

Strengthening Digital Child Protection in Asia and Africa through the Islamic Digital Protection Framework (IDPF)

Siti Ropiah,^{1*} Adamu Abubakar Muhammad,² Nur Hafieza Ismail,³ Huma Khan⁴

¹ Sekolah Tinggi Agama Islam Haji Agus Salim, Cikarang, Bekasi, Indonesia

² Department of Islamic Studies, Federal University of Kashere, Gombe State, Nigeria

³ University Malaysia Pahang Al-Sultan Abdullah, Pekan, Pahang, Malaysia

⁴ Senior research associate (SRA), CIET, National council of educational research and training (NCERT), New Delhi, India

*Corresponding Author: Siti Ropiah

E-mail: ropiah@staihas.ac.id

Article History:

Received: April 17, 2025 | Revised: September 5, 2025 | Accepted: November 25, 2025 | Published: December 30, 2025

Citation (APA Style):

Ropiah, S., Muhammad, A. A., Ismail, N. H., & Khan, H. (2025). Strengthening Digital Child Protection in Asia and Africa through the Islamic Digital Protection Framework (IDPF). *Munakahat: Journal of Islamic Family Law*, 2(1), 49–61.

Abstract

Background: Rapid digital transformation has increased children's exposure to cyberbullying, online exploitation, harmful content, privacy violations, and algorithm-driven risks. Although digital child protection regulations have expanded across Asia and Africa, comparative socio-legal studies integrating Islamic family law, child rights, and digital governance remain limited.

Objective: This study examines regulatory approaches to digital child protection in Indonesia, Malaysia, South Korea, and Nigeria and proposes the Islamic Digital Protection Framework (IDPF) as an integrative governance model.

Methods: This study employs a qualitative comparative socio-legal approach combining doctrinal legal research, regulatory comparison, documentary analysis, and policy evaluation. The analysis integrates *maqāṣid al-sharī'ah*, Child Rights Theory, Digital Governance Theory, and Legal Pluralism Theory.

Results: The findings reveal that the four jurisdictions recognize digital child protection as a regulatory priority but differ in approaches to age verification, parental responsibility, privacy protection, platform accountability, and institutional enforcement. These regulatory experiences are synthesized into the IDPF, consisting of five dimensions: adaptive regulatory compliance, technological safeguards, ethical platform governance, family and community participation, and Islamic normative values.

Conclusion: The IDPF offers a comparative socio-legal governance model that connects Islamic family law with contemporary digital governance by emphasizing legal certainty, technological accountability, ethical responsibility, and collaborative protection.

Novelty: This study introduces the IDPF as an original framework integrating Islamic legal principles, child rights, and digital governance through a comparative analysis of Asian and African jurisdictions.

Keywords: Islamic Digital Protection Framework (IDPF); digital child protection; digital governance; Islamic family law; *maqāṣid al-sharī'ah*.

INTRODUCTION

The rapid expansion of digital technologies has fundamentally reshaped children's social, educational, and economic experiences across Asia and Africa. Digital platforms provide unprecedented opportunities for learning, communication, creativity, and participation; however, they have simultaneously generated complex and transnational risks that challenge traditional models of child protection. Cyberbullying, online sexual exploitation, privacy violations, harmful algorithmic recommendations, excessive data extraction, misinformation, digital addiction, and commercial exploitation of children's personal information have become critical governance concerns requiring stronger legal and institutional responses (Abu Sarhan & Fouche, 2025; Acquah, 2025; Arif et

al., 2025; Zahoor & Lone, 2025). Furthermore, the rapid emergence of artificial intelligence (AI), biometric technologies, blockchain applications, immersive virtual environments, and algorithm-driven platforms has expanded children's digital exposure while creating new regulatory complexities related to autonomy, security, identity, and personal data protection (Gabellini et al., 2025; Han et al., 2025; Lim et al., 2025; Park et al., 2025; Zare & Jalali, 2025). Therefore, digital child protection can no longer be approached merely as a technological or criminal law issue but requires a comprehensive governance framework capable of integrating legal protection, technological accountability, ethical responsibility, and social participation.

Across Asia and Africa, governments have adopted diverse regulatory strategies reflecting differences in legal traditions, institutional capacities, technological development, and governance priorities. Indonesia represents one of the emerging comprehensive approaches through Government Regulation Number 17 of 2025 concerning Child Protection in Electronic System Administration, which establishes mandatory obligations for Electronic System Providers regarding age verification, parental consent, privacy-by-default mechanisms, digital risk assessment, content classification, complaint procedures, and platform accountability (Government of Indonesia, 2025). This child-centered regulatory framework is complemented by Law Number 27 of 2022 concerning Personal Data Protection, which strengthens principles of lawful data processing, security protection, accountability, and individual control over personal information in digital environments (Government of Indonesia, 2022).

Malaysia adopts a more integrated digital governance approach by embedding child protection within broader telecommunications, electronic communication, and personal data protection frameworks. The Communications and Multimedia Act 1998 provides the foundation for electronic communication governance and digital service regulation, while the Personal Data Protection Act 2010 establishes obligations concerning personal data processing, privacy protection, and organizational accountability (Malaysia, 1998, 2010). South Korea demonstrates a technologically advanced governance model by combining cybersecurity regulation, personal information protection, artificial intelligence governance, and youth online safety mechanisms. The Act on Promotion of Information and Communications Network Utilization and Information Protection provides a foundation for information security and responsible network management, while the Personal Information Protection Act administered by the Personal Information Protection Commission establishes comprehensive requirements concerning lawful data processing, privacy safeguards, security obligations, and institutional accountability (Republic of Korea, 2023; Personal Information Protection Commission, 2023). Meanwhile, Nigeria illustrates an emerging African regulatory model through the Child Rights Act 2003, Nigeria Data Protection Act 2023, and related implementation guidelines that seek to strengthen children's online safety, personal data protection, and institutional accountability within a rapidly expanding digital economy (Federal Republic of Nigeria, 2003, 2023; National Information Technology Development Agency, 2023). These four jurisdictions therefore provide valuable comparative settings for examining how different legal systems respond to similar digital child protection challenges through distinct regulatory pathways (Khusnaini & Aisyah, 2025; Lim et al., 2025; Khatani et al., 2025).

Existing scholarship indicates that effective digital child protection cannot depend solely on statutory regulation but requires a collaborative governance ecosystem involving governments, digital platforms, educational institutions, families, communities, and technology developers. Previous studies emphasize that regulatory effectiveness is influenced by institutional coordination, platform accountability, cybersecurity resilience, digital literacy, ethical AI governance, and parental involvement in preventing cyberbullying, online grooming, harmful content exposure, digital manipulation, and algorithmic discrimination (Herrero-Arias & Tonheim, 2025; Long et al., 2025; Saleh et al., 2025; Fraiw an & Almomani, 2025; Rahmani et al., 2025; Bai & Liu, 2025). Nevertheless, differences in constitutional structures, enforcement capacity, technological readiness, and socio-cultural contexts continue to produce significant variations in how countries design and implement digital child protection policies. Consequently, comparative analysis is necessary not only to identify regulatory similarities but also to understand how contextual factors shape the effectiveness of child-centered digital governance.

Internationally, children's protection is grounded in the Convention on the Rights of the Child (CRC), which recognizes children as rights holders entitled to protection, participation, and the fulfillment of their best interests (Convention on the Rights of the Child, 1989). Responding to digital transformation, the OECD Recommendation on Children in the Digital Environment further emphasizes child-centered governance through online safety, privacy protection, digital literacy, and shared responsibilities among governments, technology providers, families, and other stakeholders (OECD, 2021). Within Islamic family law, digital child protection represents a

contemporary application of *maqāṣid al-sharī'ah*, particularly the preservation of life (*hifẓ al-naḥs*), intellect (*hifẓ al-'aql*), lineage (*hifẓ al-nasl*), property (*hifẓ al-māl*), and human dignity. Protecting children's digital identity, privacy, psychological well-being, and online security therefore constitutes an extension of Islamic legal objectives within modern digital societies (Banurea, 2025; Nidhom & Murtadho, 2025). This perspective aligns with Children's Rights Theory, Digital Governance Theory, and Legal Pluralism Theory, which collectively highlight the importance of integrating legal norms, technological regulation, ethical values, and social participation in protecting children within digital environments.

Despite increasing academic attention to cybersecurity, artificial intelligence governance, digital privacy, and online child protection, important theoretical and practical gaps remain. Existing studies generally examine these fields separately and rarely integrate Islamic family law, comparative digital regulation, child rights, and governance theory within a unified analytical framework involving both Asian and African jurisdictions. Moreover, limited research has developed an operational governance model capable of guiding policymakers, digital platforms, educational institutions, families, and child protection agencies in responding to rapidly evolving digital risks. Addressing these limitations, this study comparatively examines Indonesia, Malaysia, South Korea, and Nigeria and proposes the Islamic Digital Protection Framework (IDPF) as an integrative governance model for strengthening digital child protection across Asia and Africa. By synthesizing *maqāṣid al-sharī'ah*, comparative law analysis, children's rights, digital governance, and legal pluralism, this study contributes a child-centered, ethically grounded, and adaptive framework for future regulatory development in increasingly complex digital ecosystems.

LITERATURE REVIEW

The rapid expansion of digital technologies has fundamentally transformed children's lives across Asia and Africa, creating unprecedented opportunities for education, communication, social interaction, and economic participation while simultaneously exposing children to increasingly complex digital risks. Cyberbullying, online sexual exploitation, privacy violations, harmful algorithms, excessive data collection, misinformation, digital addiction, and commercial exploitation of children's personal information have emerged as major global concerns requiring stronger legal protection and regulatory intervention (Abu Sarhan & Fouche, 2025; Acquah, 2025; Arif et al., 2025; Zahoor & Lone, 2025). The accelerated development of artificial intelligence (AI), biometric identification, blockchain applications, immersive virtual environments, and algorithm-driven digital platforms has further intensified regulatory challenges by expanding the scale and complexity of children's interactions within digital ecosystems. In particular, AI-driven systems create new concerns regarding automated decision-making, profiling, bias, privacy, safety, and children's rights, requiring governance approaches that prioritize child-centred design, transparency, accountability, and protection of children's best interests (UNICEF, 2021). Consequently, strengthening digital child protection has become a strategic priority that extends beyond technological regulation toward comprehensive governance capable of safeguarding children's rights, dignity, privacy, and well-being within increasingly interconnected digital societies.

Recent technological developments have further expanded scholarly discussions regarding artificial intelligence, biometric identification, blockchain systems, digital twins, and immersive metaverse platforms. While these technologies create significant opportunities for education, communication, and innovation, they simultaneously introduce new legal challenges concerning automated profiling, algorithmic discrimination, surveillance, digital identity, virtual property, and children's online autonomy (Gabellini et al., 2025; Han et al., 2025; Park et al., 2025; Rahmani et al., 2025; Bai & Liu, 2025; Zare & Jalali, 2025). UNICEF (2021) emphasizes that AI systems involving children should be developed and governed according to child-centred principles, including safety, privacy protection, fairness, transparency, accountability, and the promotion of children's rights. Cybersecurity scholarship likewise argues that sustainable digital governance depends upon integrated security architecture involving digital forensics, secure infrastructure, quantum-resistant cybersecurity, and responsible technological innovation (Ali et al., 2025; Arif et al., 2025).

Comparative legal scholarship likewise reveals considerable diversity in how countries regulate children's digital rights. Across Asia, Indonesia has strengthened child protection through Government Regulation Number 17 of 2025, Malaysia has reinforced personal data governance and online safety through integrated digital regulation, while South Korea combines advanced cybersecurity policies with proactive institutional supervision and AI governance. In Africa, Nigeria has also intensified efforts to improve digital governance through cybersecurity legislation, child protection initiatives, and increasing regulatory attention to online platforms, although

institutional implementation continues to face substantial developmental challenges. Comparative studies consistently demonstrate that regulatory effectiveness depends not only upon statutory provisions but equally upon institutional coordination, digital literacy, technological capacity, community participation, and effective enforcement mechanisms (Khiatani et al., 2025; Khusnaini & Aisyah, 2025; Lim et al., 2025; Long et al., 2025; Saleh et al., 2025; Herrero-Arias & Tonheim, 2025; Sun et al., 2025; Frosio & Obafemi, 2025). These findings suggest that although legal traditions differ across Asia and Africa, successful digital child protection increasingly relies upon collaborative governance integrating law, technology, education, and public participation.

From the perspective of Islamic family law, protecting children represents one of the principal objectives of *maqāṣid al-sharī'ah*, particularly through safeguarding religion (*ḥifẓ al-dīn*), life (*ḥifẓ al-naḥs*), intellect (*ḥifẓ al-'aql*), lineage (*ḥifẓ al-nasl*), and property (*ḥifẓ al-māl*). Auda (2008) emphasizes that *maqāṣid al-sharī'ah* should be understood through a systems approach that highlights human development, justice, welfare, and the dynamic interaction between Islamic legal principles and contemporary social realities. Contemporary Islamic legal scholarship extends these objectives beyond traditional family relations into digital environments by arguing that privacy protection, ethical artificial intelligence, cybersecurity, responsible data governance, and online dignity constitute modern manifestations of *maṣlaḥah* within rapidly evolving technological societies (Banurea, 2025; Nidhom & Murtadho, 2025). This perspective corresponds with broader interdisciplinary scholarship emphasizing that effective governance depends upon ethical communication, social innovation, institutional resilience, inclusive public policy, and human-centered regulatory design (Gholikhani Farahani et al., 2025; Islam et al., 2025; Jo et al., 2025; Matlin et al., 2025; Zakaria et al., 2025; Omar Elsaltani & Foster, 2025). Accordingly, Islamic family law offers not merely moral guidance but also a normative legal foundation capable of supporting adaptive digital governance while preserving children's dignity and welfare in increasingly complex technological ecosystems.

Despite significant advances within digital governance scholarship, several important theoretical gaps remain. Existing studies predominantly examine cybersecurity, AI governance, online privacy, platform regulation, or child welfare as separate research domains, while relatively few integrate these perspectives within a unified framework grounded in Islamic family law. Likewise, comparative analyses involving Asian and African jurisdictions remain limited, particularly those examining Indonesia, Malaysia, South Korea, and Nigeria simultaneously. Most previous research also focuses primarily on descriptive regulatory analysis without proposing an operational governance model capable of guiding policymakers, regulators, digital platforms, educational institutions, and families. Addressing these gaps, the present study develops the Islamic Digital Protection Framework (IDPF) as an integrative socio-legal model synthesizing *maqāṣid al-sharī'ah*, Comparative Law Theory, Children's Rights Theory, Digital Governance Theory, and Legal Pluralism Theory. Through comparative analysis across Asia and Africa, the IDPF positions digital child protection as an interconnected governance ecosystem integrating legal regulation, technological safeguards, ethical platform accountability, family participation, and Islamic normative principles. This model represents the principal theoretical contribution of the study by strengthening comparative scholarship on Islamic family law while offering an adaptive governance framework for protecting children in the digital era.

METHODS

This study employed a qualitative legal research design using a comparative socio-legal approach to examine regulatory frameworks governing digital child protection in Asia (Indonesia, Malaysia, and South Korea) and Africa (Nigeria) through the perspectives of Islamic family law and contemporary digital governance. Rather than measuring regulatory effectiveness quantitatively, the study sought to identify similarities, differences, regulatory convergence, institutional innovations, and normative gaps among the selected jurisdictions. The four countries were purposively selected because they represent diverse legal traditions and levels of digital governance. Indonesia represents a Muslim-majority country that recently introduced Government Regulation No. 17 of 2025 concerning Child Protection in Electronic Systems. Malaysia represents a common law-based Muslim jurisdiction with advanced personal data protection and digital governance policies. South Korea was selected because of its globally recognized regulatory framework for cybersecurity, artificial intelligence, and child online safety. Nigeria represents the African perspective as one of the continent's largest digital economies, where rapid technological development is accompanied by growing regulatory initiatives addressing cybersecurity, child protection, and digital governance. The research adopted doctrinal legal analysis integrated with comparative policy analysis to evaluate statutory regulations, institutional frameworks, and governance mechanisms within each jurisdiction. Primary legal materials consisted of national legislation relating to child protection, electronic systems, personal

data protection, cybersecurity, and digital governance, together with international legal instruments concerning children's digital rights. Secondary materials included peer-reviewed journal articles, comparative legal studies, policy reports, and contemporary scholarship published mainly during 2025 concerning artificial intelligence governance, cybersecurity regulation, digital privacy, platform accountability, Islamic family law, and comparative digital governance (Acquah, 2025; Ali et al., 2025; Arif et al., 2025; Frosio & Obafemi, 2025; Lim et al., 2025; Khiatani et al., 2025; Matlin et al., 2025).

Data collection was conducted through systematic documentary research supported by purposive literature selection. Legal documents, statutory instruments, judicial decisions, governmental policy reports, and academic publications were selected based on three inclusion criteria: (1) direct relevance to digital child protection; (2) discussion of digital governance, cybersecurity, artificial intelligence, platform responsibility, privacy protection, or Islamic family law; and (3) publication in internationally recognized scholarly journals or official government sources. The analytical process consisted of five sequential stages. First, regulatory mapping identified legal provisions relating to age verification, parental consent, privacy protection, content moderation, digital risk assessment, institutional supervision, and sanctions. Second, comparative legal analysis examined similarities and differences among Indonesia, Malaysia, South Korea, and Nigeria regarding legislative structure, institutional responsibility, enforcement mechanisms, and regulatory governance. Third, doctrinal analysis evaluated the compatibility of these regulatory approaches with *maqāṣid al-sharī'ah*, particularly *ḥifẓ al-naḥs*, *ḥifẓ al-'aql*, *ḥifẓ al-nasl*, and *ḥifẓ al-māl* as normative principles for protecting children's welfare and dignity in digital environments (Banurea, 2025; Nidhom & Murtadho, 2025). Fourth, cross-jurisdictional synthesis identified transferable regulatory principles and institutional best practices. Finally, these findings were synthesized to formulate the Islamic Digital Protection Framework (IDPF) as an integrative governance model by incorporating insights from contemporary scholarship on AI ethics, cybersecurity governance, digital inclusion, communication systems, and child-centered digital regulation (Gabellini et al., 2025; Fischer & Frennert, 2025; Park et al., 2025; Zahoor & Lone, 2025; Saleh et al., 2025; Long et al., 2025).

To enhance methodological rigor, the study employed source triangulation, theoretical triangulation, and comparative validation throughout the analytical process. Source triangulation integrated statutory regulations, governmental policy documents, international legal instruments, and interdisciplinary scholarly publications from law, information technology, cybersecurity, psychology, education, public policy, and Islamic studies. Theoretical triangulation combined Comparative Law Theory, Digital Governance Theory, Children's Rights Theory, Regulatory Governance Theory, Legal Pluralism Theory, and *maqāṣid al-sharī'ah* to provide complementary analytical perspectives for evaluating regulatory effectiveness across the selected jurisdictions. Comparative validation was undertaken by systematically cross-examining legislative approaches adopted in the four countries to identify regulatory convergence, contextual differences, and transferable governance practices. The principal methodological outcome was the development of the Islamic Digital Protection Framework (IDPF), comprising five interrelated governance dimensions: (1) regulatory compliance, (2) technological safeguards, (3) ethical platform accountability, (4) family and community participation, and (5) Islamic normative principles. Accordingly, the IDPF is proposed not merely as a conceptual framework but as an adaptive comparative governance model capable of strengthening digital child protection policies across diverse legal systems in Asia and Africa.

RESULT AND DISCUSSION

Comparative Regulatory Analysis of Digital Child Protection in Asia and Africa

The comparative analysis reveals that strengthening digital child protection has become an increasingly important regulatory priority across both Asia and Africa as governments seek to respond to the rapid expansion of digital technologies and the growing complexity of online risks affecting children. Despite differences in legal traditions, institutional capacities, and levels of technological development, Indonesia, Malaysia, South Korea, and Nigeria have all introduced legal and policy measures intended to safeguard children from cyberbullying, online sexual exploitation, privacy violations, harmful digital content, identity theft, algorithmic manipulation, and other emerging digital threats. Nevertheless, the four jurisdictions differ considerably in their regulatory orientations, institutional arrangements, enforcement mechanisms, and technological governance. These differences demonstrate that while child protection has become a universal policy objective, the pathways adopted to achieve effective digital governance remain strongly influenced by each country's constitutional framework, digital maturity, and socio-legal context (Abu Sarhan & Fouche, 2025; Arif et al., 2025; Zahoor & Lone, 2025; Khiatani et al., 2025).

Indonesia currently demonstrates one of the most comprehensive statutory approaches to digital child protection in Asia following the enactment of Government Regulation No. 17 of 2025 concerning Child Protection in Electronic System Administration. This regulation imposes mandatory obligations upon Electronic System Providers through comprehensive provisions concerning age verification, parental consent, privacy-by-default settings, digital risk assessments, content classification, complaint mechanisms, and administrative sanctions for regulatory violations. Rather than relying solely on criminal law after harm occurs, the Indonesian framework emphasizes preventive governance by requiring digital platforms to identify, evaluate, and mitigate potential risks before children become victims of digital exploitation. The regulation therefore reflects an important transition from reactive legal protection toward proactive digital governance in which platform accountability constitutes a central component of child protection policy (Khusnaini & Aisyah, 2025; Saleh et al., 2025).

Malaysia adopts a different regulatory orientation by integrating child protection within broader digital governance, privacy regulation, and cybersecurity policies. Instead of establishing a single comprehensive statute exclusively dedicated to children's digital protection, Malaysia combines multiple legal instruments governing personal data protection, electronic communications, digital services, and institutional supervision. This integrated approach provides greater regulatory flexibility while encouraging coordination among public authorities responsible for digital governance and online safety. South Korea, meanwhile, represents the most technologically advanced regulatory model among the four jurisdictions. Its legal framework combines sophisticated cybersecurity regulation, comprehensive personal information protection, artificial intelligence governance, digital literacy policies, and proactive institutional supervision. Consequently, child protection is embedded within a broader digital governance ecosystem that enables regulators to respond effectively to emerging risks associated with artificial intelligence, algorithmic decision-making, immersive digital environments, and rapidly evolving online platforms (Lim et al., 2025; Frosio & Obafemi, 2025; Han et al., 2025; Park et al., 2025; Ali et al., 2025).

From the African perspective, Nigeria illustrates an emerging yet progressively developing regulatory framework for digital child protection. National initiatives, including the Child Rights Act, the Nigeria Data Protection Act, and the Cybercrimes Act, demonstrate increasing governmental commitment to protecting children from online exploitation, cybercrime, privacy violations, and harmful digital content. However, compared with the Asian jurisdictions examined in this study, Nigeria continues to face significant challenges related to institutional coordination, enforcement capacity, digital literacy, technological infrastructure, and regulatory implementation. Nevertheless, Nigeria's experience highlights the importance of combining legislative reform with institutional strengthening, public awareness, stakeholder participation, and digital inclusion in order to ensure effective protection of children's rights within rapidly expanding digital societies. As one of Africa's largest digital economies, Nigeria provides an important comparative perspective for understanding how developing countries adapt legal frameworks to respond to accelerating technological transformation while simultaneously addressing structural governance challenges (Acquah, 2025; Abu Sarhan & Fouche, 2025).

Overall, the comparative findings demonstrate both significant convergence and important divergence among the four jurisdictions. Regulatory convergence is evident in the common recognition that governments, digital platforms, families, and regulatory institutions share responsibility for protecting children's rights in digital environments through stronger privacy safeguards, platform accountability, cybersecurity measures, and preventive governance. At the same time, substantial divergence remains regarding legislative structure, enforcement strategies, institutional capacity, technological readiness, and regulatory priorities. Indonesia emphasizes comprehensive statutory obligations imposed upon Electronic System Providers; Malaysia prioritizes integrated institutional governance and personal data protection; South Korea adopts technology-driven governance supported by advanced cybersecurity and artificial intelligence regulation; while Nigeria focuses on strengthening institutional capacity alongside the gradual development of digital governance mechanisms. These comparative findings indicate that no single jurisdiction provides a universally applicable model for digital child protection. Instead, effective governance requires adaptive regulatory approaches capable of integrating legal certainty, technological innovation, institutional coordination, ethical responsibility, and family participation according to each country's socio-legal context. These findings provide the comparative foundation for developing the Islamic Digital Protection Framework (IDPF), which is discussed in the subsequent sections as an integrative governance model for strengthening digital child protection across Asia and Africa.

Table 1. Comparative Regulatory Analysis of Digital Child Protection in Asia and Africa

Regulatory Aspect	Indonesia	Malaysia	South Korea	Nigeria
Primary Legal Framework	Government Regulation No. 17 of 2025	Personal Data Protection Act (PDPA) and digital governance regulations	PIPA, Youth Protection Act, AI and Cybersecurity regulations	Child Rights Act, Nigeria Data Protection Act, Cybercrimes Act
Regulatory Orientation	Child-centered preventive governance	Privacy and institutional governance	Technology-driven digital governance	Emerging digital child protection governance
Age Verification	Mandatory	Limited and platform-based	Advanced digital verification	Developing mechanisms
Parental Consent	Explicitly regulated	Recognized within privacy regulation	Strong parental participation	Recognized but limited implementation
Privacy Protection	Privacy-by-default and data minimization	Personal data protection compliance	Comprehensive personal information protection	Strengthened through data protection legislation
Platform Accountability	Mandatory risk assessment and administrative sanctions	Shared institutional responsibility	Proactive regulatory supervision	Gradually developing
AI and Emerging Technologies	Initial regulatory adaptation	Progressive integration	Highly advanced AI governance	Early-stage regulatory development
Institutional Enforcement	Multi-agency supervision	Coordinated institutional governance	Strong centralized regulatory institutions	Developing institutional capacity
Principal Regulatory Strength	Comprehensive statutory framework	Integrated digital governance	Advanced technological governance	Expanding legal protection framework
Major Regulatory Challenge	Cross-border enforcement	Regulatory harmonization	Balancing innovation and rights protection	Institutional capacity and implementation

Source: *Authors' analysis (2025).*

Islamic Family Law and Comparative Digital Governance Analysis

The comparative findings presented in the previous section were interpreted through the complementary perspectives of Comparative Law Theory, Child Rights Theory, Digital Governance Theory, Legal Pluralism Theory, and *maqāṣid al-sharī'ah*. Collectively, these analytical perspectives demonstrate that strengthening digital child protection in Asia and Africa extends beyond legislative reform and requires an integrated governance framework capable of balancing legal certainty, technological innovation, institutional accountability, and ethical responsibility. Although Indonesia, Malaysia, South Korea, and Nigeria pursue the common objective of safeguarding children in digital environments, each jurisdiction reflects different regulatory priorities influenced by constitutional structures, legal traditions, institutional capacity, socio-cultural values, and levels of digital transformation. Consequently, digital child protection should not be understood as a uniform legal model but rather as an adaptive governance process that responds to the particular needs and developmental context of each jurisdiction.

From the perspective of Comparative Law Theory, Indonesia adopts a comprehensive statutory approach by imposing mandatory legal obligations on Electronic System Providers through Government Regulation No. 17 of 2025. Malaysia employs a coordinated regulatory model integrating personal data protection, cybersecurity, and institutional governance within a flexible legislative framework. South Korea represents a technology-driven

regulatory system supported by advanced artificial intelligence governance, cybersecurity infrastructure, and proactive digital supervision. Nigeria, meanwhile, illustrates an emerging African regulatory model where child protection continues to evolve alongside institutional strengthening, digital inclusion, and expanding legal protection against cybercrime and online exploitation. Despite these institutional differences, all four jurisdictions demonstrate increasing convergence toward preventive digital governance by recognizing that governments, digital platforms, educational institutions, and families share collective responsibility for protecting children's rights within digital ecosystems (Arif et al., 2025; Ali et al., 2025; Frosio & Obafemi, 2025; Han et al., 2025; Lim et al., 2025).

The comparison between the Asian and African jurisdictions further reveals that technological sophistication alone does not determine the effectiveness of digital child protection. South Korea demonstrates a highly advanced digital governance ecosystem supported by artificial intelligence regulation, digital infrastructure, and institutional capacity, whereas Nigeria continues to strengthen its legal framework despite facing significant challenges in regulatory implementation, technological readiness, and public digital literacy. Indonesia and Malaysia occupy an intermediate position by progressively integrating legal regulation, institutional coordination, privacy protection, and digital governance within rapidly expanding digital societies. These findings indicate that strengthening digital child protection across Asia and Africa requires context-sensitive governance rather than the transplantation of a single regulatory model. Instead, successful governance depends upon harmonizing legal reform, institutional development, technological safeguards, public awareness, and community participation according to each country's socio-legal environment (Acquah, 2025; Khiatani et al., 2025; Long et al., 2025; Saleh et al., 2025).

From the perspective of Islamic family law, protecting children within digital environments represents a contemporary application of *maqāṣid al-sharīʿah*, particularly the preservation of life (*hiḍ al-naḥs*), intellect (*hiḍ al-ʿaql*), lineage (*hiḍ al-nasl*), and property (*hiḍ al-māl*). Modern digital threats—including cyberbullying, online grooming, algorithmic manipulation, privacy violations, identity theft, digital addiction, and exposure to harmful online content—directly threaten these fundamental objectives. Consequently, Islamic legal principles require not only reactive legal sanctions after violations occur but also preventive governance capable of minimizing risks before children's rights are compromised. This interpretation expands the contemporary understanding of *maqāṣid al-sharīʿah* by recognizing children's digital identity, online dignity, psychological well-being, informational privacy, and digital resilience as integral components of *maṣlaḥah* within modern digital society. Such an approach aligns closely with Child Rights Theory, which recognizes children's rights to privacy, security, participation, education, and protection from exploitation, while also supporting Digital Governance Theory, which emphasizes collaborative responsibility among governments, digital platforms, educational institutions, families, civil society, and religious organizations in creating safe and accountable digital ecosystems (Banurea, 2025; Nidhom & Murtadho, 2025; Hamidi et al., 2025; Monlezun, 2025; Herrero-Arias & Tonheim, 2025).

Overall, the comparative analysis demonstrates that the principal challenge facing digital child protection is no longer the absence of legal regulation but the fragmentation of governance across multiple legal and institutional domains. Existing regulatory systems generally address privacy protection, cybersecurity, child welfare, artificial intelligence, family law, and platform accountability through separate legal instruments, thereby limiting policy coherence and implementation effectiveness. The comparative experiences of Indonesia, Malaysia, South Korea, and Nigeria collectively indicate that strengthening digital child protection requires an integrated governance approach capable of harmonizing statutory regulation, technological innovation, institutional accountability, family participation, and ethical values within a single conceptual framework. These comparative findings directly informed the development of the Islamic Digital Protection Framework (IDPF). Rather than functioning solely as a theoretical construct, the IDPF represents a comparative governance model synthesized from the complementary regulatory strengths and institutional experiences of the selected Asian and African jurisdictions. The following section therefore explains the conceptual structure, governance dimensions, and policy implications of the IDPF as the principal contribution of this study toward strengthening digital child protection across Asia and Africa.

Strengthening Digital Child Protection in Asia and Africa through the Islamic Digital Protection Framework (IDPF)

The comparative analysis demonstrates that strengthening digital child protection requires more than the enactment of comprehensive legislation or the deployment of advanced technological safeguards. Instead, effective protection depends upon an integrated governance ecosystem that combines legal certainty, institutional

coordination, technological innovation, ethical responsibility, and active family participation. Although Indonesia, Malaysia, South Korea, and Nigeria differ in their constitutional structures, regulatory capacities, and levels of digital transformation, all four jurisdictions increasingly recognize children's digital safety as a strategic public policy priority. Indonesia has introduced mandatory obligations for Electronic System Providers through Government Regulation No. 17 of 2025, Malaysia continues strengthening personal data protection and online safety governance, South Korea has developed sophisticated mechanisms for digital supervision supported by technological innovation, while Nigeria is progressively improving child online protection through cybersecurity regulation, institutional reforms, and digital rights initiatives. These developments indicate that contemporary digital child protection is evolving toward collaborative governance involving governments, digital platforms, educational institutions, families, religious communities, and civil society rather than relying exclusively upon criminal sanctions or reactive legal enforcement (Khusnaini & Aisyah, 2025; Lim et al., 2025; Khiatani et al., 2025; Acquah, 2025).

From the perspective of *maqāṣid al-sharī'ah*, protecting children in digital environments extends beyond statutory compliance toward preserving comprehensive human welfare (*maṣlahah*). The objectives of preserving life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-'aql*), lineage (*ḥifẓ al-nasl*), property (*ḥifẓ al-māl*), privacy, and human dignity provide a normative foundation for evaluating whether contemporary digital governance genuinely safeguards children's rights amid rapid technological development. Islamic legal scholarship increasingly recognizes that digital privacy, ethical artificial intelligence, cybersecurity, responsible information management, and platform accountability represent contemporary manifestations of Islamic legal responsibility. Consequently, digital governance should promote not only technological innovation but also children's psychological well-being, moral development, family integrity, and human dignity in accordance with both international child rights standards and Islamic ethical principles (Banurea, 2025; Nidhom & Murtadho, 2025; Fischer & Frennert, 2025; Monlezun, 2025).

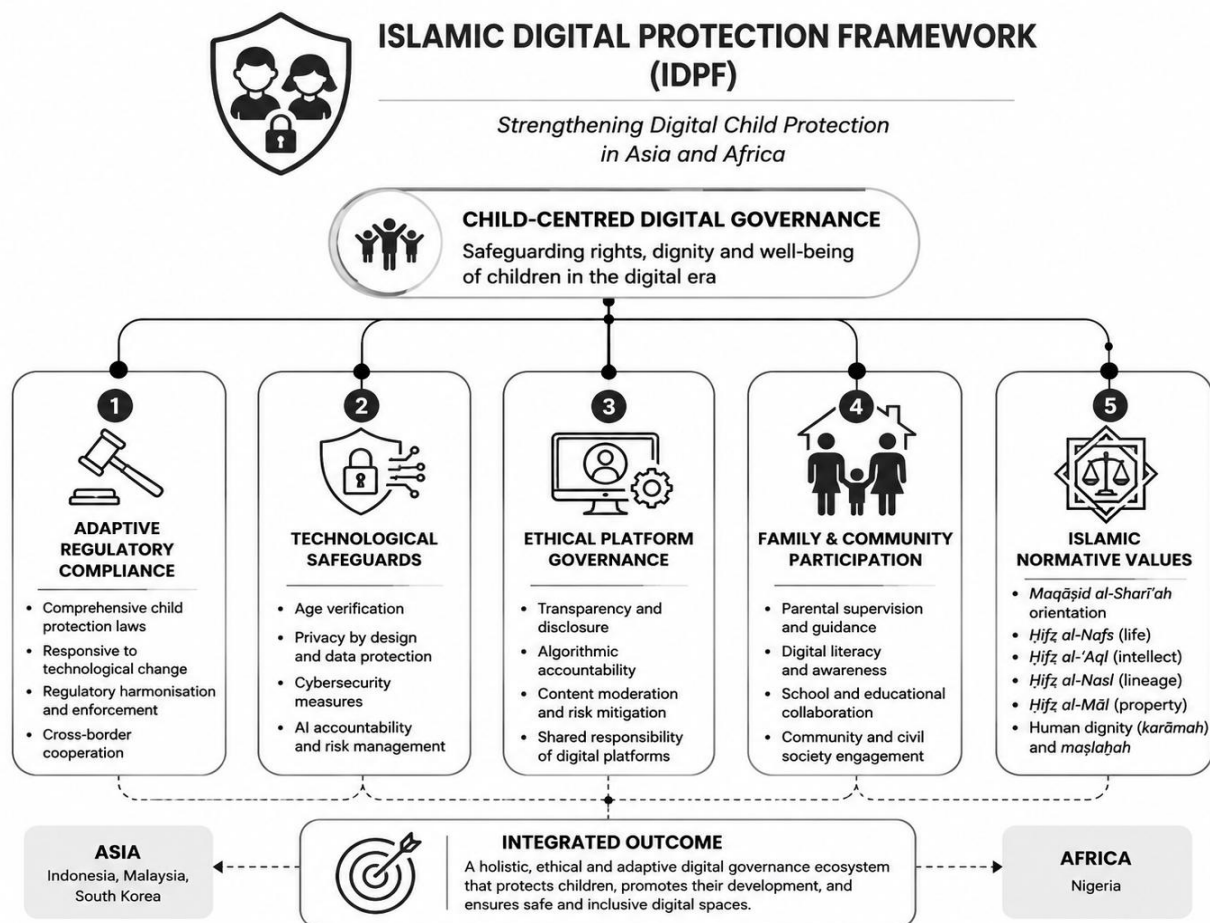
Building upon these comparative findings, this study proposes the Islamic Digital Protection Framework (IDPF) as an integrative regulatory model for strengthening digital child protection across Asia and Africa. Unlike previous studies that separately examine cybersecurity, child protection, digital governance, or Islamic family law, the IDPF synthesizes these perspectives into five mutually reinforcing governance dimensions: adaptive regulatory compliance, technological safeguards, ethical platform governance, family and community participation, and Islamic normative values. Adaptive regulatory compliance emphasizes responsive legislation capable of addressing rapidly evolving digital risks. Technological safeguards incorporate age verification, cybersecurity mechanisms, privacy-by-design, and accountable artificial intelligence. Ethical platform governance promotes transparency, algorithmic accountability, proportional responsibility, and child-centered content moderation. Family and community participation strengthens parental supervision, digital literacy, and collaborative child protection involving educational institutions and civil society. Finally, Islamic normative values integrate the objectives of *maqāṣid al-sharī'ah* into contemporary digital governance to ensure that technological development remains aligned with human dignity and social justice (Arif et al., 2025; Ali et al., 2025; Han et al., 2025; Gabellini et al., 2025).

The proposed IDPF also generates important implications for future regulatory reform. For Asian jurisdictions, the framework supports greater regional harmonization concerning children's digital rights, cross-border platform accountability, and responsible artificial intelligence governance. For African countries, particularly Nigeria, the framework provides a normative reference for integrating child protection policies with digital governance reforms while respecting local legal traditions, cultural diversity, and religious values. Furthermore, the IDPF encourages stronger institutional collaboration among governments, child protection agencies, cybersecurity authorities, educational institutions, religious organizations, technology companies, and civil society to develop preventive governance mechanisms rather than relying solely upon post-violation enforcement. As emerging technologies—including artificial intelligence, biometric systems, digital identity, blockchain applications, and metaverse platforms—continue reshaping children's digital experiences, adaptive governance becomes increasingly essential for maintaining effective legal protection (Park et al., 2025; Bai & Liu, 2025; Frosio & Obafemi, 2025; Rahmani et al., 2025; Zahoor & Lone, 2025).

Accordingly, the principal theoretical contribution of this study lies in repositioning digital child protection as an interdisciplinary governance ecosystem rather than merely a legal compliance issue. By integrating Comparative Law Theory, Child Rights Theory, Digital Governance Theory, Legal Pluralism Theory, and *maqāṣid al-sharī'ah*,

the Islamic Digital Protection Framework (IDPF) offers a comprehensive socio-legal model capable of strengthening child-centered digital governance across diverse legal systems in Asia and Africa. The framework contributes not only to the development of comparative Islamic family law scholarship but also provides practical guidance for policymakers, legislators, regulatory authorities, educational institutions, digital platform providers, and child protection agencies seeking to establish adaptive, ethically grounded, and sustainable digital governance in response to the accelerating transformation of global digital ecosystems (Saleh et al., 2025; Long et al., 2025; Herrero-Arias & Tonheim, 2025; Zakaria et al., 2025; Matlin et al., 2025).

Figure 1. Islamic Digital Protection Framework (IDPF) for Strengthening Digital Child Protection in Asia and Africa



Source: Authors' analysis (2025).

CONCLUSION

This study demonstrates that strengthening digital child protection requires an integrated governance approach that extends beyond conventional legal regulation toward a multidimensional framework combining child rights protection, digital governance, technological accountability, and Islamic legal principles. The comparative analysis of Indonesia, Malaysia, South Korea, and Nigeria reveals that although each jurisdiction has adopted different regulatory strategies reflecting its constitutional structure, technological capacity, and institutional priorities, all recognize the increasing necessity of protecting children from cyberbullying, online exploitation, privacy violations, harmful digital content, and emerging risks associated with artificial intelligence and platform-based technologies. Indonesia has introduced comprehensive obligations for Electronic System Providers through Government Regulation No. 17 of 2025, Malaysia emphasizes integrated digital governance and personal data protection, South Korea adopts technologically advanced regulatory oversight supported by proactive enforcement institutions, while Nigeria continues strengthening digital child protection through cybersecurity

legislation, child rights frameworks, and institutional reforms. These diverse regulatory experiences demonstrate that effective child protection depends not only on statutory regulation but also on institutional coordination, adaptive governance, technological innovation, and community participation.

The principal theoretical contribution of this research is the development of the Islamic Digital Protection Framework (IDPF) as an integrative socio-legal model for strengthening digital child protection in Asia and Africa. Unlike previous studies that generally examine digital governance, cybersecurity, child protection, or Islamic family law separately, the IDPF synthesizes *maqāṣid al-sharī'ah*, Child Rights Theory, Digital Governance Theory, Regulatory Governance Theory, and Comparative Law into a coherent regulatory framework. The model positions child protection as a governance ecosystem built upon five mutually reinforcing dimensions: adaptive regulatory compliance, technological safeguards, ethical platform governance, family and community participation, and Islamic normative values. Consequently, the IDPF contributes not only to the advancement of comparative Islamic family law scholarship but also to the broader discourse on digital governance by demonstrating how ethical and religious principles can complement modern regulatory approaches in protecting children's rights within rapidly evolving digital environments.

From a practical perspective, the findings provide important policy implications for governments, regulatory authorities, digital platform providers, educational institutions, and families. Policymakers should strengthen cross-border regulatory cooperation, improve age-verification mechanisms, enhance platform accountability, and establish adaptive supervisory systems capable of responding to technological developments such as artificial intelligence, biometric identification, immersive digital platforms, and algorithmic governance. Digital service providers should adopt child-centred design, privacy-by-design principles, transparent content moderation, and continuous risk assessment, while educational institutions and families should reinforce digital literacy, parental supervision, and ethical digital behaviour. Integrating these measures with Islamic ethical values promotes a balanced regulatory approach that simultaneously safeguards children's dignity, welfare, privacy, and developmental rights without undermining technological innovation.

This study is subject to several limitations. The comparative analysis focuses on four jurisdictions and relies primarily on doctrinal legal analysis, documentary research, and comparative regulatory interpretation without incorporating empirical evidence from policymakers, digital platforms, parents, educators, or children. Furthermore, because digital technologies and regulatory frameworks continue to evolve rapidly, future legal developments may require continuous refinement of the proposed framework. Accordingly, future research should expand comparative analysis to additional jurisdictions across Asia, Africa, Europe, and the Middle East, integrate empirical socio-legal methods, evaluate the practical implementation of digital child protection regulations, and examine the implications of emerging technologies—including generative artificial intelligence, immersive virtual environments, and cross-border platform governance—for the continued development of the Islamic Digital Protection Framework (IDPF).

REFERENCES

- Abu Sarhan, T. M., & Fouche, A. (2025). Child sexual grooming: Listening to victims in Jordan. *Child Abuse & Neglect*, 160, 107235. <https://doi.org/10.1016/j.chiabu.2024.107235>
- Acquah, A. (2025). AI-powered public service and persons with disabilities (PWDs): Questioning the commitment to bridging digital inclusivity gap in Ghana. *Transforming Government: People, Process and Policy*, 19, 579–595. <https://doi.org/10.1108/TG-01-2025-0013>
- Ali, S., Wadho, S. A., Talpur, K. R., et al. (2025). Next-generation quantum security: The impact of quantum computing on cybersecurity—Threats, mitigations, and solutions. *Computers and Electrical Engineering*, 128, 110649. <https://doi.org/10.1016/j.compeleceng.2025.110649>
- Arif, T., Camacho, D., & Park, J. H. (2025). Unveiling cybersecurity mysteries: A comprehensive survey on digital forensics trends, threats, and solutions in network security. *Journal of Network and Computer Applications*, 243, 104296. <https://doi.org/10.1016/j.jnca.2025.104296>
- Auda, J. (2008). *Maqasid al-Shariah as Philosophy of Islamic Law: A Systems Approach*. International Institute of Islamic Thought.
- Bai, K., & Liu, Y. (2025). Scarcity, symbolism, and social identity (3S): Unpacking drivers of conspicuous consumption of virtual gear in the metaverse. *Journal of Retailing and Consumer Services*, 87, 104396. <https://doi.org/10.1016/j.jretconser.2025.104396>

- Balta, I., Lemon, J., Popescu, C. A., et al. (2025). Food safety—The transition to artificial intelligence (AI) modus operandi. *Trends in Food Science & Technology*, 165, 105278. <https://doi.org/10.1016/j.tifs.2025.105278>
- Banurea, S. (2025). Child protection in the perspective of Islamic family law by era digital. *Jurnal Ilmiah Teunuleh: International Journal of Social Sciences*, 6, 171–180. <https://doi.org/10.51612/teunuleh.v6i2.191>
- Convention on the Rights of the Child. (1989). United Nations.
- Federal Republic of Nigeria. (2003). *Child Rights Act 2003*.
- Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act 2023*.
- Fischer, B., & Frennert, S. (2025). Towards an experiential ethics of AI and robots: A review of empirical research on human encounters. *Technological Forecasting and Social Change*, 219, 124264. <https://doi.org/10.1016/j.techfore.2025.124264>
- Fraiwan, M., & Almomani, F. (2025). Internet gaming disorder: Prevalence and associated factors among university students. *Acta Psychologica*, 260, 105690. <https://doi.org/10.1016/j.actpsy.2025.105690>
- Frosio, G., & Obafemi, F. (2025). Augmented accountability: Data access in the metaverse. *Computer Law & Security Review*, 59, 106196. <https://doi.org/10.1016/j.clsr.2025.106196>
- Gabellini, M., Regattieri, A., Bortolini, M., & Ronchi, M. (2025). Conceptualization and validation of an intelligent digital twin design framework for supply chain risk management. *International Journal of Information Management Data Insights*, 5, 100365. <https://doi.org/10.1016/j.jjime.2025.100365>
- Government of Indonesia. (2022). *Law Number 27 of 2022 concerning Personal Data Protection*.
- Government of Indonesia. (2025). *Government Regulation Number 17 of 2025 concerning Child Protection in Electronic System Administration*.
- Hamidi, M. L., Setiawan, G., & Asutay, M. (2025). The quest for sustainable mosques: A paradigm shift with the quadruple bottom line framework. *Sustainable Futures*, 9, 100588. <https://doi.org/10.1016/j.sfr.2025.100588>
- Han, H. C., Huang, D. C., & Chen, C. L. (2025). Applications of AI and blockchain in origin traceability and forensics. *CMES—Computer Modeling in Engineering and Sciences*, 145, 67–126. <https://doi.org/10.32604/cmes.2025.070944>
- Herrero-Arias, R., & Tonheim, M. (2025). The significance of religion when matching children with migrant background and foster carers. *Children and Youth Services Review*, 172, 108240. <https://doi.org/10.1016/j.chilyouth.2025.108240>
- Khiatani, P. V., Chui, W. H., & Gonsamo, D. D. (2025). Advancing child protection systems in Indonesia and Ethiopia: A comparative analysis of progress and challenges. *Child Abuse & Neglect*, 170, 107762. <https://doi.org/10.1016/j.chiabu.2025.107762>
- Khusnaini, I., & Aisyah, E. N. (2025). Regulasi perlindungan anak di ruang digital di Indonesia: Implementasi, tantangan, dan peluang implementasi. *Pro Justicia: Jurnal Hukum dan Sosial*, 5, 101–109. <https://doi.org/10.55380/projus.v5i02.1208>
- Lim, A. C. M., Ng, L. H. X., & Taeihagh, A. (2025). Biometric data landscape in Southeast Asia: Challenges and opportunities for effective regulation. *Computer Law & Security Review*, 56, 106095. <https://doi.org/10.1016/j.clsr.2024.106095>
- Long, J., Zhang, S., Chu, L., et al. (2025). Policies, resource allocation, and interventions for child and adolescent mental health in low- and middle-income countries in the Western Pacific Region: A scoping review. *The Lancet Regional Health—Western Pacific*, 62, 101674. <https://doi.org/10.1016/j.lanwpc.2025.101674>
- Malaysia. (1998). *Communications and Multimedia Act 1998 (Act 588)*.
- Malaysia. (2010). *Personal Data Protection Act 2010 (Act 709)*.
- Matlin, S. A., Claron, I. M. M., Merone, J., et al. (2025). Artificial intelligence in migrant health: A critical perspective on opportunities and risks. *The Lancet Regional Health—Europe*, 57, 101421. <https://doi.org/10.1016/j.lanepe.2025.101421>
- Monlezun, D. J. (2025). Human-centered global AI governance. In *Quantum Health AI* (pp. 179–250). Academic Press. <https://doi.org/10.1016/B978-0-443-33353-8.00010-2>
- National Information Technology Development Agency. (2023). *Nigeria Data Protection Act: General Application and Implementation Directive*.
- Nidhom, M., & Murtadho, A. (2025). Does Islam protect digital privacy? An Islamic studies approach to personal data protection. *Al-Afham: Journal of Islamic Studies*, 2, 107–128. <https://doi.org/10.62509/ajis.v2i2.260>
- OECD. (2021). *Recommendation of the Council on Children in the Digital Environment*.

- Park, S., Kim, D., Jeong, E., Jeong, D., & Park, E. (2025). Reconceptualizing the metaverse: A taxonomy for user experience analysis and insights from real-world platforms. *Technology in Society*, 81, 102852. <https://doi.org/10.1016/j.techsoc.2025.102852>
- Personal Information Protection Commission. (2023). *Personal Information Protection Act (Republic of Korea)*.
- Rahmani, M., Zakipour, M., Rahchamani, A., & Torabiyan, M. (2025). From data to experience: Can metaverse-based stores enhance parental purchase behavior in infant and children's apparel? *Telematics and Informatics Reports*, 20, 100272. <https://doi.org/10.1016/j.teler.2025.100272>
- Republic of Korea. (2023). *Act on Promotion of Information and Communications Network Utilization and Information Protection*.
- Saleh, M. N. I., Hanum, F., & Rukiyati. (2025). Stakeholders' perspectives on whole-school approaches to prevent and address bullying and cyberbullying in Indonesian high schools. *Social Sciences & Humanities Open*, 12, 102336. <https://doi.org/10.1016/j.ssaho.2025.102336>
- Sun, Y., Pinkse, J., & Bleda, M. (2025). Social media platforms' use of nonmarket strategy to manage politically contentious issues in host countries: The case of TikTok in the US market. *Journal of International Management*, 31, 101293. <https://doi.org/10.1016/j.intman.2025.101293>
- UNICEF. (2021). *Policy Guidance on AI for Children*.
- Zahoor, I., & Lone, S. A. (2025). Child computer interactions: Cognitive development and segmenting unsafe video contents: A review. *Entertainment Computing*, 53, 100931. <https://doi.org/10.1016/j.entcom.2025.100931>
- Zare, A., & Jalali, A. (2025). A prospective metaverse paradigm based on the reality-virtuality continuum and digital twins. *Recent Advances in Computer Science and Communications*, 18. <https://doi.org/10.2174/0126662558294125240307094426>