OPINION ACADEMIA

Indonesia’s online child safety needs more than an age rule

As Indonesia moves toward a March 2026 deadline for its new social media age restrictions, a "silver bullet" policy of age limits may prove ineffective without addressing deeper structural issues of platform accountability and digital privacy.

Dita Ramadhani (The Jakarta Post)

PREMIUM Jakarta Tue, February 24, 2026

Indonesia’s children are navigating the digital world far faster than the country is preparing them for its inherent risks. According to UNICEF’s 2023 baseline study, Online Knowledge and Practice of Children and Parents in Indonesia, 42 percent of children have felt uncomfortable or frightened online, while 50.3 percent have been exposed to sexual imagery on social media.

In response, Communication and Digital Affairs Minister Meutya Hafid has proposed age-limit restrictions on social media to cultivate a safer, more child-friendly digital environment. This initiative has moved forward into an implementation plan under the Child Protection in Digital Space Regulation (PP Tunas), which is expected to take effect this March.

The regulation seeks to govern access based on a platform’s risk profile, with high-risk services facing stricter limitations. Current signals suggest that teenagers aged 13 to 16 will require parental consent to create and access accounts. Platforms found in violation will face a ladder of sanctions, starting with formal warnings and escalating through fines to final access termination.

While the government’s tone is firm, the clarity of enforcement remains the central question. Under the current framework, penalties fall solely on the platforms rather than the users. Furthermore, parental consent, while reasonable on paper, often weakens enforcement in practice because it is frequently granted casually without a full grasp of a platform's specific risks or algorithmic pressures.

The most significant hurdle remains age verification. Simple self-declaration is notoriously ineffective, as anyone with a smartphone knows how easily these requirements are bypassed. Conversely, more robust verification methods, such as biometric scanning or government ID integration, raise serious privacy concerns.

Without a clear and secure approach to these checks, the policy risks either being ignored by tech-savvy youth or triggering a significant public backlash over data surveillance. Policy design must also account for everyday domestic realities like shared family devices and the use of older siblings’ accounts, which no top-down policy can fully block.

A useful point of comparison is Australia, which began implementing its Online Safety Amendment (Social Media Minimum Age) Act 2024 in December 2025. By banning children under 16 from major platforms, Australian authorities saw 4.7 million underage accounts removed in just one month, yet reports indicate that children continue to access these spaces through various backdoors.

The Australian policy sparked a fierce debate over digital rights, leading to organized protests and school walkouts. Indonesia is likely to face a similar reaction, as privacy advocates rightfully worry that robust age verification could push platforms to collect even more sensitive personal data, creating new risks for misuse.

In Indonesia, there is also a broader issue of trust, as digital regulation is often perceived as a form of state control rather than protection. Without transparency and strong safeguards, many fear that child protection measures could eventually justify wider internet restrictions.

None of this suggests that Indonesia should abandon its efforts to protect children, but rather that the government must move beyond the "silver bullet" of age limits. A credible policy must set clear obligations that establish strict, enforceable penalties for platforms that fail to moderate harmful content, rather than relying on moral appeals.

In the future, the government should treat age limits as just one component of a much broader strategy that includes transparent reporting systems and comprehensive digital literacy education. Furthermore, the regulation must protect privacy by design, limiting data collection to what is strictly necessary and providing clear transparency on how that data is shielded from misuse.

The stakes are high; a rule that looks strict but cannot be enforced will not protect children, but will instead erode public trust and create a false sense of security. As March approaches, the success of this initiative will depend on the government’s willingness to make hard choices regarding platform responsibility and regulatory restraint.

***

The writer is a communications specialist at Kiroyan Partners, with more than 12 years of experience, particularly in the development sector. The views expressed are personal,