

Legal Uncertainty, Criminal Liability, and Justice in Adolescent Cyberbullying Cases

Zalfa Aqilah Rajwa¹✉, Kiranut Thamwiset Anurakphong², Nalinrada Pimsuda Wattanakul², Ridwan Arifin^{3,4}, Auliya Rochman⁵

¹ Faculty of Law, Universitas Pendidikan Indonesia, Bandung, Indonesia

² School of Law, Bangkok University, Bangkok, Thailand

³ Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

⁴ Faculty of Law, Universitat de Barcelona, Barcelona, Spain

⁵ Auliya Rochman and Partners Law Office, Pontianak, Indonesia

✉ Corresponding Email: zalfarajwa@upi.edu

ABSTRACT

The rapid expansion of digital technology has intensified the phenomenon of cyberbullying, with adolescents constituting a particularly vulnerable group. This study examines legal uncertainty in the construction of criminal liability for cyberbullying perpetrators and evaluates the effectiveness of its enforcement within the Indonesian criminal justice system. Employing a normative-empirical juridical method, the research analyzes statutory frameworks, including the Information and Electronic Transactions Law and the Indonesian Criminal Code, alongside selected court decisions with permanent legal force. The findings reveal that although existing legal instruments may be used to prosecute cyberbullying-related conduct, the absence of an explicit legal definition of cyberbullying generates interpretative ambiguity and inconsistency in the application of offense elements. Furthermore, structural constraints such as limited digital forensic capacity and procedural challenges in evidence collection weaken enforcement effectiveness. Socio-cultural factors, including stigma and low reporting rates among adolescent victims, further exacerbate under-enforcement. This study highlights that the current legal framework has not yet adequately addressed the specific characteristics of cyberbullying as a digitally mediated form of harm. It recommends regulatory harmonization through the explicit codification of cyberbullying as a distinct offense, alongside strengthening institutional capacity and promoting digital literacy as a complementary non-penal preventive strategy. The study contributes to ongoing debates on cybercrime regulation and child protection in digital environments.

KEYWORDS *Cyberbullying, Criminal Liability, Legal Uncertainty, Adolescents, Digital Forensics*

TABLE OF CONTENTS

I. INTRODUCTION	48
II. CONCEPTUALIZING CYBERBULLYING AND LEGAL PROTECTION FOR ADOLESCENTS	52
A. <i>Cyberbullying as a Legal Concept</i>	52
B. <i>Adolescents as Subjects of Criminal Law Protection</i>	56
III. INDONESIAN LEGAL FRAMEWORK AND LEGAL UNCERTAINTY ON CYBERBULLYING	59
A. <i>Indonesian Criminal Law Framework Governing Cyberbullying</i> ...	59
B. <i>Legal Uncertainty in Determining Criminal Liability</i>	61
IV. TOWARDS REGULATORY HARMONIZATION AND NORMATIVE REFORM	64
V. STRUCTURAL, SUBSTANTIAL, AND CULTURAL OBSTACLES IN COUNTERING CYBERBULLYING	67
VI. CONCLUSION	71

I. INTRODUCTION

The rapid advancement of digital technologies has fundamentally transformed patterns of communication, social interaction, and identity formation among adolescents. While digital platforms have expanded opportunities for education, participation, and social engagement, they have simultaneously created new avenues for violence, intimidation, and psychological abuse through cyberbullying. Unlike conventional bullying, cyberbullying occurs through information and communication technologies, enabling perpetrators to inflict repeated harm regardless of geographical or temporal boundaries. The anonymity afforded by digital platforms, the rapid dissemination of harmful content, and the permanence of digital records significantly intensify the severity of victimization and complicate legal intervention.¹ Consequently, cyberbullying has evolved beyond a social or educational concern into a complex legal issue requiring effective regulatory and institutional responses.

Globally, cyberbullying has become one of the most significant threats to children's rights in digital environments. International organizations consistently report increasing levels of online harassment, humiliation, identity attacks, and hate speech targeting adolescents through social media, instant messaging applications,

¹ Sameer Hinduja, and Justin W. Patchin. *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. 2nd ed. (Thousand Oaks, California: Corwin Press, 2015); Sameer Hinduja, and Justin W. Patchin. "Connecting Adolescent Suicide to the Severity of Bullying and Cyberbullying." *Journal of School Violence* 18, no. 3 (2019): 333–346. <https://doi.org/10.1080/15388220.2018.1492417>; Robin M. Kowalski, et al. "Bullying in the Digital Age: A Critical Review and Meta-Analysis." *Psychological Bulletin* 140, no. 4 (2014): 1073–1137. <https://psycnet.apa.org/doi/10.1037/a0035618>

and other digital platforms.² Some various studies further demonstrates that cyberbullying victimization is strongly associated with depression, anxiety, social withdrawal, self-harm, and suicidal ideation among young people.³ Because cyberbullying extends beyond the physical boundaries of schools and communities, victims often experience continuous exposure to harmful conduct, making legal protection substantially more challenging than in cases of conventional bullying.⁴

From a criminal law perspective, cyberbullying is increasingly recognized as a violation of fundamental human rights, particularly the rights to dignity, privacy, personal security, and freedom from violence in digital spaces. This normative recognition is reflected in United Nations Human Rights Council Resolution 32/13, 2016⁵, which affirms that the same human rights enjoyed offline must also be protected online and emphasizes the responsibility of States to provide effective legal protection against violations committed through digital technologies.⁶ Accordingly, governments are expected to establish legal frameworks capable of ensuring accountability for online abuse while simultaneously safeguarding due process and other fundamental rights. However, translating these international principles into effective domestic criminal legislation remains a considerable challenge, particularly in jurisdictions where cyberbullying has not yet been expressly recognized as an independent criminal offense.

Indonesia exemplifies this regulatory challenge. The rapid expansion of internet access and social media use among adolescents has been accompanied by a growing number of cyberbullying incidents involving school-aged children. Nevertheless, many cases remain unreported because victims frequently fear retaliation, social stigma, secondary victimization, and ineffective legal remedies.⁷ Although cyberbullying-related conduct may be prosecuted under Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law)⁸, the Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana*, KUHP)⁹, and other sectoral legislation concerning child protection¹⁰, Indonesian criminal law does not provide

² UNESCO. *Behind the Numbers: Ending School Violence and Bullying*. (Paris: UNESCO, 2019); UNICEF. *Cyberbullying: What Is It and How to Stop It*. (New York: UNICEF, 2020).

³ Ann John, et al. "Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review." *Journal of Medical Internet Research* 20, no. 4 (2018): e129. <https://doi.org/10.2196/jmir.9044>. See also Kowalski, et al. "Bullying in the Digital Age: A Critical Review and Meta-Analysis."

⁴ Robert Slonje, Peter K. Smith, and Ann Frisé. "The Nature of Cyberbullying and Strategies for Prevention." *Computers in Human Behavior* 29, no. 1 (2013): 26–32. <https://doi.org/10.1016/j.chb.2012.05.024>

⁵ See United Nations Human Rights Council (UNHRC). *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. Resolution A/HRC/RES/32/13, 2016.

⁶ UNHRC. Resolution A/HRC/RES/32/13, 2016.

⁷ UNICEF. *Cyberbullying: What Is It and How to Stop It*.

⁸ See Republic of Indonesia. *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE Law)*. Available online at https://jdih.komdigi.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008

⁹ See Republic of Indonesia. *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Available online at <https://peraturan.bpk.go.id/details/234935/uu-no-1-tahun-2023>

¹⁰ See Republic of Indonesia. *Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak*. Available online at <https://dev-jdih.bphn.go.id/doc/1596633>; Republic of Indonesia. *Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan Atas UU Nomor 23 Tahun 2002 tentang Perlindungan Anak*. Available online at <https://dev-jdih.bphn.go.id/doc/1325858>; Republic of Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP Law)*.

a comprehensive statutory definition of cyberbullying nor explicitly codify it as a distinct criminal offense. Instead, law enforcement authorities must interpret cyberbullying through fragmented provisions concerning electronic defamation, threats, harassment, dissemination of unlawful electronic information, or other general criminal offenses. This fragmented normative framework frequently generates legal uncertainty in determining the constituent elements of criminal liability, encourages inconsistent prosecutorial and judicial interpretation, and weakens legal certainty in criminal law enforcement, particularly in cases involving adolescent perpetrators and victims whose legal interests require equal protection.

The problem of legal uncertainty becomes more complex when cyberbullying cases involve juvenile offenders. Contemporary juvenile justice systems are founded upon principles of rehabilitation, diversion, restorative justice, and the best interests of the child rather than purely punitive objectives.¹¹ At the same time, victims of cyberbullying may experience severe and long-lasting psychological harm requiring effective legal protection and meaningful access to justice. Consequently, determining criminal liability in adolescent cyberbullying cases requires balancing competing legal interests between protecting children in conflict with the law and ensuring justice for victims. This challenge is further complicated by evidentiary issues associated with electronic evidence, digital forensic investigation, attribution of online conduct, and the interpretation of criminal intent within digitally mediated interactions.

Previous studies have extensively examined cyberbullying from psychological, educational, criminological, and public health perspectives. Meta-analyses consistently demonstrate strong associations between cyberbullying victimization and adverse mental health outcomes among adolescents.¹² Other scholars have explored risk factors, online behavior, school-based prevention programs, and digital literacy interventions aimed at reducing cyberbullying among children and adolescents.¹³ Legal scholarship has primarily focused on issues of online harassment, freedom of expression, intermediary liability, privacy protection, and comparative cybercrime regulation.¹⁴ Within the Indonesian context, existing research generally discusses cyberbullying from the perspectives of victim protection, the implementation of the Electronic Information and

Available online at https://jdih.komdigi.go.id/produk_hukum/view/id/832/t/undangundang+nomor+27+tahun+2022

¹¹ See United Nations. *Convention on the Rights of the Child*, 1989.

¹² Kowalski, et al. "Bullying in the Digital Age: A Critical Review and Meta-Analysis"; John, et al. "Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review."

¹³ See Hinduja, and Patchin. *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*; Slonje, et.al. "The Nature of Cyberbullying and Strategies for Prevention.". See also Robert S. Tokunaga, "Following You Home from School: A Critical Review of Cyberbullying Research." *Computers in Human Behavior* 26, no. 3 (2010): 277–287. <https://doi.org/10.1016/j.chb.2009.11.014>

¹⁴ Danielle Keats Citron, *Hate Crimes in Cyberspace*. (Cambridge, MA: Harvard University Press, 2014); Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates*. 2nd ed. (London: Routledge, 2019).

Transactions Law, child protection policy, or restorative justice for juvenile offenders.¹⁵

Despite these important contributions, several significant gaps remain in the literature. First, relatively few studies examine cyberbullying through the analytical framework of legal uncertainty, particularly regarding the interpretation of criminal offense elements within Indonesia's fragmented criminal legislation. Second, existing scholarship rarely integrates the doctrines of criminal liability, juvenile justice principles, and digital forensic challenges into a unified legal analysis of cyberbullying prosecution. Third, although previous studies acknowledge deficiencies in victim protection and legal enforcement, limited attention has been devoted to how statutory ambiguity and inconsistent judicial interpretation affect the realization of legal certainty, justice, and accountability in adolescent cyberbullying cases. Consequently, the interaction between fragmented legal regulation, criminal liability, and the practical administration of justice remains insufficiently explored.

This study addresses these gaps by examining the legal uncertainty surrounding criminal liability for adolescent cyberbullying under Indonesian criminal law and evaluating its implications for justice within the criminal justice system. Unlike previous studies that predominantly emphasize psychological consequences, educational interventions, or general cybercrime regulation, this research combines doctrinal legal analysis with empirical examination of selected Indonesian court decisions to identify inconsistencies in statutory interpretation, evidentiary assessment, and judicial reasoning. By integrating the perspectives of criminal law, juvenile justice, and digital governance, this study provides a more comprehensive understanding of the limitations of the existing legal framework while proposing regulatory harmonization through the explicit codification of cyberbullying as a distinct criminal offense, strengthened institutional capacity in digital forensics, and the promotion of digital literacy as a complementary preventive strategy.

Accordingly, this research seeks to answer two principal questions: *first*, how does legal uncertainty influence the construction of criminal liability in adolescent cyberbullying cases under Indonesian law, and *second*, to what extent does the existing criminal justice framework achieve legal certainty, justice, and effective protection for both victims and juvenile offenders? By addressing these questions, this study contributes to the growing discourse on cybercrime regulation, child protection, and digital justice, while offering normative recommendations for strengthening Indonesia's legal response to cyberbullying in accordance with international human rights standards.

¹⁵ Afifa Kareema, Qadriya Qadriya, and Madaniyah Madaniyah. "Legal Protection for Cyberbullying Victims: A Comparative Study of Jinayah Perspective and Positive Law." *SYARIAT: Akhwal Syaksiah, Jinayah, Siyasaah and Muamalah* 2, no. 2 (2025): 57-65. <https://doi.org/10.35335/bhq5516>; Eka Nugraha Putra, "Law' Silence on Cyberbullying to Children in Indonesia." *Brawijaya Law Journal* 11, no. 1 (2024): 135-163. <https://doi.org/10.21776/ub.blj.2024.011.01.07>; Wenggedes Frensh, Madiasa Ablisar, and Mahmud Mulyadi. "Criminal Policy on Cyberbullying of Children in Indonesia." *International Journal of Cyber Criminology* 15, no. 2 (2022): 44-59. <https://doi.org/10.5281/zenodo.4766542>; M. Laena, and R. Riswadi. "Legal Protection for Child Victims of Cyber Bullying." *Proceedings of the 2nd International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2022, 16 April 2022, Semarang, Indonesia*. 2022.

II. CONCEPTUALIZING CYBERBULLYING AND LEGAL PROTECTION FOR ADOLESCENTS

A. Cyberbullying as a Legal Concept

The unprecedented growth of information and communication technologies has fundamentally transformed the manner in which individuals communicate, participate in public discourse, and exercise their rights within digital environments. Alongside these developments, cyberspace has also become a venue for the commission of various unlawful acts that were previously confined to physical interactions. One manifestation of this transformation is cyberbullying, which has evolved from being regarded as merely a social or educational concern into a complex legal issue involving criminal liability, human rights protection, and digital governance. Unlike conventional bullying, cyberbullying exploits technological infrastructures that permit harmful conduct to be committed instantaneously, anonymously, and across jurisdictions, thereby challenging the adequacy of traditional criminal law doctrines and regulatory frameworks.¹⁶

From a conceptual perspective, no universally accepted legal definition of cyberbullying currently exists. The absence of a harmonized definition reflects differences in national legal systems, regulatory priorities, and the rapid evolution of digital technologies. Nevertheless, legal scholars generally agree that cyberbullying refers to intentional conduct carried out through electronic communication technologies that causes or is likely to cause psychological, emotional, reputational, or social harm to another person.¹⁷ The emphasis on intentionality distinguishes cyberbullying from accidental online interactions, while the use of digital technologies differentiates it from conventional forms of interpersonal violence. Consequently, cyberbullying should not be understood merely as bullying occurring on the internet but as a distinct form of technology-facilitated abuse possessing unique legal characteristics.

One of the earliest systematic legal formulations was proposed by Nancy Willard¹⁸, who describes cyberbullying as the use of information and communication technologies to support deliberate, repeated, and hostile behavior intended to harm another individual. Although originally developed within educational settings, Willard's conceptualization has been widely adopted because it identifies essential legal elements relevant to criminal liability, namely intentional conduct, electronic communication, repetition, and resulting harm.¹⁹ The concept also recognizes that cyberbullying encompasses a wide spectrum of conduct extending beyond direct threats to include impersonation, dissemination of defamatory content, exclusion from digital communities, and unauthorized disclosure of personal information.²⁰

¹⁶ David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed. (Cambridge: Polity Press, 2024).

¹⁷ See Citron, *Hate Crimes in Cyberspace*.

¹⁸ Nancy Willard, *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*. (Champaign, IL: Research Press, 2007).

¹⁹ Willard.

²⁰ Willard.

Legal scholars subsequently expanded this understanding by emphasizing that cyberbullying should be examined within the broader framework of cybercrime. Wall²¹ argues that cybercrime should not be confined to offenses targeting computer systems but should also include criminal conduct facilitated by digital technologies that fundamentally alters the nature, scale, and consequences of traditional crimes. Under this perspective, cyberbullying constitutes a computer-mediated offense, whereby technology functions not merely as a communication medium but as an instrument that amplifies victimization through speed, permanence, anonymity, and global accessibility. Accordingly, cyberbullying presents legal challenges that differ substantially from those associated with conventional bullying.

Similarly, Clough²² observes that many contemporary cyber offenses blur the traditional boundaries between physical and virtual criminality because harmful conduct frequently involves multiple overlapping offenses committed simultaneously through electronic systems. A single incident of cyberbullying, for example, may simultaneously involve unlawful access to digital accounts, identity fraud, dissemination of intimate images, criminal intimidation, defamation, and violations of personal data protection. Consequently, legal systems often encounter significant difficulties in identifying the most appropriate statutory provision under which criminal liability should be established.

The legal complexity of cyberbullying is further explained by Brenner²³, who argues that cybercrime fundamentally challenges conventional assumptions regarding criminal jurisdiction, offender identification, and evidentiary procedures. Unlike traditional criminal conduct occurring within identifiable territorial boundaries, cyberbullying frequently involves perpetrators, victims, internet service providers, and digital platforms operating across multiple jurisdictions. Such transnational characteristics complicate investigations and require legal systems to adapt procedural rules concerning electronic evidence, attribution of online conduct, and international cooperation.

Danielle Citron²⁴ further conceptualizes cyberbullying as part of the broader phenomenon of cyber harassment, emphasizing that online abuse systematically undermines individual autonomy, equality, dignity, and democratic participation. According to Citron²⁵, technology has significantly magnified the capacity of perpetrators to inflict severe psychological and reputational harm through coordinated online attacks while simultaneously reducing opportunities for victims to escape abuse. Consequently, legal intervention should not merely address isolated offensive communications but should recognize the cumulative and persistent nature of digitally facilitated victimization.

The legal distinction between cyberbullying and other forms of online misconduct remains essential in determining criminal liability. Cyberbullying differs from cyberstalking, which generally involves persistent surveillance or repeated intimidation creating reasonable fear for personal safety. Likewise,

²¹ Wall, *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed.

²² Jonathan Clough, *Principles of Cybercrime*. 3rd ed. (Cambridge: Cambridge University Press, 2021).

²³ Susan W. Brenner, "Cyber-threats and the Limits of Bureaucratic Control." *Minnesota Journal of Law, Science, and Technology* 14, no. 1 (2013): 137-258. <https://dx.doi.org/10.2139/ssrn.1950725>

²⁴ See Citron, *Hate Crimes in Cyberspace*.

²⁵ See Citron.

cyberbullying differs from online defamation because defamatory conduct primarily concerns injury to reputation through false statements, whereas cyberbullying encompasses a broader range of abusive behaviors regardless of whether the disseminated information is true or false. Similarly, hate speech focuses upon discriminatory expression directed against protected groups, while cyberbullying may occur between individuals without reference to race, religion, ethnicity, gender, or other protected characteristics.²⁶ These distinctions demonstrate that cyberbullying is better understood as a multifaceted pattern of abusive conduct rather than a single criminal act.

From the perspective of substantive criminal law, the determination of criminal liability depends upon the fulfillment of the constituent elements (*actus reus* and *mens rea*) established by legislation. Ashworth²⁷ explains that criminal liability cannot be imposed solely because conduct is morally objectionable; instead, liability requires proof that the prohibited act has been expressly defined by law and accompanied by the requisite mental element. This principle reflects the broader doctrine of legality (*nullum crimen, nulla poena sine lege*), which requires criminal prohibitions to be formulated with sufficient clarity to ensure predictability, legal certainty, and protection against arbitrary prosecution.

The principle of legality has particular significance in cyberbullying regulation because technological developments frequently outpace legislative reform. As Hart²⁸ observes, the generality of legal language inevitably produces interpretative uncertainty when new forms of conduct emerge that were not contemplated during legislative drafting. Courts are therefore required to determine whether existing statutory provisions can reasonably accommodate novel technological behavior without violating the principle that criminal law must be interpreted strictly. Excessively expansive judicial interpretation risks undermining legal certainty, whereas overly restrictive interpretation may leave victims without adequate legal protection.

This tension is particularly evident in jurisdictions that have not enacted legislation specifically criminalizing cyberbullying. Instead, prosecutors frequently rely upon fragmented provisions governing criminal defamation, electronic threats, coercion, privacy violations, harassment, identity fraud, or unlawful dissemination of electronic information. While this approach enables certain forms of online abuse to be prosecuted, it often produces inconsistent legal reasoning because similar factual circumstances may be characterized differently depending upon prosecutorial discretion or judicial interpretation. Such inconsistency weakens both the deterrent function and the legitimacy of criminal law.

The international legal framework likewise reflects the absence of a uniform definition of cyberbullying. The Convention on Cybercrime (Budapest Convention 2001), the first binding international treaty addressing cybercrime, does not expressly regulate cyberbullying. Instead, it establishes procedural and substantive mechanisms for combating offenses involving computer systems, including illegal access, computer-related fraud, and offenses relating to digital evidence. Consequently, cyberbullying remains primarily regulated through domestic

²⁶ See Citron.

²⁷ Andrew Ashworth, *Principles of Criminal Law*, 9th ed. (Oxford: Oxford University Press, 2021).

²⁸ H. L. A. Hart, *The Concept of Law*, 3rd ed. (Oxford: Oxford University Press, 2012).

criminal legislation, resulting in considerable divergence among national legal systems regarding criminalization, evidentiary standards, and sanctions.²⁹

Nevertheless, international human rights law provides an important normative basis for regulating cyberbullying. The Convention on the Rights of the Child (CRC) guarantees every child the right to protection from all forms of physical or mental violence, abuse, neglect, and exploitation.³⁰ The Committee on the Rights of the Child, through General Comment No. 25³¹, further clarifies that these protections extend fully into digital environments, requiring States Parties to adopt legislative, administrative, and educational measures capable of preventing online violence against children. The General Comment recognizes that digital technologies create both opportunities and risks, thereby imposing positive obligations upon States to ensure children's safety while respecting their evolving capacities and rights in the digital.

Similarly, the United Nations Human Rights Council Resolution 32/13, 2016 affirms that the same human rights enjoyed offline must also be protected online. Although the Resolution does not specifically mention cyberbullying, its recognition of digital rights protection establishes an important normative foundation for requiring States to prevent and respond effectively to technology-facilitated abuse. Accordingly, cyberbullying should be viewed not merely as inappropriate online behavior but as conduct capable of violating internationally recognized rights to dignity, privacy, security, reputation, and psychological integrity.³²

Within the Indonesian legal system, however, these international principles have not yet been translated into a comprehensive statutory framework governing cyberbullying. Neither the Electronic Information and Transactions Law (Law No. 11 of 2008 as amended by Law No. 1 of 2024) nor the Indonesian Criminal Code (KUHP) explicitly defines cyberbullying or establishes it as an autonomous criminal offense. Instead, law enforcement authorities must interpret cyberbullying through dispersed provisions relating to defamation, threats, coercion, dissemination of prohibited electronic information, or other conventional criminal offenses. Such regulatory fragmentation creates significant legal uncertainty in determining the applicable offense, the constituent elements of criminal liability, and the proportionality of criminal sanctions.

Conceptually, therefore, cyberbullying represents more than a digital extension of conventional bullying. It constitutes a distinct form of technology-facilitated violence characterized by complex interactions between criminal law, cybercrime regulation, human rights protection, and digital governance. The absence of a universally accepted legal definition does not diminish its legal significance; rather, it highlights the necessity of developing coherent regulatory frameworks capable of reconciling the principles of legality, legal certainty, effective law enforcement, and the protection of fundamental rights. For Indonesia, this challenge is particularly pressing given the fragmented nature of existing

²⁹ Council of Europe. *Convention on Cybercrime (ETS No. 185)*. Budapest, 2001.

³⁰ See United Nations. *Convention on the Rights of the Child*, 1989.

³¹ Committee on the Rights of the Child. *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*. (Geneva: United Nations, 2021).

³² UNHRC. Resolution A/HRC/RES/32/13, 2016.

legislation and the increasing involvement of adolescents as both victims and perpetrators of cyberbullying in digital spaces.

B. Adolescents as Subjects of Criminal Law Protection

The legal protection afforded to adolescents occupies a distinctive position within contemporary criminal justice systems because children simultaneously constitute holders of fundamental rights, potential victims of crime, and, in certain circumstances, perpetrators of criminal offences. Unlike adults, adolescents are recognized as individuals undergoing continuous physical, psychological, emotional, and cognitive development. Consequently, modern legal systems generally adopt differentiated standards of criminal responsibility and legal protection that seek to balance accountability with rehabilitation and the promotion of children's best interests.³³

Internationally, the normative foundation for the protection of children is established by the Convention on the Rights of the Child (CRC), adopted by the United Nations General Assembly in 1989 and ratified by Indonesia through Presidential Decree No. 36 of 1990. Article 1 of the CRC defines a child as every human being below the age of eighteen years unless majority is attained earlier under national law. More importantly, the Convention introduces a comprehensive rights-based approach by recognizing children as autonomous rights holders rather than passive recipients of welfare or protection.

The CRC is founded upon four general principles that guide the interpretation and implementation of children's rights. These include the principle of non-discrimination (Article 2), the best interests of the child (Article 3), the right to life, survival, and development (Article 6), and the right of children to express their views in matters affecting them (Article 12). These principles are interdependent and require States Parties to ensure that all legislative, administrative, and judicial measures affecting children prioritize their welfare and developmental needs while respecting their evolving capacities.³⁴

Among these principles, the best interests of the child has emerged as the cornerstone of international child protection law. According to the Committee on the Rights of the Child, the principle functions simultaneously as a substantive right, an interpretative legal principle, and a procedural rule requiring decision-makers to assess the impact of every action upon children's rights and well-being.³⁵ Accordingly, criminal justice institutions must ensure that legal responses to cyberbullying neither neglect the rights of child victims nor impose disproportionate sanctions upon juvenile offenders.

The increasing digitalization of children's lives has expanded the scope of legal protection beyond physical environments into cyberspace. Recognizing this transformation, the Committee on the Rights of the Child adopted General

³³ Jane Fortin, "Children's Right to Know Their Origins-Too Far, Too Fast?," *Child and Family Law Quarterly* 21, no. 3 (2009): 336-355.

³⁴ John Tobin, ed. *The UN Convention on the Rights of the Child: A Commentary*. (Oxford: Oxford University Press, 2019).

³⁵ Committee on the Rights of the Child. *General Comment No. 14 (2013): On the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration*. (Geneva: United Nations, 2013).

Comment No. 25, 2021 concerning children's rights in relation to the digital environment. The General Comment affirms that States possess positive obligations to protect children from violence, exploitation, privacy violations, and psychological harm occurring through digital technologies while simultaneously ensuring children's rights to information, participation, education, and freedom of expression. Importantly, the Committee emphasizes that digital environments should provide the same level of legal protection as offline spaces.

Cyberbullying therefore represents not merely an interpersonal conflict among adolescents but a potential violation of internationally recognized children's rights. Persistent online harassment may interfere with children's rights to dignity, privacy, education, health, and healthy development, all of which are expressly protected under the CRC. Consequently, States are required to adopt effective legislative and institutional measures capable of preventing, investigating, prosecuting, and remedying technology-facilitated violence against children.

From the perspective of criminal law, however, protecting adolescents requires balancing two equally important objectives. On one hand, child victims possess the right to effective legal remedies, access to justice, and protection from secondary victimization. On the other hand, juvenile offenders remain children whose criminal responsibility must be determined in accordance with internationally accepted standards emphasizing rehabilitation rather than retribution. This dual status distinguishes juvenile justice from ordinary criminal law and necessitates specialized procedural safeguards.³⁶

The United Nations Standard Minimum Rules for the Administration of Juvenile Justice (Beijing Rules)³⁷ emphasize that juvenile justice should promote children's well-being while ensuring that any legal response remains proportionate both to the circumstances of the offender and to the nature of the offence. Likewise, the United Nations Guidelines for the Prevention of Juvenile Delinquency (Riyadh Guidelines)³⁸ encourage preventive strategies emphasizing education, social participation, family support, and community involvement rather than excessive reliance upon punitive criminal sanctions (United Nations, 1990). These instruments collectively demonstrate that criminal law should constitute the measure of last resort when addressing misconduct committed by adolescents.

These international principles are reflected in Indonesian law. The 1945 Constitution of the Republic of Indonesia, particularly Article 28B paragraph (2), guarantees every child's right to survival, growth, development, and protection from violence and discrimination. Constitutional protection is further elaborated in Law Number 35 of 2014 concerning Amendments to Law Number 23 of 2002 on Child Protection, which defines children as individuals below eighteen years of age, including children still in the womb. The statute affirms that children are entitled to protection from physical, psychological, sexual, and social violence irrespective of the environment in which such violence occurs.

³⁶ Fortin, "Children's Right to Know Their Origins-Too Far, Too Fast?."

³⁷ See United Nations. *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (The Beijing Rules)*, Adopted by General Assembly A/RES/40/33, on 29 November 1985. Available at <https://www.ohchr.org/sites/default/files/beijingrules.pdf>

³⁸ See United Nations. *United Nations Guidelines for the Prevention of Juvenile Delinquency (The Riyadh Guidelines)*, Adopted by General Assembly Resolution 45/112, on 14 December 1990. Available online at <https://www.ohchr.org/en/instruments-mechanisms/instruments/united-nations-guidelines-prevention-juvenile-delinquency-riyadh>

The Child Protection Law adopts a broad understanding of violence by recognizing not only physical abuse but also psychological harm that interferes with children's welfare and development. Although the legislation predates many contemporary manifestations of cyberbullying, its provisions concerning psychological violence provide an important normative basis for interpreting digital harassment as conduct requiring legal intervention. Nevertheless, the Law does not expressly regulate cyberbullying or establish specific mechanisms for addressing technology-facilitated abuse committed through electronic communication systems.

Protection of children involved in criminal proceedings is further governed by Law Number 11 of 2012 concerning the Juvenile Criminal Justice System (*Sistem Peradilan Pidana Anak/SPPA*). The SPPA Law fundamentally transformed Indonesian juvenile justice by replacing punitive approaches with restorative justice and diversion mechanisms. Article 5 expressly provides that the juvenile justice system shall prioritize restorative justice, while Article 7 requires diversion to be pursued whenever statutory requirements are satisfied. These provisions reflect Indonesia's commitment to implementing international standards concerning juvenile justice.

Restorative justice within the SPPA framework seeks to restore social relationships, repair harm suffered by victims, and facilitate the rehabilitation of child offenders through dialogue and community participation rather than imprisonment. As Griffith³⁹ argues, restorative justice offers a more constructive approach to criminal accountability because it emphasizes repairing harm instead of merely imposing punishment. In cases involving adolescent cyberbullying, restorative justice may therefore provide opportunities to address the emotional and relational consequences of digital victimization while reducing the long-term criminogenic effects associated with formal criminal prosecution.

Nevertheless, restorative justice should not be interpreted as eliminating criminal responsibility altogether. Ashworth⁴⁰ emphasizes that criminal liability continues to serve important functions in expressing societal condemnation of harmful conduct, protecting victims' rights, and reinforcing the normative authority of criminal law. Accordingly, restorative mechanisms must operate within clear legal boundaries that preserve accountability while respecting children's developmental needs.

The emergence of cyberbullying illustrates the inherent tension between these competing objectives. Child victims require effective legal protection against persistent digital abuse, whereas child perpetrators retain internationally recognized rights to rehabilitation, education, privacy, and reintegration into society. Excessively punitive responses risk undermining the objectives of juvenile justice, while insufficient legal intervention may deny victims meaningful access to justice and weaken public confidence in the legal system. Achieving an appropriate balance therefore requires legal frameworks that clearly define prohibited conduct while preserving judicial discretion to impose proportionate and child-sensitive responses.

³⁹ Kathy Daly Griffith, "Restorative Justice and Responsive Regulation." *Australian and New Zealand Journal of Criminology* 36, no. 1 (2003): 109-114.

⁴⁰ Ashworth, *Principles of Criminal Law*. 9th ed.

This balancing exercise is further complicated by the digital nature of cyberbullying. Electronic evidence may be rapidly deleted, manipulated, or disseminated across multiple platforms, making investigation more complex than conventional offences. At the same time, adolescents frequently lack awareness regarding the legal consequences of their online behaviour, particularly where digital interactions are perceived as informal or recreational. These realities reinforce the importance of integrating legal protection with preventive strategies such as digital literacy, parental supervision, and educational programmes, without diminishing the role of criminal law in addressing serious or repeated forms of online abuse.

Accordingly, adolescents should be understood not only as beneficiaries of legal protection but also as participants in a legal system that must reconcile multiple normative objectives, including child protection, accountability, rehabilitation, legal certainty, and justice. This conceptual framework provides the foundation for assessing whether Indonesian criminal law adequately protects adolescent victims of cyberbullying while simultaneously ensuring that juvenile offenders are treated consistently with constitutional guarantees, international human rights obligations, and the fundamental principles of juvenile justice.

III. INDONESIAN LEGAL FRAMEWORK AND LEGAL UNCERTAINTY ON CYBERBULLYING

A. Indonesian Criminal Law Framework Governing Cyberbullying

The Indonesian legal system does not yet recognize cyberbullying as an autonomous criminal offence. Instead, various forms of online abusive behaviour are regulated indirectly through a fragmented set of legal instruments that were not originally designed to address technology-facilitated interpersonal violence. This condition reflects a broader challenge in contemporary criminal law, the difficulty of adapting traditional legal categories to rapidly evolving digital conduct. As Ashworth⁴¹ argues, criminal law must maintain clarity and precision in defining prohibited conduct, yet technological development often outpaces legislative drafting, creating structural gaps in legal protection.

The primary legal instrument used to address cyberbullying-related conduct in Indonesia is Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law). The ITE Law criminalizes various forms of electronic conduct, including the dissemination of defamatory content, threats, hate speech, and the transmission of unlawful electronic information. In practice, these provisions are frequently used by law enforcement authorities to prosecute behaviours that fall within the broader spectrum of cyberbullying, even though the statute itself does not explicitly define the term “cyberbullying”.

For instance, provisions relating to electronic defamation are often used in cases involving online humiliation or reputational harm. Similarly, provisions

⁴¹ Ashworth, *Principles of Criminal Law*. 9th ed.

concerning threats and coercion may be applied when perpetrators engage in intimidating digital communication. However, these provisions are inherently reactive and offence-specific, meaning that they address individual acts rather than the broader behavioural pattern characteristic of cyberbullying. As a result, the legal framework treats cyberbullying as a collection of isolated offences rather than a unified form of technology-facilitated abuse.

In addition to the ITE Law, the Indonesian Criminal Code (KUHP) also provides general provisions that may be applied to certain manifestations of cyberbullying. These include provisions on defamation, insult, coercion, threats, and crimes against personal dignity. The newly enacted KUHP (Law No. 1 of 2023) maintains a similar structure by preserving traditional offence categories while incorporating limited updates to reflect digital developments. However, like the ITE Law, the KUHP does not specifically regulate cyberbullying as a distinct offence. Consequently, its application depends heavily on judicial interpretation and prosecutorial discretion.

The Child Protection Law (Law No. 35 of 2014, amending Law No. 23 of 2002) provides a broader normative foundation for protecting children from violence, including psychological violence. Article 76C, for example, prohibits acts of violence against children, while Article 76E addresses exploitation and other harmful conduct. Although these provisions are sufficiently broad to encompass certain forms of cyberbullying, they remain general in nature and do not explicitly address digital contexts or online behavioural patterns. This absence of specificity creates interpretative uncertainty when applying the law to cyber-based conduct.

Furthermore, Indonesia has enacted Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which introduces legal safeguards regarding the processing, storage, and dissemination of personal data. Certain forms of cyberbullying, such as doxxing or unauthorized disclosure of personal information, may fall within the scope of this law. However, the PDP Law primarily regulates data controllers and processors rather than interpersonal abusive conduct. Therefore, its relevance to cyberbullying is indirect and contingent upon the nature of the conduct and the involvement of data processing activities.

When these four instruments are examined collectively, it becomes evident that Indonesian criminal law adopts a fragmented regulatory model in addressing cyberbullying-related behaviour. Instead of establishing a unified legal category, the legal system disperses relevant provisions across multiple statutes with differing objectives, normative structures, and enforcement mechanisms. This fragmentation creates a situation in which similar factual scenarios may be prosecuted under different legal provisions, depending on interpretative choices made by investigators, prosecutors, and judges.

From a doctrinal perspective, this condition raises important concerns regarding the principle of legal certainty (*rechtszekerheid*), which is a fundamental component of the rule of law. According to H.L.A. Hart⁴², legal rules must be sufficiently clear to allow individuals to understand the consequences of their actions. Similarly, Raz⁴³ emphasizes that legal certainty requires laws to be stable, publicly accessible, and sufficiently precise to guide behaviour. In the context of

⁴² Hart, *The Concept of Law*. 3rd ed.

⁴³ Joseph Raz, *The Authority of Law*. 2nd ed. (Oxford: Oxford University Press, 2009).

cyberbullying, however, the absence of a specific statutory definition means that individuals may not be able to predict with reasonable certainty whether certain online conduct constitutes a criminal offence.

The reliance on multiple overlapping provisions also creates interpretative challenges in determining the *actus reus* and *mens rea* of cyberbullying-related offences. For example, emotional harm inflicted through repeated online harassment may not always satisfy the strict legal requirements of defamation or threat under existing statutes. This gap between social reality and legal categorization reflects what Fuller⁴⁴ describes as the “*internal morality of law*”, where legal rules must maintain coherence between declared norms and their application in practice. When such coherence is absent, the legitimacy of legal enforcement may be weakened.

Moreover, the absence of a specific cyberbullying offence limits the ability of the legal system to recognize the pattern-based nature of digital abuse. Cyberbullying is not a single act but a continuous behavioural pattern that may involve multiple actors, repeated actions, and cumulative harm. By contrast, Indonesian criminal law largely remains event-based, focusing on discrete acts rather than sustained behavioural processes. This structural mismatch further complicates the qualification of cyberbullying under existing legal provisions.

In practice, this fragmentation also affects law enforcement discretion. Investigators must select among various legal provisions depending on how the conduct is interpreted, while prosecutors must determine which charges are most appropriate based on evidentiary availability and statutory interpretation. Judges, in turn, may reach different conclusions regarding the legal classification of similar cyberbullying cases. This variability contributes to inconsistent jurisprudence, which undermines the predictability and uniformity of criminal justice outcomes.

Therefore, although Indonesian law provides multiple legal pathways to address cyberbullying-related conduct, these pathways are indirect, fragmented, and dependent on interpretative flexibility rather than explicit legislative recognition. This condition forms the structural basis of legal uncertainty, which will be further analyzed in the following subsection, particularly in relation to criminal liability and judicial inconsistency in adolescent cyberbullying cases.

B. Legal Uncertainty in Determining Criminal Liability

The absence of a specific statutory definition of cyberbullying within Indonesian criminal law generates significant uncertainty in determining criminal liability, particularly in cases involving adolescents. This uncertainty is not merely technical in nature but reflects a deeper doctrinal issue concerning the relationship between rapidly evolving digital conduct and the traditional structure of criminal law. As Ashworth emphasizes, criminal liability must be grounded in clearly defined offences that satisfy the principle of legality, ensuring that individuals can foresee the legal consequences of their actions.⁴⁵ When legal norms fail to provide such clarity, the legitimacy of criminal prosecution becomes questionable.

⁴⁴ Lon L. Fuller, *The Morality of Law*. (New Haven: Yale University Press, 1969).

⁴⁵ Ashworth, *Principles of Criminal Law*. 9th ed.

At the core of this issue lies the principle of *nullum crimen, nulla poena sine lege*, which requires that no one may be punished except on the basis of pre-existing, clear, and precise legal norms. Hart⁴⁶ argues that legal systems inevitably contain a “penumbra of uncertainty,” where the application of rules to new or unforeseen circumstances becomes ambiguous. Cyberbullying represents precisely such a penumbral case, where existing legal categories struggle to capture the complexity of digitally mediated, repetitive, and multi-platform harmful behaviour. As a result, law enforcement must rely on analogical reasoning, which may conflict with strict interpretations of criminal legality.

In the Indonesian context, this uncertainty is exacerbated by the fragmented structure of relevant legislation. As previously discussed, cyberbullying-related conduct is dispersed across the ITE Law (Law No. 1 of 2024), the KUHP (Law No. 1 of 2023), the Child Protection Law, and the Personal Data Protection Law. However, none of these instruments explicitly define cyberbullying as a distinct criminal offence. Consequently, prosecutors must “translate” online behaviour into existing offence categories such as defamation, threats, coercion, or unlawful dissemination of information. This process inevitably introduces interpretative variability, as similar factual conduct may be classified differently depending on prosecutorial strategy and judicial reasoning.

From a doctrinal perspective, this creates tension between formal legality and substantive justice. While criminal law aims to protect victims from harm, it must also ensure predictability and consistency. According to Raz⁴⁷, legal certainty requires that laws be capable of guiding behaviour in advance. However, in cyberbullying cases, individuals—particularly adolescents—may not reasonably understand that certain online interactions (such as repeated mocking, exclusion from digital groups, or meme-based humiliation) could constitute criminal conduct under defamation or harassment provisions. This gap between legal norm and social understanding weakens the preventive function of criminal law.

The uncertainty is further intensified by the structural differences between cyberbullying and traditional offences. Cyberbullying is typically characterized by continuity, repetition, and multi-actor participation, whereas Indonesian criminal law remains largely act-based and event-specific. As Clough⁴⁸ notes, cyber-enabled offences often involve a “convergence of conduct,” where multiple acts collectively produce harm. However, existing Indonesian provisions tend to isolate each act, making it difficult to legally conceptualize cyberbullying as a unified behavioural pattern. This leads to fragmentation in legal qualification, where a single cyberbullying episode may be divided into separate legal categories that fail to capture its cumulative harm.

Another layer of uncertainty arises in relation to the interpretation of *mens rea*. In traditional criminal law theory, liability requires proof of intention or at least awareness of wrongdoing. However, in adolescent cyberbullying cases, distinguishing between intentional harm, peer interaction, and digital play becomes particularly complex. Digital communication often lacks contextual cues such as tone, facial expression, or immediate feedback, making it difficult to assess intent.

⁴⁶ Hart, *The Concept of Law*. 3rd ed.

⁴⁷ Raz, *The Authority of Law*. 2nd ed.

⁴⁸ See Clough, *Principles of Cybercrime*. 3rd ed.

As Fletcher⁴⁹ argues, criminal liability must be based on “desert” and moral blameworthiness, yet the digital environment complicates the assessment of subjective culpability.

The evidentiary dimension further compounds this uncertainty. Digital evidence is inherently volatile, easily deleted, manipulated, or misattributed. Brenner⁵⁰ highlights that cybercrime investigations often face challenges in establishing attribution, jurisdiction, and authenticity of electronic data. In cyberbullying cases, determining who created, shared, or amplified harmful content may require complex forensic analysis and cooperation from digital platforms. However, disparities in investigative capacity across jurisdictions may result in inconsistent evidentiary standards, thereby affecting judicial outcomes.

Judicial inconsistency is another direct consequence of legal uncertainty. In the absence of a clear statutory framework, courts may interpret similar conduct differently depending on the selected legal provision and evidentiary assessment. Some judges may prioritize defamation provisions, while others may rely on electronic threats or child protection statutes. This variability undermines the principle of equality before the law, as similarly situated defendants may receive different legal treatment. From the perspective of legal theory, such inconsistency weakens the coherence of the legal system and reduces public trust in criminal justice institutions.

The issue becomes even more sensitive when the offender is an adolescent. Indonesian juvenile justice law, particularly the Juvenile Criminal Justice System Act (Law No. 11 of 2012, SPPA Law)⁵¹, emphasizes restorative justice and diversion. However, the absence of a clear definition of cyberbullying complicates the determination of whether diversion is appropriate or whether formal prosecution should proceed. Without clear legal categorization, decision-makers must rely heavily on discretionary judgment, which increases the risk of unequal treatment and normative inconsistency.

In addition, legal uncertainty affects the proportionality of sentencing. When cyberbullying is prosecuted under general provisions such as defamation or threats, the resulting sanctions may not reflect the actual nature of the harm caused. Some cases may be treated as minor offences despite severe psychological impact, while others may be over-criminalized due to expansive interpretation of electronic communication laws. This inconsistency raises concerns regarding the proportionality principle in criminal law, which requires that punishment correspond to the gravity of the offence.

From a theoretical standpoint, Fuller’s concept of the “internal morality of law” is also relevant.⁵² Fuller argues that law must maintain coherence, clarity, and congruence between official rules and their application. When legal systems rely excessively on analogical reasoning without clear statutory guidance, the internal morality of law is compromised. In the context of cyberbullying, this manifests in the gap between the lived reality of digital abuse and the fragmented legal tools

⁴⁹ George P. Fletcher, *Rethinking Criminal Law*. (Oxford: Oxford University Press, 2000).

⁵⁰ Brenner, “Cyber-threats and the Limits of Bureaucratic Control.”

⁵¹ See Republic of Indonesia. *Undang-Undang Republik Indonesia Nomor 11 Tahun 2012 Tentang Sistem Peradilan Pidana Anak (SPPA Law)*. Available online at <https://bphn.go.id/data/documents/12uu011.pdf>

⁵² Fuller, *The Morality of Law*.

used to address it. Therefore, the cumulative effect of these factors is a persistent state of structural legal uncertainty. This uncertainty affects all stages of criminal justice processing, from reporting and investigation to prosecution and adjudication. It also weakens deterrence, as potential offenders may not fully understand the legal consequences of their online behaviour, while victims may lack confidence in the effectiveness of legal remedies.

IV. TOWARDS REGULATORY HARMONIZATION AND NORMATIVE REFORM

The juridical construction of criminal liability for cyberbullying in Indonesia reflects a fragmented regulatory architecture that has not yet achieved normative consolidation into a unified legal framework. As previously demonstrated in Sections 2.3.1 and 2.3.2, Indonesian criminal law continues to rely on dispersed statutory instruments, particularly the Electronic Information and Transactions Law (ITE Law as amended by Law No. 1 of 2024), the Indonesian Criminal Code (Law No. 1 of 2023), the Child Protection Law (Law No. 35 of 2014), and the Personal Data Protection Law (Law No. 27 of 2022). This fragmentation results in a doctrinal condition where cyberbullying is not conceptualized as an autonomous offence but reconstructed through analogical interpretation of conventional criminal provisions.⁵³

The absence of explicit codification of cyberbullying creates a structural gap in Indonesian criminal law. Unlike jurisdictions that have introduced specific cyber-harassment statutes, Indonesia still relies on interpretative expansion of general offences such as defamation, threats, and insult. This reliance raises concerns regarding the principle of legality, particularly the requirement of strict legality (*nullum crimen sine lege stricta*), which prohibits extensive judicial interpretation that expands criminal liability beyond statutory wording.⁵⁴ As a consequence, cyberbullying is treated as a constellation of fragmented offences rather than a unified behavioural category.

Within the ITE Law framework, several provisions are frequently applied in cyberbullying cases. Article 27 paragraph (3) criminalizes the distribution of electronic information containing defamation or insult, while Article 27 paragraph (4) regulates electronic extortion and threats. Additionally, Article 27A of the amended ITE Law introduces liability for attacks on honour or reputation through electronic systems, and Article 29 addresses electronic threats causing fear. These provisions, however, remain primarily oriented toward reputational protection and public order rather than psychological harm or relational violence, which are central characteristics of cyberbullying.⁵⁵

The doctrinal limitation of these provisions becomes evident when contrasted with the sociological complexity of cyberbullying. Cyberbullying is not limited to

⁵³ See Clough, *Principles of Cybercrime*. 3rd ed. See also Brenner, “Cyber-threats and the Limits of Bureaucratic Control.”

⁵⁴ Ashworth, *Principles of Criminal Law*. 9th ed. See also Douglas Husak, *Overcriminalization: The Limits of Criminal Law*. (Oxford: Oxford University Press, 2008).

⁵⁵ See Citron, *Hate Crimes in Cyberspace*. See also Nicola Henry, Asher Flynn, and Anastasia Powell. “Technology-Facilitated Domestic and Sexual Violence: A Review.” *Violence against Women* 26, no. 15-16 (2020): 1828-1854. <https://doi.org/10.1177/1077801219875821>

defamation or threats but includes repeated humiliation, social exclusion, impersonation, identity manipulation, and digital surveillance. These behaviours often occur in patterns rather than isolated acts, creating cumulative harm that is not adequately captured by act-based criminal provisions. As Wall⁵⁶ and Yar⁵⁷ argue, cyber-enabled harm must be understood as processual and networked rather than episodic.

The Indonesian Criminal Code (KUHP) under Law No. 1 of 2023 similarly provides general provisions such as Article 310 on defamation, Article 311 on false accusation, Article 335 on coercion, and Article 368 on extortion. However, these provisions were historically designed for physical and interpersonal contexts. Their application to digital environments requires analogical reasoning, which introduces interpretative uncertainty and potential inconsistency in judicial application.⁵⁸

In addition to criminal statutes, the Child Protection Law introduces broader protective norms, particularly Article 76C, which prohibits violence against children, and Article 76E, which addresses cruel treatment. While these provisions theoretically encompass psychological harm, they do not explicitly define or regulate cyberbullying as a form of digital psychological violence. This omission creates enforcement ambiguity, especially when cyberbullying occurs exclusively in online environments without physical interaction.

The Personal Data Protection Law (Law No. 27 of 2022) introduces another dimension of regulation through Article 65 paragraphs (1) and (2), which prohibit unlawful acquisition and dissemination of personal data. However, its normative focus is primarily on data processing and institutional accountability rather than interpersonal harassment. Consequently, its applicability to cyberbullying is indirect and dependent on whether the conduct involves identifiable data misuse.

The coexistence of these overlapping statutes creates what can be described as normative fragmentation. This fragmentation undermines legal certainty, as conceptualized by Hart's theory of open texture, where legal rules fail to provide clear guidance in borderline cases.⁵⁹ Raz further argues that legal systems must maintain clarity, stability, and predictability to ensure behavioral guidance, yet cyberbullying cases often fall outside clear statutory boundaries.⁶⁰

From the perspective of criminal liability theory, Moeljatno emphasizes that criminal responsibility requires both capacity for responsibility and fault (*mens rea*).⁶¹ In cyberbullying cases, establishing *mens rea* is particularly complex due to the indirect, repetitive, and mediated nature of digital communication. Intent (*dolus*) is often inferred from behavioral patterns such as repeated postings, coordinated attacks, and sustained harassment. Digital traces such as chat logs, metadata, timestamps, and interaction frequency are used as evidentiary proxies for subjective intent. However, inferential reasoning of *mens rea* raises concerns regarding over-criminalization. As Ashworth⁶² notes, criminal liability must be based on clear and foreseeable standards to avoid arbitrary expansion. In adolescent

⁵⁶ Wall, *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed.

⁵⁷ Majid Yar, *Cybercrime and Society*. (London: SAGE Publications, 2012).

⁵⁸ George P. Fletcher, *Rethinking Criminal Law*. (Oxford: Oxford University Press, 2000); Andrew Simester, and G. R. Sullivan. *Criminal Law Theory*. (Oxford: Hart Publishing, 2019).

⁵⁹ Hart, *The Concept of Law*. 3rd ed.

⁶⁰ Raz, *The Authority of Law*. 2nd ed.

⁶¹ Moeljatno Moeljatno. *Asas-Asas Hukum Pidana*. (Jakarta: Rineka Cipta, 2008).

⁶² Ashworth, *Principles of Criminal Law*. 9th ed.

cyberbullying cases, distinguishing between intentional harm, peer interaction, and digital expression becomes particularly difficult, thereby increasing the risk of misclassification.

The *actus reus* in cyberbullying also presents doctrinal challenges. Unlike traditional offences, the *actus reus* occurs in cyberspace while harm manifests in psychological and social dimensions. This disjunction between conduct and consequence complicates traditional causality frameworks in criminal law, which were historically constructed around physical proximity and territorial jurisdiction.⁶³

Judicial practice in Indonesia reflects an evolving but inconsistent response to cyberbullying-related conduct. In Decision No. 66/Pid.Sus/2018/PN Plp and Decision No. 255/Pid.Sus/2021/PN Makassar, courts primarily applied Article 27(3) of the ITE Law, focusing on defamation through social media. The courts emphasized intentionality and unlawfulness, yet the reasoning remained centered on reputational harm rather than psychological or relational harm.

A more progressive judicial interpretation appears in Decision No. 97/Pid.Sus/2019/PN Snn, where the court recognized that online intimidation via messaging applications generates fear and emotional distress. This decision marks a shift toward recognizing psychological harm as a legally relevant consequence of digital conduct, aligning more closely with contemporary cybercrime scholarship.⁶⁴ Further development is seen in Decision No. 71/Pid.Sus/2023/PN Pdl, where the court integrated the ITE Law with the Child Protection Law in a case involving a minor victim. This decision reflects an emerging victim-centered approach, where vulnerability and psychological impact are considered in sentencing, consistent with the principles of the Convention on the Rights of the Child.⁶⁵

Despite these doctrinal and jurisprudential developments, empirical evidence indicates a significant enforcement gap. Approximately 45 percent of adolescents report experiencing cyberbullying, yet only a small fraction of cases reach judicial adjudication. This discrepancy indicates systemic under-enforcement and reflects structural barriers in reporting, investigation, and prosecution.

Such barriers include limited digital forensic capacity, lack of legal awareness among victims, evidentiary volatility in digital environments, and reluctance to report due to social stigma. Loader and Sparks⁶⁶ describe this phenomenon as “criminal justice accessibility failure,” where legal systems fail to translate normative protection into practical accessibility. The gap between prevalence and adjudication suggests that criminal law in its current form does not function effectively as a protective mechanism for adolescents. Instead, it operates selectively, reaching only cases that successfully pass through procedural and evidentiary thresholds, thereby excluding a large portion of victims from legal protection. This structural inefficiency also undermines the deterrent function of criminal law. If legal consequences are perceived as uncertain or inconsistent, potential offenders may not internalize the risks associated with cyberbullying

⁶³ Brenner, “Cyber-threats and the Limits of Bureaucratic Control.”

⁶⁴ Henry, et.al “Technology-Facilitated Domestic and Sexual Violence: A Review.”

⁶⁵ Tobin, *The UN Convention on the Rights of the Child: A Commentary*.

⁶⁶ Ian Loader, and Richard Sparks. *Public Criminology?* (London: Routledge, 2011).

behavior. This reinforces the need for clearer legal categorization and enforcement consistency.

The doctrinal analysis therefore suggests that Indonesia's current legal framework suffers from three interrelated problems: absence of codification, interpretative dependency on analogy, and inconsistent judicial application. These problems collectively weaken legal certainty and hinder effective criminal liability determination. From a theoretical standpoint, Fletcher's doctrine of fair labeling highlights the importance of accurately categorizing criminal behavior to reflect its moral and social harm.⁶⁷ Cyberbullying, when fragmented into defamation, threats, or insult, loses its conceptual integrity and fails to capture its cumulative psychological impact. Similarly, Fuller's theory of the internal morality of law emphasizes coherence between legal norms and their application.⁶⁸ The current Indonesian framework demonstrates partial coherence but lacks systemic integration, particularly in relation to digital harm affecting minors.

Therefore, regulatory harmonization becomes a normative necessity rather than a mere policy recommendation. Such harmonization would require explicit recognition of cyberbullying as a distinct offence, incorporation of psychological harm as a legal element, and alignment between criminal law, child protection law, and data protection law. In addition, harmonization must be accompanied by institutional strengthening, including improved digital forensic capacity and standardized prosecutorial guidelines. Without such structural support, even well-designed legislation would remain ineffective in practice. Ultimately, the analysis demonstrates that the Indonesian legal system is in a transitional phase, moving from analogical interpretation toward potential codification. However, until cyberbullying is explicitly regulated as a unified offence, legal uncertainty and inconsistent criminal liability will persist, particularly in cases involving adolescents.

V. STRUCTURAL, SUBSTANTIAL, AND CULTURAL OBSTACLES IN COUNTERING CYBERBULLYING

The effectiveness of criminal liability in addressing cyberbullying in Indonesia can be systematically examined through Soerjono Soekanto's theory of legal effectiveness, which posits that law enforcement outcomes are determined by the interaction of legal substance, legal structure, and legal culture.⁶⁹ Within this analytical framework, the suboptimal implementation of cyberbullying-related criminal liability reflects a systemic dysfunction across all three dimensions, rather than a singular legislative deficiency. This aligns with broader socio-legal scholarship emphasizing that cybercrime governance requires an integrated legal-institutional-cultural approach.⁷⁰

From the perspective of legal substance, Indonesian criminal law does not yet recognize cyberbullying as an autonomous offence. Instead, it relies on fragmented

⁶⁷ Fletcher, *Rethinking Criminal Law*.

⁶⁸ Fuller, *The Morality of Law*.

⁶⁹ Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. (Jakarta: Rajawali Pers, 2008).

⁷⁰ See Wall, *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed. See also Clough, *Principles of Cybercrime*. 3rd ed.

provisions dispersed across the Electronic Information and Transactions Law (ITE Law as amended by Law No. 1 of 2024), the Indonesian Criminal Code (Law No. 1 of 2023), the Child Protection Law (Law No. 35 of 2014), and the Personal Data Protection Law (Law No. 27 of 2022). This fragmented normative structure produces interpretative instability in legal application, as law enforcement must rely on analogical reasoning rather than explicit statutory codification.⁷¹ (Ashworth, 2021; Husak, 2008). The following table illustrates the doctrinal fragmentation of cyberbullying regulation within Indonesian positive law and highlights the structural limitations of each instrument:

Table 1. Fragmentation of Legal Substance in Cyberbullying Regulation in Indonesia

Cyberbullying Conduct	Legal Instrument	Relevant Article	Legal Function	Normative Limitation
Online defamation and insult	ITE Law	Art. 27(3)	Reputation protection	Narrow focus on honor, excludes psychological harm
Electronic threats and intimidation	ITE Law	Art. 27(4), Art. 29	Security protection	Requires high evidentiary threshold of threat
Attacks on honor/reputation	ITE Law (Amendment 2024)	Art. 27A	Expanded reputational offence	Still does not define cyberbullying as a category
Defamation and false accusation	KUHP	Art. 310–311	Criminal reputation protection	Offline-oriented legal construct
Coercion and harassment	KUHP	Art. 335	Public order protection	Not designed for digital repetition-based harm
Violence against children	Child Protection Law	Art. 76C	Child protection	No explicit digital/online violence framework
Personal data misuse (doxxing)	PDP Law	Art. 65(1)–(2)	Data protection	Indirect relevance to interpersonal harm

Source: Various sources, edited and analyzed by Authors

As demonstrated in Table 1, Indonesian law does not provide a unified doctrinal category for cyberbullying, but rather disperses its legal treatment across multiple regimes with different normative orientations. This fragmentation creates

⁷¹ Ashworth, *Principles of Criminal Law*. 9th ed. See also Husak, Douglas. *Overcriminalization: The Limits of Criminal Law*.

what Fletcher⁷² describes as “misaligned criminal labeling,” where conduct is legally categorized in ways that fail to reflect its social and psychological reality.

Moeljatno highlighted that criminal responsibility requires both capacity for responsibility and fault (*mens rea*), and in this case, establishing *mens rea* is particularly complex because intent is often inferred from digital behavioural patterns such as repeated messaging, coordinated harassment, or sustained online humiliation.⁷³ However, such inferential reasoning raises concerns regarding over-criminalization and evidentiary ambiguity, particularly in adolescent peer interactions where intent may be socially ambiguous.⁷⁴ Unlike traditional offences, cyberbullying involves a displaced actus reus, where the conduct occurs in cyberspace while the harm manifests in psychological and relational dimensions. This disjunction between action and consequence challenges classical causality models in criminal law and requires a reconceptualization of harm beyond physical or territorial boundaries.⁷⁵

The second dimension of Soekanto’s framework, legal structure, highlights institutional limitations in cyberbullying enforcement. Law enforcement agencies face significant disparities in digital forensic capacity, technological infrastructure, and inter-agency coordination. As cybercrime increasingly involves anonymization technologies such as VPNs and encrypted messaging platforms, attribution of criminal conduct becomes highly complex. These structural limitations often result in case discontinuation or evidentiary insufficiency.⁷⁶ The Table 2 summarizes the structural obstacles affecting enforcement effectiveness in cyberbullying cases.

As Table 2 demonstrates, structural limitations significantly reduce the effectiveness of criminal enforcement mechanisms. Cyberbullying, unlike traditional offences, requires rapid intervention due to the replicative nature of digital harm. Failure to respond promptly results in irreversible secondary victimization, as harmful content continues to circulate even after legal action is initiated.

The third dimension, legal culture, represents the most deeply rooted challenge in cyberbullying governance. Legal culture refers to societal attitudes toward law and legal institutions, which in this context significantly shape reporting behaviour and victim response. Cyberbullying is often normalized as “online joking” or informal interaction, leading to widespread underreporting among adolescent victims.⁷⁷

⁷² Fletcher, *Rethinking Criminal Law*.

⁷³ Moeljatno, *Asas-Asas Hukum Pidana*.

⁷⁴ Ashworth, *Principles of Criminal Law*. 9th ed. See also Kerr, Orin S. *Computer Crime Law*. (St. Paul, MN: West Academic, 2018).

⁷⁵ See Wall, *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed. See also Brenner, Susan W. “Cyber-threats and the Limits of Bureaucratic Control.”

⁷⁶ Yar, *Cybercrime and Society*. See also Cross, Cassandra, et al. “Responding to Cybercrime: Results of a Comparison Between Community Members and Police Personnel.” *Trends and Issues in Crime and Criminal Justice* 635 (2021): 1-20.

⁷⁷ Livingstone, Sonia, and Peter K. Smith. “Annual Research Review: Harms Experienced by Child Users of Online and Mobile Technologies.” *Journal of Child Psychology and Psychiatry* 55, no. 6 (2014): 635–654. <https://doi.org/10.1111/jcpp.12197>. See also Smahel, David, et al. *EU Kids Online Report: Survey Results from 19 Countries*. (London: London School of Economics, 2020). <https://doi.org/10.21953/lse.47fdeqj010fo>

Table 2. Structural Obstacles in Cyberbullying Law Enforcement

Structural Dimension	Description	Impact on Enforcement	Theoretical Implication
Digital forensic capacity	Unequal technical capability among investigators	Weak evidence collection and attribution failure	Institutional capacity gap. ⁷⁸
Technological anonymity	VPNs, encryption, anonymous accounts	Difficulty identifying perpetrators	Attribution problem in cybercrime. ⁷⁹
Inter-agency coordination	Limited cooperation between police, platforms, ISPs	Delayed investigations	Governance fragmentation. ⁸⁰
Procedural bureaucracy	Slow reporting and investigation procedures	Content remains viral and harmful	Temporal harm amplification. ⁸¹

Source: Various sources, edited and analyzed by Authors

Social stigma, fear of retaliation, and victim-blaming attitudes further discourage victims from seeking legal protection. This cultural environment significantly weakens the operational effectiveness of criminal law, as law enforcement depends on societal willingness to activate legal mechanisms.⁸² In many cases, victims are discouraged by their immediate social environment, including peers, educators, and even family members. The Table 3 illustrates the socio-cultural barriers influencing cyberbullying reporting and enforcement:

Table 3. Cultural Barriers to Cyberbullying Reporting and Legal Enforcement

Cultural Factor	Manifestation in Society	Effect on Legal Process	Theoretical Explanation
Normalization of cyberbullying	Viewed as “joking” or peer interaction	Underreporting of cases	Cultural minimization of harm
Victim-blaming attitudes	Victims blamed for online behavior	Reduced willingness to report	Secondary victimization theory
Fear of retaliation	Anxiety over social or digital backlash	Silence among victims	Social control theory
Low digital literacy	Limited awareness of legal rights	Lack of legal activation	Legal consciousness gap. ⁸³

Source: Various sources, edited and analyzed by Authors

⁷⁸ See Brenner, “Cyber-threats and the Limits of Bureaucratic Control.”

⁷⁹ David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed.

⁸⁰ Clough, *Principles of Cybercrime*. 3rd ed.

⁸¹ See Citron, *Hate Crimes in Cyberspace*.

⁸² See Loader, and Sparks. *Public Criminology?*

⁸³ Patricia Ewick, and Susan S. Silbey. *The Common Place of Law: Stories for Everyday Life*. (Chicago: University of Chicago Press, 1998).

As Table 3 demonstrates, legal culture functions as a gatekeeping mechanism that determines whether legal norms are activated or remain dormant. Even when legal protections exist formally, they become ineffective if societal norms discourage their utilization. The interaction of these three dimensions—substance, structure, and culture—reveals that the inefficiency of cyberbullying regulation in Indonesia is systemic rather than isolated. As Soekanto⁸⁴ argues, law cannot function effectively without alignment between normative frameworks, institutional capacity, and social acceptance.

From a policy perspective, this multidimensional failure necessitates comprehensive legal reform. The first imperative is legislative harmonization through the explicit codification of cyberbullying as a distinct offence that includes repetitive harassment, digital humiliation, impersonation, and psychological harm. The second imperative involves institutional strengthening through enhanced digital forensic capacity and improved inter-agency coordination. The third imperative requires cultural transformation through digital literacy education and victim-support mechanisms.

VI. CONCLUSION

The analysis demonstrates that the Indonesian legal framework for addressing cyberbullying remains structurally fragmented, doctrinally inconsistent, and normatively incomplete, thereby generating persistent legal uncertainty in the determination of criminal liability. Although various statutory instruments—particularly the ITE Law (as amended by Law No. 1 of 2024), the Indonesian Criminal Code (Law No. 1 of 2023), the Child Protection Law, and the Personal Data Protection Law—provide partial regulatory coverage, none of these frameworks conceptualize cyberbullying as a distinct legal offence. As a result, law enforcement relies heavily on analogical interpretation of defamation, threats, and insult provisions, which were originally designed for offline contexts and are insufficient to capture the repetitive, relational, and psychologically harmful nature of digital aggression. This condition confirms that the central problem identified in this research—legal uncertainty in constructing criminal liability for adolescent cyberbullying cases—stems not only from legislative gaps but also from structural and interpretative limitations within the criminal justice system.

In response to this problem, the study concludes that effective legal protection for adolescent victims of cyberbullying requires a shift from fragmented regulation toward a harmonized and integrated legal framework that explicitly recognizes cyberbullying as a standalone offence with clearly defined constitutive elements. Such reform must be accompanied by institutional strengthening in digital forensics, standardized prosecutorial and judicial interpretation, and enhanced victim reporting mechanisms to address enforcement gaps. Furthermore, legal reform alone is insufficient without parallel socio-cultural transformation through digital literacy and preventive education, as legal effectiveness is contingent upon societal willingness to activate legal norms. Therefore, a combined approach involving legislative codification, structural capacity-building, and cultural change

⁸⁴ Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*.

is essential to ensure legal certainty, effective criminal liability, and substantive justice for adolescent victims in the digital environment.

STATEMENTS

Acknowledgment

None

Funding Information

None

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement

The authors declare that generative artificial intelligence (AI) tools were used solely to assist in improving the clarity of language, grammar, and the organization of the manuscript during the writing process. The AI tools also supported preliminary drafting and language refinement under the direct supervision of the authors. All substantive intellectual contributions, including the conceptualization of the research, legal analysis, interpretation of data, critical evaluation of the literature, and formulation of arguments and conclusions, were undertaken exclusively by the authors. Every AI-assisted output was carefully reviewed, verified, and substantially revised to ensure its accuracy, originality, and compliance with academic and ethical standards. The authors accept full responsibility for the content of this manuscript, including the accuracy of all citations, interpretations, and conclusions presented.

REFERENCES

- Ashworth, Andrew. *Principles of Criminal Law*. 9th ed. (Oxford: Oxford University Press, 2021).
- Brenner, Susan W. "Cyber-threats and the Limits of Bureaucratic Control." *Minnesota Journal of Law, Science, and Technology* 14, no. 1 (2013): 137-258. <https://dx.doi.org/10.2139/ssrn.1950725>
- Citron, Danielle Keats. *Hate Crimes in Cyberspace*. (Cambridge, MA: Harvard University Press, 2014).
- Clough, Jonathan. *Principles of Cybercrime*. 3rd ed. (Cambridge: Cambridge University Press, 2021).

- Committee on the Rights of the Child. *General Comment No. 14 (2013): On the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration*. (Geneva: United Nations, 2013).
- Committee on the Rights of the Child.. *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*. (Geneva: United Nations, 2021).
- Council of Europe. *Convention on Cybercrime (ETS No. 185)*. Budapest, 2001.
- Cross, Cassandra, et al. "Responding to Cybercrime: Results of a Comparison Between Community Members and Police Personnel." *Trends and Issues in Crime and Criminal Justice* 635 (2021): 1-20.
- Donegan, Richard. "Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis." *The Elon Journal of Undergraduate Research in Communications* 3, no. 1 (2012): 33–42.
- Ewick, Patricia, and Susan S. Silbey. *The Common Place of Law: Stories for Everyday Life*. (Chicago: University of Chicago Press, 1998).
- Fletcher, George P. *Rethinking Criminal Law*. (Oxford: Oxford University Press, 2000).
- Fortin, Jane. "Children's Right to Know Their Origins-Too Far, Too Fast?." *Child and Family Law Quarterly* 21, no. 3 (2009): 336-355.
- Frensh, Wenggedes, Madiasa Ablisar, and Mahmud Mulyadi. "Criminal Policy on Cyberbullying of Children in Indonesia." *International Journal of Cyber Criminology* 15, no. 2 (2022): 44-59. <https://doi.org/10.5281/zenodo.4766542>
- Fuller, Lon L. *The Morality of Law*. (New Haven: Yale University Press, 1969).
- Gillespie, Alisdair A. *Cybercrime: Key Issues and Debates*. 2nd ed. (London: Routledge, 2019).
- Griffith, Kathy Daly. "Restorative Justice and Responsive Regulation." *Australian and New Zealand Journal of Criminology* 36, no. 1 (2003): 109-114.
- Hart, H. L. A. *The Concept of Law*. 3rd ed. (Oxford: Oxford University Press, 2012).
- Henry, Nicola, Asher Flynn, and Anastasia Powell. "Technology-Facilitated Domestic and Sexual Violence: A Review." *Violence against Women* 26, no. 15-16 (2020): 1828-1854. <https://doi.org/10.1177/1077801219875821>
- Hinduja, Sameer, and Justin W. Patchin. "Connecting Adolescent Suicide to the Severity of Bullying and Cyberbullying." *Journal of School Violence* 18, no. 3 (2019): 333–346. <https://doi.org/10.1080/15388220.2018.1492417>
- Hinduja, Sameer, and Justin W. Patchin. *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. 2nd ed. (Thousand Oaks, California: Corwin Press, 2015).
- Husak, Douglas. *Overcriminalization: The Limits of Criminal Law*. (Oxford: Oxford University Press, 2008).
- John, Ann, et al. "Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review." *Journal of Medical Internet Research* 20, no. 4 (2018): e129. <https://doi.org/10.2196/jmir.9044>
- Kareema, Afifa, Qadriya Qadriya, and Madaniyah Madaniyah. "Legal Protection for Cyberbullying Victims: A Comparative Study of Jinayah Perspective and Positive Law." *SYARIAT: Akhwal Syaksyah, Jinayah, Siyasah and Muamalah* 2, no. 2 (2025): 57-65. <https://doi.org/10.35335/bhqn5516>

- Kerr, Orin S. *Computer Crime Law*. (St. Paul, MN: West Academic, 2018).
- Kowalski, Robin M., et al. "Bullying in the Digital Age: A Critical Review and Meta-Analysis." *Psychological Bulletin* 140, no. 4 (2014): 1073–1137. <https://psycnet.apa.org/doi/10.1037/a0035618>
- Laena, M., and R. Riswadi. "Legal Protection for Child Victims of Cyber Bullying." *Proceedings of the 2nd International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2022, 16 April 2022, Semarang, Indonesia*. 2022.
- Lessig, Lawrence. *Code: Version 2.0*. (New York: Basic Books, 2006).
- Livingstone, Sonia, and Peter K. Smith. "Annual Research Review: Harms Experienced by Child Users of Online and Mobile Technologies." *Journal of Child Psychology and Psychiatry* 55, no. 6 (2014): 635–654. <https://doi.org/10.1111/jcpp.12197>
- Loader, Ian, and Richard Sparks. *Public Criminology?* (London: Routledge, 2011).
- Moeljatno, Moeljatno. *Asas-Asas Hukum Pidana*. (Jakarta: Rineka Cipta, 2008).
- OECD. *Children in the Digital Environment: Revised Recommendation of the OECD Council*. (Paris: OECD Publishing, 2025). Available at <https://legalinstruments.oecd.org/public/doc/272/272.en.pdf>
- Putra, Eka Nugraha. "Law' Silence on Cyberbullying to Children in Indonesia." *Brawijaya Law Journal* 11, no. 1 (2024): 135-163. <https://doi.org/10.21776/ub.blj.2024.011.01.07>
- Raz, Joseph. *The Authority of Law*. 2nd ed. (Oxford: Oxford University Press, 2009).
- Republic of Indonesia. *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Available online at <https://peraturan.bpk.go.id/details/234935/uu-no-1-tahun-2023>
- Republic of Indonesia. *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE Law)*. Available online at https://jdih.komdigi.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008
- Republic of Indonesia. *Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak*. Available online at <https://dev-jdih.bphn.go.id/doc/1596633>
- Republic of Indonesia. *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP Law)*. Available online at https://jdih.komdigi.go.id/produk_hukum/view/id/832/t/undangundang+nomor+27+tahun+2022
- Republic of Indonesia. *Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan Atas UU Nomor 23 Tahun 2002 tentang Perlindungan Anak*. Available online at <https://dev-jdih.bphn.go.id/doc/1325858>
- Republic of Indonesia. *Undang-Undang Republik Indonesia Nomor 11 Tahun 2012 Tentang Sistem Peradilan Pidana Anak (SPPA Law)*. Available online at <https://bphn.go.id/data/documents/12uu011.pdf>
- Simester, Andrew, and G. R. Sullivan. *Criminal Law Theory*. (Oxford: Hart Publishing, 2019).
- Slonje, Robert, Peter K. Smith, and Ann Frisén. "The Nature of Cyberbullying and Strategies for Prevention." *Computers in Human Behavior* 29, no. 1 (2013): 26–32. <https://doi.org/10.1016/j.chb.2012.05.024>

- Smahel, David, et al. *EU Kids Online Report: Survey Results from 19 Countries*. (London: London School of Economics, 2020). <https://doi.org/10.21953/lse.47fdeqj01ofo>
- Smith, Peter K., et al. "Cyberbullying: Its Nature and Impact in Secondary School Pupils." *Journal of Child Psychology and Psychiatry* 49, no. 4 (2008): 376–385. <https://doi.org/10.1111/j.1469-7610.2007.01846.x>
- Soekanto, Soerjono. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. (Jakarta: Rajawali Pers, 2008).
- Tobin, John, ed. *The UN Convention on the Rights of the Child: A Commentary*. (Oxford: Oxford University Press, 2019).
- Tokunaga, Robert S. "Following You Home from School: A Critical Review of Cyberbullying Research." *Computers in Human Behavior* 26, no. 3 (2010): 277–287. <https://doi.org/10.1016/j.chb.2009.11.014>
- UNESCO. *Behind the Numbers: Ending School Violence and Bullying*. (Paris: UNESCO, 2019).
- UNICEF. *Cyberbullying: What Is It and How to Stop It*. (New York: UNICEF, 2020).
- United Nations Human Rights Council. *The Promotion, Protection and Enjoyment of Human Rights on the Internet*. Resolution A/HRC/RES/32/13, 2016.
- United Nations. *Convention on the Rights of the Child*, 1989.
- United Nations. *United Nations Guidelines for the Prevention of Juvenile Delinquency (The Riyadh Guidelines)*, Adopted by General Assembly Resolution 45/112, on 14 December 1990. Available online at <https://www.ohchr.org/en/instruments-mechanisms/instruments/united-nations-guidelines-prevention-juvenile-delinquency-riyadh>
- United Nations. *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (The Beijing Rules)*, Adopted by General Assembly A/RES/40/33, on 29 November 1985. Available at <https://www.ohchr.org/sites/default/files/beijingrules.pdf>
- UNODC. *Comprehensive Study on Cybercrime*. (Vienna: United Nations Office on Drugs and Crime, 2013).
- Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed. (Cambridge: Polity Press, 2024).
- Willard, Nancy. *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*. (Champaign, IL: Research Press, 2007).
- Yar, Majid. *Cybercrime and Society*. (London: SAGE Publications, 2012).

*There is no trust more
sacred than the one the
world holds with
children*

Kofi Annan
Seventh Secretary-General of the United Nations
(1997–2006)