



DOI: <https://doi.org/10.38035/jgsp.v3i3>
<https://creativecommons.org/licenses/by/4.0/>

Legal Vacuum Analysis and the Need for Criminal Policy Reformulation in Handling Cyberbullying Cases in Indonesia based on the Perspective of Child Protection and the Law on Electronic Information and Transactions

Aji Yoga Sekar¹, Joko Setiono², Sutrisno³

¹Sekolah Tinggi Ilmu Kepolisian, Indonesia, agoyrakes230@gmail.com

²Sekolah Tinggi Ilmu Kepolisian, Indonesia, joko_setiono@ymail.com

³Sekolah Tinggi Ilmu Kepolisian, Indonesia, trisosuki@gmail.com

Corresponding Author: agoyrakes230@gmail.com¹

Abstract: The rapid development of digital technology has created a new space for internet-based crimes, one of which is cyberbullying targeting children as victims. This phenomenon continues to rise in Indonesia, in line with the high rate of social media usage among minors. Nevertheless, the existing legal system has not been sufficiently responsive in addressing cyberbullying specifically, especially when viewed from the perspective of child protection. The Law on Electronic Information and Transactions (Law No. 11 of 2008 in conjunction with Law No. 19 of 2016) does not explicitly regulate cyberbullying as a criminal offense, while the Child Protection Law (Law No. 23 of 2002 in conjunction with Law No. 35 of 2014 and Law No. 17 of 2016) also does not adequately cover digital-based violence. This normative and implementative gap creates difficulties in prosecuting perpetrators and risks neglecting the rights of children who are victims of cyberbullying. This paper analyzes the need for a reformulation of criminal policy through the establishment of specific norms that explicitly criminalize cyberbullying against children. The research uses a normative juridical approach and emphasizes the importance of integrating child protection into every criminal legal policy in the digital era. The proposed reformulation includes revising the norms in the ITE Law and the Child Protection Law, as well as strengthening the roles of law enforcement officers and digital platforms. The findings of this study highlight the urgency of criminal law reform that is not only repressive, but also preventive and rehabilitative for child victims.

Keywords: *Cyberbullying*, Children, Legal Vacuum, Electronic Information and Transactions Law (ITE Law), Child Protection, Criminal Policy Reformulation

Abstrak: Perkembangan teknologi digital yang pesat telah menciptakan ruang baru bagi kejahatan berbasis internet, salah satunya adalah perundungan siber yang menargetkan anak-anak sebagai korban. Fenomena ini terus meningkat di Indonesia, sejalan dengan tingginya tingkat penggunaan media sosial di kalangan anak-anak. Namun, sistem hukum yang ada belum cukup responsif dalam menangani perundungan siber secara khusus, terutama dari

perspektif perlindungan anak. Undang-Undang tentang Informasi dan Transaksi Elektronik (UU No. 11 Tahun 2008 junto dengan UU No. 19 Tahun 2016) tidak secara eksplisit mengatur cyberbullying sebagai tindak pidana, sementara Undang-Undang Perlindungan Anak (Undang-Undang Nomor 23 Tahun 2002 junto Undang-Undang Nomor 35 Tahun 2014 dan Undang-Undang Nomor 17 Tahun 2016) juga tidak cukup mencakup kekerasan berbasis digital. Kesenjangan normatif dan implementatif ini menimbulkan kesulitan dalam menuntut pelaku dan berisiko mengabaikan hak-hak anak yang menjadi korban cyberbullying. Makalah ini menganalisis kebutuhan akan reformulasi kebijakan pidana melalui penetapan norma-norma spesifik yang secara eksplisit mengkriminalisasi cyberbullying terhadap anak-anak. Penelitian ini menggunakan pendekatan yuridis normatif dan menekankan pentingnya mengintegrasikan perlindungan anak ke dalam setiap kebijakan hukum pidana di era digital. Reformulasi yang diusulkan meliputi revisi norma-norma dalam Undang-Undang ITE dan Undang-Undang Perlindungan Anak, serta penguatan peran aparat penegak hukum dan platform digital. Temuan penelitian ini menyoroti urgensi reformasi hukum pidana yang tidak hanya represif, tetapi juga preventif dan rehabilitatif bagi korban anak.

Kata Kunci: Cyberbullying, Anak-anak, Kekosongan Hukum, Undang-Undang Informasi dan Transaksi Elektronik (ITE Law), Perlindungan Anak, Reformulasi Kebijakan Pidana

INTRODUCTION

The phenomenon of cyberbullying against children in Indonesia is becoming increasingly alarming in line with the rapid development of information technology (Zuanda, 2024). Children's wide access to the internet through personal devices such as smartphones opens up limitless spaces for social interaction, but also creates vulnerabilities to digital-based violence (Ulfah, 2020). Children, who are still in the stages of psychological and emotional development, are particularly vulnerable to the serious effects of bullying behavior in the virtual world (Harmiasih, 2023). Common forms of cyberbullying include insults, threats, dissemination of private content, and harassment carried out anonymously or openly via social media and messaging apps (Saimima, 2020). This condition shows that the domain of violence against children has shifted not only in physical spaces, but also into digital realms that are difficult to control. Even though it is virtual, the psychological impact is real, including anxiety disorders, depression, and even suicide (Kumala, 2020).

Existing laws and regulations in Indonesia do not yet specifically provide comprehensive arrangements regarding acts of cyberbullying, especially when children are the targeted victims (Fikri, 2023). Law No. 11 of 2008 on Electronic Information and Transactions (ITE), which was amended by Law No. 19 of 2016, only regulates in general terms regarding insults and defamation in the digital realm, without explicitly mentioning bullying behaviors (Paat, 2020). Articles such as Article 27 and Article 28 remain open to multiple interpretations when defining elements like "content that violates decency" or "spreading hatred," and have yet to specifically address the motives and impacts of online bullying against children (Tan, 2022). The absence of specific offense formulations weakens law enforcement and often fails to provide adequate protection to victims. In practice, cases of cyberbullying against children are frequently not followed up due to the lack of legal certainty in classifying the offense. This situation reflects a clear normative gap in our legal system (Hafidz, 2021).

This legal vacuum becomes even more complex when linked to Law No. 23 of 2002 on Child Protection, which has undergone amendments through Law No. 35 of 2014 and Law No. 17 of 2016. These regulations do affirm that every child has the right to be protected from violence, including psychological violence (Hidayat, 2021). However, they do not explicitly encompass violence in digital or information technology-based forms, so their implementation

has not yet addressed cyberbullying as a contemporary form of violence. The existing protection instruments are still oriented toward physical and explicit violence, which can be easily proven through medical examinations or direct witnesses. In the context of digital violence, whose traces can be easily erased or disguised, evidence gathering becomes more complicated and requires more up-to-date legal approaches. This leaves children as a highly vulnerable group without clear legal protection.

Law No. 1 of 2023 on the National Criminal Code (KUHP), which was recently enacted as a revision of the old KUHP, also does not explicitly regulate cyberbullying. Although it includes provisions on insults, defamation, and the dissemination of hatred, the formulations remain general and do not yet respond to the complexities of digital violence (Amalia, 2025). The new Criminal Code does show progress in terms of embracing restorative justice values and victim protection, but it still falls short of adapting to the challenges posed by information technology. Cyberbullying, which often involves the dissemination of personal data, digital manipulation, or incitement on social media, requires its own category within national criminal law (Hutabarat, 2023). The lack of explicit legal recognition of cyberbullying leaves law enforcement heavily reliant on the subjective interpretation of law enforcers, which is highly prone to being unsympathetic toward child victims. This is a crucial reason to acknowledge the existence of legal gaps both in terms of substance and enforcement structure.

Child protection theory emphasizes that every child has inherent basic rights from birth and must be protected by the state from all forms of violence and discrimination (Arliman, 2024). The right to a sense of security, protection from psychological trauma, and optimal self-development should be prioritized in every legal policy. In the digital context, violations of these rights occur subtly, systematically, and with long-lasting effects. Cyberbullying not only harms a child's mental state but also robs them of self-confidence, safety, and emotional stability needed during their developmental stages (Freska, 2023). A legal system that neglects such forms of violence risks prolonging the suffering of children. Child protection theory demands a more holistic and adaptive legal approach to the evolving dynamics of violence today.

Criminal law theory provides a foundation that criminal law not only punishes wrongdoing but also protects the most essential legal interests in society (Angraeni, 2024). In this context, protecting children as vulnerable legal subjects is part of the primary public legal interest (Wijaya, 2023). The function of criminal law as an *ultimum remedium* must be balanced with selective but targeted policies to protect victims (Wahidah, 2025). The criminal act of cyberbullying, which has the potential to cause permanent psychological damage, falls into the category of crime that warrants criminal response when preventive efforts have failed (Isnawan, 2023). As the digital space becomes an integral part of children's social lives, criminal law must adapt to be actively present in that space. The absence of specific regulations indicates a failure of criminal law to fully carry out its protective function.

The concept of a legal vacuum helps explain why the legal system is unable to respond effectively to cases of cyberbullying. A normative vacuum occurs when the law lacks clear or explicit norms for an act that has developed in society. Meanwhile, an implementation vacuum arises when norms do exist, but cannot be enforced due to institutional limitations, lack of understanding among officials, or inadequate supporting technologies (Atikah, 2023). In the case of cyberbullying, both types of vacuum occur simultaneously. Not only are explicit normative rules absent, but also reporting mechanisms, proof gathering, and victim recovery systems have not been systematically developed. This vacuum creates structural injustice for children as victims of digital crime.

The need for legal reform cannot be delayed when the law is no longer able to meet the demands of justice in society, especially regarding vulnerable groups such as children. In this context, the legal void surrounding cyberbullying is an indicator that the legal system is no

longer adaptive to new forms of violence (Jinner Sidauruk, 2024). The reformulation of criminal policy is not merely about adding criminal threats, but about redesigning legal instruments so that they can protect victims in a real and humane way. What is needed are explicit regulations, effective reporting systems, and psychological recovery support for child victims. A child-centered legal reform effort will affirm that the state is present not only in the form of punishment but also through restorative justice. The fulfillment of children's rights in the digital space is part of the state's constitutional responsibility to protect all its citizens.

METHOD

This research employs a normative juridical method using both statutory and conceptual approaches. The statutory approach is carried out by critically and systematically examining the positive legal provisions in force in Indonesia, particularly those related to the criminal act of cyberbullying and child protection. The main laws that serve as the focus of this research include Law Number 11 of 2008 on Electronic Information and Transactions as amended by Law Number 19 of 2016, Law Number 23 of 2002 on Child Protection as amended by Law Number 35 of 2014 and Law Number 17 of 2016, as well as Law Number 1 of 2023 concerning the Criminal Code (New Criminal Code). This study also examines the extent to which these legal norms are capable of responding to legal challenges posed by the phenomenon of cyberbullying experienced by children. In addition, the conceptual approach is used to understand the fundamental concepts of child protection, children's human rights in the digital context, and the principles of restorative justice in juvenile criminal law. This approach is also employed to formulate ideas for a more just, comprehensive, and child-oriented reformulation of criminal policy. By combining these two approaches, the research aims to identify existing legal gaps and provide normative solutions that can be adopted by lawmakers in drafting more progressive and responsive regulations in line with developments in information technology.

RESULT AND DISCUSSION

Analysis of the Legal Vacuum in Handling Cyberbullying Against Children

The phenomenon of cyberbullying against children encompasses a broad spectrum in both form and intensity. Acts such as *flaming* (online verbal insults), *harassment* (sending offensive messages repeatedly), *denigration* (spreading false information to damage someone's reputation), *outing* (publicly disclosing private secrets), *impersonation* (pretending to be the victim to spread harmful content), and *cyberstalking* (repeated online threats or surveillance) frequently occur on platforms such as social media (Instagram, TikTok, WhatsApp), interactive online games, and digital discussion forums. These forms often occur covertly and intensively, making them difficult to detect through conventional legal systems. Their impact on children is far deeper due to their psychological and social vulnerability. In many cases, victims are unaware that what they are experiencing qualifies as digital violence. This lack of awareness increases the long-term risks to their mental and emotional development.

The legal instruments currently used to address cyberbullying against children, particularly through Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), do not explicitly include definitions or provisions that classify cyberbullying as a criminal offense. Frequently cited articles such as Article 27 paragraph (3) on defamation and Article 29 on threats of violence are ambiguously worded and do not specifically address the unique characteristics of cyberbullying. Article 28 paragraph (2), which prohibits hate speech based on ethnicity, religion, race, or group (SARA), also does not cover all types of offensive acts against children in non-SARA contexts. This lack of clear norms hinders legal enforcement, often from the initial stage of identifying the offense. Perpetrators may go unpunished due to normative gaps

that fail to capture the unique digital methods they employ. Meanwhile, victims are denied a sense of justice due to the limitations of existing regulations.

The issue becomes even more complex when viewed from the perspective of child protection, which should be a primary concern of the state. Law Number 23 of 2002 on Child Protection, last amended by Law Number 17 of 2016, does indeed regulate violence against children in general terms but does not explicitly cover technology-based violence. Article 9 paragraph (1) states that every child has the right to protection from all forms of violence and discrimination, but its implementation remains weak in the context of digital violence. Article 76C prohibits anyone from committing violence against children, but there is no further explanation on whether digital violence falls into this category. The criminal norms in Article 80, which stipulate penalties for physical and/or psychological violence against children, still do not accommodate the characteristics of acts that occur in cyberspace. This ambiguity causes uncertainty during the investigation and prosecution processes of cyberbullying against children.

It is important to note that there is not a single article in either the Child Protection Law or the ITE Law that directly criminalizes cyberbullying against children. As a result, law enforcement officers often struggle to find the appropriate legal basis to prosecute perpetrators. Acts such as posting insulting memes, editing and sharing manipulated images of children, or uploading humiliating content about them often do not meet the elements required under existing ITE provisions, particularly regarding the formal legal definition of defamation. In many cases, prosecutors or police are forced to draw analogies to existing articles, which risks violating the principle of legality. This illustrates a serious substantive legal vacuum in the protection of children from digital violence.

Child-friendly detection and reporting systems also pose a separate challenge. Many child victims are reluctant to report incidents out of fear of being blamed or not believed. Existing complaint services are still centralized and do not reach rural areas, leaving children in remote regions unsure of where to report. On the other hand, law enforcement officials have not yet been adequately trained to handle reports made by children. The weakness of this reporting system is a barrier to building valid and systematic data on cyberbullying incidents. Without accurate data, both preventive policies and legal interventions are difficult to design effectively. This reflects a vacuum not only in normative frameworks but also in protection mechanisms and legal responses.

The shortage of human resources in the police and prosecutor's office further exacerbates the implementation gap. Many officers lack the skills to identify digital evidence such as screenshots, chat logs, or metadata from social media uploads as valid legal evidence. Knowledge of digital forensic techniques and authentication processes remains limited. In practice, digital evidence is often deemed insufficient to support criminal proceedings due to perceptions that it is easily manipulated. This makes it difficult to prove cyberbullying cases that rely entirely on digital footprints. As a result, many cases are dropped during the investigation stage due to the failure to meet formal and material requirements.

Technical standards for handling digital evidence have not yet been nationally standardized, resulting in disparities between legal jurisdictions. Some regions have relatively advanced cyber teams, while others still rely on conventional methods to investigate cyber cases. This disparity creates inequality in access to justice for cyberbullying victims, especially children from poor families or remote areas. When an act cannot be technically proven, legal proceedings stall, and public trust in law enforcement diminishes. A national standard is needed that requires every regional police office to have a digital forensic unit with sufficient expertise and facilities.

Psychological and social barriers faced by victims also contribute significantly to the low reporting rates. Children who are victims of cyberbullying often experience trauma, fear

of stigma, and pressure from their social environments. Many feel that no one can help or understand what they are going through. In some cases, the victim's family even chooses not to report the incident for fear of "shaming" the family's reputation. These factors indicate that the legal system does not yet provide a sense of safety and comfort for children to report their experiences. When the system is not inclusive or child-friendly, the law loses its relevance in delivering true justice.

Articles in the New Criminal Code, namely Law Number 1 of 2023, have indeed revised a number of offenses previously regulated in the ITE Law, such as defamation (Articles 435–437) and hate speech (Article 263). However, these articles are still general in nature and do not specifically mention digital crimes, especially those involving children as victims. Existing legal norms remain focused on actions in the physical public space and have not yet fully adapted to the rapidly evolving digital environment. The difficulty in applying these articles to forms of cyberbullying highlights the urgent need for codification and specification of technology-based offenses, particularly those targeting vulnerable groups such as children.

A number of cyberbullying actions also intersect with elements of online harassment, which should ideally fall under Law Number 12 of 2022 on Sexual Violence Crimes. Article 14 paragraph (1) point c, for instance, regulates electronic-based sexual violence, including the distribution of sexual content without the victim's consent. However, this provision is limited to sexual violence and does not cover non-sexual insults or intimidation that frequently occur in cyberbullying against children. This illustrates the importance of regulatory integration so that approaches to cyberbullying are not fragmented and can address the full scope of digital violence. Legal reformulation is necessary to align child protection in the cyber world with the principles of human rights and substantive justice.

The Urgency of Reformulating Criminal Policy in Addressing Cyberbullying Based on Child Protection

The development of criminal policy in various countries shows that cyberbullying has been treated as a crime requiring special handling. In the United States, several states such as California and New York have specific laws criminalizing bullying behavior in cyberspace, with a child protection-based approach. The United Kingdom, through the *Malicious Communications Act 1988* and the *Communications Act 2003*, has categorized offensive communication through electronic media as a criminal offense. The Philippines enacted the *Anti-Bullying Act of 2013*, which includes cyberbullying as a prohibited act in educational environments. Lessons from these countries demonstrate that specific and firm criminal norms on cyberbullying are more effective in delivering justice to child victims. In the context of Indonesia, the absence of equivalent regulations further emphasizes the urgency of formulating specific offenses related to cyberbullying within the national legal system. This effort would reduce reliance on vague laws and strengthen the legal position of children as victims of digital violence.

A proper understanding of the nature of cyberbullying underlines the need to separate this offense from general offenses like defamation or insult. Article 27 paragraph (3) of the Electronic Information and Transactions Law (ITE Law) Number 11 of 2008 jo. Law Number 19 of 2016 does regulate defamation or insults via electronic systems, but it does not yet address the complexity of cyberbullying, especially those that affect children. Cyberbullying offenses involve psychological aspects, imbalanced power dynamics, and repeated attack patterns, which are not necessarily reflected in the standard elements of defamation. Legal proceedings also often face difficulties due to the absence of legal indicators and criteria to distinguish cyberbullying from typical online disputes or hate speech. Reformulation is necessary so that victims, law enforcement, and judges have clear guidelines for classifying and addressing

cyberbullying cases. This normative clarity will support the effectiveness of child protection in the ever-evolving digital space.

The reformulation of criminal policy in this context must also be grounded in child protection, recognizing children as legal subjects requiring special approaches. Law Number 35 of 2014, amending Law Number 23 of 2002 on Child Protection, does not explicitly include digital violence as a form of violence against children. Articles 76C and 76D mention physical and psychological violence, but do not specify that violence through digital means can also result in serious psychological harm. This legal vacuum often leaves child victims unprotected, especially when cases do not meet the threshold of direct physical violence. The inclusion of a specific clause in the definition of violence against children—covering harassment, intimidation, and threats through digital media—is therefore crucial. More inclusive regulation will facilitate legal proof and recovery for victims while also serving as a strong preventive tool for society.

Recovery for children who are victims of cyberbullying cannot rely solely on criminal prosecution of the perpetrator. The criminal justice system must integrate restorative approaches, including provisions for rehabilitation and psychological recovery for child victims. Article 59A paragraph (2)(b) of the Child Protection Law states that child victims of violence are entitled to rehabilitation, yet its implementation remains very limited in the context of digital crimes. Many victims of cyberbullying experience long-term trauma, social anxiety, or even depression, which require professional psychological support. The addition of specific norms regarding post-incident recovery services and protection will guarantee a child's right to grow up in a safe environment. The state must ensure that the legal system not only punishes perpetrators but also restores victims' well-being to prevent prolonged suffering.

The involvement of digital platforms in preventing and addressing cyberbullying must be normatively mandated in national law. Currently, there are no regulations that explicitly require social media or digital applications to provide safe and rapid reporting systems for children who are victims of digital violence. Law Number 27 of 2022 on Personal Data Protection (PDP Law) does regulate user data protection, but it does not yet address corporate responsibility in preventing the spread of harmful content such as bullying. Introducing legal obligations for digital platforms—both domestic and foreign—to actively monitor and remove cyberbullying content would be a major step forward. These obligations could be detailed in implementing regulations that cover detection standards, reporting systems, and algorithm transparency. The involvement of tech companies is an essential part of the child protection ecosystem and cannot be overlooked.

The ITE Law, as the main legal framework for regulating digital crimes, needs adjustments to make it more responsive to the conditions of child victims. Articles such as Article 27 paragraph (3), Article 28 paragraph (2), and Article 29 are often used to prosecute defamation or hoax dissemination but are not sensitive to children as vulnerable parties. Revisions to the ITE Law should include the addition of an article on cyberbullying that contains clear elements, including perpetrators who repeatedly send threatening, insulting, or harassing messages to children via digital media. Such formulation would clearly distinguish between ordinary online conflicts and digital crimes targeting children. Firm regulation will provide a stronger legal foundation for law enforcement. Legal certainty will also enhance the child's standing in judicial processes as a party entitled to special treatment.

The new national Criminal Code, Law Number 1 of 2023, opens the door for integrating provisions on digital crimes into general criminal law. Book Two of the Criminal Code, which covers offenses against personal liberty and honor—such as Article 435 on defamation—can serve as a basic framework for regulating cyberbullying if normatively expanded. Additional norms should be drafted in this Criminal Code to define cyberbullying as a specific offense against the dignity and psychological well-being of children. The existence of *lex generalis*

norms in the Criminal Code will allow synchronization with sectoral laws such as the ITE Law and the Child Protection Law as *lex specialis*. This integration is essential to avoid overlapping norms or legal vacuums in enforcement practice. Harmonization among regulations will also accelerate the legal response to the continually evolving phenomenon of cyberbullying.

The development of responsive implementing regulations in line with technological developments is an integral part of criminal policy reformulation. Many general legal provisions cannot be effectively implemented without detailed technical and operational guidelines. Ministerial regulations, government regulations, and Supreme Court circulars must be drafted with close attention to the fast-paced dynamics of the digital world. Technical aspects such as online reporting procedures, standardized digital forensics for children, and ethical guidelines for investigating child victims must be explicitly regulated. This process will create legal certainty and increase public trust—especially that of victims—in the legal system. Implementing regulations also serve as control tools to prevent misconduct by law enforcement in handling cyberbullying cases involving children.

Strengthening criminal policy to address cyberbullying cannot rely solely on repressive measures against perpetrators. The reformulation of legal norms must align with prevention efforts through education and digital literacy for both children and parents. Long-term legal strategies require the involvement of schools, families, and communities in creating a safe and supportive digital environment. This multidisciplinary approach can be incorporated into the preamble or general explanation of the regulation to strengthen the conceptual framework of criminal law. Legal norms should not function solely as tools of punishment but also as instruments of education and prevention. Inclusiveness in the formulation of criminal policy is a tangible manifestation of child protection as mandated by the constitution.

Protecting children from cyberbullying, as a continuously evolving form of digital crime, requires a legal design that is adaptive, progressive, and humane. A criminal policy reformulated with attention to the characteristics of child victims, technological developments, and online behavior will bring about significant change in the legal protection of children in Indonesia. The legal uncertainty that has long hindered case resolution must be addressed through the creation of focused and integrated norms. The state bears a constitutional obligation to provide security for all its citizens, especially children as the most vulnerable group. Through criminal policy reform based on child protection, Indonesia can build a legal system that is fairer, more effective, and more civilized in facing the challenges of digital crime in the modern era.

CONCLUSION

The handling of cyberbullying crimes targeting children still suffers from gaps, both in terms of legal norms and implementation in the field. Existing laws, such as Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), as well as Law Number 23 of 2002 on Child Protection as amended by Law Number 35 of 2014, do not specifically regulate digital violence or cyberbullying in a comprehensive manner. This situation results in ambiguity in legal application, especially when it comes to distinguishing between hate speech, general insults, and repeated digital violence against children in online spaces. The absence of specific norms leads to a reactive legal response that does not take the victim's side and fails to provide legal certainty for the harmed party, particularly children. In the context of child protection, regulations should not only impose sanctions on perpetrators but also ensure the psychosocial recovery of victims who are still in developmental stages. A reformulation of criminal policy is needed—one that classifies cyberbullying as a specific offense, using an approach that prioritizes the best interests of the child, as emphasized in Articles 4 and 21 of the Child Protection Law.

The government, together with the House of Representatives, must draft specific provisions that explicitly regulate the criminal act of cyberbullying, either through revisions to the Child Protection Law or improvements to the ITE Law. The creation of an article that clearly recognizes cyberbullying as a form of violence against children will provide a solid legal foundation for law enforcement to act swiftly and accurately in addressing such cases. Law enforcement officers, including police, prosecutors, and judges, must also receive specialized training on the characteristics of digital crimes and victim-centered approaches to prevent re-victimization of children. This effort must be supported by an accessible, child-friendly reporting system that is integrated with psychological assistance services and legal counseling. It is also essential to carry out widespread public education about the dangers of cyberbullying, involving schools, parents, and digital platforms, in order to cultivate a safe digital culture for children. Protecting children in the digital world requires more than just written regulations -it must be realized through a system of prevention, early intervention, and effective handling to secure the future of children as the next generation of the nation.

REFERENCES

- Amalia, M. R. (2025). *Kitab Undang Undang Hukum Pidana Tahun 2023*. Jambi: PT. Sonpedia Publishing Indonesia.
- Angraeni, N. B. (2024). *Hukum Pidana: Teori Komprehensif*. Jambi: PT. Sonpedia Publishing Indonesia.
- Arliman, L. (2024). Teori Dan Konsep Perlindungan Anak Di Indonesia. *Ensiklopedia of Journal*, 6(3), 325-331.
- Atikah, I. S. (2023). Yurisprudensi sebagai Upaya Koreksi terhadap Kekosongan dan Kelemahan Undang-Undang. *YUDHISTIRA: Jurnal Yurisprudensi, Hukum dan Peradilan*, 1(2), 61-69.
- Fikri, A. M. (2023). Analisis Awal Terhadap Dinamika Penanggulangan Cyberbullying di Ruang Digital Indonesia Dalam Perspektif Hukum Pidana. *UNES Law Review*, 6(1), 2306-2317.
- Freska, N. W. (2023). *Bullying dan kesehatan mental remaja*. Bantul: CV. Mitra Edukasi Negeri.
- Hafidz, J. (2021). Cyberbullying, Etika Bermedia Sosial, dan Pengaturan Hukumnya. *Jurnal Cakrawala Informasi*, 1(2), 15-32.
- Harmiasih, S. K. (2023). Dampak Bullying terhadap Sosial Emosional Anak. *JlIP-Jurnal Ilmiah Ilmu Pendidikan*, 6(11), 8703-8708.
- Hidayat, A. (2021). Kekerasan terhadap anak dan perempuan. *AL-MURABBI: Jurnal Studi Kependidikan dan Keislaman*, 8(1), 22-33.
- Hutabarat, S. A. (2023). *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. Jambi: PT. Sonpedia Publishing Indonesia.
- Isnawan, F. (2023). Tinjauan hukum pidana tentang fenomena cyberbullying yang dilakukan oleh remaja. *Jurnal Interpretasi Hukum*, 4(1), 145-163.
- Jinner Sidaurok, S. H. (2024). PERLINDUNGAN HUKUM TERHADAP ANAK KORBAN CYBERBULLYING DI INDONESIA. *JURNAL MASYARAKAT HUKUM PENDIDIKAN HARAPAN*, 2(01).
- Kumala, A. P. (2020). Dampak cyberbullying pada remaja. *Alauddin Scientific Journal of Nursing*, 1(1), 55-65.
- Paat, L. N. (2020). Kajian Hukum Terhadap Cyber Bullying Berdasarkan Undang-Undang Nomor 19 Tahun 2016. *Lex Crimen*, 9(1), 13-23.
- Saimima, I. D. (2020). Anak korban tindak pidana perundungan (cyberbullying) di media sosial. *Jurnal Kajian Ilmiah*, 20(2), 125-136.

- Tan, K. (2022). Analisa Pasal Karet Undang-Undang Informasi Dan Transaksi Elektronik Terhadap Asas Kejelasan Rumusan. *Jurnal Hukum Samudra Keadilan*, 17(1), 14-29.
- Ulfah, M. (2020). *DIGITAL PARENTING: Bagaimana Orang Tua Melindungi Anak-anak dari Bahaya Digital?* Tasikmalaya: Edu Publisher.
- Wahidah, N. (2025). Fungsi Hukum Pidana. *JUSTITIA: Journal of Justice, Law Studies, and Politic*, 1(01), 8-16.
- Wijaya, M. R. (2023). PERLINDUNGAN SUBJEK HUKUM DALAM PERKEMBANGAN TEKNOLOGI DITINJAU DARI PERSPEKTIF HUKUM DAN HAK ASASI MANUSIA. *Marwah Hukum*, 1(1), 21-28.
- Zuanda, N. R. (2024). TREN PENELITIAN CYBERBULLYING DI INDONESIA. *EDU RESEARCH*, 5(1), 55-62.