



Regulating Age Assurance for Children on Social Media: A Comparative Rights-Based Framework for Indonesia

Rahayu¹; Kholis Roisah²; Muhamad Nafi Uz Zaman³; Muhammad Hazel Nailah Akbar⁴

^{1,2,3,4}Faculty of Law, Universitas Diponegoro, Indonesia

Corresponding author's email: mnafiuazzaman@live.undip.ac.id

Article Information

Received for publication: November 12, 2025

Accepted after corrections: August 12, 2026

Keywords: Age Assurance; Best Interest for the Child; Social Media

DOI: 10.20961/yustisia.v15i2.110965

Abstract

This article examines the regulation of age assurance for children on social media in Indonesia following the enactment of Government Regulation Number 17 of 2025 concerning the Governance of electronic system for Child Protection. This study compares regulatory models of age assurance across selected jurisdictions and evaluates their compatibility with the best interests of the child, particularly in relation to privacy, proportionality, access to information and digital inclusion. Using a doctrinal legal research approach, the study examines primary legal materials and relevant secondary sources to compare regulatory models and assess their implications for children's rights. This study reveals a variety of regulatory approaches, such as the risk-based model used by the European Union and the United Kingdom, more prescriptive measures such as those in France, and a registration system using real names used in China. Meanwhile, Indonesia adopts a risk-based approach with age classification and proportional access restrictions. However, the regulation does not establish specific technical standards for age verification methods and remains substantially dependent on self-regulation by electronic system providers. This study recommends strengthening regulations through the development of auditable verification standards, compliance monitoring mechanisms, and digital literacy to ensure the best interests of children in the digital environment.

I. Introduction

The use of social media by children has become increasingly widespread amid the rapid development of information technology. This development present both opportunities and risks. On the one hand, smartphones enable children to connect with others regardless of time and geographical boundaries, but on the other hand, greater access to social media also exposes children to

various forms of online harms. Reflecting on this situation, Lizzie O'Shea notes that digital technology binds humans to places where they interact with the world and has psychological effects because social interaction and content consumption increasingly occur online(O'Shea, 2019).

Various studies show these negative impacts. A study from the Communication Studies Center at the University of Indonesia states that excessive use of social media can increase the risk of online predatory crimes, pornography, violence, cyberbullying, invasion of privacy, and identity theft (Triastuti, Indra, et al., 2017). This vulnerability is associated with several factors, including excessive disclosure of personal information and the fear of missing out on the latest news (FOMO). Other research also states that the increasing volume and frequency of social media use will lead to addiction or dependence(Triastuti, A, et al., 2017). This can certainly affect children's social lives and relationships with their families(Triastuti, Indra, et al., 2017).

One factor contributing to children's vulnerability in the online space is the prevalence of websites with negative content. This is evidenced by the blocking of 2,624,750 sites by the Indonesian Ministry of Communication and Information from August 2018 to September 2021, including 1,536,346 from websites and 1,088,404 from social media, most of which contained pornographic content(Dewi, 2023). This number has the potential to continue to increase as the number of websites grows exponentially. According to the results of research by Murfiah Dewi Wulandari et al., children in elementary school aged 10-11 years old have a low ability to narrate and report incidents of sexual violence(Wulandari & al., 2020). This is not much different from what happens in Canada, where 93% of 33,000 people in Canada indicated that they did not report their children's experiences of sexual violence to the police. This situation is concerning because only a small portion of these criminal acts are detected and reported (Tufford & Lee, 2020). This situation has led to the implementation of policies restricting children's access to social media.

From a human rights perspective, the right to information is a fundamental right that must be fulfilled, protected, and respected by the state and every individual. This right applies in principle to everyone, including children(Rahayu, 2015). This provision is also regulated in international conventions such as the Convention on the Rights of the Child (CRC), specifically Articles 13 and 17, which affirm children's rights to seek, receive and impart information, and the state's responsibility to provide safe and useful access to information for children. In the Indonesian Constitution, Article 28F of the 1945 Constitution also emphasizes that everyone has the right to use all functions and access to information, both electronic and non-electronic, available in various forms such as images, sounds, videos, writings, and others through available media or channels. However, the right to access information is not absolute and may be subject to lawful restrictions that satisfy applicable legality, legitimate-aim, necessity and proportionality requirements.

The principle of the best interests of the child in international instruments such as the CRC places children as the primary consideration in all decisions, whether made by the government, the private sector, or the community, with

regard to their survival and development. This principle necessitates legal protection that focuses on fulfilling children's rights, thereby preventing and overcoming situations that are detrimental to them and lead to violations of their rights (Fitriani, 2016). This principle forms the basis for child protection regulations, influenced by their vulnerability to physical, verbal, psychological, and sexual violence in the digital space (Achmad, 2020).

Several countries have strictly limited the use of social media for children, including France (minimum age of 15) (Dw.com, 2024), China (minimum age of 14), Germany, and several states in the United States (minimum age of 18) (Presianta, 2024), as well as Australia, which in November 2024 also established regulations restricting the use of social media for children. Under these regulations, social media companies or platforms such as Instagram, Facebook, Meta, and TikTok must establish mechanisms to prevent children from accessing social media. If these rules are violated, companies that fail to prevent children under the age of 16 from having social media accounts will be fined up to 49.5 million Australian dollars (approximately Rp511 billion) (Voa Indonesia, 2024). Meanwhile, in Germany, children under the age of 16 need parental permission before they can access certain services in cyberspace (Supermana, 2025). Meanwhile, the United States requires technology companies to obtain parental consent for children to access user data under the age of 13 (Dw.com, 2024).

In Indonesia, awareness of the urgency of protecting children in the digital space is also reflected in the latest national policy, namely Government Regulation Number 17 of 2025 on the Implementation of Electronic Systems in Child Protection (hereinafter Gov-Reg 17/2025) and regulated technically through the Regulation of the Minister of Communication and Digital Number 9 of 2026 (hereinafter Min-Reg 9/2026). These regulations were introduced in response to the increasingly complex threats faced by children in the virtual world, ranging from exposure to pornography, online sexual exploitation, online gambling, to content that encourages violence and intolerance. Gov-Reg 17/2025 explicitly regulates the age limit for children accessing social media (Paat, 2025), while also obligating Electronic System Providers to implement age verification systems (Fajri, 2025).

In fact, social media platforms already have rules regarding the minimum age for accessing their services. Usually, a warning and consent form will appear before using their features or content. For example, the minimum age to access Instagram, Twitter, and YouTube is 13 years old, while the minimum age to have a TikTok account is 14 years old. However, in practice, there is no clear verification from social media platforms to ensure whether users meet the required age qualifications or not. This loophole is often exploited by children to bypass the registration verification process (Pratiwi & Anna, 2021).

Several countries have attempted to address this verification problem through regulation. For example, the UK's Online Safety Act requires digital platform providers to implement age assurance to prevent children from accessing harmful content, with strict supervision by Ofcom. Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024 explicitly prohibits

children under the age of 16 from having social media accounts and requires platforms to take reasonable steps to ensure compliance. The European Union, through the Digital Services Act (DSA), promotes a risk-based approach by encouraging the use of privacy-preserving technology in age verification, while China and South Korea emphasize a digital identity system based on real-name registration (real-name system).

Based on literature review, this diversity of regulatory practices shows that there is no single universal model that is completely effective and free from weaknesses (Jarvie & Renaud, 2024; Livingstone et al., 2024; Shaffique & Van Der Hof, 2026). Some methods, such as official identity verification, do provide legal certainty, but pose privacy and exclusion risks for certain groups. Meanwhile, AI-based or age estimation methods are faster and more practical, but prone to bias and technical errors (Anda et al., 2020; Ganel et al., 2022). Therefore, the main debate in global literature and policy practice lies not only in the technical effectiveness of age verification, but also in the balance between child protection, respect for human rights, and the sustainability of the digital ecosystem (Rocha, 2026).

However, existing studies on age verification have largely focused on mapping the regulatory approaches adopted by different jurisdictions and identifying the practical and legal challenges in implementing these models to protect children (Jarvie & Renaud, 2024; Köhler-Dauner et al., 2025). While such comparative analyses provide important insights into regulatory diversity, they have yet to sufficiently address which regulatory model, or combination of regulatory safeguards, can best reconcile the best interests of the child with other fundamental rights and interests in the digital environment. Limited attention has been given to developing a normative framework for assessing age verification models not merely in terms of their effectiveness in identifying or estimating a user's age, but also in terms of their proportionality and privacy implications.

In this context, it is interesting to look at Gov-Reg 17/2025 and Min-Reg 9/2026, which formulates policies on age verification for children on social media. This issue is significant because the issue of age verification is not only related to the technical aspects of digital technology, but also concerns the dimensions of child rights protection, privacy, and the state's obligation to ensure optimal child growth and development. This study was conducted by comparing Gov-Reg 17/2025 and Min-Reg 9/2026 with similar policies in several other countries. From this study, various policy models will be obtained from the practices of countries in regulating restrictions on children's rights in accessing social media. The analysis focuses not only on the normativity of the rules but also on the potential obstacles and barriers that may arise when this policy is implemented.

This study goes beyond comparing regulatory practices across jurisdictions by developing a rights-based comparative framework for evaluating age verification models through the principle of the best interests of the child. It argues that the appropriate regulatory model should not be assessed solely by its level of age-assurance accuracy, but also by its ability to

balance effective child protection with the protection of children's other fundamental rights. On this basis, the study critically evaluates the regulatory models identified across jurisdictions and draws lessons for Indonesia in designing an age verification framework that is proportionate, privacy-preserving and consistent with the best interests of the child.

II. Fulfilling Children's Rights to Obtain Digital Information and the State's Responsibility to Protect Children from Cybercrime on Social Media

With the development of information and communication technology, digital devices become an integral part and a dependency in various sectors that support life (Vandewater & Lee, 2009), so that the process of integrating information technology into children's lives can be easier, especially for the use of digital devices in accessing information systems such as mobile phones, computers, and especially social media. According to the 2025 OECD report entitled "How's Life for Children in the Digital Age?", around 70% of children aged around 10 already have their own smartphones, although this figure varies from country to country (OECD, 2025a). The OECD also reported that in 2021, 93% of 10-year-olds had internet access, compared to 85% a decade earlier. In 2022, 97% of 15-year-old students in OECD countries lived in homes with internet access (OECD, 2025a).

The widespread use of digital technologies by children raises questions concerning the extent to which regulatory intervention can protect children without unduly restricting their digital rights, thereby directly exerting a significant and unpredictable influence on their long-term development (Nagy & Fazekas, 2018). This raises the question of the extent to which regulations can limit and protect children so that they can safely access digital information systems.

A. The Right of Children to a Digital Environment: A Global Overview

The fulfilment of children's rights in the digital sphere is outlined in General Comment Number 25 of the Convention on the Rights of the Child (CRC) of 2021, which emphasises the importance of a digital environment that is in line with the principle of the best interests of the child. This principle is a context-dependent and dynamic standard that must be assessed in the light of the specific circumstances of each regulatory intervention. State Parties are obliged to ensure that in every action related to the provision, regulation, design, management, and use of the digital environment, the best interests of the child are always the primary consideration.

The principle of the best interests of the child constitutes the central normative framework of this study. Although age assurance is generally designed to prevent children from accessing harmful or age-inappropriate content, the protection of children cannot be understood solely in terms of restricting access. Any regulatory intervention concerning children's participation in the digital environment must also take into account the broader range of rights and interests affected by the intervention. Accordingly, this

study treats the best interests of the child not merely as the objective of age assurance regulation, but as an analytical and evaluative standard for assessing the legitimacy and proportionality of different regulatory models.

Fulfilling this right requires collaboration between the government, digital service providers, and parents or guardians. Each actor has different but interrelated responsibilities. The state, as the regulator, must formulate clear, consistent policies and regulations based on international instruments. Meanwhile, companies are responsible for ensuring the fulfillment of children's rights while accessing their services, especially in data processing and protecting children's privacy. This is important because the processing of children's personal data for commercial purposes has the potential to result in violations or abuse of children's rights.

Any potential violations of children's privacy rights must be mitigated by companies based on ethical standards and international principles such as data minimization, proportionality, specificity, and legitimacy. Meanwhile, parents or guardians play a role as supervisors and primary companions in children's use of digital technology, including ensuring that children's digital literacy develops in a balanced manner (eSafety Commissioner, 2023). The collaboration between these three actors will determine the extent to which the digital environment can truly realize the best interests of children.

Thus, while collaboration between the state, companies, and parents is an important prerequisite for ensuring children's rights in the digital space, real challenges arise from the nature of digitalization itself, which presents new and increasingly complex risks. The transformation of deviant behavior, which was previously limited to physical spaces, has now migrated and escalated to the online realm, requiring more adaptive and comprehensive protection strategies. The increasing pace of digitalization has actually led to an increase in the severity of harmful conduct, especially among children (Mitchell et al., 2007).

Based on the perspective of child development theory, individuals under the age of 18 are still in the phase of cognitive, emotional, and social growth. At this stage, their ability to make decisions, regulate emotions, engage in social reasoning, and form their identity is still undergoing active development. This means that children's capacity to assess risks and understand long-term consequences is not yet fully mature, including in the context of digital space usage (Christakis & Hale, 2025). The psychological and mental condition of children, who are still in this stage of development, becomes even more complex when faced with technological advances.

There are variations of sexual violence that were originally conventional (physical) in nature but have evolved with various modifications through digital means, such as cyber grooming, sextortion, deepfake pornography, and non-consensual pornography or revenge porn. This complexity is exacerbated by the nature of the virtual world, which allows perpetrators to remain anonymous (not easily identifiable), enables harmful content or actions to spread quickly (amplification), and makes it difficult to remove traces. As a result, online sexual violence can have a greater impact, as perpetrators take advantage of the ease of technology to harass others (Jamaludin, 2024).

Therefore, internationally, countries have committed to limiting the minimum age for children to access social media. They have a common standard in setting the minimum age for children at 13 years old, as in the Children's Online Privacy Protection Act (COPPA) and the General Data Protection Regulation (GDPR) of the European Union (Brennan & Phippen, 2021). The age of 13 is considered to be the age at which children are capable of thinking, acting, and processing information obtained through social media, although in various regions and socio-cultural conditions, there are variations in the developmental age of children. This minimum age limit may change to keep pace with progress in the modern era, based on the argument that the internet experience has developed significantly compared to the 1990s (Canales, 2025).

B. Children and Social Media: A Reality and Regulation in Indonesia

The reality of internet penetration, especially social media, among children in Indonesia shows high numbers. More than 80% of individuals aged 5-24 years in Indonesia have accessed the internet, with 67.65% of them using social media, making it one of the main digital activities after entertainment (BPS, 2024). Likewise, children have faced various dangerous risks in the digital space. UNICEF data from 2023 shows that 45% of 2,777 children have experienced online bullying, while 32.1% of 510 children have shared personal information with strangers, and 24% have met in person with individuals they met online (U-Report Indonesia, 2019; UNICEF Indonesia, 2023). Additionally, more than 5.5 million cases of child pornography have been detected in the last four years, making Indonesia the fourth country with the highest number of cases globally (KPI, 2024). Easy access and minimal parental/guardian supervision are the biggest factors for children accessing social media. Therefore, children's vulnerability to dangerous risks in the digital space deserves special attention from the government (Sitompul et al., 2025).

A report from Neurosensum in 2021, an independent artificial intelligence (AI)-based research company, revealed that 87% of children in Indonesia have interacted with social media before the age of 13. Interestingly, these children come from low-income families, and 92% of them have been familiar with social media from an early age (Firdausya, 2021). Furthermore, of the 92% of children from low-income families, 54% have used social media before the age of 6 (Jamaludin, 2024). This report not only highlights the inadequate supervision of digital spaces, particularly social media, for children, but also identifies economic factors that influence digital education for both parents and children.

The urgency of formulating policies oriented towards the best interests of children is crucial in order to provide comprehensive protection. The absence of strong regulations has the potential to increase the risk of exposure to dangers in the digital space for children, especially given the limitations of the self-regulatory mechanisms implemented by Electronic System Providers (ESPs). In this context, the Ministry of Communication and Digital Affairs occupies a strategic position to ensure that children benefit from technology in

line with their developmental stages. Based on this urgency and analysis of the impact of social media on children, the Indonesian government enacted Government Regulation Number 17 of 2025 concerning the Governance of Electronic System Providers in Child Protection.

In general, there are four main focuses of Gov-Reg 17/2025, including: (i) cross-stakeholder collaboration, which includes the obligations of the government, ESPs, and the community (parents/guardians); (ii) age classification/determination, risk classification, and age verification implementation; (iii) law enforcement, ranging from supervision, follow-up on reports or complaints to the imposition of sanctions, and (iv) efforts to improve digital literacy, as preventive measures to prevent child abuse in the digital space.

Gov-Reg 17/2025 not only functions as a derivative regulation of the Electronic Information and Transaction Law (ITE Law), but is also drafted by adopting good practices from various jurisdictions. One of the main references is the Age-Appropriate Design Code (AADC) in the United Kingdom, which has its normative roots in the European Union's General Data Protection Regulation (GDPR). Thus, Gov-Reg 17/2025 can be seen as a legal instrument that combines national and international protection standards.

To assess the suitability of Gov-Reg 17/2025 in limiting and protecting children's rights in the digital space, a comparative approach is needed. This approach aims to identify best practices from other countries that have already regulated similar issues, while assessing the strengths and weaknesses of Gov-Reg 17/2025. The European Union with its GDPR, particularly the AADC provisions, is the main reference in the development of Gov-Reg 17/2025 norms. The GDPR regulates children's rights in the digital space through Article 8. This article stipulates that the processing of children's personal data is only permitted for children aged 16 years and above, with the possibility of lowering the minimum age limit to 13 years. However, this regulation is still general in nature and only refers to the term "information society services" without further elaboration on age categories or digital service specifications.

Unlike the GDPR, Gov-Reg 17/2025 provides more detailed regulations regarding child protection. Article 20 paragraph (4) of Gov-Reg 17/2025 divides children into five age categories, all of which still require parental consent. The age categories are based on developmental stages, namely: 3–5 years; 6–9 years; 10–12 years; 13–15 years; and 16–18 years. The provisions are as follows:

- a. children under 13 years of age can only use social media through accounts on products, services, and features that are "specifically designed" for children with low risk profiles.
- b. children aged 13–16 (category d) may have accounts on products, services, and features with a low risk profile.
- c. children aged 16–18 (category e) are allowed to have accounts on all digital products, services, and features.

The comparative analysis shows that Gov-Reg 17/2025 provides greater specificity in certain areas, particularly regarding age categorization and

children's access to particular digital products, services, and features. In addition, the age grouping in Gov-Reg 17/2025 allows for more contextual application of regulations, adjusting to the stages of child development. However, it should be noted that there are substantial similarities between the two legal instruments. Both Article 8 paragraph (1) of the GDPR and Article 21 paragraph (1) letter b of Gov-Reg 17/2025 stipulate that children who are 13 years of age or older are allowed to have digital accounts without the requirement for a special design for the products or services used.

Overall, Gov-Reg 17/2025 provides more detailed age categorization and service-specific access rules than the GDPR in the areas examined above. This regulation not only adopts international practices but also develops them through an age-based approach and digital service risk profiles, thereby providing more measurable protection that is tailored to children's needs.

III. Child Verification Assurance as an Effort to Promote the Best Interests of Children

Age assurance for children accessing social media is a necessity when faced with the reality that online life has become the main space for children's interactions. Some children are even exposed to services that are strictly prohibited, such as gambling, pornography sites, and dating platforms (Gambling Commission, 2024; Thurman & Obster, 2021). This situation shows that the digital space not only expands opportunities for children to learn and interact, but also presents risks that can harm their best interests. Therefore, the need to formulate age assurance mechanisms is crucial. The following discussion focuses on the basic principles of age assurance, globally developed age verification models and methods, and regulatory practices in various countries and their implications for policy design in Indonesia.

A. Basic Principles of Age Assurance for Children

Age assurance essentially refers to a process used to determine whether a person falls into the category of a child (a specific age group) and to ensure that they receive online services that are appropriate for their developmental needs (OECD, 2025b). This system is not only applied to social media, but also to platforms that provide content or services with certain age restrictions, such as digital banking, movie streaming services, video sharing platforms, and shopping sites that sell adult-only products. The implementation of age assurance begins with the setting of age limits based on a specific age range for which legal protection applies in a jurisdiction. The system then estimates the user's age through a verification process to estimate or verify the user's age, which affects content and service adjustments and even blocks access for users who do not meet the age requirements (5Rights Foundation, 2021).

The implementation of age assurance involves the government as the regulator, social media platforms as service providers, and children and parents as supervisors. The government sets the age range of children as the minimum limit, including the obligations and standards that must be met by platforms.

Platforms are responsible for risk management, from determining appropriate services, processing and protecting data, to escalating actions in the event of violations.

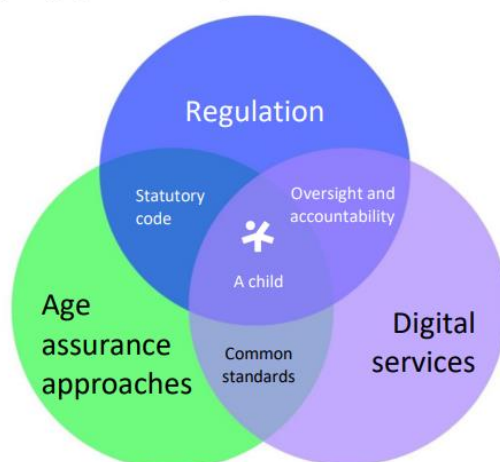


Figure1 : Stakeholder Relationships in Child Protection in Digital Services
(Source:eSafety Commissioner, 2024)

Service providers occupy a strategic position because they interact directly with children through risk assessment mechanisms. In the Child Rights Impact Assessment study by the UK Digital Futures Commission, risk assessment is carried out through know your customer, impact/risk mapping, complaint services, and real-time monitoring (Mukherjee et al., 2021).

Various age assurance methods have indeed been developed, such as official identity verification (ID card, passport), third-party data checks, biometrics, and AI-based technology that estimates age through photos, voice, or user movement patterns. However, the most basic and still frequently used technology is self-declaration, which involves entering the date, month, and year of birth when registering an account. Although there are several variations, the discourse on which method is most appropriate always revolves around two choices: verifying a child's age through self-declaration, which is simple but easy to falsify, or the vulnerability of misuse of children's personal data when more advanced verification methods are used, such as ID cards, biometrics, and AI profiling. Both have their own advantages and risks.

The first option, self-declaration, is the simplest and easiest method, requiring only the entry of a date of birth or the checking of a box asking whether the user meets the minimum age requirement. On social media platforms, self-declaration-based verification has several fundamental weaknesses, such as age falsification and assistance from third parties like relatives, friends, or family members to enter their age. As a result, children can still access social media services without strict supervision (Smirnova et al., 2021; Stemler et al., 2021).

In fact, social media platforms such as Instagram, Facebook, and YouTube have set a minimum age of 13 to access their platforms. However, they do not have a verified mechanism to ensure that children cannot access or create accounts (Meurens, 2022). A study by Tomasz Huk shows that 71.97% of 157

children aged 10 to 12 in Poland admitted to having a Facebook account created by manipulating their identity to attract other users, even though they were aware of the age restrictions they were violating (Huk, 2016). Children may not understand the impact of pretending to be older on their user experience or their digital identity/footprint. This shows that age restrictions through self-declaration methods are still not effective enough in preventing children from accessing social media (Meurens, 2022).

The issue of children's data in the first option is not a major concern, as the data collected is only information that is sometimes not clearly verified and no documents are collected. Therefore, this option has a relatively low data protection risk with a low level of certainty in verifying children's ages, as it relies on the honesty of children in reporting their ages (OFCOM UK, 2020).

The second option focuses on advanced verification that requires the collection of children's personal data, such as ID card verification, biometrics, and AI profiling. For the verification of children's identity documents, they are usually required to upload official identity documents, such as identity cards or passports, which can then be verified against official population databases. At this point, it seems to offer a high level of assurance, but it actually has complex problems, namely (i) the issue of children's personal data being collected in increasing amounts to determine the age of users, which requires higher standards of security, retention, storage, and data accountability; (ii) the issue of document fraud, by uploading someone else's ID card or a fake document; and (iii) the issue of fairness, where not all children have access to official documents, for example, due to immigration status and statelessness (5Rights Foundation, 2021; ICO UK, 2021). This method is actually most commonly used for age verification on platforms that offer services to users over the age of 18, which emphasize proving that the user is an adult, such as banking, dating apps, and video and music streaming sites.

Biometric methods such as height, gait, voice, facial features, and fingerprints can also serve as alternatives, though they similarly raise concerns about the protection of children's personal data. Generally, analysis of biometric data can estimate age without recognizing or identifying the individual. Facial analysis compares the user's facial features with a large data set that has been used to train the technology through machine learning (ICO UK, 2021). In addition to the issue of protecting children's personal data, the use of biometric data must also be accompanied by security standards, purpose limitations, and accountability.

Other verification methods, such as AI profiling, are actually far more complex because they require a set of processed data to analyze and draw conclusions about users, or to predict and determine aspects of user behavior. This data is collected from everything users do when connected to a particular website or application. For example, how long they spend on a web page, the time they access services and their interests, location, and friends. This method poses risks in the processing of children's data, ranging from potential inaccuracies if the data quality is poor and data collection exceeds what is needed (ICO UK, 2021).

There are many other methods that continue to evolve, such as cross-account authentication, third-party age assurance providers¹ (companies that provide age assurance services on a business-to-business basis), and account holder confirmation (control or approval by an adult, such as a parent or guardian). All of these alternative methods have one thing in common: the high vulnerability of children's personal data used in age verification. This vulnerability has led to real-world consequences, as seen in several cases of child data protection breaches in the UK.

In March 2025, the UK Information Commissioner's Office (ICO) investigated TikTok, Reddit, and Imgur for processing data on children aged 13-17, which allegedly caused harm to children, such as data leaks and increased screen time beyond standard limits. TikTok itself has an algorithm generated from user activity while using the application. Previously, TikTok had been fined £12.7 million by the ICO for violating child data protection laws. The ICO estimates that TikTok allowed up to 1.4 million children under the age of 13 in the UK to use its platform in 2020, even though its own regulations do not allow children of that age to create accounts (ICO UK, 2023). Meanwhile, Reddit and Imgur were investigated for implementing age verification technology that allowed children under 13 to have accounts (Gerken, 2025). However, according to the international GDPR standards, the processing and collection of personal data must have an explicit and legitimate purpose, and the data must not be further processed in a manner incompatible with that purpose (Article 5(1)(b), GDPR).

To make the comparison more analytical, the age-assurance methods are assessed according to several common criteria: accuracy, privacy risk, proportionality and inclusiveness. These criteria are derived from the competing considerations identified in the literature and are used to assess the relative strengths and weaknesses of each mechanism. The following table outlines various age assurance methods and their relevance to children's social media.

¹ Yoti (a third party that works with the platform). Advantages: Fast (seconds). No official ID required. Disadvantages: Potential algorithm bias (low accuracy for certain age groups or ethnicities). Privacy issues related to biometric data.

Table 1. Comparison of Age Assurance Methods and Their Relevance to Children's Social Media

Method	How It Works	Accuracy	Privacy risk	Proportionality	Advantages for Children	Disadvantages/Risks for Children
Self-declaration	Users fill in their own date, month, and year of birth when registering, or provide confirmation checks that they are above a certain age.	Low (can be manipulated by the user)	Low (no valid data was collected)	High (relatively limited interference with children's other rights).	Easy to understand, fast, does not require sensitive personal data.	Very easy to forge and ineffective in protecting children from adult content.
ID Verification (ID Card Verification)	Upload or scan official identity documents and verify them based on government population data				High accuracy due to specific data, difficult to forge, and safer for children.	High privacy risk if data is leaked and requires strong data security infrastructure.
Parental Consent / Parental Control	Parents provide consent or manage their child's account through an app or parental control feature.	Low-Medium (depends on the reliability of the mechanism used to authenticate and verify the parent and child)	Medium (require processing information about both the child and parent/guardian)	Low-Medium (may be justified for higher-risk services, but requiring parental consent universally may be excessive)	Gives parents full control and increases supervision of children's activities.	Effective only if parents actively monitor and may lead to privacy conflicts between children and parents.
AI-based Age Estimation using biometric	The system estimates the user's age through facial analysis, voice	Medium (relies heavily on behavioural inference,	High (involve extensive behavioural or biometric	Medium (potentially less intrusive than ID verification,	No official documents required, fast process,	Potential algorithmic bias, potential inaccuracies

data or AI Profiling	analysis, or online behavior analysis.	the result can become even more uncertain)	inference, creating profiling and information al- autonomy risks)	but extensive profiling may interfere with privacy and autonomy)	and can be done automatical ly.	in age estimation, and privacy issues related to biometric data.
Third-party Age Verification Services	The platform uses third parties to verify user age without the main platform storing personal data.	Medium-High (depends on the underlying verification technology and the reliability of the third-party provider)	Medium-High (reduce disclosure to platforms but introduces additional data-processing)	Medium-High (reduce disclosure to platforms, but creates additional data-processing)	Reduces the risk of data misuse by the main platform, and verification tends to be accurate.	Privacy risks remain with the third party and require trust in the service provider.

Source: From various sources processed by the author

Based on research by the 5Rights Foundation, which tested each age assurance method against standards such as privacy, data proportionality, ease of use, experience enhancement, security, redress options, accessibility and inclusivity, transparency/accountability, and levels of friction. The 5Rights Foundation's assessment indicates that third-party age assurance providers performed relatively well across several standards, while AI profiling raised greater concerns regarding privacy, transparency, and accountability.

Regardless of the various age assurance method options, the important point is that these methods are not seen as the end goal, but rather the first step in anticipating the presence of children in the digital world. Although the approach will vary, there are several general standards that must be applied by both the government and platforms. For example, the application of privacy law through data minimization and restrictions on specific purposes necessary to determine the age of users. In particular, companies should not use age assurance as an excuse for aggressive data collection practices or as a reason to avoid implementing children's rights (5Rights Foundation, 2021).

Age assurance must be carried out in proportion to the risks and with clear objectives. In addition, its implementation must be easy for children to use, which means that children must understand what steps to take. Furthermore, social media platforms must have a system with a high level of security that is transparent, accountable, and subject to agreed standards (5Rights Foundation, 2021). The age assurance system must adhere to the principle of data minimization to reduce the risks associated with data collection. Data should only be used for its intended purpose. Every user must be provided with information about how their data may be used, stored, or collected, as well as information about how to protect their privacy. There must be adequate oversight of the system to ensure reliability and to remedy data or privacy breaches (eSafety Commissioner, 2023).

Despite its important role in protecting children from online risks, age assurance may also create competing risks to children's other rights, particularly privacy and personal data protection (Livingstone et al., 2024). This tension is particularly evident in identity verification, biometric verification, facial age estimation, and AI-based profiling. While stronger verification mechanisms may provide greater certainty in determining a user's age, they may also require greater collection or processing of children's personal or biometric data (Ganel et al., 2022). Therefore, a higher level of age-assurance certainty does not necessarily mean that a regulatory model better serves the best interests of the child.

From the perspective of the best interests of the child, age verification should therefore satisfy the principles of necessity, proportionality, and data minimization. The information collected should be limited to what is necessary to establish whether a user meets the relevant age threshold, and more intrusive methods should only be required where they are justified by the level of risk involved. This approach also recognizes children's informational autonomy, meaning that children should not be treated solely as objects of protection whose personal information can be extensively collected in the name of safety.

B. Age Assurance Regulation Models on Social Media for Children in Various Countries and Their Implications for Policy Design in Indonesia

Seeing the various methods that have developed in age assurance, various countries have responded through their national regulations. The selection of jurisdictions for this comparative analysis is based on two principal considerations: (i) the prior establishment of a normative regulatory framework for age assurance or children's online protection and (ii) the diversity of regulatory models represented by those frameworks.

The jurisdictions examined in this study were selected because their regulatory responses to children's access to digital services had been established or substantially developed before Indonesia introduced its current regulatory framework. Their experiences therefore provide relevant regulatory precedents against which Indonesia's emerging framework can be assessed. The selection of these jurisdictions is therefore not intended to suggest that they constitute an exhaustive representation of global age-assurance regulation. Rather, they were purposively selected to capture different regulatory archetypes and degrees of regulatory intervention, ranging from risk-based and flexible approaches to prescriptive, parental-consent, minimum-age prohibition, identity-based, and platform-dependent models.

The objective is therefore not to determine which jurisdiction has the most effective model in absolute terms, but to identify the regulatory design principles and safeguards necessary for an age-assurance framework that is consistent with the best interests of the child, and to draw regulatory lessons for Indonesia. To summarize the comparative framework and the diversity of regulatory models identified, the following table presents the selected jurisdictions according to the common parameters outlined above.

Table 2. Age assurance regulatory models for social media for children

Country	Legal instruments/policies	Age assurance methods or common practices	Analysis
European Union (EU)	EU Digital Services Act (DSA) and EU Audiovisual Media Services Directive (AVMSD)	Does not require a specific method, but takes a risk-based approach whereby platforms classified as very large online platforms (VLOPs) must implement additional, more advanced strategies. The EU is currently developing the EU Digital Identity Wallet as one of the age assurance method options to maintain privacy and protection measures.	This risk-based approach is a strategy that can be applied by considering the reach of the platform. This means that this approach does not treat all platforms equally in terms of DSA obligations. In addition, the EU Digital Identity Wallet is expected to be able to balance age verification and privacy protection through the principle of data minimization.
United Kingdom (UK)	The Online Safety Act 2023 and Ofcom Guidance require platforms to protect children and implement age assurance for harmful/restricted content.	Platforms are required to use methods that are proportional to the risk to child protection. The higher the risk, the more Ofcom recommends "high assurance" methods such as uploading ID cards, credit card checks, and age estimation based on photos/AI. The implementation of these methods must always adhere to personal data protection from the outset.	The emphasis on risk-based age assurance obligations is proportional to the level of danger, so this approach strikes a balance between child protection and technological innovation flexibility. However, the main challenge lies in the potential for privacy intrusion, especially when "high assurance" methods such as ID verification or biometrics are applied, making compliance with the principle of data protection by design a crucial aspect.
France	The French Audiovisual and Digital Communication Regulatory Authority (Arcom) and Secure and Regulate Digital Space (SREN).	Age verification is mandatory for adult/pornographic sites using ID card upload or third-party systems. For other digital services, there is a double consent requirement from parents/guardians for children under 15 years of age.	French regulations adopt a prescriptive approach, emphasizing the obligation of age verification, particularly for adult websites through ID cards or third parties, as well as the implementation of double parental consent for children under 15 years old on digital services. This model emphasizes family-authorized protection,

but it may raise privacy concerns and access barriers, especially when digital infrastructure or parental literacy is limited.

Germany	JMStV (State Treaty on Youth Media Protection) and AVMSD (Audiovisual Media Services Directive)	Age verification practices through AI-based facial age estimation (e.g., Yoti Age Scan, Ageware AI), as an innovative and more user-friendly alternative. Previously, conventional methods were considered inefficient. Additionally, the technology used will align with the EU's plans through Digital Identity Wallet	This approach is more user-friendly while aligning with the EU's Digital Identity Wallet initiative. However, the challenge is ensuring technical accuracy and data privacy protection remain intact amid the adoption of new technology.
The United States (federal) and several states	COPPA (Child Online Privacy Protection Act), which regulates the collection of data from children under 13 (parental consent), and the Kids Online Safety Act (KOSA) (still in draft form). In addition, many states have also issued their own regulations.	In general, there is no single verification mechanism at the federal government level. Practices vary by state. States such as Utah, Texas, and Arkansas restrict social media to users over the age of 18, unless they have parental permission (To Create The Social Media Safety Act, 2023). Florida prohibits social media accounts for those under the age of 14 and requires parental permission for those aged 15–16.	As a federal country, the USA shows regulatory fragmentation between the federal and state levels. COPPA only focuses on protecting the data of children under 13, while state regulations extend the age limit to 16–18. The absence of uniform national standards creates legal uncertainty for platforms, even though the state-based approach reflects a high level of concern for child protection in the digital realm.
Australia	The Online Safety Act 2021 and the Online Safety Amendment (Social Media Minimum Age) Act 2024 prohibit accounts for those under 16 on certain platforms.	Platforms are required to take reasonable steps to prevent users under 16 from accessing social media. Currently, Australia has not specifically decided on the method to be used, but development is leaning towards age estimation technology using AI.	This approach provides flexibility for platforms, though it may introduce technical uncertainties in implementation. The focus on developing AI-based age estimation technology indicates a shift toward more innovative solutions, yet challenges remain regarding accuracy and the protection of children's personal data.

China	Cybersecurity Law includes Cyberspace Administration of China (CAC)	Real-name registration mechanism through the National Network Identity Authentication system verification. The platform will verify digital national IDs with official identities (ID cards, biometrics) for access to many services. The age verification process is carried out implicitly through the national ID.	This approach is effective in ensuring age accuracy and facilitating state surveillance, but it sacrifices digital anonymity and poses a significant risk to children's privacy. This model reflects the priority of social control and national security over the protection of children's rights to personal data confidentiality.
Japan	There are no specific laws or regulations governing age checks for all social media(Tomoko, 2025) .	Age restrictions and the mechanisms or methods chosen are adjusted to the internal provisions of the social media platform. However, specifically for dating apps and platforms that contain pornographic content, uploading an ID (ID card/passport) is required for age verification.	This approach provides flexibility but creates uncertainty and potential loopholes in child protection. Exceptions only apply to high-risk services such as dating apps and pornography sites that require ID verification, indicating that Japanese regulations are still sectoral and reactive rather than comprehensive.
South Korea	The Act on Promotion of Information and Communication Network Utilization and Information Protection (ICN Act), which was replaced by the Personal Information Protection Act (PIPA) of 2011, as well as the Korea Communications Commission's	Previously, age verification practices had a broad scope, namely through Resident Registration Numbers. However, currently the mechanism is carried out in a combined and tiered manner through a verification system using i-PIN, SMS, and other methods. Meanwhile, strict regulations are in place in certain sectors, such as game applications and dating apps.	This approach is relatively comprehensive and provides a high level of accuracy, especially in high-risk sectors such as online games and dating apps. However, this approach also raises concerns about privacy and potential data misuse, given the high dependence on national identity, as stated by the South Korean Constitutional Court, which ruled that the use of this method should not be too broad.

Source: From various sources processed by the author

Based on the table, several countries need to be highlighted because they have specific regulations on social media and can serve as examples for the development of age assurance regulations. For example, countries that are members of the EU already have concerns about restricting children's access to social media, including the issue of personal data protection. The EU, as a regional organization, has the power to bind its member states. The EU itself has a Digital Services Act (DSA) that must be complied with by all digital platforms. The EU even determines the classification of "very large online platforms" (VLOPs), which are services that reach more than 10% of the EU population, or around 45 million people. to meet additional obligations, such as content moderation, stronger protection for minors through the development of age verification tools, and increased transparency and accountability(European Commission, 2023).

The EU is currently developing the Digital Identity Regulation (DIA), which introduces the EU Digital Identity Wallet, a technology that allows every EU citizen to securely store, manage, and use their identity and personal documents in digital form. It functions as identity authentication and ensures interoperability across all EU member states. This is a solution to the issue of personal data protection when faced with age assurance methods. This is because the EU Digital Identity Wallet will authenticate identities and share information such as age without revealing other personal details(eSafety Commissioner, 2024), thereby reducing the risk of personal data leaks and enhancing privacy protection. This mechanism is still undergoing large-scale trials involving 360 public and private entities in 26 other member states(eSafety Commissioner, 2024).

The initiation of the EU Digital Identity Wallet development not only introduces a technical instrument for age verification but also prioritizes privacy concerns. By providing age verification options without revealing other personal data, the European Union is trying to strengthen protection measures while upholding the principle of data minimization mandated by the GDPR. This shows that the European Union is building a comprehensive regulatory model: flexible, risk-based, and innovative, providing a more structured basis for child protection in the digital space without hindering the development of technology and the digital market.

Unlike the EU, the UK, through Ofcom (Office of Communications), already has Ofcom Guidance that regulates technical guidelines on age assurance for children(Ofcom UK, 2024a). This guidance further regulates the assessment of services that can be accessed by children, risk assessment to identify the risks posed by services to children, strict age verification, and the determination of algorithms that filter harmful content from children's timelines(Ofcom UK, 2024b) . The UK government itself already has the Online Safety Act 2023, which requires platforms, including social media, to strictly

implement age assurance when there is primary priority content (PPC), namely if it contains pornography and content that promotes suicide, self-harm, or eating disorders.

In its guidelines, Ofcom still gives platforms flexibility in determining proportional methods according to their services. Whether the service falls under Service Part 3, user-to-user platforms or search services such as social media, forums, search engines, or falls under Service Part 5, platforms that publish pornographic content themselves. Ofcom recommends a "high-assurance" approach for platforms with Service Part 5, such as facial age estimation, open banking, photo-identification (photo-ID) matching, mobile network operator (MNO) age checks, credit card checks, digital identity services, and email-based age estimation(Ofcom UK, 2025) . Meanwhile, platforms with Service Part 3 are required to conduct a Children's Access Assessment. These high assurance recommendations actually carry a high risk, especially for children's personal data. Therefore, to ensure that the age assurance process is effective, platforms must ensure that the process meets the following four criteria: technical accuracy, robustness, reliability, and fairness.

While the UK's approach through Ofcom emphasizes risk-based flexibility and technical reliability in the age assurance process, France, through the French Audiovisual and Digital Communication Regulatory Authority (Arcom), has taken a more prescriptive path by issuing Law No. 2023-566, colloquially known as the 'Digital Majority Law'. This regulation not only regulates age verification, but also explicitly requires parental consent for children under 15 to have social media accounts, thereby reinforcing a family authorization-based model of child protection. This means that "Double Consent" is required, namely an agreement between a legally recognized guardian and the child regarding the use of personal data, primarily for marketing, advertising, and creating account profiles on social networks and gaming platforms (Sitompul et al., 2025). Social media platforms are also required to verify the age of new registrants and verify parental consent for registrants under the age of 15. If not, the platform must reject registrants under the age of 15 (Legifrance, 2025). In addition, France has enacted a new law on Secure and Regulate Digital Space (SREN) as a national framework for the implementation of the EU DSA(Froge, 2024). The regulation authorizes Arcom to request the blocking or removal of online public communication services and video-sharing platform services that disseminate pornographic content.

On the other hand, Australia, a country that has specific regulations on Social Media Law in 2024, is currently developing guidance by the Australian eSafety Commissioner, 2025. As a rule developed from Australia's Online Safety Act, this new regulation explicitly prohibits social media platforms from restricting the creation of accounts for Australian children under the age of 16 and gives platforms the authority to take reasonable steps to prevent this.

Currently, the regulation is still in a transition period until it comes into effect in December 2025(Australian Government, 2024).

Several specific provisions of the Social Media Law regulate penalties for social media platforms that do not comply, with fines of AUD \$49.5 million and a prohibition on using or disclosing any personal information collected during the use of platform services for purposes outside the provisions of(Corrs Chamber Westgarth, 2025). Platforms must also implement some form of age assurance to identify whether an account holder is under the age of 16, as a form of "taking reasonable steps." Regarding the age assurance method, Australia has not yet decided specifically which method to choose. However, the development tends towards age estimation technology using AI, because the self-declaration method is considered ineffective(Julie Inman Grant, 2025).

Meanwhile, several US states also have specific regulations on social media that impose restrictions on children of varying ages. Utah, Texas, and Arkansas restrict social media to users over the age of 18, unless they have parental consent. Florida prohibits social media accounts for those under the age of 14 and requires parental consent for those aged 15–16. Similarly, there are various age verification methods, such as self-declaration in Colorado and Texas, government ID in Louisiana, commercially reasonable efforts in Georgia, New York, and Tennessee, and no specific regulations in Florida and Utah(OECD, 2025b) .

The same approach is also taken by Asian countries, such as China, South Korea, and Japan. China itself can even be an example where age assurance regulations, including supervision, are quite strict. This is in line with government control over people's social lives, including online activities. The anonymity that is the basis of social media is being eroded, because China implements real-name registration (official identity documents), which is considered an effective legal instrument to strengthen state control in the digital space. Service providers are required to verify the identity of users through national identity cards or other official documents. This mechanism is carried out through the National Network Identity Authentication, which implements NFC ID and facial recognition. Children under the age of 14 must apply through their parents, while those between the ages of 14 and 18 remain under the supervision of a guardian. All social media/online activities are monitored by government authorities through the Cyberspace Administration of China (CAC)(Sitompul et al., 2025). Although this mechanism has been criticized for restricting freedom of expression and posing a major risk to personal data protection(J.-A. Lee & Liu, 2016), the Chinese government remains convinced that this mechanism can be a solution to restrict children's access to social media.

In line with the Chinese government, South Korea also has a complex age assurance mechanism, which has undergone a long journey since 2004. Starting from the Resident Registration Numbers (RRN) mechanism to verification based

on the Internet Real Name System. South Korea conducts tiered verification according to risk levels, namely through identity verification for access above 19 years of age and by telephone for ages above 15 years. Through the Act on Promotion of Information and Communication Network Utilization and Information Protection (ICN Act), which was replaced by the Personal Information Protection Act (PIPA) of 2011, the Korea Communications Commission (KCC) designated three mobile operators as identity verification agencies. This designation allows phone numbers to be used as an alternative authentication method. In 2017, the KCC also added seven credit card companies as identity verification agencies, allowing credit card numbers and mobile transactions to be included as alternative identification methods. The issue of child data protection is addressed through PIPA 2011, whereby data of children under 14 years of age may only be processed with parental consent, and they have the right to request correction or deletion of data (S. (Helen) Lee & Lee, 2025) . Unlike China and South Korea, Japan does not yet have specific regulations governing age assurance. The methods and criteria for determining age are left to individual platforms, resulting in no standardized approach.

After reviewing several regulations related to age assurance methods in several countries, the question then arises as to what the age assurance provisions are in Indonesia, particularly those related to children's access to social media. There are at least three (3) related regulations, including:

Table 3. Regulations Related to Child Protection in Digital Services (Social Media)

Regulation	Focus	Description
Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (Amendment to the ITE Law), specifically Articles 16A and 16B.	These regulations form the basis for child protection that must be implemented by Electronic System Providers (ESPs) when using digital products, services, and features. In general, ESPs are required to provide information regarding the minimum age limit for children who can use their products or services; mechanisms for verifying child users; and mechanisms for reporting misuse of products, services, and features that violate or have the potential to violate children's rights.	As a basic rule, this amendment to the ITE Law does not explicitly explain specific methods for verifying child users, but only imposes an obligation on ESOs.
Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)	specifically classifies children's data as specific data, so that the processing of children's personal data is also carried out in a specific manner. The mechanism must obtain the consent of the child's parents and/or guardians (parental consent), because children are still vulnerable to the dangers of social media(Bernike* & Andersen, 2023) .	This provision is important as a basis when ESPs processes data during age verification. Although there are specific methods such as parental consent, there are no derivative regulations explaining the technical aspects of these methods.
Government Regulation Number 17 of 2025 concerning the Governance of Electronic System Implementation in Child Protection (Gov-Reg 17/2025),	regulates a number of provisions in the protection of children, mainly regarding age verification mechanisms (platforms are required to implement a proportional and risk-based age verification system) and parental controls (providing effective parental control features). In age verification, platforms must adjust to the risks to children's rights that may arise from the operation of products, services, and features.	Technically, this PP does not specify a particular method, but provides guidelines in the form of risk levels and age classifications or categories for children.

Source: From various sources processed by the author

Additionally, the Gov-Reg 17/2025 Regulation includes several specific restrictions, such as:

- a. prohibiting the profiling of children by any means or method, such as for the purpose of offering products or services or for other purposes;
- b. limiting data processing solely for the purpose of verifying a child's age and not for other purposes;
- c. deleting data used for verification after the child's age has been verified.

Referring to these regulations, Indonesia itself can be categorized as a country that does not specifically regulate the methods that ESPs must use. The government only provides general guidelines and risk-based classifications for each ESPs. This is evidenced in the academic study of Gov-Reg 17/2025, which states that the responsibility for verification can be delegated to ESPs, as is widely practiced in other countries. The consideration is that ESPs are deemed to have the capacity to comply with regulations related to age verification. Meanwhile, the role of the government in this matter, specifically the Ministry of Communication and Digital Affairs, is to conduct supervision, ranging from monitoring, receiving reports or complaints, to taking action on reports or complaints, as well as implementing controls based on the results of inspections.

C. Critical Analysis for Indonesia

Gov-Reg 17/2025 is the first regulation in Indonesia that specifically provides a legal framework for child protection in the digital and social media. The presence of this regulation can be seen as a significant normative leap, considering that previously, child protection in cyberspace was only partially regulated through the PDP Law, that focuses on providing the general legal framework governing the processing of personal data (in general).

The processing of personal data for age assurance must have an appropriate legal basis. Article 20 of the PDP Law requires a Personal Data Controller to have a lawful basis for processing, including valid consent or other legally recognized grounds. This is particularly relevant where age assurance involves identity documents, facial images, biometric information, or other information capable of identifying or profiling a child.

The principles governing processing under the PDP Law are also directly relevant to the design of age-assurance systems. In particular, age assurance should be subject to purpose limitation and data minimization, so that information collected to establish whether a user satisfies a particular age threshold is not subsequently used for unrelated purposes. The system

should also limit the retention of verification information and provide for deletion or destruction when the applicable retention period has expired or when there is no longer a lawful basis for retaining the information.

Caution is required where age assurance involves biometric data. The PDP Law classifies biometric data as specific Personal Data, thereby subjecting it to heightened legal protection. Consequently, the use of facial recognition or other biometric technologies for age verification should not be regarded as automatically justified merely because it may provide greater certainty regarding a user's age.

One notable feature of Gov-Reg 17/2025 is the introduction of a risk-based approach, which divides children into three age groups (under 13 years old, 13–15 years old, and 16–17 years old), accompanied by access restriction mechanisms that are proportional to the level of maturity of the child. This approach reflects an attempt to incorporate the principle of the best interests of the child into the regulatory framework of the best interests of the child as mandated by the Convention on the Rights of the Child (CRC) and General Comment No. 25 on children's rights in the digital world. Several countries have done the same thing by classifying children's ages into several groups. The basic argument is that each stage of a child's growth and development has different cognitive, emotional, and social characteristics, so their capacity to understand risks, make decisions, and access digital information cannot be generalized. Age-specific regulation may allow regulators to differentiate obligations according to children's developmental stages, although such differentiation must remain proportionate and consistent with other children's rights. In addition to providing legal certainty, this age classification also allows for differentiation of responsibilities for both parents and Electronic System Providers in providing safe, appropriate, and developmentally appropriate digital access. Gov-Reg 17/2025 also emphasizes the obligation of both public and private Electronic System Providers to implement age verification and parental control mechanisms. The presence of this feature is in line with practices in various jurisdictions, such as the Children's Access Assessment in the UK's Online Safety Act and the double parental consent requirement in France.

However, it should be critically noted that Gov-Reg 17/2025 does not actually specify the verification methods or technical standards that must be used by ESPs. This omission may lead to inconsistent implementation across electronic system provider and may permit verification practices that satisfy formal regulatory requirements without providing meaningful protection for children. In comparison, the European Union, in developing the Digital Services Act (DSA) and Digital Identity Wallet, involved public consultation and large-scale trials prior to implementation. This process not only

strengthens the legitimacy of the regulation but also increases the level of industry compliance due to the direct participation of stakeholders. Thus, although Gov-Reg 17/2025 has shown normative progress, the absence of a clear methodology and consultative mechanism has the potential to weaken the effectiveness of the regulation and compliance by ESPs in practice.

Furthermore, this regulation still has a number of weaknesses that could hamper its effective implementation. First, Gov-Reg 17/2025 does not set minimum technical standards for age verification methods. Unlike the UK Ofcom guidelines, which require the application of four main principles (technical accuracy, robustness, reliability, fairness), Gov-Reg 17/2025 only stipulates general obligations without clear performance measures. This has the potential to create disparities in the quality of implementation between platforms, especially if each ESP interprets age verification obligations differently.

The obligation of ESPs to verify age should correspond to the level of risk associated with the product, service, or feature rather than requiring the most intrusive form of verification in every circumstance. A service presenting a higher risk of harm to children may justify a higher level of age assurance, whereas lower-risk services should be able to rely on less intrusive mechanisms. This approach is consistent with the principle that the best interests of the child cannot be achieved simply by maximizing restrictions. The regulatory objective of protecting children must be balanced against their rights to privacy, access to information, participation, and autonomy. Therefore, the level of assurance required should be proportionate to the risk and should use the least intrusive mechanism reasonably capable of achieving the protective objective.

Second, the use of third parties in age assurance services is not regulated within a comprehensive trust framework. In fact, global experience shows that the involvement of third-party providers poses significant risks related to privacy, data security, and legal accountability, especially if these service providers are not subject to national regulations. Where platforms outsource age verification to specialized providers, the transfer of the verification process to a third party should not transfer responsibility for children's rights.

The regulatory framework should therefore clearly establish the responsibilities of platforms, verification providers, and other entities involved in the processing chain. Age-assurance providers should be required to apply data minimization, purpose limitation, security and appropriate deletion mechanisms. Where possible, the verification process should confirm only the relevant age attribute rather than disclose the child's complete identity to the platform. This is particularly important because the use of identity documents, biometric information, facial age

estimation, or AI-based profiling may create additional risks to children's privacy and informational autonomy (Lueks et al., 2026)

Third, Gov-Reg 17/2025 also does not fully address the challenge of the digital divide in Indonesia. Age verification requirements based on official documents or biometrics have the potential to exclude children from poor families, who may not have access to formal identity documents or adequate digital devices. As a result, protective measures may unintentionally create exclusionary effects and exacerbate existing inequalities in digital access.

A verification system that incorrectly identifies an adult as a child, or a child as belonging to a prohibited age category, may prevent legitimate access to information, education, communication, or other digital services (Laura Hyun Kyung Oh, 2023). These risks may disproportionately affect children who lack access to government identification documents, have limited technological resources, have disabilities, or experience difficulties with particular verification technologies. Consequently, age assurance should not depend exclusively on a single technological mechanism. The regulatory framework should provide alternative verification pathways where appropriate and establish accessible mechanisms through which users can challenge an inaccurate age determination. Platforms and verification providers should also provide clear information concerning the basis and consequences of verification decisions and establish effective complaint and review procedures.

Overall, Gov-Reg 17/2025 represents a significant development in Indonesia's regulatory framework for child protection in the digital environment, because it places the protection of children in the digital space within a comprehensive, risk-based, and data protection principle-based legal framework. However, this regulation still needs strengthening in terms of technical aspects, supervision, inclusiveness, and an accountability framework for third parties. Without improvements in these aspects, there is a risk that Gov-Reg 17/2025 will only become a declarative regulation that is difficult to implement consistently in the field. Therefore, in the future, more detailed technical guidelines, harmonization between authorities, and periodic evaluations are needed so that Gov-Reg 17/2025 can truly become an effective instrument in ensuring the best interests of the child in Indonesia's digital space.

IV. Conclusion

Age assurance should not be treated as a stand-alone solution for protecting children on social media. Any age verification system is essentially just an instrument to ensure that digital services related to children must always prioritize the best interests of the child. It is important to note that not all age

assurance models require the same level of assurance; their implementation must be tailored to national conditions, practical needs, and most importantly, how the country is able to develop models that are effective and economically efficient. From a broader perspective, age assurance is an integral part of efforts to build a digital ecosystem that is suitable for children.

The best interests of the child should therefore operate as a balancing and evaluative principle rather than merely as a justification for restricting children's access to digital services. An age-assurance model serves the best interests of the child when it provides effective protection against online harm while minimizing unnecessary interference with privacy, access to information, freedom of expression, autonomy, inclusion, and other children's rights. The Indonesian government, through Gov-Reg 17/2025 and Min-Reg 9/2026, still has room to conduct further studies, particularly related to (i) standard technical age verification that is uniform and auditable; and (ii) compliance monitoring mechanisms to ensure the compliance of Electronic System Providers.

For Indonesia, the comparative analysis supports a risk-calibrated and rights-preserving approach to age assurance in Indonesia. Under this model, the level and method of age assurance should correspond to the level of risk associated with the relevant digital service, product, or feature, rather than imposing a uniform and equally intrusive verification requirement across all services. Higher-risk services may justify stronger forms of age assurance, whereas lower-risk services should rely, where appropriate, on less intrusive mechanisms. This approach allows the regulatory system to remain proportionate while maintaining its primary objective of protecting children from online harms. The absence of clear technical standards has the potential to cause variations in implementation between platforms and open the door to formalistic practices that only fulfill administrative obligations without actually protecting children. Therefore, Indonesia requires clearly formulated, consistent, auditable, and credible technical standards to ensure that age-assurance mechanisms are implemented consistently across electronic system provider.

V. Acknowledgments

The paper was presented at the 4th PCINU Netherlands Biennial International Conference. The author(s) would like to express sincere gratitude to the Institute for Research and Community Services, Universitas Diponegoro (LPPM UNDIP) for providing financial support through the International Publication Research Scheme under contract number 222-375/UN7.D2/PP/IV/2025. This support has been invaluable in carrying out the research and preparing this article.

References:

- 5Rights Foundation. (2021). *But how do they know it is a child? Age Assurance in the Digital World*.
- Achmad, A. (2020). Dualisme Penerapan Hukum bagi Pelaku Kekerasan Seksual terhadap Anak. *LITIGASI*, 20, 267–290.
- Anda, F., Becker, B. A., Lillis, D., Le-Khac, N.-A., & Scanlon, M. (2020). *Assessing the Influencing Factors on the Accuracy of Underage Facial Age Estimation*. <https://doi.org/10.48550/ARXIV.2012.01179>
- Australian Government. (2024). *Social media minimum age legislation passed*. Australian Government. <https://www.infrastructure.gov.au/departments/media/news/social-media-minimum-age-legislation-passed>
- Bernike*, D., & Andersen, C. (2023). Presence of Age Restrictions for Children to Have Social Media Accounts in Law Number 27 of 2022 Concerning Personal Data Protection. *Riwayat*, 6(1), 23–28. <https://doi.org/10.24815/jr.v6i1.29208>
- Brennan, M., & Phippen, A. (2021). *Child Protection and Safeguarding Technologies Appropriate or Excessive 'Solutions' to Social Problems?* Routledge.
- Canales, K. (2025). *Silicon Valley Says Kids over the Age of 13 Can Handle the Big, Bad World of Social Media. Experts Say That's the Result of a 'problematic.'* INSIDER. <https://www.businessinsider.com/why-you-must-be-13-facebook-instagram-problematic-law-coppa-2022-1>
- Corrs Chamber Westgarth. (2025). *Social media use in Australia to be restricted for under 16s*. Corrs Chamber Westgarth. <https://www.corrs.com.au/insights/social-media-use-in-australia-to-be-restricted-for-under-16s>
- Dewi, I. R. (2023, April 16). 2,6 Juta Konten Negatif Diblokir Kominfo, Setengahnya Ternyata Pornografi. *Sindinews.Com*.
- Dw.com. (2024, November 29). TikTok, Meta Kritik UU Batas Usia Pengguna Medsos Australia. *Dw.Com*.
- eSafety Commissioner. (2023). *Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography*.
- eSafety Commissioner. (2024). *Tech Trends Issues Paper Age Assurance*.
- European Commission. (2023). *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

- Fajri, D. A. (2025, February 4). Wamen Pendidikan Dasar: Aturan Pembatasan Media Sosial pada Anak Paling Rasional. *Tempo.Co*.
- Firdausya, I. (2021, April 16). Survei: 87% Anak Indonesia Main Medsos sebelum 13 Tahun. *Media Indonesia*.
- Fitriani, R. (2016). Peranan Penyelenggara Perlindungan Anak dalam Melindungi dan Memenuhi Hak-Hak Anak. *Jurnal Hukum Samudra Keadilan*, 11(2).
- Froge, P.-E. (2024). *The French law on the regulation of games including NFT is passed: Place your bets*. BCLP. <https://www.bclplaw.com/en-US/events-insights-news/the-french-law-on-the-regulation-of-games-including-nft-is-promulgated-place-your-bets.html>
- Gambling Commission. (2024). *Young People and Gambling 2020: Official statistics*. Gambling Commission. <https://www.gamblingcommission.gov.uk/statistics-and-research/publication/young-people-and-gambling-2020>
- Ganel, T., Sofer, C., & Goodale, M. A. (2022). Biases in human perception of facial age are present and more exaggerated in current AI technology. *Scientific Reports*, 12(1), 22519. <https://doi.org/10.1038/s41598-022-27009-w>
- Gerken, T. (2025). TikTok investigated over use of children's data. *BBC.Com*.
- Huk, T. (2016). Use of Facebook by Children Aged 10-12. Presence in Social Media Despite the Prohibition. *New Educational Review*, 46(1), 17–28. <https://doi.org/10.15804/TNER.2016.46.4.01>
- ICO UK. (2021). *Information Commissioner's opinion: Age Assurance for the Children's Code Information*.
- ICO UK. (2023). *ICO fines TikTok £12.7 million for misusing children's data*. <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/>
- Jamaludin, A. (2024). Age Verification Regulation in Social Media Platform Usage: Preventive Measures Against Online Child Sexual Violence. *Jurnal Bina Mulia Hukum*, 8(2), 276–295. <https://doi.org/10.23920/jbmh.v8i2.1311>
- Jarvie, C., & Renaud, K. (2024). Online Age Verification: Government Legislation, Supplier Responsibilization, and Public Perceptions. *Children*, 11(9), 1068. <https://doi.org/10.3390/children11091068>
- Julie Inman Grant. (2025). *Behind the screen: The reality of age assurance and social media access for young Australians*.
- Köhler-Dauner, F., Peter, L., Sitarski, E., Chauviré-Geib, K., Haag, A.-C., & Fegert, J. M. (2025). Digital child protection in social networks: Age verification and age-tiered regulation in Europe. *Child and Adolescent*

- Laura Hyun Kyung Oh. (2023). *Children's Data Privacy: Children's Rights To Data Privacy And What We Can Learn From Overseas* [Thesis]. University of Auckland.
- Lee, J.-A., & Liu, C.-Y. (2016). Real-Name Registration Rules and the Fading Digital Anonymity in China. *Washington International Law Journal*, 25(1).
- Lee, S. (Helen), & Lee, M. J. (2025). *South Korea's Approach to Age Assurance*. Tech Policy Press.
- Legifrance. (2025). *LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique*. Legifrance.
<https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/>
- Livingstone, S., Nair, A., Stoilova, M., Van Der Hof, S., & Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. *The International Journal of Children's Rights*, 32(3), 721-747.
<https://doi.org/10.1163/15718182-32030001>
- Lueks, W., Dreyer, S., Federrath, H., & Simon, J. (2026). *Assessing Age Assurance Technologies: Effectiveness, Side-Effects, and Acceptance* (Version 1). arXiv.
<https://doi.org/10.48550/ARXIV.2603.25695>
- Meurens, N. (2022). *Child Safety by Design That Works against Online Sexual Exploitation of Children*. Down to Zero Alliance.
- Mitchell, K. J., Finkelhor, D., & Becker-Blease, K. A. (2007). Linking Youth Internet and Conventional Problems: Findings from a Clinical Perspective. *Journal of Aggression, Maltreatment and Trauma*, 15(2), 39-58.
https://doi.org/10.1300/J146v15n02_03
- Mukherjee, S., Pothong, K., & Livingstone, S. (2021). *Child Rights Impact Assessment: A tool to realise children's rights in the digital environment*.
- Nagy, A., & Fazekas, A. (2018). *Perspectives on Youth: Young People in a Digitalised World* (European Commission and Council of Europe, Ed.). Council of Europe.
- OECD. (2025a). *How's Life for Children in the Digital Age?*
<https://doi.org/https://doi.org/10.1787/0854b900-en>
- OECD. (2025b). *The Legal and Policy Landscape of Age Assurance Online For Child Safety and Well-Being*.
- OFCOM UK. (2020). *Children and parents: Media use and attitudes report*.

- Ofcom UK. (2024a). *Consultation: Guidance for service providers publishing pornographic content*. Ofcom UK. <https://www.ofcom.org.uk/online-safety/protecting-children/guidance-service-providers-pornographic-content>
- Ofcom UK. (2024b). *Statement: Protecting children from harms online*. Ofcom UK. <https://www.ofcom.org.uk/online-safety/protecting-children/protecting-children-from-harms-online>
- Ofcom UK. (2025). *Guidance on highly effective age assurance and other Part 5 duties For Part 5 services*.
- O'Shea, L. (2019). *Future Histories: What Ada Lovelace, Tom Paine, and the Paris Commune Can Teach Us about Digital Technology*. Verso.
- Paat, Y. P. (2025, February 4). Aturan Pembatasan Media Sosial untuk Anak Disiapkan via PP atau UU. *Beritasatu.Com*.
- Pratiwi, R. S., & Anna, L. K. (2021, March 30). Mudahnya Mengakali Batasan Umur di Media Sosial. *Kompas.Com*.
- Presianta, A. (2024, December 9). Perlukah Pembatasan Media Sosial? *Tempo.Co*.
- Rahayu. (2015). *Hukum Hak Asasi Manusia*. Undip Press.
- Rocha, J. F. (2026). Age assurance mechanisms in digital environments: Technical options, legal limits and proportionality criteria. *Brazilian Journal of Law, Technology and Innovation*, 4(1), 54–74. <https://doi.org/10.59224/bjlti.v4i1.54-74>
- Shaffique, M. R., & Van Der Hof, S. (2026). Behavioural profiling for age assurance: Do the ends justify the means? *International Data Privacy Law*, 16(1), ipaf012. <https://doi.org/10.1093/idpl/ipaf012>
- Sitompul, J., Fibrianti, S., Ardiansyah, F. H., Rouli, M. J., & Purgativa, P. D. (2025). *Kajian Akademik Perlindungan Anak dalam Penyelenggaraan Sistem Elektronik*. Kementerian Komunikasi dan Digital RI.
- Smirnova, S., Livingstone, S., & Stoilova, M. (2021). Understanding of User Needs and Problems: A Rapid Evidence Review of Age Assurance and Parental Controls. *Monograph, euConsent*.
- Stemler, A., Prayuti, A. J. and Y., Jamaludin, A., Achmad, A., Giles, C., Rosmalinda, E. I. and, al., et E. A. G.-C. et, Young, G. K., Helen C. Whittle and Anthony R. Beech, C. E. H.-G., al., H. A.-S. et, Lee, H. E. Y. and C. H., McNealy, J. E., Stathis, M. J., Marinakis, M. M., Reid, J. A., Jones, S., Joleby, M., al., et E. A. G.-C. et, Franks, M. A., ... Lee, B. (2021). Young Users' Social Media Addiction: Causes, Consequences and Preventions. *Journal of Child Sexual Abuse*, 20(1), 235–249. <https://doi.org/10.1007/s10560-020-00656-6>

- Supermana, R. (2025, February 4). Menkominfo Paparkan Usulan Aturan Pembatasan Akses Medsos Anak-anak. *Rri.Co.Id*.
- Thurman, N., & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. *Policy & Internet*, 13(3), 415–432. <https://doi.org/10.1002/POI3.250>
- To Create The Social Media Safety Act (2023).
- Tomoko, S. (2025). Keeping Japanese Children Safe in Cyberspace: Weighing the Roles of Government, Business, and Family. *Nippon.Com*.
- Triastuti, E., A, P., & V, N. H. (2017). *Peta Jalan Perlindungan Anak Indonesia di Internet: Suatu Pengantar*. Kementerian Komunikasi dan Informatika RI.
- Triastuti, E., Indra, D. A. W., & Nurul, A. (2017). *Kajian Dampak Penggunaan Media Sosial Bagi Anak dan Remaja*. Pusat Kajian Komunikasi Departemen Ilmu Komunikasi FISIP UI.
- Tufford, L., & Lee, B. (2020). Relationship Repair Strategies When Reporting Child Abuse and Neglect. *Child and Adolescent Social Work Journal*, 37(3), 235–249. <https://doi.org/10.1007/s10560-020-00656-6>
- Vandewater, Elizabeth A, & Lee, Sook-Jung. (2009). Measuring Children's Media Use in the Digital Age: Issues and Challenges. *American Behavioral Scientist*, 52(8), 1152–1176. <https://doi.org/10.1177/0002764209331539>
- Voa Indonesia. (2024, November 30). Larangan Medsos untuk Anak di Bawah 16 Tahun di Australia Picu Pro dan Kontra. *VOA Indonesia*.
- Wulandari, M. D., & al., et. (2020). Children's Knowledge and Skills Related to Self-Protection from Sexual Abuse in Central Java Indonesia. *Journal of Child Sexual Abuse*, 29(5), 499–512. <https://doi.org/10.1080/10538712.2019.1703231>