MILRev
Metro Islamic Law Review
Scientific Islamic Law Journal Of Sharia Faculty
MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

Child Protection from Cyber Violence: An Analysis of CRC General Comment No. 25 and Contemporary Islamic Ethical Perspectives in Indonesia and Malaysia

Author:
Rizki Adi Pinandito[1*], Hartiwiningsih[2], Muhammad Rustamaji[3]

Affiliation:
[1,2,3]Universitas Sebelas Maret Surakarta, Indonesia

Corresponding author:
*rizkyadipinandito@student.uns.ac.id

Doi: 10.32332/milrev.v5i1.12762

Dates:
Received 15 September, 2025
Revised 26 February, 2026
Accepted 01 April, 2026
Published 17 April, 2026

Read Online:

Scan this QR code with your mobile device or smart phone to read online

Abstract: The research aims to analyze the extent to which both countries have developed regulatory and institutional mechanisms to safeguard children from digital harm and to formulate an integrative model of protection that aligns international child rights standards with contemporary Islamic ethical values. In this context, Islamic ethical principles derived from *maqāṣid al-sharīʿah* are positioned as a normative foundation for strengthening digital child protection. This research employs normative or doctrinal legal research using statutory, conceptual, and comparative approaches to examine relevant legal norms, principles, and doctrines in Indonesia and Malaysia, alongside the ethical framework of *maqāṣid al-sharīʿah*. The findings indicate that the regulatory framework for child protection from cyber violence in Indonesia has shown normative progress and policy alignment with the CRC and General Comment No. 25, yet its implementation remains partial and fragmented. In comparison, Malaysia demonstrates relatively more structured institutional coordination in addressing online risks to children. Based on this comparative synthesis, the study proposes an ideal ius constituendum model of integrative and coherent protection through a systemic risk-based regulatory design grounded in the principles of *maṣlaḥah* and *sadd al-dharā'i* (harm prevention), while reinforcing justice (*'adl*) through equal service standards, including for children in remote and disadvantaged regions. Academically, this study contributes to the development of contemporary Islamic legal scholarship by bridging international child rights standards with Islamic ethical principles in the context of digital governance. It also offers a conceptual framework for integrating CRC/GC25 norms with *maqāṣid al-sharīʿah* as a complementary ethical foundation for shaping responsive, culturally grounded cyber child protection policies in Muslim-majority societies.

Keywords: Child Protection; CRC General Comment No. 25; Cyber Violence; Islamic Ethical Perspectives.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

INTRODUCTION

Children's mental health is a crucial foundation for their growth and development, and any threat to their physical and emotional safety can have long-lasting consequences for their wellbeing.[1] As a trust bestowed upon them by Allah *Subhanahuwata'ala*, children must be cared for and protected in all their interests, physical, psychological, intellectual, rights, and dignity. Protecting children is not solely the responsibility of their biological parents, but is the responsibility of all of us. As a religion steeped in compassion (*rahmatan lil alamin*), Islam places special and serious emphasis on children, from the time they are still in their mother's womb until they reach adulthood.[2] This compassion. The Qur'an describes children as a comfort to the eyes and heart (*qurrata a'yun*).[3] It's said this way because when a child looks into the eyes, a feeling of happiness is evoked. Therefore, children are a priceless treasure for parents. However, children are considered weak legal subjects due to their limited ability to understand, claim, and defend their own rights. This condition places them in a more vulnerable position to various forms of violations and exploitation.

Thus, the principle of protecting children as a trust and as vulnerable subjects demands a strengthened legal system that not only recognizes children's rights but also ensures effective mechanisms for their fulfillment. Implementing children's rights requires a strong and responsive legal system that not only recognizes children's rights but also integrates them into national and international legal structures.[4] Within the scope of international law, the 1989 Convention on the Rights of the Child (CRC) serves as a comprehensive legal framework that sets standards for legal protection for children against

---

[1] Murray, Lisa, Penny Levickis, Laura McFarland, Patricia Eadie, Lynn Lee-Pang, Jon Quach, and Jane Page, 'Supporting Young Children's Social–Emotional Wellbeing in Early Childhood Education and Care: Perspectives from the Sector' , Education Sciences 15, no. 5 (May 2005): 569, https://doi.org/10.3390/educsci15050569

[2] Rattry Risnawaty,' The Concept of Forming Shaleh Children According to Islamic Education', International Journal Education and Computer Studies (IJECS) 3 (2), (July 2023): 42-51, https://doi.org/10.35870/ijecs.v3i2.1802

[3] Ipah Hatipah, Rumba Triana, Syaeful Rokim, 'Anak Sebagai Qurratu A'yun Dalam Perspektif Al-Qur'an', Al - Tadabbur: Jurnal Ilmu Al-Qur'an dan Tafsir, 3(2),(October 2018):137-156, https://doi.org/10.30868/at.v3i02.314

[4] Laura Lundy, 'Children's Rights from an International Perspective',The Rights of the Child (April 2023):3-6, https://doi.org/10.1163/9789004511163_002 .

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

all forms of violence. Meanwhile, General Comment No. 25 provides a more specific guideline for state obligations to protect children in cyberspace and to ensure that every child's rights are protected, including the right to be free from cyber violence. These state obligations include strengthening prevention, complaint reporting mechanisms, responsive reporting, and victim redress.[5] These guidelines require an approach that focuses not only on prosecution but also on building an integrative and coherent protection cycle, from prevention to victim redress and digital footprints.

In this way, child protection is not only a state duty but also a collective responsibility that must be addressed through collaboration among government, society, and families. Therefore, a philosophical approach that emphasizes the dignity, freedom, and human rights of children, combined with progressive laws, can form a strong foundation for elevating children's status as legal subjects, equal to adults in receiving protection and respect for their rights. Data collected from the Online Information System for the Protection of Women and Children (Simfoni PPA) recorded 7,842 cases of violence against children between January and June 2024, with 5,552 victims being girls and 1,930 victims being boys.[6] Since 2019, sexual violence has consistently been the type of violence with the highest number of victims.[7] Based on research reports, assessments, and surveys conducted by ECPAT Indonesia, there was a significant increase in cases of child sexual exploitation in cyberspace from 2020 to 2022.[8] The 2022 Disrupting Harm study found that 2% of child internet users aged 12-17 in Indonesia were victims of serious cases of online sexual exploitation and harassment. Research with the Down to Zero Alliance in 2020 even found that 3 in 10 child respondents had experienced child sexual exploitation in cyberspace in Indonesia.

---

[5] Gevan Naufal Wala, 'Legal Protection for Child Victims of Digital-Based Sexual Crimes', Imperium Research, 1(1),(July 2025):30-37, https://doi.org/10.38035/IMPERIUM.v1i1

[6] Adelia Nur Cahyani, Et.Al,' Psychosocial Intervention As An Effort To Prevent Victimization Of Boy Victims Of Sexual Violence', JKPI: Jurnal Konseling Pendidikan Islam, 6(2), (May 2025): 71-83, https://doi.org/10.32806/jkpi.v6i2.777

[7] Dylan Aldianza Ramadhan, Charina Putri Besila, 'The Phenomenon of Sexual Violence among Adolescents in the Jurisdiction of the West Jakarta National Police Resort and Its Prevention Efforts', Fiat Justisia, 13(2), (April 2019): 115-128, https://doi.org/10.25041/fiatjustisia.v13no2.1574

[8] Muhammad Rayhan Murtadha, 'Psyshield Center: A Collaborative Program For Indonesian Students To Combat Cybersexual Exploitation', GPH-International Journal of Educational Research, 8(04), 9april 2025):22-34, https://doi.org/10.5281/zenodo.15347718

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

According to UNICEF's Safe Online Global report, Malaysia ranks 9th out of 12 countries featured in the 2020-2021 OCSEA Prevalence table.[9] Malaysia has a higher prevalence rate, almost double that of Indonesia, at 4.0%. Data compiled by the Internet Watch Foundation (IWF) shows that Malaysia recorded 12,656 CSAM reports from January to June 2025, equivalent to 78% of the total 2024 reports (16,238). The victim data involved children aged 7-10 and 11-13 years. Another study states that 1 in 4 children in Malaysia has been exposed to sexual content. The threat of sexual violence targeting children in Malaysian cyberspace tends to increase. A joint operation between the Malaysian police and the Malaysian Communications and Multimedia Commission (later named Ops Pedo 2.0) has succeeded in apprehending 31 suspects and confiscating more than 880,000 pieces of data related to online child sexual violence networks.[10] This shows that an approach that relies solely on reactive policies (deleting content/blocking sites) will always be left behind in the speed of production, distribution, and replication of CSAM content in cyberspace.

In this study, Malaysia was chosen as a comparison country due to similarities in socio-cultural and religious backgrounds. Both countries are predominantly Muslim, have strong family values, and tend to be conservative regarding issues of violence against children, particularly sexual violence. Furthermore, Indonesia and Malaysia are both bound by the CRC framework, although they have different approaches to its implementation. Furthermore, the author chose Malaysia because it offers a variety of protection designs that are still in line with Indonesia's. Therefore, this is useful in developing an ideal model for Indonesia.

The novelty of this research lies in its attempt to formulate a holistic and integrated model of child rights protection, which specifically emphasizes the application of the principles contained in the Convention on the Rights of the Child and General Comment

[9] ECPAT, INTERPOL and UNICEF, 'Disrupting Harm in Malaysia: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence Against Children', (2022), https://safeonline.global/wp-content/uploads/2023/12/DH_Malaysia_ONLINE_FINAL.pdf

[10] Kementerian Pembangunan Wanita, Keluarga dan Masyarakat, Malaysia, 'Laporan Pemantauan Media KPWKM', (Oktober 2025), https://kpwkm.gov.my/uploads/content-downloads/file_20251027110004.pdf

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

No. 25 in the context of protecting children's rights to be free from violence in cyberspace. Furthermore, this research incorporates the perspective of Islamic law, *maqāṣid al-sharī'ah*, as an ethical foundation that emphasizes protecting children's rights to be free from violence in cyberspace. Ultimately, the purpose of this study is to identify and discover a model of legal protection for children's rights to be free from violence in cyberspace in Indonesia based on the Convention on the Rights of the Child (CRC), as well as to identify and discover an ideal model for protecting children's rights in cyberspace through a comparative study of Indonesia–Malaysia. This article also places Islamic legal values, especially *maqāṣid al-sharī'ah*. These values are used as an ethical foundation that strengthens child protection in cyberspace, especially in maintaining dignity (*karāmah*), benefit (*maṣlaḥah*), honor (*hifẓ al-'ird*), and fair access ('*adl*).

METHOD

The research conducted in the preparation of this article adopts a normative/doctrinal legal research method,[11] relying on secondary data collected through library research and systematic document review. The data consist of primary legal materials, particularly relevant Indonesian legislation and applicable international legal instruments, with the Convention on the Rights of the Child (CRC) and General Comment No. 25 (GC25) serving as the main normative benchmarks, alongside secondary legal materials such as peer-reviewed journal articles, institutional reports, and policy documents. The research applies qualitative normative analysis by interpreting legal norms and principles,[12] evaluating regulatory obligations, and assessing their coherence with the standards and state duties articulated in the CRC and GC25 to formulate an ideal model for protecting children's rights to be free from violence in cyberspace in Indonesia.

[11] Laksana, Andri Winjaya, Akhmad Ikraam, and Anila Robbani. "The Liability of Criminal Law for Perpetrators of Goods Embezzlement." *Journal of Justice Dialectical* 2, no. 2 (2024): 70-83. DOI: https://doi.org/10.70720/jjd.v2i2.50

[12] Mashdurohatun, Anis, Eid Abed Alhaleem Maslat Harahsheh, Muhammad Irwan Datuiding, Abun Hasbulloh Syambas, and Prasetiyo Adhi Wibowo. "Contemporary Reassessment of Punishment in Islamic Sharia and Secular Law: A Comparative Study of Justice and Penal Philosophy." *MILRev: Metro Islamic Law Review* 5, no. 1 (2026): 80-100. DOI: https://doi.org/10.32332/milrev.v5i1.11887

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

In this framework, *maqāṣid al-sharī'ah* is deliberately positioned not as positive law or a source of binding legal rules, but as a form of theoretical legitimacy that strengthens the conceptual foundation of the proposed model. Specifically, *maqāṣid al-sharī'ah* is used as a value-based justificatory framework that supports the model's orientation toward safeguarding human dignity (*karāmah*), promoting public welfare (*maṣlaḥah*), protecting honour and personal integrity (*ḥifẓ al-'irḍ*), and ensuring justice and fair access ('*adl*), thereby providing a coherent ethical-philosophical grounding that complements and does not replace the rights-based obligations derived from the CRC and GC25.

RESULTS AND DISCUSSION

Legal Protection of Children from Cyber Violence in Indonesia: A CRC and General Comment No. 25 Perspective

The current model of legal protection for children in cyberspace in Indonesia is the result of a regulatory construction that has developed gradually and reacted to the dynamics of digital technology.[13] Although various legal instruments have been formulated, including laws, government regulations, and sectoral policies, the overall framework remains fragmented. It has not yet formed a complete and consistent protection system as required by the Convention on the Rights of the Child (CRC) and General Comment No. 25 (2021). In this context, mapping the legal protection model for children in cyberspace in Indonesia will be limited to the Penal approach.

The penal approach is a legal instrument[14] that serves to protect a criminal mechanism for perpetrators of cyber violence against children. This approach is crucial to ensure a deterrent effect. Normatively, Indonesia has three main regulations related to violence against children in cyberspace: the Child Protection Law, the Electronic Information and Transactions Law, and the 2025 National Regulation on Cyber Crimes. Law Number 35 of 2014 concerning Child Protection still shows fundamental weaknesses

[13] Muhammad Rafifnafia Hertianto, 'Tinjauan Yuridis Terhadap Perlindungan Anak Dalam Ruang Siber di Indonesia', jurnal Hukum dan Pembangungan (JHP), 51(3), (September 2025):555-573, http://dx.doi.org/10.21143/jhp.vol51.no3.3123

[14] Laksana, Andri Winjaya, Adhi Budi Susilo, Peni Rinda Listyawati, Setiawan Widiyoko, and Toni Triyanto. "Legal Uncertainty in Law Enforcement for Drug Addicts Resulting in Criminal Disparity." *Yuridika* 40, no. 2 (2025): 253-270. DOI: https://doi.org/10.20473/ydk.v40i2.68153

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

in protecting children from forms of violence that occur in the digital space. Although the law expands the state's obligation to provide special protection as stated in Article 59A, and emphasizes the prohibition against acts of violence through Article 76C, the normative framework that is built still relies on the understanding of violence in the traditional context, namely, physical, psychological, or sexual violence that occurs in conventional social spaces. Thus, the law does not explicitly recognize digital-based violence as a separate category, even though the development of digital technology has created a new arena in which violence can be carried out with characteristics, modes, and impacts fundamentally different from conventional violence.

This lack of explicit recognition raises serious issues in positioning digital violence as an object of legal protection. Although Articles 59A and 76C can be interpreted more broadly to include technology-mediated violence, this extension is implicit and lacks a clear legal definition. In the context of legal dogma, the use of an expanded interpretation without an explicit normative basis may conflict with the principle of legality, which requires clarity in the elements of a criminal act. Digital violence has certain characteristics that cannot always be subordinated to the categories of psychological or sexual violence as defined in the law. As a result, law enforcement can only interpret cases of digital violence through analogy, a methodologically weak approach that carries the risk of legal uncertainty, as analogy addresses only gaps in cases, not conceptual ones.

This conceptual weakness is further apparent when the law fails to define "cyberviolence" or the forms of violence that commonly occur in the digital environment. There is no explanation for cybergrooming, online enticement, sextortion, digital harassment, deepfake child pornography, or other forms of digital manipulation that are now part of the reality of violence against children. This lack of legal definition makes child protection in the digital space fragmented, uncoordinated, and inconsistent in practice. Law enforcement officials may apply different norms when handling similar cases, depending on their respective understandings of the elements of violence contained in the Child Protection Law or other criminal provisions deemed relevant. This inconsistency not only undermines the effectiveness of law enforcement but also diminishes the universality

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

of child protection as a human right, which the state should firmly and comprehensively guarantee.

The lack of a conceptual definition of digital violence in the Child Protection Law is not merely a technical regulatory issue but a structural one that demonstrates the unpreparedness of the ius constitutum to address changing forms of violence in the digital era. Cyberviolence is borderless, occurs through anonymous identities, and is mediated by algorithms that serve to amplify risks, expand the perpetrator's reach, and increase the likelihood of re-victimization.[15] These characteristics cannot be reduced to conventional forms of violence, so the lack of a legal definition prevents the state from providing proportional protection for children as demanded by technological developments. Furthermore, the absence of a formal definition of cyberviolence indicates a legislative delay in responding to the dynamics of cyberspace. When regulations fail to keep pace with evolving risks, laws lose their relevance and lag far behind current realities. Yet, the Committee on the Rights of the Child, through General Comment No. 25 (2021), explicitly affirms that states are obliged to identify, regulate, and prevent all forms of violence occurring in the digital environment, including technology-mediated violence and practices unknown under traditional law. Therefore, the absence of normative recognition in the Child Protection Law demonstrates a discrepancy between national and international standards and illustrates that child protection in the digital space has not yet been recognized as a fundamental issue in national legal policy.

From the theoretical perspective used in this dissertation, particularly Dworkin's approach to law as integrity, the law must reflect moral coherence and internal consistency between recognized principles and their implementation in regulatory structures.[16] The state has stated its commitment to protecting children from all forms of violence, but the law's inability to categorize digital violence as a stand-alone threat indicates a discrepancy

[15] Seung Min Bae,' Characteristics and Treatment of Cyberviolence Trauma in Children and Adolescents', J Korean Acad Child Adolesc Psychiatry;35(3), (March 2024):169-174, https://doi.org/10.5765/jkacap.240005

[16] Agam Ibnu Asa, 'The Evolution of Ronald Dworkin's Legal Philosophy: From Interpretivism to Integrity', Abjad: Journal of Humanities & Education, 3(2), (August 2025): 111-124, https://doi.org/10.62079/abjad.v3i2.88

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

between the principles of child protection and the normative instruments used to realize them. This inconsistency also indicates a failure to respect children's rights as understood in the theory of rights, which treats children's rights as a trump that overrides the limitations of sectoral regulations.

Thus, the conceptual weakness in the Child Protection Law is not simply a matter of definition or a lack of technical terminology, but a fundamental problem that undermines the entire penal approach to protecting children from digital-based violence. When the category of digital violence is not explicitly recognized, the state lacks a sufficient normative basis for establishing an effective protection regime. Law enforcement officials lack certainty in interpreting criminal incidents, victims lack recognition of the forms of violence they experience, and the national legal framework fails to meet international protection standards. Therefore, normative reconstruction is necessary to ensure that the concept of violence in the Child Protection Law explicitly and comprehensively encompasses the phenomenon of digital violence as a modern threat requiring legal protection on a par with physical, psychological, and sexual violence.

The second amendment to the Electronic Information and Transactions Law, enacted by Law Number 1 of 2024, continues to raise serious conceptual and normative issues regarding child protection in the digital space. Although the amendment regulates several new aspects and improves several previous provisions, the law still exhibits a fundamental weakness. It tends to reduce violence against children to merely a general violation, without giving specific weight to the nature of child sexual exploitation. International standards qualify child sexual exploitation as one of the most serious forms of violation of human dignity.[17] This reduction not only creates a normative gap in child protection but also weakens the state's ability to provide a legal response commensurate with the level of harm posed by digital exploitation of children.

[17] Witasya Aurelia Sulaeman. Beniharmoni Harefa, Handar Subhandi Bakhtiar,' Law Enforcement Against the Crime of Sexual Exploitation of Children in the Legal Systems of Indonesia and Malaysia', International Journal of Social Welfare and Family Law (IJSW), 2(3), (June 2025):1-16, https://doi.org/10.62951/ijsw.v2i3.362

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

One of the clearest manifestations of this reduction can be seen in the formulation of Article 27 paragraph (1) and Article 45A paragraph (1) of the ITE Law, which does not differentiate between adult pornography and child pornography. The article prohibits the distribution, transmission, and making accessible of content that violates general decency, but does not provide a specific classification for content involving children. This lack of differentiation shows that the law treats child pornography as part of the broad category of "content that violates decency," rather than as a form of child sexual exploitation that must receive the most stringent legal treatment. In fact, the Convention on the Rights of the Child (CRC) expressly requires states to qualify all forms of child sexual exploitation as serious violations that require a different legal response from violations of general decency.

This reduction has a significant impact on the construction of child protection because the ITE Law does not normatively view child sexual exploitation as an issue requiring a separate legal regime. In law enforcement practice, this can obscure the seriousness of acts involving children, as law enforcement officials lack a strong normative basis for treating child pornography as inherently more damaging than adult pornography.[18] When the law equates the two into the same category, legal treatment becomes less sensitive to the special vulnerabilities experienced by child victims. It fails to understand the dynamics of digital-based sexual exploitation, which are far more complex than conventional violations of morality.

Normatively, Government Regulation Number 17 of 2025 on the Governance of Electronic Systems for Child Protection (PP TUNAS) represents a significant leap in Indonesia's child protection regime in the digital space. Through Chapter II (Articles 2–22), this PP for the first time establishes comprehensive obligations for E-Commerce: starting from general obligations for child protection (Article 2), expanding the subject of public and private E-Commerce (Article 3), the scope of services used or likely to be used by children (Article 4), assessing the risk level of products and features (Article 5), to detailed technical obligations related to child DPIA, built-in privacy settings, prohibition of covert techniques, prohibition of profiling, limitation of geolocation collection, age

[18] Ateret Gewirtz-Meydan, 'The Complex Experience Of Child Pornography Survivors',Child Abuse&Neglect, Volume 80, (June 2018):238-248, https://doi.org/10.1016/j.chiabu.2018.03.031

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

verification, age segmentation, and reporting mechanisms (Articles 6–22). This strengthening is reinforced by Chapter III on supervision (Articles 24–27, 31–37) and Chapter IV on administrative sanctions (Articles 38–44), which, overall, build a modern, risk-based E-Commerce governance architecture.

However, this progress has not yet fully created an integrative framework across sectors and legal regimes. Although the TUNAS Government Regulation regulates certain oversight and coordination through the authority of the Minister (Articles 24, 27), inspection and coordination mechanisms with ministries/agencies and law enforcement (Article 34), and information sharing and reporting of suspected criminal acts (Article 37 letters e–f), these regulations are still general in nature and do not explicitly establish operational links with other regimes, such as the Child Protection Law, the TPKS Law, the PDP Law, and the SPPA Law. From a law as integrity perspective, an ideal legal system should be read as a "whole story" regarding how children are protected from violence, both physical and digital. In this context, the TUNAS Government Regulation appears strong in the realm of PSE governance but remains a "regulatory island" not yet fully integrated with other norms governing the criminal, civil, and social dimensions of child protection.

As a result, child protection in the digital space remains segmented: violations of technical obligations under the PSE are processed through administrative sanctions under the TUNAS Government Regulation; violence and exploitation of children are processed through the Child Protection Law and the TPKS Law; the PDP Law regulates personal data violations, while education and social policies operate through sectoral regulations. Without a clearly stated integrative design, ensuring that all forms of violence in the digital space will be addressed through consistent, coordinated, and child-centered state mechanisms remains dependent on institutional initiatives, rather than a truly integrated legal framework.

The TUNAS Government Regulation has addressed several important aspects of algorithmic risk and system design. The obligation to assess risks for products, services, and features (Article 5), the obligation to conduct a Personal Data Protection Impact Assessment (DPIA) for children (Article 7), and the prohibition on the use of covert methods or techniques (dark patterns) (Article 7 paragraph (2), Article 17), restrictions on

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457
the collection of precise geolocation (Article 18), and the prohibition on child profiling (Article 19) demonstrate that regulators are aware of the structural risks arising from the way digital systems are designed and operated.

However, when viewed in light of General Comment No. 25 (2021), the TUNAS Government Regulation still leaves conceptual weaknesses. First, this regulation does not explicitly require assessing the algorithmic impact of recommendation systems, news feeds, rankings, and content amplification mechanisms that significantly shape children's digital experiences. The risk assessment in Article 5 and the DPIA in Article 7 focus more on data processing and feature risks, but do not require ESOs to systematically test how their algorithms may amplify exposure to harmful content, encourage addictive behavior, or trigger repeated digital trauma.

Overall, the current model for protecting children from cyberviolence in Indonesia contains many elements aligned with the Convention on the Rights of the Child (CRC) and General Comment No. 25 on children's rights in the digital environment. However, it remains fragmented, partially oriented, and has not yet formed a comprehensive, consistent, and child-rights-centered framework. On the one hand, penal instruments such as the ITE Law and the Child Protection Law have provided a legal basis for criminalizing acts relevant to Articles 19 and 34 of the CRC, including various forms of violence and sexual exploitation of children mediated by information technology. On the other hand, the TUNAS Government Regulation and a series of non-penal instruments—the Ministry of Education, Culture, Research, and Technology's Digital Literacy Guidelines, the National Digital Literacy Movement (Siberkreasi), the PPKSP Technical Guidelines 49/M/2023, outreach and training programs, and the development of the belajar.kemdikbud.go.id platform—demonstrate the state's commitment to fulfilling its positive obligations in the dimensions of prevention, education, governance, and strengthening the capacity of the parenting ecosystem. From a normative perspective, this framework has internalized several core principles of the CRC and GC No. 25: the best interests of the child, protection from all forms of violence, the importance of digital literacy, non-discrimination, and recognition of the role of private digital actors. However, when tested against the standard of "all appropriate legislative, administrative, social, and

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

educational measures" in Article 19 of the CRC and the holistic approach of GC No. 25, it is clear that the existing model is far from adequate to address the complexity of violence against children in cyberspace.

The ITE Law and the Child Protection Law have affirmed the state's obligation to protect children from violence and exploitation, including those mediated by technology, by regulating the crimes of child pornography, sexual exploitation, deceit, and indecent inducement, and various forms of physical and psychological violence. From the CRC's perspective, this configuration can be considered relatively compliant with Articles 19, 34, and 39: the state not only recognizes children's rights to protection but also provides law enforcement mechanisms, criminal penalties, and a special protection framework that can, in theory, be extended to the digital realm. Similarly, the basic principles of the Child Protection Law – non-discrimination, the best interests of the child, the right to life, growth and development, and respect for the views of the child – are declaratively aligned with the general principles of the CRC and the general principles of GC No. 25 concerning non-discrimination, best interests, the right to development, and respect for the views of the child. The construction of state obligations, funding arrangements, the establishment of the Indonesian Child Protection Commission (KPAI), and the special protection scheme (Articles 59–59A) also provide an institutional structure compatible with the demands of GC No. 25. 25 for online protection to be integrated into existing national child protection systems.

The TUNAS Government Regulation strengthens this compliance dimension by explicitly incorporating principles closely aligned with GC No. 25: a risk-based approach, safety-by-design and privacy-by-design obligations, age verification settings, high-privacy default settings, a prohibition on manipulative practices and child profiling, and the affirmation that the best interests of children must be placed above the commercial interests of Electronic System Providers. By regulating the obligations and oversight of Electronic System Operator as private digital actors, this PP normatively fulfills the demands of GC No. 25 that the state should not stop at general regulations, but also regulate the design of digital services, system architecture, and business practices of technology companies to ensure children's protection from the risks of digital content,

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

contact, and behavior.[19] From an international legal perspective, this is significant progress because it marks a shift from the paradigm of "child-proofing the child" to "child-proofing the digital environment".

However, despite this level of normative conformity, several gaps remain that prevent it from fully aligning with the CRC and GC No. 25, particularly in the context of protecting children from cyber violence. First, almost all penal instruments still operate from an analog paradigm: there is no explicit recognition of the category of "cyber violence against children." Digital violence, such as cyberbullying, doxing, reputational damage, the distribution of embarrassing content, or non-explicit sextortion, has not been regulated as a specific cluster of violence against children, but rather is accommodated fragmentarily through a combination of general provisions on psychological violence, defamation, or morality. This has implications for weak legal certainty, inconsistent enforcement, and difficulties in proving, ultimately leading to the unfulfilled standards for protection against digital violence as outlined in GC No. 25.

Secondly, the existing regime remains highly actor-centric and repressive, while the dimensions of recovery and social reintegration for child victims of digital violence have not been specifically and operationally regulated. Article 39 of the CRC requires the state to take all necessary steps to ensure the physical and psychological recovery and social reintegration of victims in an environment that restores their dignity and self-esteem. In the context of digital violence, this includes the need for content takedown, restoration of digital traces, psychosocial support for re-traumatization due to the virality of content, and protection from re-victimization in online and offline environments. In fact, the ITE Law, the Child Protection Law, and the TUNAS Government Regulation do not yet provide a recovery scheme explicitly designed to address the characteristics of "digital trauma"; the recovery function is more assumed to be the domain of sectoral policies or ad hoc initiatives, rather than a legally enforceable right of victims. This demonstrates the gap between the state's obligations under the CRC and the actualization of victim recovery within the framework of child protection in cyberspace.

[19] Devi Novira, Et Al,' Legal Protection of Children's Personal Data in the Digital Era', Journal of Social Research, 3(9), (August 2024):1-10, https://doi.org/10.55324/josr.v3i9.2195

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

Third, although the TUNAS Government Regulation regulates the administrative obligations of ESE and provides administrative sanction mechanisms, it cannot—hierarchically or materially—create penal categories or criminal enforcement authority for forms of sexual exploitation and serious violence in the digital space. The absence of an explicit normative bridge between the TUNAS Government Regulation and the criminal regimes in the ITE Law and the Child Protection Law means that the state's obligation to take "all appropriate measures," including effective cross-sectoral criminal enforcement, is not fully guaranteed. In other words, the TUNAS Government Regulation strengthens the governance and prevention dimensions. However, it does not address the need for systemic integration between administrative regulations and criminal enforcement as recommended by GC No. 25 within the framework of comprehensive policy and strategy.

This situation simultaneously serves as both an academic and normative justification for the need to design a "re-model" for protecting children from violence in cyberspace in Indonesia. This re-model must be built on the principles of the CRC and GC No. 25, coherently combining penal and non-penal approaches, strengthening victim recovery and reintegration, integrating platform governance and algorithmic risk, and placing children at the center of policy design. Therefore, formulating an ideal protection model involves not only patching existing deficiencies but also restructuring the architecture of child protection in the digital space in a more comprehensive, equitable manner, and consistent with constitutional mandates and international standards on children's rights.

Indonesia–Malaysia Comparative Synthesis: The Key Need to Design an Ideal Model of Child Protection from Cyber Violence in Indonesia

A comparison of protection models for children's rights to freedom from violence in cyberspace between Indonesia and Malaysia indicates that both countries have sought to strengthen child protection through regulations imposing obligations on digital service providers. However, after researchers tested the Penal approach protection models of both countries using the Convention on the Rights of the Child and General Comment No. 25, they found differences in the regulations. Indonesia is relatively stronger in designing

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

preventive governance and administrative oversight of electronic system providers. In contrast, Malaysia tends to prioritize operational considerations when formulating technical obligations, layered reporting procedures, and accountability tools. The results of this comparison will not be used to replicate Malaysian legal instruments into Indonesian legal instruments. Rather, they will be used to compile a gap map that highlights areas that need strengthening in designing a model for protecting children's rights free from violence in Indonesian cyberspace. The main comparisons are summarized in the following table.

Table 1: Comparison of Models of Protection of Children's Rights to be Free from Violence in Cyberspace between Indonesia and Malaysia

Dimensions	**Indonesia (current condition)**	**Malaysia (benchmark)**	**Gaps to the Convention on the Rights of the Child & General Comment No. 25**	**The direction of Indonesia's re-model (ius constituendum)**
Platform Obligations and Harmful Content Response Mechanisms	The Government Regulation on Governance of Electronic System Implementation in Child Protection strengthens platform governance-based prevention but does not explicitly require impact assessments of recommendation	The Online Safety Act 2024 (Act No. 866) establishes design-based prevention obligations, including specific obligations for child users (control of recommendation systems, restrictions on features that prolong use), as	Indonesia's obligations have not addressed the "systemic risks" arising from algorithms and platform design, even though General Comment 25 requires child-centered service design	Require algorithmic impact assessments and risk audits of recommendation systems; limit addictive design features for child accounts; and require a measurable, auditable, and regularly reported

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

	systems or limit designs that encourage excessive use by children.	well as an online safety plan as a compliance document.	and safety "from design."	"child safety plan" document.
Child-Friendly Reporting Mechanisms and Response Services	The Government Regulation on the Governance of Electronic Systems for Child Protection provides a complaint channel but does not yet regulate in detail safe and child-friendly digital reporting, does not regulate the review of report rejections, and has not yet established standard cross-agency procedures for rapid response and the securing of digital evidence.	The Online Safety Act 2024 requires acknowledgement of receipt of reports, written status updates, assessments within a specified timeframe, and a review mechanism for rejections. For priority harmful content, immediate action is required, including temporary access restrictions and subsequent decision-making.	According to General Comment 25, reporting must be truly child-friendly (easy, safe, identity-protecting, and prompt) and linked to effective responses; without review, without differentiating levels of harm, and without safeguarding evidence, reporting risks relegating itself to administrative procedures.	Establish reporting as a "procedural right": require confirmation of receipt and handling status, response deadlines, and review of denials; implement a distinction between priority and non-priority cases; mandate the safeguarding of digital evidence; and incorporate child participation in evaluating the mechanism's effectiveness.
Victim Recovery and	The Government Regulation on the Governance of	The Child Act 2001 provides a robust child	Article 39 of the Convention on	Add a chapter on recovery for victims of digital

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

Recovery Mechanisms	Electronic Systems for Child Protection focuses on prevention and administrative sanctions, but does not include any obligation to rehabilitate victims of digital violence, including referrals for recovery services and digital footprint recovery. The recovery framework in the Child Protection Law remains insufficiently digital and therefore does not address repeated trauma or persistent digital footprints.	protection system for recovery, including recognition of emotional harm and rapid response through institutional mechanisms; the Online Safety Act 2024 strengthens the mechanism for making harmful content inaccessible as a regulatory remedy, but still requires operational integration for full recovery of victims.	the Rights of the Child and General Comment No. 25 require physical and psychological recovery and social reintegration; in the digital context, recovery must include eliminating ongoing sources of trauma (content distribution, re-uploading, identity theft). Indonesia does not yet have operational digital victim recovery norms linked to reporting and content removal.	violence: mandatory referrals for ongoing psychosocial services, a "digital recovery package" (cross-platform deletion, prevention of re-uploading, restoration of digital traces), and an integrated response chain from reporting to recovery; as well as reformulation of the offense so that child exploitation is not reduced to common morality and digital evidence does not burden child victims.

Source: Author's interpretation

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

The table above shows that the main gap in Indonesia lies not in the absence of norms, but in the following three areas. First, platform obligations still don't fully address the systemic risks posed by recommendation systems and designs that encourage excessive use (endless scrolling). Second, available reporting mechanisms are not child-friendly, safe, and integrated with rapid response and digital evidence security. Third, there are no explicit, technically operational norms for reparation for victims of cyber violence. This includes repairing digital footprints to prevent re-traumatization.

Therefore, the formulation of an ideal model for protecting children's rights from violence in Indonesian cyberspace is the result of academic reasoning derived from a critical evaluation of the current protection model. If the Convention on the Rights of the Child is understood as a minimum standard, then the ideal model (ius constituendum) must be formulated based on "minimum requirements" that effectively protect children's rights. These minimum requirements serve as a measuring framework: without fulfilling these minimum components, child protection in the digital space will always be fragile, fragmented, or merely procedural. Based on the Convention on the Rights of the Child and General Comment No. 25, these minimum requirements include at least five components.[20]

First, safety by design. The ideal model should ensure child safety is built into the service architecture: systemic risk controls, including algorithmic risks and designs that encourage overuse; child data protection as a baseline standard; and child-friendly safety tools. Second, child-friendly and secure reporting mechanisms. Reporting is not only available but also designed for children to use: simple, protects identity, minimizes secondary victimization, and provides certainty of process (confirmation of receipt, handling status, review). Third, a rapid response based on the level of harm accompanied by evidence preservation. Given that digital evidence is easily lost and impacts can spread within hours, the ideal model needs to distinguish between priority and non-priority cases,

[20] Yohannes Eneyew Ayalew, Valerie Verdoodt, Eva Lievens, 'General Comment No. 25 on Children's Rights in Relation to the Digital Environment: Implications for Children's Right to Privacy and Data Protection in Africa', Human Rights Law Review, 24(3), (June 2024): 1-18, https://doi.org/10.1093/hrlr/ngae018

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

allow for proportionate interim measures, and integrate digital evidence preservation to prevent child victims from facing a disproportionate burden of proof. Fourth, victim recovery, including digital recovery. Recovery should include psychosocial services and digital footprint recovery mechanisms to break the cycle of re-victimization, including technical support to remove, limit the distribution, and prevent re-uploading of content harmful to children. Fifth, cross-sector coordination and accountability. The ideal model should build an integrated chain of protection across institutions and regimes, accompanied by performance indicators and evaluation mechanisms so that protection can be measured and accountability held.

Based on the above considerations, the draft requirements for formulating an ideal integrative model for the Protection of Children's Rights to be Free from Violence in Cyberspace in Indonesia, through both penal and non-penal approaches, were identified.

Table 2: Design of an Ideal Integrative Model for the Protection of Children's Rights to be Free from Violence in Cyberspace in Indonesia

Protection Chain Stage	Field Situation	Non-Penal Path (Front Line))	Penal Path (Escalation)	Minimum Principles/Standards	Key Indicators
Prevention of systemic risk	Risks arise from risky service design, recommendations, and features.	Safety standards by design; due diligence; algorithm impact audits; design restrictions that encourage overuse in children.	Not dominant (criminal is not the main instrument).	Risk-based governance; age-appropriate design; amplification control.	Reducing exposure to harmful content; following up on audit results.
Child-friendly reporting	Children/families need a safe and easy entrance.	Multi-channel one-stop shop; status tracking; confidentiality SOP.	Reports that meet the threshold can be flagged for escalation.	Accessibility, confidentiality, and accountability of the process.	Time of report recognition; level of report completion.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

Rapid response based on danger level	Priority content must be stopped immediately to prevent further spread.	Immediate mitigation (temporary takedown/reduction of coverage/access closure).	Activate law enforcement if there are criminal/high-risk elements.	Priority protocol; response time standard.	Mitigation time; number of priority cases handled.
Minimum digital evidence security	Evidence is quickly lost; families are often technically incapacitated.	Minimum evidence SOP; service node technical assistance; referral to forensic unit.	Formal preservation; chain of custody; request for data in a legitimate procedure.	Minimum evidence does not burden the victim; the evidence's validity is maintained.	Percentage of cases with minimum evidence; preservation time.
Law enforcement (escalation path)	The perpetrators must be prosecuted and prevented from repeating their actions.	Process assistance, identity protection, and victim support.	Child-friendly investigation – prosecution –sentencing; cross-jurisdictional cooperation.	Child-friendly justice; due process; victim protection.	Process consistency; no identity leaks; successful enforcement.
Victim recovery (psychosocial + digital footprint)	Trauma can recur; content can resurface.	Rujukan layanan psikososial; pemulihan jejak digital; pendampingan keluarga.	Recovery does not wait for a verdict; protection of victims throughout the criminal process.	Victim-centric; recovery has been running in parallel since reporting.	Reference time, re-upload rate, and recovery sustainability.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

System monitoring and evaluation	Without indicators, protection becomes symbolic.	Compliance audits; secure transparency reports;	Escalation of enforcement in the event of gross negligence or repeated violations.	Indicator-based accountability; policy correction.	Key Performance Indicators (KPI) response, evidence, recovery, and audit compliance.

Data Source: Author's Interpretation.

The ideal model doesn't place penal and non-penal approaches in parallel or in separate branches. Non-penal approaches should be the frontline of prevention and rapid response through platform risk governance, literacy, reporting, and mitigation. The penal approach serves as an escalation track when there is a criminal element, high risk of recurrence, or the need for coercive state intervention to stop violations and prosecute perpetrators. In an integrative design, victim recovery must occur across all channels. Recovery does not await a criminal verdict; it must begin with reporting to prevent re-traumatization and re-victimization. This integration ensures that the state not only prosecutes perpetrators but also reduces systemic risks and restores victims as part of its comprehensive child protection obligations.

Based on the description above, the ideal model for child protection in cyberspace places a non-penal approach as a preventive-structural pillar through platform risk governance, integrated reporting, and operational recovery services, while simultaneously linking it with a penal approach as a digital evidence-based escalation pathway and child-friendly justice. The values of justice in the Indonesian legal system are also rooted in Pancasila.[21] With this design, prevention, rapid response, enforcement, and recovery operate as a coherent, measurable, and accountable series of protections, thereby

[21] Edi, Prasetyo, Andri Winjaya Laksana, 'Legal Responsibility of Medical Specialist For Illness or Death: The Essence of Justice', Jurnal Hukum Unissula, 42(1), (March 2026): 97-114 https://dx.doi.org/10.26532/jh.v42i1.49705

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

simultaneously closing the systemic risk gap, the reporting-response-evidence gap, and the victim recovery gap.

Legitimacy of Islamic Legal Theory *maqāṣid al-sharī'ah* in the Integrative Ideal Model of Protection of Children's Rights to be Free from violence in cyberspace in Indonesia

In the design of child protection in cyberspace outlined above, the *maqāṣid al-sharī'ah* can serve as an ethical foundation that complements the positive legal framework. Conceptually, *maqāṣid al-sharī'ah* departs from the teleological perspective that law does not end with formal compliance with norms, but is directed toward protective goals that guarantee human dignity and prevent social harm.[22] In the context of child protection, this approach is relevant because cyberspace presents forms of violence that are not always easily addressed through legalistic logic alone (e.g., systemic risks from platform design, algorithmic amplification, and persistent digital footprints). Therefore, maqāṣid can be read as a normative justification for child protection in cyberspace, orienting it towards substantive outcomes: preventing harm, protecting rights, and restoring victims with dignity.

First, the value of dignity (*karāmah*) confers ethical legitimacy on children as subjects of rights who should not be reduced to "objects of regulation" or mere victim statistics.[23] *Karāmah* demands protection that rejects all forms of human degradation, including degradation arising not only from the perpetrator but also from child-unfriendly handling processes, identity leaks, or intimidating reporting mechanisms. Thus, *karāmah* strengthens the argument that child protection policies in cyberspace must be child-centered: maintaining confidentiality, minimizing re-victimization, and ensuring psychosocial recovery from the outset. In this logic, "justice" is not simply understood as

[22] Iffatin Nur, Syahrul Adam, M. Ngizzul Muttaqien,' Maqāṣid al-Sharī'at: The Main Reference and Ethical-Spiritual Foundation for the Dynamization Process of Islamic Law',AHKAM, 20(2), (2020), https://share.google/3QNteaM3FXyC8oTDC

[23] Bilal Ahmad Malik, 'Dignity Embodies Duty: Islamic Perspective on Combating Hate Speech', DE Gruyter, 20(1), (December 2022): 1-27, https://doi.org/10.1515/mwjhr-2022-0003

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

punishing the perpetrator, but also as restoring the dignity of children who have been injured by exposure, stigma, or the loss of digital control over their bodies and identities.

Second, the value of public benefit (*maṣlaḥah*) in building child protection in cyberspace must prioritize prevention and risk reduction as a moral priority. *Maṣlaḥah* positions the law as an instrument aimed at providing public benefits and preventing mafsadah (harm)[24], thus aligning with a risk-based governance approach: safety standards from design, restrictions on risky features, impact audits, and rapid response to harmful content. From a *maṣlaḥah* perspective, delays in mitigating or in allowing the spread of content harmful to children are not merely technical issues but ethical failures, because they allow the harm to spread. Therefore, *maṣlaḥah* strengthens the policy orientation towards the effectiveness of protection—measured by reduced exposure, rapid response, and controlled re-distribution—as a tangible manifestation of the "benefit" that must be realized through digital governance.

Third, the value of honor (*hifẓ al-'ird*) provides the most operational legitimacy in the context of digital-based violence related to sexuality, exploitation, blackmail, and the dissemination of intimate content. *Hifẓ al-'ird* asserts that human honor is an imperative that must be safeguarded[25]; thus, child protection must emphasize confidentiality, anti-exposure, and reputation restoration and control of digital identity. In cyberspace, honor is not only attacked at the time of the incident but can also be continuously damaged through persistent digital traces and re-uploads. Therefore, *hifẓ al-'ird* provides an ethical basis for recognizing that victim recovery should not stop at the psychological level, but must include the restoration of digital traces: mechanisms for deletion, prevention of re-uploads, and technical support that restores the victim's control over their self-representation. Here, it is clear that the maqāṣid provide an ethical argument for

[24] Asmawi, Arsadani, Hanna,' Theory of Maslahah (Public Interest) and Its Relevance to Indonesian Corruption Eradication Law.', In Proceedings of the 1st International Conference on Recent Innovations (ICRI 2018): 148-157, https://doi.org/10.5220/0009920101480157

[25] Riska Harnysah Harahap, Risalan Basri Harahap,' Maqashid Ash-Sharia Principles in Child Protection', El-Thawalib, 3(4), (August 2022):691-701, https://doi.org/10.24952/el-thawalib.v3i4.5945

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

integrating the dimension of "digital recovery" into victims' rights, not as an additional policy.

Fourth, the value of access justice (*'adl*) serves as a legitimacy that child protection must be equal and inclusive, regardless of social class, digital literacy, or proximity to service centers. [26]*'adl* demands that children in 3T areas, children with disabilities, or families with limited technical capabilities still have equal access to reporting channels, assistance, minimum evidence security, and recovery services. In this context, justice is not merely procedural equality, but rather equality of ability to obtain protection. Therefore, *'adl* strengthens the argument for the need for easily accessible multi-channel reporting channels, SOPs that do not burden victims with technical requirements, and minimum service standards that can be accounted for through performance indicators. Access justice also demands structural accountability: protection systems must be auditable and evaluable so that they work not only for viral cases, but for all children.

Thus, the *maqāṣid al-sharī'ah* provides strong theoretical legitimacy for positioning Islamic legal values as an ethical framework for strengthening child protection in cyberspace. *Karāmah* ensures protection is oriented towards restoring dignity; *maṣlaḥah* emphasizes the priority of prevention and effectiveness; *hifẓ al-'ird* provides a normative basis for confidentiality and the restoration of digital traces; and *'adl* locks in the necessity of equal and inclusive access to protection. These four values, when integrated, provide theoretical justification for the design of child protection in cyberspace as a system that is not only legal but also substantially just, benefit-oriented, and that guarantees the honor and dignity of children as a trust that must be maintained.

CONCLUSION

This study concludes that the current configuration of child protection policies against cyber violence in Indonesia and Malaysia reflects a combination of penal and non-

[26] Ainul Masruroh, Mahmutarom Mahmutarom, 'Safeguarding Children from Online Sexual Exploitation: A Legal and Maqāṣid al-Sharī'ah Approach', Islamica, 19(1), (September 2024):168-198, https://doi.org/10.15642/islamica.2024.19.1.168-198

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

penal regulatory approaches that have generally incorporated the principles of the Convention on the Rights of the Child (CRC) and General Comment No. 25 (GC25). However, the implementation of these frameworks remains fragmented and has not yet been fully consolidated within a comprehensive, child-rights-centered protection system. The comparative analysis indicates that effective protection requires an integrated regulatory architecture rather than isolated sectoral policies. Such an approach should establish a coherent cycle of protection comprising risk-based prevention, reporting, rapid response mechanisms, digital evidence protection, content mitigation or removal, and referral systems for recovery, including the restoration of children's digital footprints and psychological wellbeing.

Within this framework, contemporary Islamic ethical perspectives derived from *maqāṣid al-sharī'ah* provide an important normative foundation for strengthening the governance of cyber child protection. The principles of *karāmah* (human dignity), *maṣlaḥah* (public benefit), *ḥifẓ al-'irḍ* (protection of honor and personal integrity), and *'adl* (justice) complement international human rights standards by emphasizing harm prevention, dignified recovery, and equal access to protection services. The integration of CRC/GC25 norms with these ethical principles offers a more holistic model of protection, where the effectiveness of child protection in the digital environment is measured not only by legal compliance or punishment of perpetrators, but also by the reduction of systemic digital risks, the restoration of children's control over their digital identity and representation, and the availability of inclusive protection services for all children. For future research, empirical and socio-legal studies are needed to assess the practical implementation of this integrative protection model, particularly in evaluating institutional readiness, cross-sectoral coordination, and the effectiveness of digital governance mechanisms in responding to cyber violence against children. Further comparative research involving broader jurisdictions and interdisciplinary approaches may also enrich the development of child protection frameworks that integrate international human rights standards with contemporary Islamic ethical perspectives in the digital era.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

ACKNOWLEDGEMENTS

The author hereby expresses profound appreciation to the Rector of Universitas Sebelas Maret (UNS) for his unwavering support, leadership, and commitment to fostering an academic climate conducive to meaningful scholarly work. The author also extends sincere gratitude to the Rector of Sultan Agung Islamic University (UNISSULA) Semarang and the Dean of the Faculty of Law, UNISSULA, for their continued support, institutional guidance, and commitment to strengthening academic excellence. Deep gratitude is further conveyed to the entire academic community of UNS and UNISSULA—including faculty members, administrative personnel, and supporting staff—whose dedication, cooperation, and professional assistance have significantly contributed to the successful completion of this research. Their collective efforts and encouragement are sincerely acknowledged and deeply valued.

AUTHOR CONTRIBUTIONS STATEMENT

RAP contributed to the conceptualisation of the research framework, developed the overall study design and methodology, and led the drafting of the manuscript. HH supervised the research process, strengthened the theoretical foundations, and provided critical revisions to enhance the manuscript's conceptual coherence and methodological rigor. MR conducted the comparative legal analysis, handled statutory and doctrinal interpretation, and integrated contemporary perspectives on cyberspace governance and child protection into the final manuscript.

CONFLICT OF INTEREST

The authors declare that there are no conflicts of interest in relation to this research. The study was conceived, conducted, and prepared independently, and no financial, institutional, or professional relationships influenced the research design, data collection, analysis, interpretation, or conclusions. All materials and information were obtained and used in accordance with applicable academic ethical standards. The views and findings presented in this article represent the authors' own scholarly assessment and are free from external interference, ensuring the integrity and credibility of the study.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457

AI USAGE STATEMENT

AI tools were used solely for language editing and formatting. All ideas, analyses, interpretations, and conclusions are entirely the authors' own, and all AI-assisted outputs were reviewed to ensure academic integrity.

BIBLIOGRAPHY

Adelia Nur Cahyani, et al.,' Psychosocial Intervention as An Effort to Prevent Victimization of Boy Victims of Sexual Violence', JKPI: Jurnal Konseling Pendidikan Islam, 6 (2), (May 2025): 71-83, https://doi.org/10.32806/jkpi.v6i2.777

Agam Ibnu Asa, 'The Evolution of Ronald Dworkin's Legal Philosophy: From Interpretivism to Integrity', Abjad: Journal of Humanities & Education, 3 (2), (August 2025): 111-124, https://doi.org/10.62079/abjad.v3i2.88

Ainul Masruroh, Mahmutarom Mahmutarom, 'Safeguarding Children from Online Sexual Exploitation: A Legal and Maqāṣid al-Sharī'ah Approach', Islamica, 19 (1), (September 2024):168-198, https://doi.org/10.15642/islamica.2024.19.1.168-198

Asmawi, Arsadani, Hanna,' Theory of Maslahah (Public Interest) and Its Relevance to Indonesian Corruption Eradication Law.', In Proceedings of the 1st International Conference on Recent Innovations (ICRI 2018): 148-157, https://doi.org/10.5220/0009920101480157

Ateret Gewirtz-Meydan, 'The Complex Experience Of Child Pornography Survivors', Child Abuse & Neglect, Volume 80, (June 2018): 238-248, https://doi.org/10.1016/j.chiabu.2018.03.031

Bilal Ahmad Malik, 'Dignity Embodies Duty: Islamic Perspective on Combating Hate Speech', DE Gruyter, 20 (1), (December 2022): 1-27, https://doi.org/10.1515/mwjhr-2022-0003

Devi Novira, et al.,' Legal Protection of Children's Personal Data in the Digital Era', Journal Of Social Research, 3 (9), (August 2024): 1-10, https://doi.org/10.55324/josr.v3i9.2195

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457
Dylan Aldianza Ramadhan, Charina Putri Besila, 'The Phenomenon of Sexual Violence among Adolescents in the Jurisdiction of the West Jakarta National Police Resort and Its Prevention Efforts', Fiat Justisia, 13 (2), (April 2019): 115-128, https://doi.org/10.25041/fiatjustisia.v13no2.1574

ECPAT, INTERPOL, and UNICEF, 'Disrupting Harm in Malaysia: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence Against Children (2022), https://safeonline.global/wp-content/uploads/2023/12/DH_Malaysia_ONLINE_FINAL.pdf

Edi, Prasetyo, Andri Winjaya Laksana, 'Legal Responsibility of Medical Specialist For Illness or Death: The Essence of Justice', Jurnal Hukum Unissula, 42 (1), (March 2026): 97-114 https://dx.doi.org/10.26532/jh.v42i1.49705

Gevan Naufal Wala, 'Legal Protection for Child Victims of Digital-Based Sexual Crimes', Imperium Research, 1 (1), (July 2025): 30-37, https://doi.org/10.38035/IMPERIUM.v1i1

Iffatin Nur, Syahrul Adam, M. Ngizzul Muttaqien,' Maqāṣid al-Sharī'at: The Main Reference and Ethical-Spiritual Foundation for the Dynamization Process of Islamic Law', AHKAM, 20 (2), (2020), https://share.google/3QNteaM3FXyC8oTDC

Ipah Hatipah, Rumba Triana, Syaeful Rokim, 'Anak Sebagai Qurratu A'yun Dalam Perspektif Al-Qur'an', Al - Tadabbur: Jurnal Ilmu Al-Qur'an dan Tafsir, 3 (2), (October 2018): 137-156, https://doi.org/10.30868/at.v3i02.314

Kementerian Pembangunan Wanita, Keluarga dan Masyarakat, Malaysia, 'Laporan Pemantauan Media KPWKM', (Oktober 2025), https://kpwkm.gov.my/uploads/content-downloads/file_20251027110004.pdf

Laksana, Andri Winjaya, Akhmad Ikraam, and Anila Robbani. "The Liability of Criminal Law for Perpetrators of Goods Embezzlement." *Journal of Justice Dialectical* 2, no. 2 (2024): 70-83. DOI: https://doi.org/10.70720/jjd.v2i2.50

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457
Laksana, Andri Winjaya, Adhi Budi Susilo, Peni Rinda Listyawati, Setiawan Widiyoko, and Toni Triyanto. "Legal Uncertainty in Law Enforcement for Drug Addicts Resulting in Criminal Disparity." *Yuridika* 40, no. 2 (2025): 253-270. DOI: https://doi.org/10.20473/ydk.v40i2.68153

Laura Lundy, 'Children's Rights from an International Perspective', the Rights of the Child (April 2023): 3-6, https://doi.org/10.1163/9789004511163_002.

Mashdurohatun, Anis, Eid Abed Alhaleem Maslat Harahsheh, Muhammad Irwan Datuiding, Abun Hasbulloh Syambas, and Prasetiyo Adhi Wibowo. "Contemporary Reassessment of Punishment in Islamic Sharia and Secular Law: A Comparative Study of Justice and Penal Philosophy." *MILRev: Metro Islamic Law Review* 5, no. 1 (2026): 80-100. DOI: https://doi.org/10.32332/milrev.v5i1.11887

Muhammad Rafifnafia Hertianto, 'Tinjauan Yuridis Terhadap Perlindungan Anak Dalam Ruang Siber Di Indonesia', jurnal Hukum dan Pembangungan (JHP), 51(3), (September 2025):555-573, http://dx.doi.org/10.21143/jhp.vol51.no3.3123

Muhammad Rayhan Murtadha, 'Psyshield Center: A Collaborative Program For Indonesian Students To Combat Cybersexual Exploitation', GPH-International Journal of Educational Research, 8(04), 9april 2025):22-34, https://doi.org/10.5281/zenodo.15347718

Murray, Lisa, Penny Levickis, Laura McFarland, Patricia Eadie, Lynn Lee-Pang, Jon Quach, and Jane Page, 'Supporting Young Children's Social–Emotional Wellbeing in Early Childhood Education and Care: Perspectives from the Sector' , Education Sciences 15, no. 5 (May 2005): 569, https://doi.org/10.3390/educsci15050569

Rattry Risnawaty,' The Concept of Forming Shaleh Children According to Islamic Education', International Journal Education and Computer Studies (IJECS) 3 (2), (July 2023): 42-51, https://doi.org/10.35870/ijecs.v3i2.1802

Riska Harnysah Harahap, Risalan Basri Harahap,' Maqashid Ash-Sharia Principles In Child Protection', El-Thawalib, 3(4), (August 2022): 691-701, https://doi.org/10.24952/el-thawalib.v3i4.5945

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 427-457
Seung Min Bae,' Characteristics and Treatment of Cyberviolence Trauma in Children and Adolescents', J Korean Acad Child Adolesc Psychiatry; 35 (3), (March 2024): 169-174, https://doi.org/10.5765/jkacap.240005

Witasya Aurelia Sulaeman. Beniharmoni Harefa, Handar Subhandi Bakhtiar,' Law Enforcement Against the Crime of Sexual Exploitation of Children in the Legal Systems of Indonesia and Malaysia', International Journal of Social Welfare and Family Law (IJSW), 2(3), (June 2025):1-16, https://doi.org/10.62951/ijsw.v2i3.362

Yohannes Eneyew Ayalew, Valerie Verdoodt, Eva Lievens, 'General Comment No. 25 on Children's Rights in Relation to the Digital Environment: Implications for Children's Right to Privacy and Data Protection in Africa', Human Rights Law Review, 24(3), (June 2024): 1-18, https://doi.org/10.1093/hrlr/ngae018