

Strengthening Children's Digital Identity Governance under Islamic Family Law: A Maqāṣid-Based Comparative Framework

Muslimin bin Abdussyakur Kasmuri,^{1*} Supaprawat Siripipatthanakul,² Muhammad Furqan,³
Zohaib Hassan Sain⁴

¹ Pondok Pesantren Darussalam Sindangsari Purwadadi, Ciamis, West Java, Indonesia

² Bangkokthonburi University, Bangkok, Thailand

³ Universitas Samudra, Aceh, Indonesia

⁴ Superior University, Lahore, Punjab, Pakistan

*Corresponding author: Muslimin bin Abdussyakur Kasmuri

E-mail: likmuslimin@gmail.com

Article History:

Received: November 5, 2025 | Revised: May 18, 2026 | Accepted: June 20, 2026 | Published: June 30, 2026

Citation (APA Style):

Kasmuri, M. B. A., Siripipatthanakul, S., Furqan, M., & Sain, Z. H. (2026). Strengthening Children's Digital Identity Governance under Islamic Family Law: A Maqāṣid-Based Comparative Framework. *Munakahat: Journal of Islamic Family Law*, 2(2), 45–58.

Abstract

Background: The rapid expansion of digital identity systems has increased children's participation in digital environments while exposing them to privacy violations, identity theft, cyber exploitation, and long-term data misuse. Existing studies primarily address these issues from technological or regulatory perspectives, with limited integration of Islamic family law into children's digital identity governance.

Objective: This study examines children's digital identity governance in Indonesia, Estonia, and the United Arab Emirates and develops a governance framework grounded in *maqāṣid al-sharī'ah*.

Methods: A qualitative doctrinal and comparative legal approach was employed by analyzing legislation, child protection and personal data protection laws, digital governance policies, institutional documents, and recent scholarly literature. The analysis combines comparative legal methods with *maqāṣid al-sharī'ah* principles.

Results: Indonesia emphasizes family-centered legal protection and parental responsibility, Estonia demonstrates institutionally integrated digital identity governance supported by secure digital infrastructure, and the United Arab Emirates combines technological innovation with Islamic legal values. These findings are synthesized into the Maqāṣid-Based Children's Digital Identity Governance (MCDIG) Framework, comprising parental digital responsibility, legal protection, secure digital infrastructure, family digital literacy, and collaborative institutional governance.

Conclusion: Effective children's digital identity governance requires an integrated legal, technological, ethical, and institutional approach that balances digital innovation with child protection and family responsibility while strengthening contemporary Islamic family law.

Novelty: This study proposes the MCDIG Framework, integrating *maqāṣid al-sharī'ah*, comparative legal analysis, children's digital rights, and digital governance into a unified child-centered framework for protecting children's digital identities.

Keywords: Children's Digital Identity; Child Protection; Family Law; *Maqāṣid al-Sharī'ah*; Digital Governance.

INTRODUCTION

The rapid expansion of digital technologies has fundamentally transformed children's participation in education, healthcare, financial services, social media, and digital public administration through increasingly sophisticated digital identity systems. Beyond enabling secure access to digital services, digital identity has become an essential component of contemporary governance by reshaping interactions between citizens and public institutions while enhancing service integration, administrative efficiency, and institutional accountability (Atar et al., 2025; Janssen

et al., 2025). Consequently, digital identity is no longer merely a technical authentication mechanism but a legal and governance issue closely associated with public value, individual rights, and the protection of human dignity within digital societies (Lin & Wang, 2026). Despite these benefits, children remain among the most vulnerable users of digital ecosystems because they are disproportionately exposed to identity theft, unauthorized personal data processing, cyber exploitation, algorithmic surveillance, and long-term privacy risks (Apps et al., 2025; Li, 2025; Bayar & Sezgin, 2026; Volz, 2026). Recent scholarship therefore argues that effective digital governance must move beyond technological solutions by integrating legal safeguards, ethical responsibility, institutional accountability, and child protection into a coherent governance framework capable of balancing innovation with children's best interests (Alsharif & Hnit, 2025; Guenduez et al., 2025; Naghmouchi et al., 2025; Casalini & Zavolokina, 2025; Beltrán, 2025; Kun, 2025; Casarosa et al., 2025; Chen et al., 2025; Imandeka et al., 2026).

Within this broader governance discourse, Islamic family law offers an important normative and ethical perspective for protecting children's rights in the digital era. The objectives of *maqāṣid al-sharī'ah* emphasize the preservation of human dignity, intellect, lineage, life, and property, thereby extending legal protection beyond physical welfare to encompass emerging digital challenges affecting children (Al-Shatibi, 1920; Auda, 2008; Kamali, 2008). Contemporary scholarship further demonstrates that Islamic family law continues to evolve through contextual interpretation and legislative reform in response to changing social realities, including questions of justice, institutional transformation, and governance within Muslim societies (Akhtar, 2026; Aghbalou, 2026). Building upon this development, recent studies have explored digital parenting, cyber protection, ethical governance, and family resilience in digital environments (Muharir & Lousada, 2024; Muyassar et al., 2024; Banurea, 2025; Kurniawan et al., 2024; Ja'far et al., 2026; Lestianingsih et al., 2025; Tan et al., 2025; Yildirim et al., 2025; Muchtarom et al., 2026; Evgin et al., 2026). Nevertheless, existing studies predominantly employ *maqāṣid al-sharī'ah* as a normative justification for digital ethics rather than as an analytical framework for evaluating children's digital identity governance across different legal systems, leaving a significant conceptual gap in comparative Islamic family law research.

Existing scholarship on children's digital identity governance can be grouped into four interrelated streams. The first emphasizes cybersecurity, artificial intelligence, and privacy-preserving technologies as mechanisms for reducing digital risks and strengthening identity protection (Alraddadi et al., 2025; Hossain & Islam, 2025; Hasnain et al., 2025). The second examines digital government, public digital infrastructure, and national digital identity systems, highlighting how institutional integration and interoperable digital services improve governance effectiveness (Lusi et al., 2025; Janssen et al., 2025; Naghmouchi et al., 2025; Mota & Klein, 2025). The third focuses on legal regulation of personal data, children's digital rights, and human-rights-based governance in response to increasing concerns over privacy, surveillance, and algorithmic decision-making (Beltrán, 2025; Lim et al., 2025; Li, 2025; Long et al., 2025). The fourth explores the contemporary application of Islamic law and *maqāṣid al-sharī'ah* in responding to technological transformation, including digital rights, ethical governance, and emerging regulatory challenges (Arminsyah, 2025; Marluwi et al., 2025; Mashdurohaturun et al., 2026; Azam et al., 2026). Although these strands have substantially advanced understanding within their respective domains, they remain largely disconnected. Consequently, current scholarship has yet to develop an integrated governance framework that simultaneously incorporates comparative legal analysis, children's digital rights, digital governance, and Islamic family law.

These limitations reveal several important research gaps. First, previous studies rarely employ Islamic family law as an analytical framework for evaluating children's digital identity governance, instead treating *maqāṣid al-sharī'ah* primarily as a normative or ethical justification. Second, comparative legal analyses involving jurisdictions with contrasting legal and technological characteristics remain limited, particularly with respect to Indonesia, Estonia, and the United Arab Emirates. These jurisdictions represent three complementary governance models: Indonesia emphasizes family-centered legal protection and parental responsibility; Estonia exemplifies a mature digital identity ecosystem supported by integrated public digital infrastructure; and the United Arab Emirates combines rapid technological innovation with Islamic legal values and state-led digital governance. Third, existing literature generally prioritizes technological or regulatory solutions while paying comparatively less attention to the interaction between legal protection, family responsibility, institutional governance, and digital ethics. As a result, no comprehensive model currently explains how these dimensions can be integrated to strengthen children's digital identity protection within contemporary Islamic family law.

Accordingly, this study addresses three research questions: (1) How do Indonesia, Estonia, and the United Arab Emirates regulate children's digital identity within their respective legal systems? (2) How can *maqāṣid al-sharī'ah* function as an analytical framework for evaluating children's digital identity governance? (3) What governance model can strengthen children's digital identity protection within contemporary Islamic family law? To answer these questions, the study adopts a qualitative doctrinal and comparative legal approach integrating comparative law, digital governance, child protection, and Islamic family law. Its principal contribution is the development of the Maqāṣid-Based Children's Digital Identity Governance (MCDIG) Framework, which reconceptualizes *maqāṣid al-sharī'ah* not merely as a normative foundation but as an analytical governance framework integrating parental digital responsibility, protection of children's personal data, secure digital infrastructure, family digital literacy, and collaborative institutional governance. By bridging fragmented strands of scholarship, this study extends contemporary Islamic family law into the field of digital identity governance while offering practical guidance for policymakers seeking child-centered, ethically grounded, and technologically adaptive governance models in the digital era.

LITERATURE REVIEW

Children's digital identity governance has become a central topic in contemporary legal and governance scholarship as digital technologies increasingly mediate children's interactions with education, healthcare, financial services, social media, and public administration. Early studies primarily conceptualized digital identity as a technical mechanism for authentication, electronic identification, and secure access to online services (Withorn et al., 2021). More recent scholarship, however, demonstrates a significant conceptual shift by recognizing digital identity as a multidimensional construct encompassing legal status, personal autonomy, informational privacy, and the exercise of fundamental rights within digital societies (Apps et al., 2025; Cameron et al., 2025; Alsharif & Hnit, 2025; Guenduez et al., 2025; Janssen et al., 2025; Li, 2025; Naghmouchi et al., 2025; Bayar & Sezgin, 2026). This evolution reflects a broader transition in digital governance research from technology-centered approaches toward governance models that emphasize accountability, institutional legitimacy, and human-centered regulation. Nevertheless, scholarly debate persists regarding the most appropriate governance architecture for protecting children's digital identities. One strand of literature prioritizes cybersecurity, encryption, digital authentication, secure infrastructure, and institutional readiness as the principal mechanisms for mitigating digital risks. Recent studies further demonstrate that effective cybersecurity depends not only on technological safeguards but also on coherent policy frameworks, users' security behavior, and organizational preparedness in managing digital vulnerabilities (Alraddadi et al., 2025; Hasnain et al., 2025; Hossain & Islam, 2025; Oroni & Xianping, 2025). In contrast, another body of scholarship argues that technological solutions alone are insufficient unless supported by comprehensive legal regulation, ethical governance, institutional accountability, and active family participation (Beltrán, 2025; Campos & Coutinho, 2025; Casalini & Zavolokina, 2025; Casarosa et al., 2025; Kun, 2025). Complementing these perspectives, Roihanah et al. (2026) emphasize that responsive legislative design should strengthen coordination among the state, legal institutions, and families to enhance social resilience and protect vulnerable groups. Collectively, these studies indicate that children's digital identity governance should be understood as an integrated governance ecosystem that combines technological, legal, institutional, and social dimensions rather than relying exclusively on technical innovation.

This expanding body of literature also demonstrates that children's digital identity has evolved beyond a technical issue into a multidimensional governance challenge involving human rights, cybersecurity, digital ethics, and family protection (Alsharif & Hnit, 2025; Guenduez et al., 2025; Naghmouchi et al., 2025). Within broader debates on digital governance, scholars increasingly argue that technological transformation simultaneously creates new opportunities for innovation and new normative challenges concerning privacy, autonomy, inclusion, accountability, and the protection of vulnerable populations (Morrell, 2025). Consequently, digital identity governance can no longer be evaluated solely in terms of technological performance or administrative efficiency but must also be assessed according to its ability to safeguard fundamental rights and promote public trust. Existing governance models increasingly advocate rights-based approaches that integrate technological innovation with legal certainty, ethical responsibility, and institutional accountability. Despite this growing consensus, current scholarship remains largely fragmented because technological, legal, ethical, and family-centered perspectives are often examined independently rather than within a unified analytical framework. This fragmentation is particularly evident in studies concerning children, where cybersecurity research frequently overlooks family governance, while legal scholarship tends to underemphasize technological implementation and institutional coordination. As a result, the literature has yet to produce a comprehensive framework capable of

systematically integrating digital governance, children's rights, institutional responsibility, and family protection into a coherent model for evaluating children's digital identity governance. Such a gap provides the conceptual foundation for developing a more holistic governance framework that accommodates both technological advancement and child-centered legal protection.

Within Islamic family law, the protection of children has long been understood as an integral component of the broader objectives of *maqāṣid al-sharī'ah*. Classical scholars conceptualized these objectives through the preservation of religion (*hifẓ al-dīn*), life (*hifẓ al-nafs*), intellect (*hifẓ al-'aql*), lineage (*hifẓ al-nasl*), and property (*hifẓ al-māl*) as the fundamental principles guiding Islamic legal reasoning (Al-Shatibi, 1920; Auda, 2008; Kamali, 2008). Contemporary scholarship has subsequently expanded these principles to address legal questions arising from digital transformation, including digital ethics, online privacy, electronic consent, algorithmic governance, and responsible technology use (Kurniawan et al., 2024; Muharir & Lousada, 2024; Muyassar et al., 2024; Arminsyah, 2025; Mukaromah et al., 2025; Lestianingsih et al., 2025; Banurea, 2025; Azam et al., 2026; Ja'far et al., 2026; Mashdurohatur et al., 2026). Parallel developments have also highlighted the growing importance of digital parenting, family resilience, and digital literacy in protecting children within increasingly interconnected digital environments. Despite these advances, most studies continue to employ *maqāṣid al-sharī'ah* primarily as a normative or philosophical justification for legal reform rather than as an operational analytical framework for evaluating governance effectiveness. Consequently, the interaction between Islamic legal objectives, institutional governance, digital infrastructure, and children's digital rights remains theoretically underdeveloped. This conceptual limitation suggests that Islamic family law possesses greater analytical potential than currently reflected in the literature, particularly for assessing whether governance systems effectively preserve children's welfare, dignity, and long-term interests within rapidly evolving digital ecosystems.

Another prominent debate concerns the relationship between digital governance, cybersecurity, and children's digital rights. Existing scholarship consistently recognizes that children are disproportionately exposed to identity theft, unauthorized personal data processing, algorithmic profiling, cyber exploitation, online surveillance, and long-term privacy risks associated with digital participation (Apps et al., 2025; Li, 2025; Long et al., 2025; Saleh et al., 2025; Bayar & Sezgin, 2026). Nevertheless, the proposed governance responses remain divided across disciplinary perspectives. Regulatory-oriented studies prioritize comprehensive personal data protection legislation, privacy compliance, age-verification mechanisms, and institutional accountability as the principal safeguards for children's rights (Beltrán, 2025; Lim et al., 2025; Kun, 2025; Volz, 2026). By contrast, family-centered scholarship emphasizes parental mediation, digital literacy, ethical education, and community engagement as equally important mechanisms for strengthening children's resilience in digital environments (Tan et al., 2025; Yildirim et al., 2025; Evgin et al., 2026; Muchtarom et al., 2026). Complementing these perspectives, empirical evidence demonstrates that information security awareness among students and teachers significantly contributes to reducing digital risks within educational settings, underscoring the importance of behavioral readiness alongside technological safeguards (Perkasa et al., 2026). Rather than supporting a single governance approach, the cumulative evidence suggests that effective protection of children's digital identities requires coordinated interaction among legal institutions, families, educational organizations, technology providers, and digital infrastructure. Accordingly, sustainable governance should be conceptualized as a collaborative ecosystem integrating legal certainty, cybersecurity, ethical responsibility, institutional coordination, and family participation into a unified child-centered governance strategy.

Building upon these debates, the present study argues that existing scholarship remains fragmented because technological governance, Islamic family law, children's digital rights, and comparative legal analysis continue to develop largely in parallel rather than through an integrated analytical framework. While previous studies have individually examined cybersecurity, digital government, personal data protection, or *maqāṣid al-sharī'ah*, few have systematically analyzed how these dimensions interact in shaping children's digital identity governance across jurisdictions with different legal traditions and institutional capacities. More importantly, comparative scholarship has not yet translated the principles of *maqāṣid al-sharī'ah* into measurable governance components capable of evaluating regulatory coherence, institutional effectiveness, and family responsibility simultaneously. To address this theoretical gap, this study conceptualizes Maqāṣid-Based Children's Digital Identity Governance (MCDIG) as an integrative analytical framework that synthesizes comparative legal governance with the objectives of Islamic family law. The framework operationalizes five mutually reinforcing dimensions—parental digital responsibility, protection of children's personal data, secure digital infrastructure, family digital literacy, and collaborative institutional governance—as practical indicators for evaluating child-centered digital

governance. In doing so, the study extends the application of *maqāṣid al-sharī'ah* beyond its conventional normative role by positioning it as an evaluative framework capable of connecting legal protection, technological governance, institutional accountability, and ethical responsibility within contemporary digital society. This theoretical synthesis establishes the analytical foundation for the comparative discussion presented in the subsequent sections while clarifying the study's principal contribution to both digital governance scholarship and contemporary Islamic family law.

METHODS

This study adopts a qualitative doctrinal and comparative legal research design to examine children's digital identity governance from the perspective of Islamic family law. The doctrinal approach is employed to systematically analyze legal norms, statutory provisions, institutional regulations, and policy frameworks governing children's digital identity, personal data protection, cybersecurity, and family responsibility. Rather than merely describing legal provisions, this approach evaluates the normative coherence of legal systems in responding to emerging digital challenges affecting children's rights. To strengthen the analysis, the study incorporates a comparative legal approach that identifies similarities, differences, institutional characteristics, and transferable governance practices across Indonesia, Estonia, and the United Arab Emirates. These jurisdictions were selected purposively because they represent three complementary models of digital governance and family regulation. Indonesia reflects a family-centered legal system shaped by national legislation and Islamic family law; Estonia represents one of the world's most mature digital governance ecosystems characterized by integrated digital identity infrastructure, interoperability, and secure public digital services; whereas the United Arab Emirates illustrates a governance model combining rapid technological innovation with Islamic legal values and state-led digital transformation. The comparative design enables the identification of both jurisdiction-specific characteristics and broader governance principles applicable across different legal traditions. The analysis is guided by the principles of *maqāṣid al-sharī'ah*, particularly the preservation of human dignity (*ḥifẓ al-karāmah*), intellect (*ḥifẓ al-'aql*), lineage (*ḥifẓ al-nasl*), and property (*ḥifẓ al-māl*), which function as analytical criteria for evaluating whether contemporary legal and institutional arrangements effectively protect children's welfare within digital environments (Al-Shatibi, 1920; Auda, 2008; Kamali, 2008).

The research relies on both primary and secondary legal materials selected through purposive sampling based on their authority, relevance, and contribution to the research objectives. Primary legal materials include constitutions, statutes, child protection legislation, personal data protection laws, digital identity regulations, cybersecurity policies, government regulations, judicial documents, institutional guidelines, and official policy reports issued by competent authorities in Indonesia, Estonia, and the United Arab Emirates. Secondary legal materials consist of peer-reviewed journal articles, scholarly books, international reports, and academic publications concerning Islamic family law, *maqāṣid al-sharī'ah*, comparative law, digital governance, cybersecurity, children's digital rights, and digital ethics. The integration of these materials facilitates a comprehensive assessment of both normative legal developments and contemporary scholarly debates. Consistent with previous governance research, this multidisciplinary evidence base is necessary because effective digital identity governance depends on the interaction of technological capacity, institutional accountability, legal certainty, and ethical responsibility rather than on isolated regulatory interventions (Janssen et al., 2025; Guenduez et al., 2025; Volz et al., 2025). Accordingly, the selected legal materials provide a robust basis for evaluating how different jurisdictions balance technological innovation, child protection, family responsibility, and institutional governance while responding to the challenges of digital transformation.

The analytical procedure was conducted through four sequential stages to ensure methodological transparency, analytical consistency, and research reproducibility. First, all legal and academic materials were collected, reviewed, and classified into four analytical themes: children's digital identity protection, parental and family responsibility, digital governance and cybersecurity, and the principles of *maqāṣid al-sharī'ah*. Second, a cross-jurisdictional comparative analysis was undertaken to identify regulatory convergence and divergence, institutional strengths and weaknesses, governance mechanisms, and policy transferability among the three jurisdictions. Third, the comparative findings were interpreted through the analytical lens of *maqāṣid al-sharī'ah* to assess the extent to which each legal system promotes the protection of children's dignity, digital rights, and sustainable family governance. Rather than functioning solely as a normative reference, *maqāṣid al-sharī'ah* was operationalized as an evaluative framework for assessing legal coherence, institutional effectiveness, and governance performance across different regulatory settings. Finally, the synthesized findings informed the development of the Maqāṣid-Based Children's Digital Identity Governance (MCDIG) Framework, comprising

five interrelated dimensions: parental digital responsibility, legal protection of children's personal data, secure digital infrastructure, family digital literacy, and collaborative institutional governance. To enhance analytical validity, doctrinal analysis, comparative legal interpretation, and literature triangulation were employed by systematically comparing statutory provisions, institutional policies, and contemporary academic scholarship across the three jurisdictions. This methodological strategy strengthens the credibility, transparency, and reproducibility of the research while demonstrating that Islamic family law and *maqāṣid al-sharī'ah* can function not only as normative foundations but also as analytical instruments for evaluating children's digital identity governance within contemporary comparative legal scholarship.

RESULTS AND DISCUSSION

Comparative Governance Models for Children's Digital Identity Protection

The comparative analysis demonstrates that children's digital identity protection has developed into a multidimensional governance issue that extends beyond conventional personal data regulation. It involves the interaction of child protection principles, family responsibility, institutional accountability, and technological security. Across Indonesia, Estonia, and the United Arab Emirates, children's digital identity is increasingly recognized as an essential element of contemporary governance because children remain particularly vulnerable to identity misuse, unauthorized data processing, online exploitation, and long-term privacy risks due to their limited legal capacity and digital awareness. Nevertheless, each jurisdiction adopts a distinct governance model shaped by its legal traditions, institutional capacity, technological development, and socio-cultural values. While Indonesia emphasizes family-based protection and parental responsibility, Estonia prioritizes secure digital infrastructure and institutional interoperability, whereas the United Arab Emirates combines technological transformation with regulatory supervision and family-oriented governance. These variations indicate that effective children's digital identity governance requires a balanced relationship between families, governments, and digital institutions rather than reliance on a single regulatory mechanism.

Table 1. Comparative Governance Models for Children's Digital Identity Protection

Governance Dimension	Indonesia	Estonia	United Arab Emirates
Regulatory orientation	Family-centered child protection integrated with personal data governance	Secure digital identity ecosystem supported by interoperable public infrastructure	Technology-driven governance integrated with regulatory oversight and cultural values
Primary governance actor	Parents supported by state regulation and child protection institutions	State institutions supported by trusted digital systems	Government leadership combined with family responsibility
Institutional strength	Normative protection through family law, child protection regulation, and personal data governance	Advanced digital infrastructure, institutional trust, and digital service integration	Coordinated digital transformation and centralized regulatory capacity
Main limitation	Uneven digital literacy, fragmented implementation, and infrastructure disparities	Privacy risks arising from extensive digital integration and data connectivity	Balancing innovation, privacy protection, and ethical governance
Transferable lesson	Strengthening parental responsibility and family-based governance	Developing secure, accountable, and interoperable digital identity systems	Integrating technology, regulation, and socio-cultural legitimacy

Source: Author's comparative analysis (2026).

The comparative findings reveal that Indonesia, Estonia, and the United Arab Emirates represent three different governance orientations in protecting children's digital identity. Indonesia adopts a family-centered model in which parents function as the primary actors responsible for children's welfare, including supervision of digital activities. This approach corresponds with the principle that children's protection begins within the family, where parental responsibility extends beyond physical care toward moral, educational, and digital guidance. Within the context of Islamic family law, this model reflects the importance of parental guardianship (*wilāyah al-usrah*) and responsibility for safeguarding children's interests in changing social environments (Kurniawan et al., 2024;

Muharir & Lousada, 2024; Muyassar et al., 2024; Banurea, 2025). However, Indonesia's family-centered governance remains challenged by differences in digital literacy, unequal access to technological resources, and variations in institutional implementation.

In contrast, Estonia demonstrates an infrastructure-based governance model in which children's digital identity protection is closely connected with secure electronic identification systems, institutional interoperability, and public trust in digital services. Rather than placing primary responsibility on families, Estonia relies heavily on state capacity to establish reliable digital ecosystems capable of protecting citizens' identities, including children. This model illustrates how technological infrastructure and institutional accountability can strengthen digital governance effectiveness (Janssen et al., 2025; Lusi et al., 2025; Naghmouchi et al., 2025). Nevertheless, the high level of digital integration also creates new challenges, particularly concerning cybersecurity, data concentration, and the protection of children's privacy within interconnected systems.

The United Arab Emirates represents a hybrid governance model that combines technological modernization, centralized regulatory coordination, and family-oriented socio-cultural values. Unlike Estonia's primarily infrastructure-driven approach and Indonesia's family-centered model, the UAE integrates digital transformation strategies with regulatory supervision and cultural legitimacy. This approach demonstrates how rapid technological development can coexist with ethical considerations and Islamic values related to human dignity and social responsibility (Guenduez et al., 2025; Hamdan et al., 2026). However, its continuing challenge lies in maintaining equilibrium between technological innovation, regulatory control, and the protection of children's fundamental rights in digital environments.

The comparison further demonstrates that no single governance model provides a complete solution for children's digital identity protection. Indonesia contributes a strong normative foundation through parental responsibility and child-centered legal principles, Estonia provides valuable experience in secure digital infrastructure and institutional interoperability, while the United Arab Emirates illustrates the possibility of harmonizing technological innovation with cultural and ethical values. Therefore, comparative policy learning should not be understood as the direct adoption of one jurisdiction's model but as the integration of complementary governance practices adapted to local legal and social contexts. These findings establish the foundation for the subsequent analysis, which examines how *maqāṣid al-sharī'ah* can function as an evaluative framework for assessing the effectiveness and ethical orientation of children's digital identity governance.

Maqāṣid al-Sharī'ah as an Evaluative Framework for Digital Identity Governance

The comparative findings demonstrate that children's digital identity governance cannot be evaluated solely through technological performance, regulatory compliance, or institutional efficiency. A comprehensive assessment requires an analytical framework capable of examining whether governance arrangements effectively preserve children's dignity, welfare, legal identity, and long-term interests. In this regard, *maqāṣid al-sharī'ah* provides a relevant evaluative framework because it emphasizes the realization of *maṣlaḥah* (benefit) and the prevention of *mafsadah* (harm) as fundamental objectives of Islamic law. Unlike conventional approaches that primarily assess digital governance from technological or administrative perspectives, this study applies *maqāṣid al-sharī'ah* as an analytical instrument to evaluate how Indonesia, Estonia, and the United Arab Emirates protect children's digital identity within different legal and institutional contexts. This approach extends *maqāṣid* beyond doctrinal interpretation by positioning it as a practical framework for assessing contemporary legal challenges, including digital privacy, identity protection, and child welfare (Al-Shatibi, 1920; Auda, 2008; Kamali, 2008). Recent scholarship also demonstrates that *maqāṣid al-sharī'ah* can function as an operational framework for analysing contemporary family resilience and legal development, thereby strengthening its relevance for emerging issues in digital society (Rozikin et al., 2025).

The application of *maqāṣid al-sharī'ah* in this study further recognizes that effective digital identity governance depends not only on the existence of legal norms but also on institutional capacity, technological reliability, and ethical responsibility. Digital transformation requires alignment between technological systems, administrative structures, and institutional actors responsible for protecting public interests (Lu et al., 2025). This perspective explains why Estonia's digital identity ecosystem demonstrates strong institutional integration, while Indonesia continues to face challenges related to implementation capacity and digital literacy. At the same time, contemporary technology governance emphasizes that digital innovation should remain human-centered by prioritizing dignity, accountability, and social responsibility rather than merely pursuing technological efficiency

(Monlezun, 2025). These principles correspond with *maqāṣid al-sharīʿah*, which evaluates legal arrangements according to their ability to preserve human welfare and prevent harm.

The first analytical dimension is *ḥifẓ al-naḥs* (protection of life) and *ḥifẓ al-ʿaql* (protection of intellect), which reflect the obligation to protect children's physical, psychological, and intellectual development within digital environments. Indonesia addresses these objectives primarily through child protection regulations, parental supervision, and family-based digital literacy initiatives that seek to prevent online harm while supporting children's responsible digital participation (Kurniawan et al., 2024; Muharir & Lousada, 2024; Muyassar et al., 2024; Banurea, 2025; Muchtarom et al., 2026). Estonia operationalizes these objectives through secure digital infrastructure, trusted electronic identification, and cybersecurity mechanisms designed to reduce risks of identity misuse and unauthorized access (Janssen et al., 2025; Lusi et al., 2025; Naghmouchi et al., 2025). Meanwhile, the United Arab Emirates combines technological innovation with regulatory supervision and family-oriented governance, seeking to maintain children's safety while ensuring that digital transformation remains consistent with ethical and cultural values (Guenduez et al., 2025; Hamdan et al., 2026). Although implemented through different institutional mechanisms, all three jurisdictions demonstrate a shared commitment to minimizing digital harm and supporting children's healthy development.

Table 2. Maqāṣid al-Sharīʿah Evaluation of Children's Digital Identity Governance

Maqāṣid Dimension	Indonesia	Estonia	United Arab Emirates	Comparative Assessment
<i>Ḥifẓ al-naḥs</i> (Protection of life)	Child protection laws and parental supervision reduce risks of online exploitation and digital harm	Secure digital infrastructure and cybersecurity mechanisms protect children from identity-related threats	Integrated digital regulation promotes children's online safety within family-oriented governance	All jurisdictions prioritize child safety through different governance mechanisms
<i>Ḥifẓ al-ʿaql</i> (Protection of intellect)	Family-based digital literacy and parental guidance support children's cognitive development	Trusted digital services reduce exposure to unsafe digital environments	Digital innovation is complemented by ethical governance and educational initiatives	Protection of children's intellectual development requires education, technology, and regulation

Source: Author's analytical synthesis (2026).

Beyond the protection of life and intellect, the dimensions of *ḥifẓ al-naḥs* (protection of lineage and family integrity) and *ḥifẓ al-māl* (protection of property and legitimate interests) provide further analytical perspectives for understanding children's digital identity governance. Within contemporary Islamic family law, *ḥifẓ al-naḥs* extends beyond biological lineage to include the preservation of children's dignity, legal identity, family relationships, and social recognition. In digital society, children's identities are increasingly represented through electronic records, educational platforms, healthcare systems, and public digital services. Therefore, inadequate protection of children's personal data may affect not only privacy but also legal identity, family integrity, and future social participation. Indonesia addresses this dimension through parental responsibility and child protection principles, while Estonia strengthens legal identity through secure digital identity systems and institutional interoperability. The United Arab Emirates combines technological development with regulatory oversight and family-oriented governance, demonstrating how digital identity protection can be aligned with social and cultural legitimacy. These findings indicate that *ḥifẓ al-naḥs* provides a valuable framework for assessing whether digital governance mechanisms preserve children's identity and family relationships in an increasingly digital society.

Similarly, *ḥifẓ al-māl* (protection of property and legitimate interests) expands the understanding of children's digital identity as a valuable legal asset requiring protection. Although classical Islamic jurisprudence primarily associates this principle with material property, contemporary legal developments recognize that personal data, digital credentials, and electronic identities possess significant economic and legal value (Auda, 2008; Kamali, 2008; Beltrán, 2025; Kun, 2025; Volz, 2026). Indonesia seeks to protect these interests through personal data protection regulation and institutional safeguards, although implementation challenges remain. Estonia provides

a technologically integrated model through secure authentication, encrypted data exchange, and institutional accountability. The United Arab Emirates strengthens this objective through centralized digital governance and continuous technological innovation. From the perspective of *ḥifẓ al-māl*, effective digital identity governance requires not only legal protection but also reliable technological systems capable of preserving children's digital assets throughout their life course.

The application of the four *maqāṣid* dimensions demonstrates that no jurisdiction independently fulfills all normative and institutional requirements of children's digital identity governance. Indonesia contributes a strong family-centered approach based on parental responsibility and child welfare principles; Estonia provides advanced experience in secure digital infrastructure and institutional interoperability; while the United Arab Emirates demonstrates how technological innovation can be integrated with Islamic values and socio-cultural legitimacy. Therefore, *maqāṣid al-sharī'ah* functions not merely as a philosophical justification for legal reform but as an analytical framework for evaluating whether governance systems effectively protect children's welfare, dignity, identity, and future participation. This synthesis provides the conceptual foundation for the development of the *Maqāṣid-Based Children's Digital Identity Governance (MCDIG) Framework* in the following section, which integrates comparative legal insights with Islamic legal objectives to formulate a more comprehensive model of child-centered digital governance.

Developing the MCDIG Framework: Integrating Islamic Legal Objectives and Digital Governance

The comparative analysis and the application of *maqāṣid al-sharī'ah* demonstrate that existing approaches to children's digital identity governance remain fragmented across different regulatory and disciplinary perspectives. Digital governance studies generally emphasize institutional efficiency, technological infrastructure, interoperability, and administrative capacity, while cybersecurity research focuses primarily on technical protection mechanisms and resilience against digital threats. Meanwhile, children's rights scholarship highlights privacy protection, legal safeguards, and vulnerability reduction, whereas Islamic family law research has traditionally focused on parental responsibility, family protection, and ethical obligations. Although these perspectives provide valuable contributions, they often operate separately and do not fully address the complex relationship between technological development, family responsibility, institutional governance, and children's digital rights. Therefore, this study proposes the *Maqāṣid-Based Children's Digital Identity Governance (MCDIG) Framework* as an integrated governance model that synthesizes comparative legal insights, Islamic legal objectives, and contemporary digital governance principles.

The MCDIG Framework is developed by integrating transferable governance lessons from Indonesia, Estonia, and the United Arab Emirates through the evaluative lens of *maqāṣid al-sharī'ah*. Rather than replicating the regulatory approach of a particular jurisdiction, the framework combines complementary strengths identified through comparative analysis. Indonesia contributes a family-centered governance orientation that emphasizes parental responsibility and child welfare protection. Estonia provides lessons regarding secure digital identity infrastructure, institutional interoperability, and public trust in digital systems. The United Arab Emirates demonstrates how technological modernization can be combined with regulatory coordination, cultural legitimacy, and Islamic socio-legal values. By integrating these dimensions, the MCDIG Framework conceptualizes children's digital identity not merely as technical information requiring protection but as an essential component of children's dignity, legal identity, family integrity, and future participation in society.

Table 3. The *Maqāṣid*-Based Children's Digital Identity Governance (MCDIG) Framework

Framework Component	Governance Function	<i>Maqāṣid al-Sharī'ah</i> Dimension	Expected Governance Outcome
Parental digital responsibility	Digital supervision, informed consent, ethical guidance, and protection of children's interests	<i>Ḥifẓ al-nasl, ḥifẓ al-'aql</i>	Responsible family-based digital protection
Legal protection of children's personal data	Privacy regulation, legal certainty, and protection of children's digital rights	<i>Ḥifẓ al-māl, ḥifẓ al-nafs</i>	Protection against identity misuse and digital exploitation
Secure digital infrastructure	Authentication, interoperability, cybersecurity, and reliable digital identity systems	<i>Ḥifẓ al-nafs, ḥifẓ al-māl</i>	Trusted and resilient digital identity ecosystem

Framework Component	Governance Function	Maqāṣid al-Sharī'ah Dimension	Expected Governance Outcome
Family digital literacy	Digital awareness, ethical education, and risk prevention capacity	<i>Hifẓ al-'aql, hifẓ al-nasl</i>	Improved family and children's digital resilience
Collaborative institutional governance	Coordination among governments, schools, technology providers, and families	Integration of all maqāṣid dimensions	Sustainable child-centered digital governance

Source: Developed by the authors (2026).

The five components of the MCDIG Framework function as an interconnected governance ecosystem rather than isolated regulatory mechanisms. First, parental digital responsibility recognizes the family as a fundamental institution in protecting children's digital welfare by ensuring supervision, ethical guidance, and informed decision-making. Second, legal protection of children's personal data provides enforceable safeguards that prevent unauthorized processing, identity exploitation, and misuse of children's digital information. Third, secure digital infrastructure establishes the technological foundation required to maintain confidentiality, integrity, and reliability of children's digital identities. Fourth, family digital literacy strengthens the capacity of parents and children to understand digital risks and participate responsibly in online environments. Fifth, collaborative institutional governance integrates the responsibilities of government agencies, educational institutions, technology providers, and families into a coordinated protection system. Together, these components reflect the holistic orientation of maqāṣid al-sharī'ah, where children's welfare is achieved through the simultaneous realization of legal, ethical, technological, and institutional objectives.

The originality of the MCDIG Framework lies in its integration of comparative legal analysis, Islamic family law, maqāṣid al-sharī'ah, children's digital rights, and digital governance into a single conceptual model. Existing approaches frequently prioritize one dimension, such as technological security, regulatory compliance, or ethical responsibility, without sufficiently integrating these elements into a unified governance structure. In contrast, the MCDIG Framework positions children's digital identity protection as a multidimensional governance challenge in which family responsibility, legal regulation, technological capacity, and institutional collaboration operate as mutually reinforcing elements. This approach extends contemporary Islamic family law scholarship by demonstrating that maqāṣid al-sharī'ah can function not only as a normative foundation but also as an operational framework for evaluating and designing governance responses to emerging digital challenges.

From a practical perspective, the MCDIG Framework provides a transferable reference for policymakers, child protection institutions, data protection authorities, educational organizations, digital service providers, and families seeking to develop child-centered digital governance strategies. The framework does not require identical implementation across different jurisdictions; rather, it provides adaptable principles that can be adjusted according to local legal systems, institutional capacities, and socio-cultural conditions. Accordingly, the MCDIG Framework contributes to the development of a more comprehensive approach to children's digital identity governance by bridging Islamic legal objectives with contemporary digital governance needs. Through this integration, the framework offers a pathway for strengthening children's digital protection while ensuring that technological innovation remains aligned with human dignity, ethical responsibility, and the best interests of children.

CONCLUSION

This study concludes that children's digital identity governance represents an emerging dimension of contemporary Islamic family law that requires integration between legal protection, technological security, family responsibility, and institutional governance. The comparative findings demonstrate that Indonesia, Estonia, and the United Arab Emirates adopt distinct governance models shaped by their legal traditions, institutional capacities, and socio-cultural contexts. Indonesia reflects a family-centered governance model based on parental responsibility, child protection principles, and personal data regulation. Estonia represents an infrastructure-based model supported by secure digital identity systems, interoperable digital services, and institutional trust. Meanwhile, the United Arab Emirates illustrates a hybrid governance model combining technological innovation, regulatory coordination, and Islamic socio-cultural values. These findings confirm that no single national model

can comprehensively address the complexity of children's digital identity protection; instead, sustainable governance requires adaptive integration of complementary legal, technological, and institutional practices.

This study further demonstrates that *maqāṣid al-sharī'ah* functions not only as a normative foundation but also as an analytical framework for evaluating children's digital identity governance. Through the dimensions of *ḥifẓ al-nafs* (protection of life), *ḥifẓ al-'aql* (protection of intellect), *ḥifẓ al-nasl* (protection of lineage and family integrity), and *ḥifẓ al-māl* (protection of property and legitimate interests), digital identity protection can be understood as part of broader efforts to preserve children's dignity, welfare, legal identity, and future participation in society. This perspective expands the application of Islamic legal objectives beyond conventional family issues toward emerging challenges in digital society.

Building upon comparative analysis and *maqāṣid* evaluation, this study develops the *Maqāṣid*-Based Children's Digital Identity Governance (MCDIG) Framework as an integrated model for strengthening child-centered digital identity protection. The framework consists of five interconnected components: parental digital responsibility, legal protection of children's personal data, secure digital infrastructure, family digital literacy, and collaborative institutional governance. The principal novelty of this study lies in repositioning *maqāṣid al-sharī'ah* from a primarily normative reference into an operational framework for evaluating and designing digital governance responses affecting children. By integrating Islamic family law, comparative legal analysis, children's digital rights, and contemporary digital governance, the MCDIG Framework provides a comprehensive approach that moves beyond fragmented technological or regulatory solutions. The framework offers theoretical contributions by extending Islamic family law scholarship into the digital domain and practical implications for policymakers, child protection institutions, educational organizations, families, and digital service providers seeking to balance technological innovation with ethical responsibility and children's best interests.

Nevertheless, this study has several limitations. First, it employs a doctrinal and comparative legal approach based primarily on legislation, institutional policies, regulatory documents, and scholarly literature; therefore, it does not incorporate empirical perspectives from children, parents, policymakers, or technology providers. Second, the comparative scope is limited to Indonesia, Estonia, and the United Arab Emirates, requiring further research to examine the applicability of the proposed framework across different legal and socio-cultural contexts. Third, the MCDIG Framework remains a conceptual model requiring empirical validation and implementation assessment. Future research may examine the framework through comparative field studies, digital parenting surveys, institutional governance evaluations, and empirical studies of children's experiences within digital identity systems. Despite these limitations, this study provides an initial foundation for developing child-centered digital identity governance by demonstrating how Islamic legal objectives, comparative legal insights, and digital governance principles can be integrated into an adaptive and comprehensive framework for protecting children in the digital era.

REFERENCES

- Aghbalou, O. (2026). Family Law, *Maqāṣid al-Sharī'ah*, and State Resilience: A Comparative Study of Legislative Reform in Muslim Jurisdictions. *Mazahibuna: Jurnal Perbandingan Mazhab*, 8(1), 39–56. <https://doi.org/10.24252/mazahibuna.vi.64188>
- Akhtar, J. (2026). Reinterpreting religious authority: Women as Islamic jurists for addressing gender justice in Pakistan. *Women's Studies International Forum*, 116, 103300. <https://doi.org/10.1016/j.wsif.2026.103300>
- Alraddadi, R., Alshayeb, M., Mahmood, S., & Niazi, M. (2025). Enhancing cybersecurity in smart and cognitive cities: A systematic mapping of AI-based techniques. *Array*, 28, 100606. <https://doi.org/10.1016/j.array.2025.100606>
- Alsharif, M., & Hnit, H. (2025). Digital human rights: Legal debates and emerging foundations under the international bill of human rights. *Social Sciences & Humanities Open*, 12, 102160. <https://doi.org/10.1016/j.ssaho.2025.102160>
- Al-Shatibi, I. ibn Musa. (1920). *Al-Muwafaqat fi usul al-shari'ah*. Matba'at al-Maktabah al-Tijariyyah.
- Apps, T., Beckman, K., & Ng, R. (2025). Special issue: Datafied by default: Examining the intersect between children's digital rights and education. *Computers and Education Open*, 9, 100237. <https://doi.org/10.1016/j.caeo.2024.100237>
- Arminsyah, A. (2025). *Maqasid al-Shariah* in contemporary legal systems: An analysis of digital rights and privacy protection. *Al-Qadha: Jurnal Hukum Islam dan Perundang-Undangan*, 12(2), 289–308. <https://doi.org/10.32505/qadha.v12i2.11178>

- Atar, E., Güler, F., & Usta, Y. (2025). Digital transformation in local governance: A study on opportunities and challenges in Türkiye. *Transforming Government: People, Process and Policy*, 19(4), 725–747. <https://doi.org/10.1108/TG-03-2025-0053>
- Auda, J. (2008). *Maqasid al-shariah as philosophy of Islamic law: A systems approach*. International Institute of Islamic Thought.
- Azam, M., Pharaon, R. A. K. M., Mahdy, E., Albabili, M. A. I., Alsyouf, B., & Bagayev, B. (2026). AI-driven Sharia governance in Islamic digital payment systems: Developing a contemporary Islamic law framework for ethical and regulatory compliance. *Nusantara: Journal of Law Studies*, 5(2), 849–880. <https://doi.org/10.66325/nusantaralaw.v5i2.339>
- Banurea, S. (2025). Child protection in the perspective of Islamic family law by era digital. *Jurnal Ilmiah Teunuleh: International Journal of Social Sciences*, 6(2), 171–180. <https://doi.org/10.51612/teunuleh.v6i2.191>
- Bayar, Ö., & Sezgin, S. (2026). Child sexual exploitation and abuse in digital environments: Mapping two decades of research. *Child Abuse & Neglect*, 179, 108179. <https://doi.org/10.1016/j.chiabu.2026.108179>
- Beltrán, M. (2025). AI algorithms under scrutiny: GDPR, DSA, AI Act and CRA as pillars for algorithmic security and privacy in the European Union. *Computers & Security*, 158, 104628. <https://doi.org/10.1016/j.cose.2025.104628>
- Cameron, L. D., Conzon, V. M., & Lam, L. (2025). Selling the self: Neo-normative control and the platform paradox. *Research in Organizational Behavior*, 45, 100230. <https://doi.org/10.1016/j.riob.2025.100230>
- Campos, D. M., & Coutinho, C. (2025). Safeguarding the future: Forecasting cybersecurity and privacy challenges and solutions in emerging technologies for SMEs. *Procedia Computer Science*, 263, 712–718. <https://doi.org/10.1016/j.procs.2025.07.085>
- Casalini, F., & Zavolokina, L. (2025). From private platforms to public value: An exploratory analysis of privately owned public service digital platforms in Italy. *Government Information Quarterly*, 42(4), 102090. <https://doi.org/10.1016/j.giq.2025.102090>
- Casarosa, F., Comandé, G., & Fortuna, J. (2025). Proposing ELDA methodology: Ethical and legal by design and assessment for cybersecurity solutions. *Computer Law & Security Review*, 59, 106220. <https://doi.org/10.1016/j.clsr.2025.106220>
- Chen, H., Li, C., Liu, J., & Xu, R. (2025). Navigating digital frontiers: The impact of China's cybersecurity law on corporate digital innovation. *International Review of Financial Analysis*, 103, 104182. <https://doi.org/10.1016/j.irfa.2025.104182>
- Evgin, D., Karabulut, R., & Deniz, S. (2026). Digital parenting, self-efficacy, and family support among parents of children with disabilities. *Journal of Pediatric Nursing*, 88, 635–644. <https://doi.org/10.1016/j.pedn.2026.03.041>
- Guenduez, A. A., Walker, N., & Demircioglu, M. A. (2025). Digital ethics: Global trends and divergent paths. *Government Information Quarterly*, 42(3), 102050. <https://doi.org/10.1016/j.giq.2025.102050>
- Hamdan, R., Hamdan, A. M., & El Khoury, R. (2026). Revisiting the CSR–performance nexus: Insights from multiple theoretical lenses applied in the UAE. *Competitiveness Review*, 36(5), 1082–1111. <https://doi.org/10.1108/CR-08-2025-0279>
- Hariyani, D., Hariyani, P., Choudhary, S., & Mishra, S. (2026). Digital technologies for achieving SDG 11 targets: A holistic systems-level perspective. *Sustainable Cities and Society: Advances*, 2(2), 100064. <https://doi.org/10.1016/j.scsadv.2026.100064>
- Hasnain, M., Ghani, I., Smith, D., Daud, A., & Jeong, S. R. (2025). Cybersecurity challenges in blockchain-based social media networks: A comprehensive review. *Blockchain: Research and Applications*, 6(3), 100290. <https://doi.org/10.1016/j.bcr.2025.100290>
- Hossain, M. A., & Islam, M. S. (2025). Towards decentralized cybersecurity: A novel privacy-preserving federated learning approach for botnet attack detection. *Blockchain: Research and Applications*, 100355. <https://doi.org/10.1016/j.bcr.2025.100355>
- Imandeka, E., Hidayanto, A. N., Oktavia Hadi Putra, P., & Mahmud, M. (2026). Building smart prisons: Developing a context-specific digital transformation framework for Indonesia. *International Journal of Information Management Data Insights*, 6(1), 100405. <https://doi.org/10.1016/j.jjimei.2026.100405>
- Ja'far, S., Yaqin, H., Iffah, I., Hodri, H., & Sanuri, S. (2026). Digital fiqh and maqāṣid al-sharī'ah in the online condition: A digital hermeneutic critique of algorithmic power for Islamic epistemic sovereignty. *Samarah: Jurnal Hukum Keluarga dan Hukum Islam*, 10(1), 550–571. <https://doi.org/10.22373/sjhk.v10.i1.31868>

- Janssen, M., Zhang, H., Ojo, A., Nikiforova, A., Loukis, E., Pereira, G. V., Scholl, H. J., Liu, H. K., Durkiewicz, J., Hughes, L., Zheng, L., Anthopoulos, L., Panagiotopoulos, P., Janowski, T., & Dwivedi, Y. K. (2025). Reflections on the nature of digital government research: Marking the 50th anniversary of *Government Information Quarterly*. *Government Information Quarterly*, 42(4), 102086. <https://doi.org/10.1016/j.giq.2025.102086>
- Kamali, M. H. (2008). *Maqasid al-shari'ah made simple*. International Institute of Islamic Thought.
- Kun, E. (2025). Searching for the appropriate legal basis for personal data processing for cybersecurity purposes under the NIS 2 Directive: Legal obligation and/or legitimate interest? *Computer Law & Security Review*, 56, 106098. <https://doi.org/10.1016/j.clsr.2024.106098>
- Kurniawan, P., Ahmatnizar, A., & Ridwan, M. (2024). The transformation of Islamic family law in the digital era: A sociological legal analysis of marriage and divorce regulations in Indonesia. *Madania: Jurnal Kajian Keislaman*, 28(2), 179–190. <https://doi.org/10.29300/madania.v28i2.5146>
- Lestianingsih, E. N., Ahyani, H., Muharir, Lathif, A. M. M., Lousada, S. A. N., Mutmainah, N., & Atiqoh, U. (2025). Maqāṣid al-Sharī'ah al-Shatibi in the digital era: Contemporary perspectives on halal lifestyle and technology in Indonesia. *Al-Mawarid Jurnal Syariah dan Hukum (JSYH)*, 7(1), Article 1. <https://doi.org/10.20885/mawarid.vol7.iss1.art4>
- Li, J. (2025). Reflection on data right protection for minors in the digital age. *Children and Youth Services Review*, 170, 108167. <https://doi.org/10.1016/j.childyouth.2025.108167>
- Lim, A. C. M., Ng, L. H. X., & Taihagh, 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>
- Lin, Z., & Wang, C. (2026). Embedding of public value in central bank digital currencies: Human rights implications in digital payment systems. *Computer Law & Security Review*, 62, 106366. <https://doi.org/10.1016/j.clsr.2026.106366>
- Long, J., Zhang, S., Chu, L., Balkian, J., Giovannucci, I., Mui, C., Luan, Y., Chang, O., Chanthavilay, P., Goundar, K., Luvsan, M.-E., Kennedy, E., Nguyen, D., Ann Phoa, P. K., Ramirez, C. M., Tran, B. X., Yi, S., Valera, P. M., Tep, S., ... Lu, C. (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>
- Lu, B., Guo, Y., Zhang, S., & Dong, P. (2025). Digital government and the structural determinants of political participation among street-level bureaucrats in China. *International Journal of Electronic Government Research*, 21(1). <https://doi.org/10.4018/IJEGR.388562>
- Lusi, J., Lorenz, B., & Pappel, I. (2025). Innovation or reinvention? A systematic and bibliometric review of public sector digital infrastructure. *Journal of Open Innovation: Technology, Market, and Complexity*, 11(3), 100593. <https://doi.org/10.1016/j.joitmc.2025.100593>
- Marluwi, M., Baihaqi, B., Musadad, A., Zahro, U. I., & Pujiati, T. (2025). Maqāṣid al-sharī'ah as a governance framework: Institutionalizing child protection in Pontianak. *Mawaddah: Jurnal Hukum Keluarga Islam*, 3(2), 305–334. <https://doi.org/10.52496/mjhki.v3i2.34>
- Mashdurohatur, A., Naimah, Rahmadi, R., Ismayana, & Suparjo, H. (2026). Beyond formal legality: A maqashid al-shari'ah approach to ethical legitimacy in electronic consent across notarial, healthcare, and child protection practices. *Al-Istinbath: Jurnal Hukum Islam*, 11(1), 411–435. <https://doi.org/10.29240/jhi.v11i1.16236>
- Monlezun, D. J. (2025). Quantum physics to personalist quantum metaphysics: Human-centered global AI governance. In K. Bassil & J. L. Boyd (Eds.), *Quantum health AI* (pp. 179–250). Academic Press. <https://doi.org/10.1016/B978-0-443-33353-8.00010-2>
- Morrell, S. (2025). Why (not) talk about human rights? Politics in the Global Digital Compact. *Telecommunications Policy*, 49(10), 103077. <https://doi.org/10.1016/j.telpol.2025.103077>
- Mota, E. C., & Klein, P. G. (2025). Extrusive effects of digital government: Reframing the citizen–state relationship. *Government Information Quarterly*, 42(3), 102064. <https://doi.org/10.1016/j.giq.2025.102064>
- Muchtaron, M., Raharjo, & bin Selamat, A. Z. (2026). Preventing gadget misuse in children to enhance family resilience: Integrating religious values, digital literacy, and community participation in rural Indonesia. *Social Sciences & Humanities Open*, 13, 102922. <https://doi.org/10.1016/j.ssaho.2026.102922>
- Muharir, M., & Lousada, S. A. N. (2024). Maqāṣid al-sharī'ah in the digital era: Challenges in Islamic family law and halal lifestyle in Indonesia. *Munakahat: Journal of Islamic Family Law*, 1(1), 34–45. <https://doi.org/10.5281/zenodo.20802201>

- Mukaromah, D. F., Rahim, A., & Khafidz, H. A. (2025b). Leveraging Artificial Intelligence for Efficient and Transparent ZISWAF Management: Comparative Insights from Indonesia and Malaysia. *Munakahat: Journal of Islamic Family Law*, 1(2), 25–37. <https://doi.org/10.5281/zenodo.21235737>
- Muyassar, Y. R., Dawi, K., Muhayan, Sitorus, A. P. M. C., & Setiawan, A. (2024). Cyber law and Islamic family law: Safeguarding women's and children's rights in the digital world. *Arus Jurnal Sosial dan Humaniora*, 4(3), 1942–1951. <https://doi.org/10.57250/ajsh.v4i3.807>
- Naghmouchi, M., Laurent, M., Levallois-Barth, C., & Kaaniche, N. (2025). Perspectives on national digital identity systems. *Blockchain: Research and Applications*, 6, 100429. <https://doi.org/10.1016/j.bcr.2025.100429>
- Oroni, C. Z., & Xianping, F. (2025). Evaluating the influence of cybersecurity policies and cybersecurity behavior on institutional security performance in remote learning: The moderating role of technological readiness. *Sustainable Futures*, 10, 101554. <https://doi.org/10.1016/j.sfr.2025.101554>
- Perkasa, D. A., Setiawan, B., Satriawan, A. B., & Asmoro, T. O. (2026). Measuring information security behaviour of high school students and teachers. *Procedia Computer Science*, 284, 1455–1462. <https://doi.org/10.1016/j.procs.2026.07.135>
- Roihanah, R., Rokamah, R., & Mufidah, L. (2026). Sharia, state, and family: Towards a responsive legislative design for household resilience in Indonesia. *Asy-Syir'ah: Jurnal Ilmu Syari'ah dan Hukum*, 60(1), 45–61. <https://doi.org/10.14421/ajish.v60i1.1669>
- Rozikin, O., Mukhlas, O. S., Rosadi, A., Fauzia, I., Muharir, M., Ahyani, H., & Adnan, N. I. M. (2025). Contextualizing maqāṣid al-sharī'ah in indigenous legal practices: A comparative study of family resilience in Kasepuhan Ciptagelar and Kampung Naga. *Nurani: Jurnal Kajian Syari'ah dan Masyarakat*, 25(2), 344–362. <https://doi.org/10.19109/nurani.v25i2.27760>
- 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>
- Tan, C. Y., Xu, N., Liang, M., & Li, L. (2025). Meta-analysis of associations between digital parenting and children's digital wellbeing. *Educational Research Review*, 48, 100699. <https://doi.org/10.1016/j.edurev.2025.100699>
- Volz, F., Münch, C., Lohmüller, M., & Küffner, C. (2025). From data jungle to data governance in digital ecosystems: Empirical evidence from a multiple holistic case study. *Journal of Business Research*, 201, 115747. <https://doi.org/10.1016/j.jbusres.2025.115747>
- Volz, S. (2026). Age restrictions as a tool for enhancing children's online safety: An analysis with special reference to Australian law. *Computer Law & Security Review*, 61, 106278. <https://doi.org/10.1016/j.clsr.2026.106278>
- Withorn, T., Eslami, J., Lee, H., Clarke, M., Caffrey, C., Springfield, C., Ospina, D., Andora, A., Castañeda, A., Mitchell, A., Kimmitt, J. M., Vermeer, W., & Haas, A. (2021). Library instruction and information literacy 2020. *Reference Services Review*, 49(3/4), 329–418. <https://doi.org/10.1108/RSR-07-2021-0046>
- Yildirim, Y., Demirel, S. C., & Avcioglu, B. (2025). Shaping children's digital futures: The role of parenting strategies in regulating children's technology use. *Acta Psychologica*, 258, 105265. <https://doi.org/10.1016/j.actpsy.2025.105265>