

For citation:

Nestoras, A., & Bulski, K. (2025). Age Verification In The Digital Era: Tech-Neutral Options For Safety, Privacy, And Innovation. *Media Dialogues / Medijski dijalozi*, Vol. 18, No. 1, 2025, pp. 7–16. DOI:

Age Verification In The Digital Era: Tech-Neutral Options For Safety, Privacy, And Innovation

Dr. Antonios NESTORAS

European Policy Innovation Council

Krzysztof BULSKI

European Policy Innovation Council

Article Info

Received: | Published online:

DOI:

Abstract

The increasing exposure of children to digital media environments has intensified policy debates on age verification as a mechanism of media governance. Within Europe and beyond, age verification is increasingly framed as a necessary condition for protecting minors from harmful content, exploitation, and inappropriate platform practices. At the same time, age verification introduces new challenges related to privacy, surveillance, concentration of power, and the normalization of identity checks in everyday media use. This article examines age verification not primarily as a technical solution, but as a regulatory and socio-political instrument embedded in digital media infrastructures. Drawing on media theory, political economy of platforms, and contemporary European regulatory debates, the article analyses the main age verification technologies, compares their implications for privacy and media power, and evaluates alternative regulatory options. It argues that age verification constitutes a new form of infrastructural media control that, if poorly governed, risks reinforcing platform dominance and weakening media literacy. The article concludes that effective digital media governance must remain technology-neutral, proportionate, and embedded within a broader framework that combines child protection, fundamental rights, and democratic oversight of media infrastructures.

Keywords: age verification, digital media governance, children and media, privacy, platform power, media regulation

© 2025 Author(s). Published by Media Dialogues / Medijski dijalozi.
This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

1. Introduction: Age Verification as a Media Governance Challenge

Digital media have become a central environment for children's socialization, learning, and cultural participation. Platforms for video sharing, social networking, gaming, and messaging now shape everyday communication practices from an early age. While these environments offer significant opportunities, they also expose minors to risks such as harmful content, sexual exploitation, grooming, disinformation, and addictive design patterns. As a result, child protection has emerged as a dominant theme in contemporary digital media policy.

Age verification has increasingly been positioned as a core response to these challenges. Policymakers and platform operators argue that the ability to determine whether a user is a child is a prerequisite for applying appropriate safeguards. In this framing, age verification appears as a neutral technical measure that enables compliance with legal obligations and supports responsible media environments.

However, age verification is not merely a technical instrument. It represents a structural intervention into digital media systems that reshapes access, control, and power relations. By determining who may participate in digital spaces and under what conditions, age verification functions as a form of media governance embedded in infrastructure rather than content regulation. This raises fundamental questions about privacy, autonomy, platform dominance, and the role of education versus technological enforcement.

Technology-neutral regulation does not imply normative indifference to governance outcomes. While this article does not advocate the mandatory adoption of a single technical solution, it evaluates age verification approaches against consistent criteria derived from media governance theory, including proportionality, power distribution, privacy preservation, and democratic accountability. Technology neutrality, in this sense, refers to regulatory openness rather than analytical equivalence.

This article approaches age verification as a regulatory and cultural phenomenon within digital media governance. Rather than advocating a single technological solution, it examines the broader implications of different age verification models and regulatory options. The analysis is guided by the following questions: How does age verification reshape power relations in digital media ecosystems? What are the trade-offs between child protection, privacy, and platform power? And how can regulation avoid reinforcing structural inequalities while pursuing legitimate safety objectives?

2. Age Verification in the Current European Regulatory Landscape

Age verification has moved rapidly from a speculative policy concept to a concrete regulatory requirement within the European digital governance framework. Recent and ongoing legislative developments situate age verification at the intersection of child protection, platform accountability, and fundamental rights. The Digital Services Act requires platforms to assess and mitigate systemic risks to minors and explicitly frames age-appropriate design and access controls as potential compliance mechanisms. In parallel, the Audiovisual Media Services Directive obliges video-sharing platforms to protect minors from harmful content, prompting several Member States to introduce national age verification requirements.

Debates surrounding the proposed CSA Regulation further reinforce age verification as a recurring regulatory instrument in the EU policy repertoire.

This evolving landscape is characterised by increasing regulatory pressure combined with significant uncertainty regarding implementation models. Divergent national approaches are already emerging, raising concerns about fragmentation of the Digital Single Market and uneven governance outcomes. Against this backdrop, age verification should be understood not merely as a compliance tool, but as a structural intervention that redistributes responsibility, authority, and power within digital media ecosystems. The governance implications of this shift extend beyond legal conformity and warrant critical examination at the infrastructural and cultural level.

While the Digital Services Act emphasizes systemic risk mitigation and due diligence, the Audiovisual Media Services Directive focuses on content exposure, and the proposed CSA Regulation extends into private communications, creating distinct yet overlapping rationales for age verification.

3. Digital Media for Children and the Risk of Gatekeeper-Centric Verification

Debates on children and the media have long oscillated between protection and empowerment. Early media theories emphasized the vulnerability of children to harmful influences, justifying regulatory interventions such as content classification and broadcasting restrictions. Later approaches highlighted children's agency, interpretive capacities, and the importance of media literacy. (Buckingham, D. 2005; Anderson, J. 2008)

Digital media complicate this dichotomy. Children are no longer passive recipients of media content, but active participants in networked communication. They create content, engage in social interaction, and navigate complex algorithmic environments. At the same time, platforms

monetize attention and personal data, often prioritizing engagement over well-being. (Zuboff, S. 2022)

Age verification reflects a renewed emphasis on protection through control. By categorizing users according to age thresholds, platforms can restrict access to content or functionalities. While this may reduce certain risks, it also reinforces a model of governance based on exclusion and surveillance rather than education and empowerment. From a media-cultural perspective, this raises concerns about the long-term effects of growing up in heavily regulated and verified media environments.

A particularly consequential governance shift arises when age verification functions migrate from individual services to device-level or operating-system infrastructures. In such configurations, age attributes and parental status are determined upstream, embedded within device ecosystems, and subsequently signalled to a wide range of media services. While often justified on grounds of usability or consistency, this model effectively delegates media access governance to actors that already exercise significant infrastructural power.

From a media governance perspective, this development risks transforming dominant device ecosystems into de facto gatekeepers of age-based participation in digital culture. Decisions about verification standards, enforcement thresholds, and data retention become embedded in technical systems that operate largely outside democratic scrutiny. This form of infrastructural delegation concentrates authority at the operating-system level and weakens pluralism by reducing the capacity of individual media services to define proportionate, context-sensitive access rules.

Such architectures also blur the boundary between safety enforcement and identity management. When age signals persist across contexts and services, verification ceases to be a situational safeguard and becomes a general condition of participation. This shift exemplifies the broader transition from content regulation to infrastructural control and underscores the need to scrutinise where, and by whom, media governance power is exercised.

This concentration arises because operating system providers control default settings, interoperability standards, and enforcement mechanisms, allowing them to define verification parameters that downstream media services must accept in order to remain accessible to users.

3. Infrastructural Media Governance

Age verification differs from traditional media regulation in its focus of control. Whereas broadcast regulation focused on content standards and public oversight, age verification is increasingly implemented at the infrastructural level. Decisions about verification methods, thresholds, and enforcement are often delegated to platforms, operating systems, or third-party providers.

This infrastructural turn has significant implications. First, it shifts governance from visible, contestable rules to embedded technical systems that operate largely out of public view. Second, it centralizes control in the hands of actors who already dominate digital media markets. Third, it reframes media access as conditional upon verification, normalizing identity checks as a prerequisite for participation.

From a media governance perspective, age verification can therefore be understood as a gatekeeping mechanism that operates upstream of content moderation. It regulates who may enter communicative spaces, rather than what may be communicated within them.

4. Overview of Age Verification Technologies in Digital Media

Age verification technologies encompass a wide range of approaches, each with distinct implications for accuracy, privacy, usability, and power distribution. No single technology currently satisfies all regulatory and normative objectives. For clarity, this article distinguishes between age verification (confirmation against a threshold), age estimation (probabilistic inference), and age attributes (binary or categorical signals issued after verification). These approaches entail distinct privacy and governance implications.

4.1 Self-Declaration Systems

Self-declaration systems require users to state their age or confirm they meet an age threshold.

Strengths:

- Minimal friction and universal accessibility
- No additional infrastructure or sensitive data processing

Limitations:

- Easily bypassed
- Provides no meaningful assurance
- Ineffective in medium- and high-risk media environments

Self-declaration functions primarily as a symbolic signal rather than a protective measure.

4.2 Document-Based Verification

Document-based verification relies on official identity documents or national electronic identity systems.

Strengths:

- High accuracy
- Clear legal recognition

Limitations:

- Processing of highly sensitive personal data
- Exclusion risks for minors without documents or parental support
- High friction and usability barriers

While suitable for specific high-risk contexts, document-based verification raises proportionality concerns when applied broadly across digital media.

4.3 Device-Based Age Signals

Device-based approaches rely on operating system settings, family accounts, or parental controls to signal age attributes.

Strengths:

- Low friction
- Minimal data disclosure to individual services

Limitations:

- No guarantee that the device owner is the user
- Strong dependency on dominant operating system providers
- Interoperability challenges

These approaches risk turning device ecosystems into de facto authorities over media access.

4.4 Biometric Age Estimation

Biometric age estimation uses facial images, voice analysis, or behavioural patterns to estimate age.

Strengths:

- Does not require formal identification
- Can be frictionless when implemented responsibly

Limitations:

- Variable accuracy across demographic groups
- Sensitive under data protection law
- Public trust and surveillance concerns

Biometric approaches require strict safeguards and transparent governance.

4.5 Third-Party Verification and Privacy-Preserving Tokens

In this model, a trusted intermediary verifies age and issues a reusable age attribute.

Strengths:

- Strong data minimisation
- Separation between verification and media access
- High interoperability potential

Limitations:

- Requires certification and governance frameworks
- Risk of market concentration among intermediaries

This approach aligns with media governance principles if properly regulated. An important governance distinction within third-party verification models lies in the separation between age verification and media access. In privacy-preserving architectures, verification is conducted independently by a trusted intermediary, while media services receive only a minimal age attribute, such as confirmation that a user exceeds a given threshold. Identity data and underlying documentation remain outside the media service's control.

From a media governance perspective, this separation mitigates the concentration of informational power and limits the capacity of platforms to repurpose verification data for profiling or behavioural regulation. When properly governed, such models reduce incentives for identity accumulation while preserving the ability to apply proportionate safeguards. However, they also introduce new governance challenges related to the certification, accountability, and market concentration of intermediaries, underscoring the need for public oversight rather than purely technical solutions.

Table 1
Comparative Assessment of Age Verification Technologies

Technology Type	Accuracy	Privacy Impact	User Experience	Interoperability	Media Governance Implications
Self-declaration	Low	Very low	Very high	High	Symbolic protection only
Document-based	High	Very high	Low	Medium	Strong control, high exclusion
Device-based	Medium	Low	High	Low	Platform and OS gatekeeping
Biometric estimation	Medium	High	High	Medium	Surveillance risk
Third-party tokens	Medium to high	Low	High	High	Requires strong governance

Note: The comparative assessment is qualitative and based on a synthesis of regulatory guidance, academic literature, and documented implementation practices. Ratings reflect relative tendencies rather than absolute performance and may vary depending on specific deployment contexts.

6. Privacy, Surveillance, and Identity in Digital Media Use

Age verification inevitably intersects with privacy. Even systems designed to minimize data collection contribute to the normalization of verification as a condition of media participation. Over time, this may reshape cultural expectations about anonymity and access.

A central structural risk associated with age verification is the phenomenon of identity creep. This occurs when data or attributes initially collected for a narrowly defined protective purpose gradually acquire broader functional roles across digital systems. In the context of age verification, identity creep may arise through the persistence of age attributes, their reuse across multiple services, or their storage within system-level infrastructures that mediate access to diverse media environments.

Over time, such arrangements can transform age verification from a contextual safeguard into a generalised identity requirement. When age signals become durable, interoperable, and automatically enforced, users are no longer verified for specific interactions but categorised in advance. This process reshapes expectations of anonymity and access, particularly for children, who may internalise verification as a normal precondition of participation in digital culture. The risk is not limited to data misuse, but extends to the gradual redefinition of identity, autonomy, and agency within mediated environments.

For children, growing up in verified environments may normalize surveillance and conditional access. From a media studies perspective, this raises concerns about identity formation and the internalization of control mechanisms.

Moreover, verification infrastructures, once established, may be repurposed for other objectives, including profiling or behavioural regulation. This phenomenon of identity creep represents a structural risk in digital media governance.

7. Platform Power and Market Structure

Age verification regimes interact closely with platform power. Large platforms and operating system providers are better positioned to implement verification systems and absorb compliance costs. Smaller media actors may become dependent on proprietary verification infrastructures.

This dynamic risks reinforcing media concentration and undermining pluralism. When access control is centralized at the infrastructural level, democratic oversight becomes more difficult, and alternative media ecosystems struggle to compete.

From a political economy perspective, age verification can therefore function as a mechanism of market consolidation if not carefully governed.

8. Regulatory Options for Age Verification Governance

Rather than mandating a single solution, regulators face multiple design options.

Option 1. Minimum Regulatory Requirements

Establishing baseline standards for transparency, data minimisation, and accountability without prescribing technologies.

Option 2. Privacy-Preserving Age Attributes

Encouraging separation between verification and access through certified intermediaries.

Option 3. Regulatory Sandboxes

Allowing controlled experimentation to generate evidence and assess unintended consequences.

Option 4. Optional Public Digital Identity Integration

Allowing, but not requiring, public digital identity systems as verification pathways.

Option 5. Risk-Based Tiering

Aligning verification requirements with the risk profile of media services.

Option 6. Strict Conditions on Biometric Verification

Limiting biometric approaches to narrowly defined contexts with strong safeguards.

Table 2
Regulatory Options for Age Verification

Regulatory Option	Key Features	Benefits	Risks
Minimum standards	Tech-neutral baselines	Reduces fragmentation	Limited enforcement
Privacy-preserving tokens	Separation of roles	Strong privacy	Governance complexity
Sandboxes	Controlled testing	Evidence-based policy	Slow impact
Public identity integration	High assurance	Long-term trust	Access barriers
Risk-based tiering	Proportionality	Reduced burden	Classification disputes
Biometric conditions	Strict safeguards	Rights protection	Innovation limits

9. Media Literacy and Democratic Oversight

The limits of age verification as a governance instrument become particularly visible when examined through patterns of user adaptation and circumvention. These dynamics underscore that technical control cannot substitute for media literacy, but must operate alongside educational and cultural strategies that enable informed participation.

This enforcement reality highlights the limits of technical control as a standalone governance strategy. When verification becomes the primary response to complex social risks, it risks producing formal compliance without

substantive safety gains. Media literacy, transparency, and critical engagement remain essential components of democratic media governance, enabling children and caregivers to navigate digital environments with understanding rather than passive exclusion.

Technological measures alone cannot address the complex risks children face in digital media environments. Media literacy remains essential. Education, transparency, and critical engagement empower children to navigate media responsibly.

A governance model that prioritizes verification over literacy risks producing compliance without understanding. Democratic media systems require informed users, not merely regulated ones.

10. Conclusion

Age verification has emerged as a central element of contemporary digital media governance. While it addresses legitimate concerns about child protection, it also introduces significant risks related to privacy, surveillance, and platform power.

This article has argued that age verification should be understood as an infrastructural media governance mechanism rather than a neutral technical fix. Effective regulation must remain proportionate, technology-neutral, and embedded within a broader framework that includes media literacy, competition safeguards, and democratic oversight.

By framing age verification as an infrastructural form of media governance, this article contributes to current debates by shifting attention from compliance and accuracy toward power, culture, and democratic accountability. The challenge is not whether age verification should exist, but how it is embedded within media systems that shape participation, identity, and authority. Addressing this challenge requires governance models that protect children without normalizing surveillance or entrenching infrastructural dominance.

Literature

- Anderson, J. (2008) Media Literacy, the First 100 Years: A Cultural Analysis. In: The SAGE Handbook of Child Development, Multiculturalism, and Media. Joy K. Asamen, Meshia L. Ellis and Gordon L. Berry Editors, Thousand Oaks, CA: SAGE Publications, Inc. pp. 381-410 Available at: <<https://doi.org/10.4135/9781412982771.n25>> [Accessed 21 Dec 2025].
- Buckingham, D. (2005), *The Media Literacy of Children and Young People*, LONDON.
- Zuboff, S. (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory*, 3(3). <https://doi.org/10.1177/26317877221129290> (Original work published 2022)