorrere la trasparenza totale di milioni di utenti, ma garantire che la protezione dei più vulnerabili non si trasformi nel definitivo baratto della libertà collettiva.

Bibliografia

- AGCOM, delibera n. 96/25/CONS dell'8 aprile 2025 (pubblicata 12 maggio 2025).
- Parlamento europeo, risoluzione legislativa e voto del 9 luglio 2026 sulla proroga della deroga ePrivacy (P10_TA(2026)0266).
- Digital Services Act (Regolamento UE 2022/2065).