

Legal Updates on the Prevention and Handling System for Child Victims of Exposure to Digital Radicalism through Social Media and Online Games from a Child Protection Perspective

Fani Asiah Pratidina*, Vita Mayastinasari, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; fanipratidina@yahoo.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; mamayovi@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; kif.92pw@gmail.com

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6328>

*Correspondence: Fani Asiah Pratidina

Email: fanipratidina@yahoo.com

Received: 08/08/2026

Accepted: 27/08/2026

Published: 31/08/2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license (<http://creativecommons.org/licenses/by-sa/4.0/>).

Abstract: *The development of social media and online games has transformed the pattern of radicalism, spreading from conventional methods to digital radicalism, which is more hidden, interactive, and difficult to monitor by conventional legal systems. Children are a vulnerable group to exposure to radical ideology due to the high intensity of digital space use, weak digital literacy, and the influence of social media algorithms and online game virtual communities that form echo chambers and soft radicalization. This study aims to analyze the legal problems in preventing and handling child victims of exposure to digital radicalism through social media and online games, and to formulate an ideal legal reconstruction and reform from the perspective of child protection in Indonesia. This study employs a normative juridical method with statutory and conceptual approaches through an analysis of various regulations related to child protection, cyber law, and the eradication of terrorism. The results show that the Indonesian legal system is still partial and does not have specific regulations regarding the protection of children from exposure to digital radicalism, including weak supervision of digital platforms, the absence of a national early detection system, and the dominance of a repressive approach in handling children exposed to radicalism. Therefore, legal reform is needed through reformulating digital-based child protection regulations, strengthening the legal responsibility of social*

media and online gaming platforms, establishing a national digital early warning system, harmonizing child protection laws with cyber and criminal law, and developing a child-specific deradicalization model based on psychological rehabilitation and social reintegration. These legal reforms are expected to build a child protection system that is preventive, rehabilitative, humane, and responsive to developments in digital technology in Indonesia.

Keywords: Legal Reform; Digital Radicalism; Child Protection; Social Media; Online Games.

Introduction

The development of information and communication technology has transformed patterns of social interaction, including among children, through the widespread use of the internet, social media, and online games as virtual, interactive spaces without geographical boundaries (Wirany, 2022). Children in the digital era no longer only interact within the physical space of family and school, but also live in a digital ecosystem shaped by platform algorithms such as TikTok, Instagram, YouTube, Discord, Telegram, Roblox, PUBG, Free Fire, and various other online gaming platforms that enable real-time communication

between users across countries (Miyazaki, 2024). This development has shifted the spread of radicalism from conventional methods based on physical meetings to digital forms that are more covert, widespread, and difficult for law enforcement to detect. Digital radicalism grows through algorithmic mechanisms that create echo chambers and filter bubbles, causing children to be repeatedly exposed to content with the same ideological patterns (Bastian, 2021). In this context, online games no longer function solely as entertainment but have evolved into virtual communities that foster emotional connections, group identity, and the internalization of specific ideological values through chat rooms, voice communication, clan systems, live streaming, and anonymous interaction (Ahdiyat, 2018). The phenomenon of gamification propaganda also demonstrates how narratives of violence, heroism, identity hostility, and the glorification of extreme actions are packaged in visual forms, game missions, memes, and short videos that are more easily accepted by children. The shift in radicalization patterns demonstrates that the threat of extreme ideology now operates through digital spaces that are not fully accessible by conventional legal instruments, resulting in existing regulations lagging behind technological developments and the spread of digital-based radicalism.

Children exposed to digital radicalism are a group with high levels of psychological, social, and digital vulnerability due to their identity development, need for social recognition, and search for self-meaning. This vulnerability is exacerbated by low digital literacy, weak family supervision, and the high intensity of social media and online game use in daily life. From a digital psychology perspective, children are easily influenced by emotional manipulation techniques such as fear propaganda, identity affirmation, emotional belonging, and persuasive narratives used by radical groups to slowly build emotional closeness. (Maharani, 2025) Therefore, children exposed to digital radicalism cannot be positioned solely as potential perpetrators, but must be seen as victims of an exploitative and manipulative digital system. This perspective is in line with the principle of child protection in Article 28B paragraph (2) of the 1945 Constitution of the Republic of Indonesia, which emphasizes that every child has the right to survival, growth, and development and the right to protection from violence and discrimination. In addition, Article 59 paragraph (1) and Article 59 paragraph (2) letter k of Law Number 35 of 2014 concerning Amendments to Law Number 23 of 2002 concerning Child Protection emphasize the state's obligation to provide special protection to child victims of terrorist networks and extreme violence. (Hutagalung, 2025) The principle of the best interests of the child, as stipulated in the Convention on the Rights of the Child, which has been ratified through Presidential Decree Number 36 of 1990, also requires that all state policies and actions towards children must prioritize the best interests of the child (Darwanta, 2020). Thus, the victim approach to children exposed to digital radicalism is important because children are essentially the ones affected by the failure of the national digital protection system.

Social media and online games have evolved into strategic media for spreading radical ideology through more subtle and adaptive methods than conventional propaganda. Radical groups utilize live streaming, direct messaging, community forums, voice rooms, and clan communities within online games to gradually build social and ideological relationships with children without being easily detected. (Setianto, 2018) Propaganda narratives are conveyed through memes, short videos, visual symbols, struggle jargon,

glorification of violence, and conflict simulations, all packaged in digital entertainment, making them appear normal and devoid of direct threats. This soft radicalization phenomenon demonstrates that the radicalization process is not always carried out through explicit doctrine, but can occur through the formation of group identities, the strengthening of hate sentiments, and the gradual normalization of violence. (Lubis, D., & Siregar, 2020) The problem becomes increasingly complex because most digital platforms and online game servers operate across national jurisdictions, complicating national law enforcement and oversight. From a cyber law perspective, this situation demonstrates the limitations of national legal sovereignty in controlling the flow of transnational digital content. In fact, Article 16 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions stipulates the obligation of electronic system providers to operate electronic systems reliably, securely, and responsibly. Furthermore, Article 40 paragraph (2a) of the ITE Law authorizes the government to terminate access to electronic information containing unlawful content. (Nofanda, 2025) However, these provisions are still general in nature and do not specifically regulate the obligations of social media platforms and online games to prevent exposure to radicalism among children, thus creating a normative vacuum regarding digital platform responsibilities for child protection.

The Indonesian legal system for preventing digital radicalism among children is fundamentally partial, repressive, and unable to address the complexity of contemporary digital threats. Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism still focuses on a state security approach and prosecution of perpetrators of terrorist acts, thus not specifically regulating mechanisms for the protection, rehabilitation, and deradicalization of child victims of exposure to digital radicalism (Shabirin, 2025). Meanwhile, the Child Protection Law does not explicitly regulate the categories of child victims of digital radicalism or the state's obligation to conduct early detection of exposure to extreme ideologies through social media and online games. This situation indicates a legal vacuum and regulatory disharmony between child protection law, cyber law, and counterterrorism law. Furthermore, there is no national legal standard for early identification of children exposed to digital radicalism, no mechanism for monitoring digital platform algorithms, and weak coordination between the National Counterterrorism Agency, the Indonesian National Police, the Ministry of Communication and Digital, educational institutions, and digital platform operators. As a result, the legal system tends to act after extreme acts have occurred, rather than at the prevention and recovery stage. It is despite Article 71D of the Child Protection Law affirming the state's obligation to provide special protection and supervision for children from various forms of threats that endanger their development (Zuhudin, 2023). Thus, the current weak legal construction shows that national regulations have not been able to anticipate the transformation of digital radicalization patterns that systematically and covertly target children.

The penal approach to handling children exposed to radicalism also raises various legal and human rights problems because children are often positioned solely as a security threat without considering aspects of victimology and child protection. In law enforcement practices, a repressive approach has the potential to lead to criminalization, social stigmatization, discrimination, and psychological damage to children who are actually in a

vulnerable position and manipulated by digital propaganda systems. The overly dominant security perspective causes the rehabilitative and deradicalization approaches for children to be less than optimal. This is despite Law Number 11 of 2012 concerning the Juvenile Criminal Justice System, which affirms that the resolution of juvenile cases must prioritize diversion and restorative justice as a form of protection for the child's best interests. Article 5 of the Juvenile Justice System Law even emphasizes that the juvenile criminal justice system must prioritize a restorative justice approach at every stage of the investigation. (Huda, M. D., & Putra, 2025) Therefore, children exposed to digital radicalism should be treated as subjects of protection requiring social rehabilitation, psychological recovery, digital education, and social reintegration, not simply objects of punishment. In this context, a child-centered approach is crucial so that the state focuses not only on national security but also ensures the protection of children's rights as part of human rights guaranteed by the constitution and international legal instruments.

These weaknesses demonstrate the urgency of comprehensive and integrated legal reforms in the prevention and treatment of child victims of digital radicalism through social media and online games. Legal reforms are needed to build a regulatory system that adapts to developments in digital technology through a preventive, rehabilitative, and humane approach based on child protection. Legal reforms need to be directed at strengthening the legal obligations of digital platforms and online game operators to monitor content, detect risky algorithms, protect child data, and provide a rapid reporting mechanism for digital radicalism activities. Furthermore, synchronization between criminal law, child protection law, and cyber law is necessary to prevent sectoral and overlapping efforts in handling digital radicalism against children. The state also needs to develop a technology-based early warning system, strengthen national digital literacy, and develop a child deradicalization model that focuses on psychological recovery and social reintegration. This legal reform aligns with the objectives of a state based on the rule of law, as affirmed in Article 1 paragraph (3) of the 1945 Constitution, which requires the protection of citizens' rights through a legal system that is adaptive and responsive to societal developments. Therefore, the reconstruction of the legal system for preventing and handling child victims of exposure to digital radicalism is an urgent need to ensure child protection amidst the ever-evolving, complex, and transnational transformation of the digital space.

Methodology

This research employs a normative juridical research method that focuses on the examination of legal norms, legal principles, legal theory, and the synchronization of laws and regulations related to the system for preventing and handling child victims of exposure to digital radicalism through social media and online games from a child protection perspective. The approaches used include a statutory approach and a conceptual approach. The legislative approach is carried out by examining various relevant regulations, including the 1945 Constitution of the Republic of Indonesia, Law Number 35 of 2014 concerning Child Protection, Law Number 11 of 2012 concerning the Juvenile Criminal Justice System, Law Number 19 of 2016 concerning Electronic Information and Transactions, Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, as well as various other regulations and policies related to cybersecurity, child protection, and countering digital

radicalism. Meanwhile, a conceptual approach is used to examine the concepts of the rule of law, child protection, victim-centered approaches, restorative justice, deradicalization, digital security, and legal reform as the theoretical foundation for developing an ideal legal framework. The study uses primary, secondary, and tertiary legal materials collected through literature research. All legal materials were then analyzed qualitatively using descriptive-analytical and prescriptive methods to find normative gaps, regulatory disharmony, and formulate legal reform constructions that are responsive to the development of digital radicalism against children in Indonesia.

Result and Discussion

Legal Issues in the Prevention and Treatment of Child Victims of Exposure to Digital Radicalism Through Social Media and Online Games in Indonesia

The development of digital technology has created a major transformation in children's social interaction patterns through the internet, social media, and online games, which have increasingly become important virtual spaces for communication and social interaction. Children no longer interact solely through physical environments such as family, school, and social communities, but also participate in digital ecosystems shaped by platform design, recommendation systems, and virtual online gaming communities. Academic discussions concerning digital radicalization have identified the possibility that social media platforms, encrypted communication spaces, discussion forums, live streaming, and online gaming communities may be used for ideological dissemination, networking, and recruitment. The concepts of echo chambers, algorithmic amplification, gamification of propaganda, and digitally mediated ideological interaction are therefore used in this study as analytical concepts derived from relevant literature rather than as independent empirical findings produced by this normative juridical research (Saputra, 2024).

Accordingly, this study does not seek to measure the statistical prevalence of child exposure, the frequency of radicalization through online games, or the effectiveness of existing monitoring systems. Rather, these developments are treated as the factual and technological context described in relevant academic and institutional discourse for examining whether the existing Indonesian legal framework is sufficiently capable of providing preventive and protective mechanisms for children. The normative issue examined is therefore the adequacy of child protection, cyber law, and counterterrorism regulations in responding to the possibility of ideological exposure and technology-based radicalization involving children.

For the purpose of this study, several concepts must be distinguished in order to avoid treating all forms of controversial or radical expression as legally equivalent. Digital radicalism refers to the manifestation, dissemination, or circulation of radical ideological narratives through digital technologies and online environments. Digital radicalization refers to the dynamic process through which an individual may be exposed to, interact with, internalize, reinforce, or become mobilized by radical ideological narratives through digital communication and virtual communities. Thus, digital radicalism

refers primarily to the phenomenon or content, whereas digital radicalization refers to the process affecting an individual.

Exposure to radical ideology refers to the initial encounter or repeated contact with content, symbols, narratives, communities, or communication associated with radical or extremist ideas. Exposure alone does not establish that a child has adopted, accepted, or acted upon such ideas. Soft radicalization, in contrast, refers to a gradual and indirect process of ideological influence that may occur through repeated narratives of hatred, glorification of violence, identity polarization, manipulation, or entertainment-based communication without immediately involving explicit recruitment or direct calls to commit violence. Extremist propaganda refers to digital content intentionally designed to promote, justify, recruit for, facilitate, or encourage ideologically motivated violence or other conduct prohibited by law.

These distinctions are essential because a child who merely encounters controversial, ideological, religious, political, or even extremist material cannot automatically be categorized as radicalized. Legal intervention should only be considered when exposure develops into objectively identifiable indicators of ideological internalization, recruitment vulnerability, repeated engagement with violent extremist networks, advocacy or glorification of unlawful violence, preparation for prohibited acts, or other circumstances requiring child protection. In this context, Article 28B paragraph (2) of the 1945 Constitution affirms every child's right to protection and development, while Article 59 paragraph (1) and Article 59 paragraph (2) letter k of Law Number 35 of 2014 provide the basis for special protection of children in vulnerable circumstances, including children affected by terrorist networks. Article 69B further emphasizes education, social rehabilitation, psychosocial support, and protection for such children (Sudiarti, 2024).

The spread of radical ideology through social media and online games takes advantage of interactive digital features that enable radicalization to occur gradually and covertly. Features such as chat rooms, voice communication, live streaming, clan systems, and online gaming forums are used to build emotional bonds and group solidarity with children in ways that are difficult for law enforcement to detect. Digital propaganda patterns are no longer carried out frontally, but rather through soft radicalization in the form of spreading hate narratives, glorifying violence, strengthening group identities, and psychological manipulation packaged in the form of digital entertainment. Radical groups also utilize the anonymity and encryption of digital platforms to avoid state surveillance so that the recruitment process and the spread of ideology can take place across countries on a massive scale. (Aisy et al., 2019) From a cyber law perspective, this condition shows the limitations of state jurisdiction in overseeing the global digital space. In fact, Article 40 paragraph (2a) of Law Number 19 of 2016 concerning Information and Electronic Transactions gives the government the authority to terminate access to electronic information that contains unlawful content. Moreover, Article 16 of the ITE Law also stipulates the obligation of electronic system providers to operate electronic systems reliably, securely, and responsibly. However, this provision is still general and does not specifically address the responsibilities of social media and online gaming platforms in

preventing children's exposure to radicalism, including the obligation to monitor algorithms, protect children in digital communities, and provide a mechanism for reporting radical activity promptly and effectively.

The weakness of the Indonesian legal system in preventing and addressing digital radicalism against children is also evident in the regulatory disharmony between child protection law, cyber law, and counterterrorism law. Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism essentially emphasizes a state security approach and prosecution of perpetrators of terrorist acts. Although Article 43A regulates the prevention of criminal acts of terrorism through national preparedness, counter-radicalization, and deradicalization, its provisions do not specifically target child protection in the digital space. Similarly, the Child Protection Law does not comprehensively regulate the definition, indicators, or identification mechanisms for child victims of exposure to digital radicalism. This situation creates a legal vacuum, leaving the state without clear legal instruments for preventing, monitoring, and rehabilitating children exposed to radical ideology through social media and online games. Furthermore, the absence of national standards regarding an early warning system for digital radical content means that handling remains reactive after a child is involved in extremist acts. The weak coordination between the National Counterterrorism Agency (BNPT), the Indonesian National Police (Polri), the Ministry of Communication and Digital, educational institutions, and digital platform operators also demonstrates that the national legal system is not yet integrated in addressing the threat of digital radicalism against children.

Another problem in handling children exposed to digital radicalism is the dominant penal and security approach, which tends to position children as threats to the state, rather than as victims of digital system manipulation and ideological propaganda. This repressive approach has the potential to lead to criminalization, social stigmatization, discrimination, and psychological distress for children who are already in a vulnerable position. In law enforcement practices, children exposed to radical ideology are often directly linked to the threat of terrorism without considering the underlying psychological, social, and digital vulnerabilities. Despite Article 3(g) of Law Number 11 of 2012 concerning the Juvenile Criminal Justice System stipulating that every child has the right not to be arrested, detained, or imprisoned except as a last resort and for the shortest possible time. Furthermore, Article 5 of the Juvenile Justice System Law emphasizes that the juvenile criminal justice system must prioritize a restorative justice approach, while Article 7 mandates diversion at every level of juvenile case investigation. These provisions demonstrate that the Indonesian legal system actually requires a child-centered approach and the protection of children's best interests in every legal process. However, in the context of digital radicalism, rehabilitative and deradicalization approaches for children have not been optimal because the law enforcement system is still dominated by the paradigm of national security and punishment.

These various problems demonstrate that the Indonesian legal system is not yet fully capable of addressing the transformational threat of digital radicalism targeting children through social media and online games. Existing regulations remain partial, sectoral, and

unresponsive to the rapid development of digital technology. The absence of specific regulations regarding digital platform obligations, weak algorithmic oversight, the absence of an early detection system, and the dominance of a repressive approach indicate an urgent need for legal reform in the child protection system in the digital space. According to Article 1, paragraph (3) of the 1945 Constitution of the Republic of Indonesia, the state, as the executor of power, is obligated to guarantee the protection of citizens' rights through a legal system that is adaptive and responsive to societal developments. Furthermore, Article 71D of the Child Protection Law also emphasizes the responsibility of the state and government to provide effective special protection for children.

Policies and Systems for Handling Children Exposed to Digital Radicalism through Social Media and Online Games from a Child Protection Perspective

Policies and systems for handling children exposed to digital radicalism through social media and online games must fundamentally be placed within the framework of child protection and respect for human rights, as children are a vulnerable group who lack psychological maturity and the ability to optimally filter information in the digital space. From a child protection law perspective, children exposed to radical ideology cannot be positioned solely as perpetrators or threats to state security, but must be viewed as victims of a manipulative and exploitative digital system. The principle of the best interests of the child, as stipulated in the Convention on the Rights of the Child, ratified through Presidential Decree Number 36 of 1990, requires all state policies related to children to prioritize the best interests of children. This principle is also reflected in Article 2 of Law Number 35 of 2014 concerning Child Protection, which emphasizes that child protection is implemented based on the principles of non-discrimination, the best interests of the child, the right to life and development, and respect for the child's opinions. Therefore, the system for handling children exposed to digital radicalism must be directed at preventive, rehabilitative, and educational approaches through psychological recovery, strengthening digital literacy, and social reintegration, rather than simply punishment. In this context, a victim approach is crucial because children are essentially victims of exposure to radical ideology that develops through social media and online games, exploiting children's psychological and social weaknesses in the digital space.

The application of a restorative justice and child-centered approach to handling children exposed to digital radicalism is an important part of the legal protection system for children. This approach aligns with Law Number 11 of 2012 concerning the Juvenile Criminal Justice System, which places the best interests of children as the top priority in every legal process. Article 5 of the Juvenile Criminal Justice System Law emphasizes that the juvenile criminal justice system must prioritize a restorative justice approach, while Article 6 states that restorative justice aims to achieve peace, resolve juvenile cases outside the judicial process, prevent children from being deprived of liberty, and instill responsibility in children. Furthermore, Article 7 of the Juvenile Criminal Justice Law requires diversion at every level of juvenile case investigation. These provisions demonstrate that the Indonesian legal system fundamentally recognizes the importance of a rehabilitative and restorative approach for children in conflict with the law, including

children exposed to digital radicalism. However, in practice, in handling extremism and radicalism cases, a security and repressive approach remains dominant, often positioning children as ideological threats and objects of state surveillance. This situation creates the risk of criminalization and social stigmatization for children who actually require psychological rehabilitation and social assistance. Therefore, the system for handling children exposed to digital radicalism must be built using a child-centered approach that views children as subjects of legal protection, not merely objects of security measures.

The state's role in the prevention and handling system for child victims of digital radicalism is crucial as a form of constitutional responsibility to protect children's rights in the era of digital transformation. Article 28B paragraph (2) of the 1945 Constitution of the Republic of Indonesia affirms that every child has the right to protection from violence and discrimination. This provision is reinforced by Article 20 of the Child Protection Law, which states that the state, government, regional governments, communities, families, and parents are obliged and responsible for implementing child protection. In the context of digital radicalism, the state's responsibility is not limited to legal enforcement but also encompasses prevention, education, digital supervision, rehabilitation, and social reintegration of children. The National Counterterrorism Agency, based on Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, has the authority to implement counter-radicalization and deradicalization, as stipulated in Articles 43A and 43D. However, existing counter-radicalization policies still focus primarily on security approaches and have not specifically developed a digital-based child protection system. Similarly, the Indonesian National Police (Polri) still places more emphasis on repressive law enforcement against terrorist activities than on developing a child protection and digital security prevention system. Therefore, it is necessary to strengthen more integrated state policies oriented toward child protection in addressing the threat of digital radicalism.

In addition to the state, families, schools, and communities hold a strategic position in preventing children's exposure to digital radicalism by strengthening social supervision and digital literacy. The family is the primary environment for the formation of a child's character and mindset, so monitoring the use of social media and online games must be carried out actively and educationally. Schools also have a responsibility to foster character education, tolerance, and digital literacy as a bulwark against the spread of extremist ideologies in the digital space. Article 9, paragraph (1) of the Child Protection Law emphasizes that every child has the right to receive education and instruction for personal development according to their interests and talents. The provision demonstrates that education functions not only as a transfer of knowledge but also as an instrument for the formation of social and national values. However, weak national digital literacy leaves many children unable to recognize radical propaganda packaged in digital entertainment, memes, short videos, and virtual online gaming communities. The situation is exacerbated by minimal community involvement in digital space monitoring and weak coordination between families, schools, and the government. Therefore, the system for handling children exposed to digital radicalism must involve a collaborative approach through strengthening

national digital literacy, tolerance education, community-based social supervision, and building family resilience in the face of the threat of extreme ideologies in the digital space.

In digital space supervision, social media platforms and online games have a crucial responsibility in preventing the spread of radical content targeting children. Article 16 of Law Number 19 of 2016 concerning Electronic Information and Transactions requires electronic system providers to operate electronic systems reliably, securely, and responsibly. Furthermore, Article 40 paragraph (2a) of the ITE Law authorizes the government to terminate access to electronic information containing unlawful content. However, current national regulations do not specifically address the obligations of digital platforms to protect children from exposure to digital radicalism, including content moderation, algorithm monitoring, reporting suspicious activity, and limiting children's access to high-risk digital communities. Unlike several countries, such as the United Kingdom through the Prevent Strategy and Online Safety Act and the European Union through the Digital Services Act, which have begun to regulate the responsibilities of digital platforms for protecting child users in cyberspace, Indonesia still lacks specific regulations governing algorithm monitoring and protecting children from digital radical content. This situation indicates that the Indonesian legal system is still lagging behind in dealing with increasingly complex and transnational developments in information technology, requiring a reformulation of legal policies that are more adaptive to the threat of digital radicalism against children.

These various weaknesses indicate that the system for handling children exposed to digital radicalism in Indonesia remains sectoral, reactive, and not yet comprehensively integrated from a child protection perspective. The dominant approach remains oriented toward state security and repressive law enforcement, thus failing to fully address the psychological recovery, social rehabilitation, and reintegration of children into society. This is despite Article 71D of the Child Protection Law affirming the state's obligation to provide effective special protection for children through supervision, prevention, care, and rehabilitation.

Reconstruction and Legal Update of the System for Preventing and Handling Child Victims of Exposure to Digital Radicalism through Social Media and Online Games from a Child Protection Perspective in Indonesia

Reconstruction and legal update of the system for preventing and handling child victims of exposure to digital radicalism through social media and online games must begin with a reformulation of national regulations that explicitly recognize children who experience verified and harmful exposure to digital radicalization as subjects of special legal protection. This update may be achieved through a revision of Law Number 35 of 2014 concerning Child Protection by adding the category of "child victims of exposure to digital radicalism and technology-based extremism" as a form of special state protection under Article 59 paragraph (2).

A child should qualify for this legal status not merely because the child has viewed, accessed, or accidentally encountered controversial or extremist content. The classification should require a professional, child-sensitive, and multi-disciplinary assessment indicating

one or more objective conditions, namely: repeated or targeted exposure to extremist recruitment or propaganda; active involvement in high-risk communication or recruitment networks; evidence of psychological manipulation or coercive ideological influence; persistent glorification or justification of unlawful violence combined with contextual risk indicators; or other circumstances demonstrating that the child's development, safety, psychological condition, or social environment has been adversely affected by technology-based extremist activity.

The assessment should follow a graduated intervention model. Level I exposure involves incidental or limited contact and should primarily result in education, digital literacy, and family guidance. Level II vulnerability involves repeated exposure or interaction requiring counseling, psychosocial assessment, and strengthened family supervision. Level III intervention involves verified indicators of ideological manipulation, recruitment, or connection with violent extremist activity and may require structured rehabilitation and protective intervention. Level IV criminal involvement should only apply where the child is alleged to have independently committed conduct meeting the statutory elements of a criminal offense, in which case the safeguards of Law Number 11 of 2012 concerning the Juvenile Criminal Justice System must apply. This graduated model ensures that child protection does not transform ordinary exposure or curiosity into a basis for stigmatization, unnecessary surveillance, or criminalization.

Legal reform must also be directed at strengthening the legal responsibility of social media and online game platforms as part of the child protection system in the digital space. In this context, a revision of Law Number 19 of 2016 concerning Electronic Information and Transactions is necessary to add a legal obligation for electronic system operators to implement child digital safety protection against the spread of radical ideology. Digital platforms must have an artificial intelligence-based content moderation system capable of automatically detecting extremist propaganda, hate speech, radical symbols, and digital recruitment patterns for children. Furthermore, social media and online gaming platforms must provide panic buttons and emergency reporting systems specifically for child protection, directly connected to Komdigi, the National Counterterrorism Agency (BNPT), and the Indonesian National Police. The government also needs to implement mandatory age verification systems and parental control protection on online gaming and social media platforms that feature open communication between users. To enforce the law, the state needs to impose administrative sanctions, restrict access, and even revoke operational permits on digital platforms that fail to prevent the spread of radicalism among children. These concrete steps are necessary because digital platforms have largely acted as neutral technological spaces without clear legal responsibilities for child safety in cyberspace.

The establishment of a Cyber Child Protection Monitoring Center and National Digital Early Warning System should constitute a central component of the reconstructed legal framework. However, the system should not function as a mechanism for indiscriminate monitoring of children's private online activities. Its operation must be based on the principles of legality, necessity, proportionality, data minimization, the best interests of the child, purpose limitation, and enhanced protection of children's personal data. The

Center should primarily conduct systemic risk analysis of publicly available or lawfully accessible digital content, patterns of coordinated extremist recruitment, high-risk virtual communities, and verified threats directed at children. Access to individually identifiable information should be restricted and permitted only where there is a specific legal basis and a demonstrable child-protection or national-security purpose. Routine monitoring must not involve unrestricted access to private communications, encrypted accounts, or children's personal data without the authorization and safeguards required by law.

In institutional terms, KPAI and the relevant child-protection authority should exercise primary responsibility for child case management and protection decisions, while BNPT should provide expertise concerning terrorism and radicalization risks; Polri should exercise law-enforcement authority where criminal conduct is indicated; Komdigi should coordinate platform regulation and digital-system compliance; educational and child-protection institutions should provide assessment and rehabilitation; and families should participate in child-centered intervention and recovery. No participating institution should automatically obtain unrestricted access to the national database. Sensitive data sharing should follow a role-based access system, whereby each institution may access only the information necessary for its statutory function. Every access, transfer, modification, and disclosure of data must be recorded through an auditable system. Children's identifiable information should be retained only for the period necessary for protection, assessment, rehabilitation, or legally authorized proceedings and should subsequently be deleted, anonymized, or otherwise securely disposed of.

The reconstruction of the legal system for handling children exposed to digital radicalism must also prioritize a rehabilitative and humanistic approach by strengthening child-specific deradicalization mechanisms based on psychological recovery and social reintegration. To date, an overly dominant security approach has often positioned children as ideological threats, neglecting their psychological and developmental aspects. Therefore, it is necessary to establish Child Digital Deradicalization Centers at the national and regional levels, involving child psychologists, psychiatrists, social workers, educators, moderate religious leaders, and cybersecurity experts in the rehabilitation process for children exposed to digital radicalism. Deradicalization programs must be implemented through educational and psychosocial approaches such as digital counseling, mental rehabilitation, tolerance education, social therapy, and family support. Furthermore, the government needs to develop a Digital Peace Ambassador program for children and adolescents as part of a counter-narrative strategy against radical propaganda on social media and online games. This procedure aligns with the principles of restorative justice and the best interests of the child, as stipulated in Law Number 11 of 2012 concerning the Juvenile Criminal Justice System and the Convention on the Rights of the Child. Thus, children are no longer positioned as mere objects of punishment, but as subjects of legal protection who must be restored and returned to a healthy social environment.

Legal reforms must also be implemented through the harmonization of criminal law, child protection law, and cyber law to prevent sectoral and overlapping responses to digital radicalism against children. The government needs to establish a unified regulation in the

form of a Child Protection Law in the Digital Space that integrates cybersecurity, child data protection, digital extremism prevention, and technology platform responsibilities within a single national legal system. This regulation should clarify the division of authority between institutions such as the National Counterterrorism Agency (BNPT), the National Police, Komdigi (Digital Commission for Child Protection), the Indonesian Child Protection Commission (KPAI), and educational institutions to prevent overlapping authority in monitoring and handling cases. Specifically, an Integrated Child Digital Protection System is needed to enable rapid data exchange and coordination between agencies through a single national database. Furthermore, the government needs to establish national operational standards for handling children exposed to digital radicalism, including identification, psychological assessment, rehabilitation, and social reintegration. This regulatory harmonization is crucial to address the weaknesses of the current legal system, which is still fragmented and lacks an effective national coordination model to address the threat of technology-based digital radicalism.

The child-specific rehabilitation and deradicalization model should not be evaluated solely on the basis of ideological conformity or a child's willingness to repeat prescribed narratives. Success must instead be measured through child-protection and developmental indicators. These indicators may include psychological stabilization; reduced vulnerability to manipulation and violent recruitment; improved critical digital literacy; the ability to identify harmful online content and coercive recruitment; restoration of healthy family and social relationships; regular participation in education or other age-appropriate social activities; the absence of verified continuing involvement in violent extremist recruitment or unlawful networks; and sustained social reintegration during a defined follow-up period. Assessment should be conducted periodically by a multidisciplinary team consisting, where appropriate, of child psychologists, social workers, educators, digital-safety specialists, and other competent professionals. No child should be considered to have failed rehabilitation merely because of lawful religious, political, or ideological beliefs. Intervention must focus on reducing harm, coercion, vulnerability, and the risk of violence rather than imposing ideological uniformity. The process should also provide a review mechanism to ensure that restrictive interventions are terminated once they are no longer necessary and proportionate.

Legal reconstruction and reform in the prevention and handling system for child victims of exposure to digital radicalism must be directed at developing a national legal system that is responsive to technological developments and oriented towards comprehensively protecting children's rights. The state cannot simply rely on a repressive approach and content blocking; it must also build a digital child protection ecosystem that encompasses adaptive regulations, technological oversight, digital education, psychological rehabilitation, and strengthening community social resilience. In particular, the government needs to establish a National Roadmap for Protecting Children from Digital Radicalism for 2026–2045 as a long-term strategic policy. The roadmap should include targets for strengthening regulations, developing digital monitoring technology, improving national digital literacy, and building a community-based deradicalization system. Furthermore, the

state needs to strengthen international cooperation with global platforms and international organizations in data exchange and monitoring cross-border radical propaganda. This legal reconstruction is a form of responsibility of the rule of law state, as affirmed in Article 1 paragraph (3) and Article 28B paragraph (2) of the 1945 Constitution of the Republic of Indonesia, which requires effective protection of children's rights amidst increasingly complex and transnational digital technology developments.

Conclusion

Based on the research results and discussion, it can be concluded that the development of social media and online games has transformed the spread of radicalism from conventional methods to digital radicalism, which is more covert, widespread, and difficult to monitor by conventional legal systems. Children are the most vulnerable group to exposure to radical ideology because they are in the identity-searching phase, have suboptimal digital literacy levels, and are highly active in digital spaces shaped by social media algorithms and online gaming virtual communities. The Indonesian legal system is fundamentally unable to fully address this growing threat because regulations on child protection, cyber law, and counterterrorism law are still operating partially and lack an integrated legal framework for protecting children from digital radicalism. These weaknesses are evident in the lack of specific regulations regarding child victims of exposure to digital radicalism, weak oversight of social media and online gaming platforms, the lack of a national early detection system, and the continued dominance of a repressive approach in handling children exposed to radical ideology. Therefore, legal reconstruction and reform are needed through reformulating digital-based child protection regulations, strengthening the legal responsibility of digital platforms, establishing a national early warning system, harmonizing child protection laws with cyber and criminal law, and developing a child-specific deradicalization model based on psychological rehabilitation, restorative justice, and social reintegration. These legal reforms are crucial for building a child protection system that is adaptive to developments in digital technology while ensuring the protection of children's rights in a democratic, human rights-based state governed by the rule of law.

As a follow-up to the findings of this study, the government needs to immediately revise the Child Protection Law and the Information and Electronic Transactions Law by including specific provisions regarding the protection of children from exposure to digital radicalism through social media and online games, including the legal obligations of digital platforms to moderate content, monitor algorithms, and protect child users. Furthermore, the government needs to establish integrated regulations regarding child protection in the digital space that integrate the authority of the National Counterterrorism Agency, the Indonesian National Police, the Ministry of Communication and Digital, educational institutions, and child protection agencies into a single, technology-based national coordination system. The state also needs to establish a national digital monitoring center based on artificial intelligence to detect radical propaganda against children in real time and establish digital rehabilitation and deradicalization centers specifically for children at the national and regional levels. In the education sector, schools are required to implement anti-radicalism digital literacy programs and strengthen tolerance education as part of the

national curriculum, while families need to be empowered through digital monitoring education programs for children. Furthermore, Indonesia needs to strengthen international cooperation with global platforms and other countries in monitoring transnational extremist propaganda and developing a digital safety system for children. Thus, legal reform is not only oriented towards repressive law enforcement, but also towards building a child protection system that is preventive, rehabilitative, humanistic, and responsive to future developments in digital technology.

References

- Ahdiyat, M. A. (2018). Analisis Keterlibatan Komunitas dalam Industri Permainan Daring di Indonesia. *Interaksi: Jurnal Ilmu Komunikasi*, 105–115.
- Aisy et al., B. R. (2019). Penegakan kontra radikalisme melalui media sosial oleh pemerintah dalam menangkalkan radikalisme. *Jurnal Hukum Magnum Opus*.
- Bastian, O. A. (2021). Urgensi literasi digital dalam menangkalkan radikalisme pada generasi millennial di era revolusi industri 4.0. *Jurnal Dinamika Sosial Budaya*, 126–133.
- Darwanta, A. (2020). Penerapan Prinsip Terbaik Untuk Anak (The Best Interest of The Child) dalam Pemenuhan Hak Anak di Lembaga Pembinaan Khusus Anak. *Reformasi Hukum*, 60–76.
- Huda, M. D., & Putra, A. G. (2025). Strategi Pencegahan Terorisme Melalui Pendidikan Karakter Dan Literasi Digital Di Kalangan Remaja. *Jurnal Riset Multidisiplin Edukasi*, 462–474.
- Hutagalung, R. H. (2025). Tinjauan Hukum Terhadap Anak-anak Terpapar Radikalisme dan Terorisme Menurut Hukum Positif di Indonesia. *Future Academia: The Journal of Multidisciplinary Research on Scientific and Advanced*, 769–780.
- Lubis, D., & Siregar, H. S. (2020). Bahaya radikalisme terhadap moralitas remaja melalui teknologi informasi (media sosial). *Aplikasia: Jurnal Aplikasi Ilmu-Ilmu Agama*, 21–34.
- Maharani, A. K. (2025). Pengaruh Media Sosial terhadap Radikalisme di Kalangan Gen Z: Studi Kasus di Pekanbaru. *Jurnal Kajian Hukum Dan Sosial Budaya*, 08–11.
- Miyazaki, A. F. (2024). Tantangan dan solusi dalam menghadapi era digital: Pendidikan anak di zaman teknologi. *JUPEIS: Jurnal Pendidikan Dan Ilmu Sosial*, 127–135.
- Nofanda, S. (2025). Kewenangan pemerintah melakukan keputusan akses sistem elektronik dalam perspektif Undang-Undang Informasi dan Transaksi Elektronik. *JUSTITIABLE-Jurnal Hukum*, 24–45.
- Saputra, T. E. (2024). Strategi Kepolisian Republik Indonesia Dalam Penanganan Anak Yang Terpapar Radikalisme Di Lingkungan Keluarga. *Vifada Assumption Journal of Law*, 13–25.
- Setianto, W. A. (2018). Literasi Konten Radikal di Media Online. *Jurnal Ilmu Komunikasi*, 75–88.
- Shabirin, A. (2025). Asas Legalitas dalam Penanggulangan Radikalisme Online: Perspektif Hukum Pidana Indonesia. *Jejak Digital: Jurnal Ilmiah Multidisiplin*, 333–344.
- Sudiarti, E. F. (2024). Peningkatan Pemahaman Siswa Mengenai Pengaruh Media Sosial terhadap Radikalisme di Kalangan Pelajar melalui Penyuluhan Hukum tentang Paham Radikalisme. *Pengabdianmu: Jurnal Ilmiah Pengabdian Kepada Masyarakat*, 859–866.

-
- Wiryany, D. S. (2022). Perkembangan teknologi informasi dan komunikasi terhadap perubahan sistem komunikasi Indonesia. *Jurnal Nomosleca*, 242–252.
- Zuhudin, M. H. (2023). Analisa yuridis perlindungan anak terlantar sebagai kewajiban negara dalam perspektif hukum positif di indonesia. *Unizar Recht Journal (URJ)*.