GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

**DOI:** https://doi.org/10.38035/gijlss.v4i2


# Child Rights Protection Compliance Ecosystem in Indonesia: Harmonization of the CRC, Digital Risks, Legal Pluralism, and Participation

**Muhammad Fachri Said[1*], Syawal Amirul Syah[2], Andika Prawira Buana[3], Andi Sri Rezky Wulandari[4]**
[1]Universitas Muslim, Makasar, Indonesia, Fachri.said@umi.ac.id
[2]Universitas Almarisah Madani, Makasar, Indonesia, syawalamirulsyah@univeral.ac.id
[3]Universitas Muslim, Indonesia, Makasar, Indonesia, andika.prawira@umi.ac.id
[4]Universitas Muslim, Indonesia, Makasar, Indonesia, srirezky.wulandari@umi.ac.id

*Corresponding Author: Fachri.said@umi.ac.id[1]

**Abstract:** This article examined the minimum obligations of the Convention on the Rights of the Child (CRC) can be operationalized in the Indonesian context, which was characterized by legal pluralism and accelerating digital risks. Using normative legal research methods through legislative, conceptual, and limited comparative approaches, this study maps CRC standards and General Comments (particularly GC 5, GC 12, and GC 25) onto national norms, institutional mandates, and implementation-enforcement mechanisms. The findings showed the main problem was not merely a lack of norms, but rather an implementation enforcement gap in the compliance infrastructure: coherence between regimes (child protection, data protection, and platform governance), capacity and coordination across actors, and the absence of auditable procedural indicators to test best interests, protection, and participation. This article proposes a "compliance ecosystem" framework that combines (i) implementation guidelines based on Best Interests Assessment and reason-giving as a bridge for legal pluralism, (ii) protective regulations in the digital space that place the obligation of risk assessment and mitigation on electronic system/platform operators, and (iii) child participation designs that can demonstrate influence through procedural standards and outcome-based monitoring and evaluation.

**Keywords:** Children's rights, CRC, Legal Pluralism, Digital Risks, Personal Data Protection, Compliance Ecosystem, Child Participation.

## INTRODUCTION

Contemporary human rights law developments place children not merely as objects of welfare, but as legal subjects (rights-holders) with specific vulnerabilities. Consequently, general human rights guarantees were often inadequate without protection, services, and remedies specifically designed for children. The consolidation of international normative

standards is articulated through the Convention on the Rights of the Child (CRC), which establishes minimum standards for states' obligations to respect, protect, and fulfill children's rights through legislation, policies, services, and effective redress mechanisms (United Nations, 1989).

However, the formal adoption of international standards does not automatically result in effective protection at the domestic level. The UN Committee on the Rights of the Child emphasizes the existence of "general measures of implementation" as a condition for the CRC to work in practice, including harmonization of legislation, cross-sectoral coordination, independent monitoring, budgeting, data collection, and remediation that is accessible to children (Committee on the Rights of the Child, 2009). In other words, enforcement needs to be understood broadly: not only criminal prosecution, but also the delivery of protection services, prevention, risk identification, referral, recovery, and administrative accountability (Hodgkin et al., 2007).

This article departs from the thesis that the main problem in the implementation of children's rights is the compliance ecosystem—namely, the integrated configuration of (i) the quality and clarity of rules, (ii) the design of mandates and institutional capacity, and (iii) the operational mechanisms of implementation and the accountability tools (implementation). The effectiveness of CRC obligation harmonization is therefore assessed through minimum testable indicators, such as: consistency of norms and division of authority; SOPs for cross-sector coordination and referral; adequacy of funding and human resources; child-friendly complaint and redress channels; and corrective and transparent monitoring & evaluation (M&E).

The urgency of strengthening the compliance ecosystem is becoming increasingly apparent in a pluralistic legal system. The literature on legal pluralism asserts that the social validity of a norm is not determined solely by formal legality, but rather by the coexistence and competition of various normative orders that exist within society (Griffiths, 1986)(Merry, 1988). For Indonesia, this pluralism serves as a "stress test" for the minimum standards of the CRC: whether the principles of best interests, non discrimination, and protection from violence are truly the testing standards in decisions and service practices when encountering diverse socio-religious norms.

The next complexity comes from the acceleration of digital technology, which expands the forms of child vulnerability for example, cyberbullying, online exploitation, privacy violations, and the processing of children's data for commercial purposes. General Comment No. 25 affirms that CRC obligations apply fully in the digital space, requiring states to adapt regulations, governance, oversight, and effective remedies (Committee on the Rights of the Child, 2021). A doctrinal reading of GC25 also emphasizes the need for contextual translation, particularly regarding children's privacy and data protection, so that international obligations are transformed into enforceable operational standards (Ayalew et al., 2024).

In addition, the dimension of child participation often stops at normative recognition. General Comment No. 12 emphasizes that the right to be heard requires mechanisms that allow children's views to be expressed and considered appropriately (Committee on the Rights of the Child, 2009). In the literature, Lundy's framework emphasizes that "voice" is not enough without space, audience, and influence meaning that the design of procedures must demonstrate how children's input actually influences decisions (Lundy, 2007).

Although previous studies have been rich in each of these areas CRC implementation, legal pluralism, child protection in the digital space, and child participation the limitations that remain prominent are the fragmentation of analysis and the absence of testable governance measurement tools. Many studies discuss pluralism as a context without providing measurable institutional indicators; digital studies highlight new threats without linking them to cross-sectoral compliance infrastructure; while participation studies are often

normative without procedural design, standards for proving "influence," and corrective M&E. In the context of Indonesia's multilevel governance, this gap weakens the state's ability to translate formal commitments into accountable practical protections (Griffiths, 1986)(Merry, 1988)(Committee on the Rights of the Child, 2003)(Hodgkin et al., 2007)(Committee on the Rights of the Child, 2021).

Therefore, the scientific contribution (novelty) of this article lies in three layers. First, conceptual contribution: shifting the focus from formal harmonization to substantive harmonization based on rules–institutions–implementation. Second, integrative contribution: integrating legal pluralism, digital risks, and child participation as a "stress test" into a single evaluation framework. Third, an operational contribution: proposing minimum auditable indicators such as coordination and referral SOPs, child-friendly complaint and redress channels, service standards, and corrective M&E that the effectiveness of child protection can be tested transparently and replicated across sectors/regions.

Based on this landscape, this article was guided by three research questions: (1) how do the CRC and General Comments shape the minimum standards of state obligations that must be operationalized at the domestic level; (2) how can the mapping of CRC obligations to Indonesian national norms and related institutions be carried out in a measurable manner; and (3) how can an ecosystem-based compliance harmonization model strengthen child protection amid legal pluralism and digital risks.

## METHOD

This study employs normative legal research (doctrinal legal research) using legislative and conceptual approaches. It examines the coherence of legal norms, institutional design, and implementation mechanisms in fulfilling CRC obligations in Indonesia.

Primary legal materials include the Convention on the Rights of the Child, Presidential Decree No. 36 of 1990, Law No. 23 of 2002 on Child Protection as amended by Law No. 35 of 2014 and Law No. 17 of 2016, Law No. 27 of 2022 on Personal Data Protection, Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 1 of 2024, and Government Regulation No. 71 of 2019. Secondary materials include the UN Committee on the Rights of the Child's General Comments (GC 5, GC 12, GC 25), CRC implementation guidelines, and relevant scholarly literature.

The analysis proceeds in three stages: (1) identifying minimum CRC obligations and general measures of implementation; (2) mapping these obligations onto national norms, institutions, and implementation mechanisms; and (3) assessing implementation gaps using minimum indicators (procedures, complaint/redress mechanisms, capacity, and monitoring and evaluation).

This study is limited to normative analysis without empirical measurement, aiming to provide a governance diagnosis and testable recommendations for further research.

## RESULTS AND DISCUSSION

This study finds that Indonesia has established a relatively comprehensive normative framework for the protection of children's rights through the integration of the Convention on the Rights of the Child (CRC) into national legal instruments, including child protection law, personal data protection law, and digital governance regulations. The mapping of CRC obligations to national norms, institutions, and implementation mechanisms indicates a shift from principle-based regulation toward a more duty-based and procedural compliance structure.

However, the findings reveal that the main challenge lies not in the absence of legal norms, but in an implementation–enforcement gap within the compliance ecosystem. This gap is reflected in several dimensions: lack of coherence across regulatory regimes (child

protection, data protection, and platform governance), fragmented institutional coordination, limited enforcement capacity, and the absence of auditable procedural indicators to operationalize key CRC principles such as best interests, protection, and child participation.

The analysis further shows that the existing legal framework remains institutionally fragmented, with responsibilities distributed across multiple agencies without a unified implementation mechanism. In addition, legal pluralism contributes to inconsistent application of child protection standards across different social and legal contexts, while digital governance frameworks have not yet fully translated child protection obligations into measurable risk-based and compliance-oriented standards.

Overall, these findings demonstrate that although Indonesia has achieved formal harmonization of CRC obligations, substantive implementation remains weak due to systemic gaps in governance, coordination, and accountability mechanisms.

**CRC Minimum Standards and General Measures of Implementation**

The CRC establishes four general principles that guide all implementation: non discrimination (Article 2), the best interests of the child (Article 3), the right to life, survival, and development (Article 6), and respect for the views of the child (Article 12). These principles are not merely declarative; they serve as standards for assessing policies, procedures, and decisions that affect children (United Nations, 1989).

The UN Committee on the Rights of the Child emphasizes that the implementation of the CRC requires "general measures" that include coherent legislation, cross-sectoral coordination, independent monitoring bodies, complaint mechanisms accessible to children, data collection, and rights-based budgeting (Committee on the Rights of the Child, 2003). Within the framework of state obligations, these general measures link norms with capacity and procedures so that rights do not remain mere text, but are realized as tangible services and protection. Operationally, state obligations can be understood through the respect–protect–fulfill framework. The respect dimension requires states to refrain from actions that violate children's rights (e.g., processing children's data without a legal basis). The protect dimension requires states to exercise due diligence to prevent and address violations by third parties including private actors and digital platforms. The fulfill dimension requires the state to provide child-friendly services, remedies, and access to justice.

**Mapping CRC Obligations to Indonesian National and Institutional Norms.**

Indonesia ratified the CRC through Presidential Decree No. 36 of 1990, which established the CRC as an important normative reference in the formulation and interpretation of child protection policies. At the legislative level, the main regime was established through the Child Protection Law “Law of the Republic of Indonesia Number 23 of 2002 Concerning Child Protection”. and its amendments (Law of the Republic of Indonesia Number 35 of 2014 on Amendments to Law Number 23 of 2002 on Child Protection, n.d.)(Law of the Republic of Indonesia Number 17 of 2016 Concerning the Stipulation of Government Regulation in Lieu of Law Number 1 of 2016 Concerning the Second Amendment ( ) to Law Number 23 of 2002 Concerning Child Protection into Law, n.d.), while issues of child privacy and data are reinforced through the Personal Data Protection Law (Law of the Republic of Indonesia Number 27 of 2022 Concerning Personal Data Protection, n.d.) and the obligations of platforms/PSEs are strengthened through the second amendment to the ITE Law (Law of the Republic of Indonesia Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions, n.d.). To test whether the harmonization is substantive, this article uses a layered mapping: CRC obligations → national norms → institutions → implementation mechanisms → minimum indicators. This mapping helps identify

breakpoints where international obligations lose their effectiveness due to procedural gaps, overlapping mandates, or unmeasurable indicators.

| CRC obligations | National norms | Institutions | Mechanisms | Enforcement | Indicator |
|---|---|---|---|---|---|
| Art. 3 (best interests); Art. 4(implement ation measures) | Law 23/2002 with. Law 35/2014; sectoral policies/standard operating procedures | KPPPA; Local Government; Law Enforcement Officials | Best Interests Assessment (BIA) + documentation of reasons; service referrals | Compliance audit; administrative sanctions; correction of decisions/proc edures | There is a BIA SOP; documented evidence of considerations; referral response time |
| Art. 12 (right to be heard) | Law 23/2002; child-friendly service/judicial procedures | Court; Police/prosecutor; social services | Child-friendly interviews; assistance; policy consultation forums | Internal oversight; remediation for violations procedures | Access to voice e-audience influence; evidence that children's views are considered (Lundy test) |
| Art. 16 (privacy) + GC25 (digital) | Law 27/2022 (Articles 25, 46); ITE Law in conjunction with Law 1/2024 (Article 16A) | PDP Authority (mandate of the law); Komdigi; BSSN; PSE/Platform | Processing basis + parental/guardian consent; incident notification; privacy-by-design | Administrative sanctions; criminal sanctions (PDP Law/ITE Law) if applicable | Child consent compliance; notification ≤3×24 hours; DPIA for child services; complaint channel |
| Art. 19 (protection from violence) | Law 23/2002 in conjunction with Law 35/2014; Law 17/2016 | KPPPA; Police; Prosecutor's Office; LPSK/UPTD PPA | Prevention; integrated services; rehabilitation; victim referral | Criminal (violence/explo itation); witness/victim protection | Number of integrated services; response time; recovery; reduction of revictimization |
| Art. 34 (sexual exploitation) + GC25 | Law 17/2016; provisions on content & access to PSE | APG; Komdigi; platform; law enforcement | Takedown; reporting; cross border cooperation / providers | Criminal penalties for perpetrators; sanctions for platforms in case of negligence | SLA takedown; rapid reporting; tracking / coordination mechanisms |
| Art. 2 (non-discriminatio n) | Law 23/2002; inclusive regional policies | Local government; education/health/so cial services | Afirmative access to services for vulnerable children | Ombudsman / inspectorat; strategic litigation | Disaggregated data; service coverage nan; no administrative barriers |

**Mapping CRC obligations to Indonesian national and institutional norms.**

1. The Child Protection Law as an umbrella norm. Law 23/2002 in conjunction with Law 35/2014 and Law 17/2016 provides a framework of principles, rights, and obligations of the state/community/parents in child protection, while strengthening enforcement aspects in certain forms of violence and exploitation. Institutionally, the Indonesian Child Protection Commission (KPAI) is maintained as an independent institution that performs monitoring and advocacy functions for child protection, thereby acting as a hub of normative-institutional accountability.
2. The PDP Law and child privacy as a testable obligation. Law 27/2022 introduces a more stringent data protection regime, including regulations on the processing of children's personal data that require parental/guardian consent (Article 25). In the event of a personal data protection failure, the data controller is required to notify the data subject

and the agency within 3×24 hours at the latest (Article 46). These two provisions are important for children's rights because they transform the principle of privacy into an auditable procedural obligation: the presence or absence of a basis for processing, valid consent, and incident response protocols.

3. The ITE Law after the second amendment and the obligation of PSEs to protect children. Law 1/2024 adds Article 16A, which requires Electronic System Operators (PSEs) to provide protection for children who use or access electronic systems, and gives the Government the authority to order system adjustments or certain actions. Violations of these orders may result in administrative sanctions. This norm strengthens the "protect" dimension in the digital space because it shifts the burden of protection not only to the state/family, but also to the design and governance of systems by private actors.
4. PP PSTE and system security standards. PP 71/2019 emphasizes the aspects of security, reliability, and responsibility in the operation of electronic systems and transactions. Although not specifically related to children, this PP provides a normative basis for system security standards (security baseline) that are relevant to the protection of children's data, especially when public services rely on digital infrastructure.

The mapping above suggests that Indonesia has moved from a principle-based child protection model toward a more duty-based and auditable compliance architecture. In contrast to earlier frameworks that were largely declaratory, the combined operation of the Child Protection Law, the PDP Law, the amended ITE Law, and PP PSTE indicates a gradual proceduralization of CRC obligations: rights are translated into verifiable duties (lawful basis, consent traceability, breach notification timeline, and platform adjustment orders). However, this architecture appears institutionally fragmented. KPAI functions as a monitoring and advocacy hub, yet key enforcement levers remain dispersed across sectoral regulators and administrative agencies. As a result, implementation may vary across forums and sectors, particularly where child protection depends on cross-agency coordination rather than a single chain of command. This finding reveals that regulatory density alone does not guarantee equivalent protection outcomes.

A second analytical issue concerns normative fit and operational coherence. The parental/guardian consent model under the PDP Law is important, but it may be insufficient when read against CRC principles on the child's evolving capacities and best interests, especially for adolescents in high-risk digital environments. Similarly, Article 16A of the ITE Law strengthens the protective burden on PSEs, yet its effectiveness tends to depend on whether "protection" is operationalized into measurable due-diligence standards, documented risk controls, and sanction triggers. Meanwhile, PP 71/2019 provides security baselines, but because it is not child-specific, it does not by itself resolve thresholds for child-risk classification, age-sensitive design, or escalated incident handling. Therefore, harmonization should move beyond textual alignment toward an integrated compliance matrix that links each CRC-relevant obligation to clear indicators, responsible institutions, audit trails, and referral-correction pathways. Such an approach would more credibly bridge the gap between formal legality and actual protection performance.

**Testing the Resilience of Legal Pluralism: From Formal Harmonization to Implementation Guidelines.**

Legal pluralism means that CRC harmonization cannot stop at the synchronization of regulatory texts. In family issues (guardianship, parenting, and social practices that could potentially harm children), the interaction between state norms and religious/customary norms can result in variations in implementation. The literature on legal pluralism reminds us that socially "applicable" standards may differ from formally "applicable" standards, so

compliance designs must read the social arena where norms are produced and enforced (Griffiths, 1986)(Merry, 1988).

This divergence is analytically significant because it shifts the real unit of compliance from statutory provisions to decision-making arenas. Where families rely on religious or customary forums due to accessibility, speed, cost, and perceived legitimacy, normative authority tends to be redistributed from state institutions to community-based adjudicators. As a result, implementation may display patterned selective compliance: norms perceived as culturally consonant are adopted, whereas rights-protective safeguards that require formal reasoning (e.g., explicit best-interests analysis, child participation, and written justification) may be inconsistently applied. In this sense, the protection gap appears to arise not only from doctrinal conflict, but also from procedural asymmetry across parallel forums.

In practice, the "stress test" of pluralism is often most evident in family issues such as child marriage, parenting, and informal dispute resolution mechanisms. A number of socio-legal studies confirm that conflicts or negotiations between state law and religious/customary norms can result in gaps in protection, especially when informal forums are more accessible or considered more legitimate in the community (Wadjo et al., 2025)(Mohsi et al., 2025). Therefore, effective harmonization strategies need to combine the substantive standards of the CRC with procedural tools that can be implemented across forums for example, BIA obligations, recording of reasons, and clear referral and correction mechanisms.

In this context, a more realistic harmonization strategy is to normalize CRC-based procedures particularly best interests into mandatory implementation guidelines. For example, for every administrative decision or ruling that affects children, the obligation to conduct a Best Interests Assessment (BIA) and record the considerations (reason giving) can serve as a "bridge" between the normative values of the CRC and the various forums of implementation (administrative, social services, and judicial).

The implication is that harmonization indicators are not sufficient in the form of norms alone, but rather the existence of procedures and evidence of implementation: whether BIA is carried out, whether children's views are heard, and whether there are effective correction/appeal mechanisms.

**The Duty to Protect in the Digital Space: Accountability of Private Actors and Enforcement Mechanisms.**

General Comment No. 25 emphasizes that states must regulate the business world to respect children's rights in the digital space, including through security standards, risk assessment, age-appropriate design, and complaint mechanisms that are accessible to children. Thus, the duty to protect works through regulation, supervision, and rem ediation of the behavior of private actors (Committee on the Rights of the Child, 2021).

In Indonesia, two normative nodes reinforce this approach. First, Article 16A of Law 1/2024 requires PSEs to provide protection for children and comply with adjustment orders from the government. Second, the PDP Law affirms the child consent regime (Article 25) and the obligation to notify incidents (Article 46). This combination enables the strengthening of compliance-by-design: (i) ex ante obligations (risk mitigation and access/feature control), and (ii) ex post obligations (incident response and recovery).

The ransomware incident at the Temporary National Data Center (PDNS) on June 20, 2024, is often seen as a reminder that cybersecurity is a prerequisite for the protection of rights, including children's rights to privacy and data security. Within the framework of the compliance ecosystem, this incident shows that minimum security standards and incident response governance must be treated as part of general measures of implementation, not merely technical issues (Indonesian House of Representatives, 2024).

From an enforcement perspective, effective design requires the orchestration of instruments: administrative sanctions to enforce rapid compliance (e.g., system adjustment orders and administrative fines), as well as criminal instruments for serious violations (exploitation, dissemination of child sexual content, or data processing without a legitimate basis that meets the elements of a criminal offense). These mechanisms need to be complemented by child-friendly complaint channels, recovery services, and outcome-based M&E so that enforcement does not stop at symbolism.

1. The landscape of digital risks to children

The literature maps digital risks to children as a spectrum that includes cyberbullying and online harassment, grooming, sextortion, dissemination of child sexual abuse material (CSAM), data privacy violations, and new threats such as deepfakes and virtual identity theft. This complexity shows that protecting children in the digital space cannot be simplified into a matter of morality or cyber security alone, but requires the simultaneous orchestration of law, education, recovery services, and platform governance (Chandrasekara, 2025)(Rajapaksha et al., 2025).

Interpersonal harms are repeatedly identified as core child online risks, including cyberbullying and broader forms of online harassment (Zulqadri et al., 2022)(P et al., 2024)(Majebi & Hamza, 2021). A conceptual analysis focused on children's online navigation in India explicitly lists cyberbullying and predation among key threats and highlights gaps in digital literacy and parental oversight as compounding factors (P et al., 2024). Online learning safety work likewise includes cyberbullying among the threat set associated with internet use in educational contexts (Zulqadri et al., 2022). Research on digital footprints provides a complementary mechanism: higher exposure of personal traces online is associated with increased susceptibility to cyber victimization outcomes such as identity theft, cyberstalking, and online harassment (study conducted among internet users in India), reinforcing the link between data exposure and interpersonal harm (D & Kumar, 2025). Adolescent risk research (preprint) further frames exposure to online risks in relation to online behaviors and examines disparities and vulnerabilities (including gender disparities), supporting the premise that risk is not evenly distributed across youth populations.(Savoia et al., 2021)

Taken together, these studies suggest that child online risk is better understood as a layered risk ecosystem rather than isolated incidents of bullying or harassment. In this ecosystem, interpersonal harms appear to emerge from the interaction of three mechanisms: (i) behavioral exposure (high-frequency posting, public interaction, risky contact patterns), (ii) data exposure (persistent digital footprints that increase traceability and targeting), and (iii) protection gaps (uneven digital literacy, limited parental mediation, and inconsistent institutional response). Thus, cyberbullying and predation should not be treated solely as peer-behavior problems; they also indicate weaknesses in platform governance and safety architecture. This interpretation reveals why similar online activities may produce very different outcomes across children: vulnerability is mediated by context, identity, and the quality of protective infrastructure.

A further implication is that prevention models centered only on awareness campaigns may be necessary but insufficient. While digital literacy and parental oversight remain important, the evidence indicates that effective mitigation likely depends on multi-level interventions: safety-by-design obligations for platforms, stronger default privacy settings for minors, proactive detection and escalation pathways in schools, and accessible reporting–redress mechanisms that are sensitive to age and gender-based vulnerabilities. In contrast to one-size-fits-all strategies, a risk-differentiated approach appears more consistent with the empirical pattern that harms are unevenly distributed. This also strengthens the argument that children's online safety should be operationalized

through auditable duties across actors (families, schools, platforms, and regulators), not framed as an individual responsibility of children alone.

Within the compliance ecosystem framework, risk mapping needs to be translated into minimum operational standards: risk definitions, identification and reporting protocols, and clear service referrals. The 4Cs model (contact, content, conduct, contract) can be used as a policy taxonomy to ensure that legal and policy instruments respond not only to one type of hazard but cover all relevant risk categories (Jang & Ko, 2023).

2. Platform responsibility: lessons from the DSA and Online Safety Act

Online safety regulations in various jurisdictions show a tendency to shift governance from simply taking down content to a risk-based regulation model: platforms are required to conduct risk assessments, implement mitigation measures, and open up more space for audit and accountability (Nash & Felton, 2024)(Murray & Leiser, 2025). In practice, the "Trusted Flagger" mechanism and hotline networks are also considered effective in accelerating the handling of harmful content, especially related to child sexual exploitation material, by combining the expertise of civil society and the compliance obligations of platforms (Fragopoulou & Kokolaki, 2025). This lesson is relevant for Indonesia to clarify minimum standards for risk assessment, response procedures, and child-friendly reporting channels as a compliance infrastructure package, not merely as prohibitive norms.

3. Prevention based on literacy and parenting

Beyond enforcement, the duty to protect also requires prevention strategies that strengthen the capacity of children, families, and schools. Digital safety literacy programs at the elementary level have been reported to increase risk awareness and protective skills, especially when accompanied by situational exercises and teacher support (Martin et al., 2024)(Krikelas, 2025). At the family level, the effectiveness of protection is greatly influenced by parental mediation patterns between technical restrictions, active guidance, and open communication which need to be balanced so as not to weaken children's digital resilience (Hassan et al., 2025)(Banić & Orehovački, 2024). In the context of Muslim families, the integration of ethical values into digital education has also been reported to help build safe and dignified behavioral norms (Sholihah & Nurhayati, 2024).

4. Critical note: age verification and the risk of techno-solutionism

The literature warns that child safety policies that are overly oriented towards technical "checklists" risk falling into techno-solutionism: assuming that complex social problems (violence, exploitation, and power relations) can be solved primarily through legally mandated technological features (Angel & Boyd, 2024). The issue of age verification is often promoted as a quick fix, but a few analyses point to the risk of "false promises" and side effects on privacy and access if not designed proportionally and accountably (Angel & Boyd, 2024). Therefore, age verification policies need to be tied to the principles of data minimization, independent auditing, and the choice of mechanisms that do not shift the burden of protection solely onto children.

**Child participation and proving "influence" in policy/decision-making processes.**

Child participation is an element that is often missing when harmonization is narrowed down to regulatory synchronization. General Comment No. 12 emphasizes that states must provide opportunities for children to express their views and ensure that those views are given weight in accordance with their age and maturity (Committee on the Rights of the Child, 2009).

The Lundy framework enriches the aspect of proving implementation: meaningful participation requires (i) space a safe space for children to express their views; (ii) voice support for children to express themselves; (iii) audiences who actually listen; and (iv)

influence traces of the influence of children's views on the outcome of decisions (Lundy, 2007). From an ecosystem compliance perspective, these four components can be used as minimum procedural indicators, particularly in the process of protection services, regional policy formulation, and child-friendly judicial processes.

Without these indicators, participation is prone to becoming a formality. Therefore, participation mechanisms need to be integrated with documentation (reason-giving) and corrective M&E obligations so that participation can be assessed transparently.

## CONCLUSION

This article showed that the harmonization of CRC obligations in Indonesia should not be interpreted merely as the synchronization of regulatory texts, but rather as the development of an auditable compliance ecosystem: coherence between regimes (child protection, privacy/data, and digital governance), institutional capacity and coordination, and procedural indicators that test best interests, protection, and participation. Legal pluralism requires a procedure-based harmonization strategy (BIA, reason-giving, and correction mechanisms) to ensure that CRC standards remain consistent across various implementation forums.

In the digital realm, strengthening the duty to protect needs to be directed at the accountability of private actors through a risk-based approach (risk assessment and mitigation), compliance-by-design, and child-friendly reporting and redress channels. Lessons from the global platform regime underscore the importance of combining administrative instruments (adjustment orders, audits, fines) and criminal instruments for serious violations, with caution against techno-solutionism and privacy risks from age verification policies.

Key recommendations that can be tested in further research and policy work are: (1) requiring Best Interests Assessments and recording of reasons for decisions/rulings that affect children; (2) developing a 4Cs risk taxonomy as the basis for minimum standards for cross-sector digital risk management; (3) clarifying the obligations of risk assessment and mitigation for PSEs/platforms and child-friendly reporting mechanisms; (4) integrating digital safety literacy into the curriculum and strengthening the capacity of parents and teachers; and (5) developing outcome-based M&E that measures victim recovery, prevention effectiveness, and platform compliance on an ongoing basis.

## REFERENCES

Angel, M. P., & Boyd, D. (2024). Techno-legal solutionism: Regulating children's online safety in the United States. *Proceedings of the 2024 Symposium on Computer Science and Law*, 86–97.

Ayalew, Y. E., Verdoodt, V., & Lievens, E. (2024). 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), ngae018.

Banić, L., & Orehovački, T. (2024). A comparison of parenting strategies in a digital environment: A systematic literature review. *Multimodal Technologies and Interaction*, *8*(4), 32.

Chandrasekara, C. M. N. T. K. (2025). *Child protection in the digital age: A policy analysis of Sri Lanka's cybersecurity measures and legal frameworks*. International Conference on Child Protection 2025.

Committee on the Rights of the Child. (2003). *General comment No. 5 (2003): General measures of implementation of the Convention on the Rights of the Child (CRC/GC/2003/5)*.

Committee on the Rights of the Child. (2009). *General comment No. 12 (2009): The right of*

*the child to be heard*.

Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25)*.

D, D., & Kumar, G. V. (2025). Impact of Digital Footprints on Cyber Victimization. *Advanced International Journal for Research*, *6*(5). https://doi.org/10.63363/aijfr.2025.v06i05.1671

Fragopoulou, P., & Kokolaki, E. (2025). OA20248. SafeLine: Shaping the future of online safety in the DSA era. *European Journal of Public Health*, *35*(Supplement_5), ckaf165-014.

Government Regulation of the Republic of Indonesia Number 71 of 2019 Concerning the Implementation of Electronic Systems and Transactions.

Griffiths, J. (1986). What is legal pluralism? *The Journal of Legal Pluralism and Unofficial Law*, *18*(24), 1–55.

Hassan, S., Ahmad, R., Abd Wahab, A., Mohammed, F., & Purbasari, A. (2025). Parental Strategies for Mitigating Online Threats and Enhancing Children's Cybersecurity Awareness. *Journal of Information and Communication Technology*, *24*(4), 111–134.

Hodgkin, R., Newell, P., & UNICEF. (2007). *Implementation Handbook for the Convention on the Rights of the Child (Fully revised 3rd ed.)*.

Indonesian House of Representatives. (2024). *Weak security of the Temporary National Data Center (PDNS) against cyber attacks (Brief Info, XVI(13), P3DI)*.

Jang, Y., & Ko, B. (2023). Online safety for children and youth under the 4Cs framework—A focus on digital policies in Australia, Canada, and the UK. *Children*, *10*(8), 1415.

Krikelas, I. (2025). Promoting Cybersecurity Awareness in Primary Education: A Classroom Approach to Online Safety Education. *European Journal of Contemporary Education and E-Learning*, *3*(6), 34–44.

Law of the Republic of Indonesia Number 1 of 2024 Concerning the Second Amendment to Law Number 11 of 2008 Concerning Electronic Information and Transactions.

Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions.

Law of the Republic of Indonesia Number 17 of 2016 Concerning the Stipulation of Government Regulation in Lieu of Law Number 1 of 2016 Concerning the Second Amendment ( ) to Law Number 23 of 2002 Concerning Child Protection into Law.

Law of the Republic of Indonesia Number 23 of 2002 Concerning Child Protection.

Law of the Republic of Indonesia Number 27 of 2022 Concerning Personal Data Protection.

Law of the Republic of Indonesia Number 35 of 2014 on Amendments to Law Number 23 of 2002 on Child Protection.

Lundy, L. (2007). 'Voice'is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child. *British Educational Research Journal*, *33*(6), 927–942.

Majebi, N. L., & Hamza, O. (2021). Child Safety in the Digital Age: Historical Lessons From Media Regulation and Their Application to Modern Cybersecurity Policies. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(1), 735–742. https://doi.org/10.54660/.ijmrge.2021.2.1.735-742

Martin, F., Mushi, D., Bacak, J., Wang, W., Ahlgrim-Delzell, L., & Polly, D. (2024). Elementary student experiences from digital safety immersion summer program. *Educational Media International*, *61*(3), 321–343.

Merry, S. E. (1988). Legal pluralism. *Law & Society Review*, *22*(5), 869–896. https://doi.org/https://doi.org/10.2307/3053638

Mohsi, M., Romli, M., Zakaria, S., & Fudholi, M. (2025). Harmonizing Legal Pluralism in Marriage Laws: Policy Challenges on Child Marriage in Madura. *Al-Ahkam: Jurnal*

*Ilmu Syari'ah Dan Hukum*, *10*(2), 100–118.

Murray, A., & Leiser, M. (2025). Rethinking Safety-by-Design and Techno-Solutionism for the Regulation of Child Sexual Abuse Material. *Technology and Regulation*, *2025*, 137–171.

Nash, V., & Felton, L. (2024). Treating the symptoms or the disease? Analysing the UK Online Safety Act's approach to digital regulation. *Policy & Internet*, *16*(4), 818–832.

P, A. M., Raneesha, K., & S.R., A. (2024). Virtual Shadows: Protecting Children From Invisible Threats in the Digital World. *Shanlax International Journal of Arts Science and Humanities*, *12*(S1-Sep), 41–51. https://doi.org/10.34293/sijash.v12is1-sep.8174

Presidential Decree of the Republic of Indonesia Number 36 of 1990 Concerning the Ratification of the Convention on the Rights of the Child.

Rajapaksha, R., Gamlath, G. R. Y. M., & Herath, H. M. D. S. (2025). *Safeguarding childhood in the digital age: Legal and social responses to online child exploitation in Sri Lanka*. International Conference on Child Protection 2025.

Savoia, E., Harriman, N. W., Su, M., Cote, T., & Shortland, N. (2021). *Adolescents' Exposure to Online Risks: Gender Disparities and Vulnerabilities Related to Online Behaviors*. https://doi.org/10.20944/preprints202103.0498.v1

Sholihah, H., & Nurhayati, S. (2024). Child protection in the digital age through education in the islamic educational environment. *JIE (Journal of Islamic Education)*, *9*(1), 200–218.

United Nations. (1989). *Convention on the Rights of the Child*.

Wadjo, H. Z., Saimima, J. M., & Salmon, H. C. J. (2025). Clifford. Jonas. (2025). Conflict of customary law and positive law in determining the status of children: Criminal implications for children's rights and legal protection. *Journal of Adat Recht*.

Zulqadri, D. M., Mustadi, A., & Retnawati, H. (2022). Digital Safety During Online Learning: What We Do to Protect Our Student? *Jurnal Iqra*, *7*(1), 178–191. https://doi.org/10.25217/ji.v7i1.1746