

# Criminal Liability for Cyberbullying Perpetrators from the Perspective of Indonesian Criminal Law

Fadilla Dwi Maharani<sup>1</sup>, Padrisan Jamba<sup>2</sup>

Universitas Putera Batam  
Email: pb220710025@upbatam.ac.id

Cyberbullying is one form of crime in the digital space that has serious impacts on victims, both psychologically, socially, and economically. The characteristics of this crime, such as the anonymity of perpetrators, its wide reach, and the rapid dissemination of information, pose distinct challenges to the enforcement of criminal law. This study aims to analyze the criminal liability of cyberbullying perpetrators from the perspective of Indonesian criminal law and to identify obstacles in efforts to provide legal protection for victims. The research method employed is a normative juridical approach through library research, conducted by examining statutory regulations, legal doctrines, and relevant literature. The results of the study indicate that criminal liability for cyberbullying perpetrators is fundamentally supported by existing legal frameworks, primarily through Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016, as well as provisions in the Indonesian Criminal Code, particularly Articles 310 and 311 concerning defamation. Nevertheless, the implementation of these legal provisions continues to face various obstacles, including the limited understanding of law enforcement officials, difficulties in digital evidence collection, technological developments that are not balanced with regulatory updates, and the low level of public awareness in reporting cases. Therefore, more comprehensive efforts are required through regulatory strengthening, capacity building for law enforcement authorities, inter-agency cooperation, and digital education and literacy to ensure effective legal protection for victims of cyberbullying in Indonesia.

**Keywords:** Criminal liability, cyberbullying, ITE Law, criminal law, victim protection

---

This is an open access article under the [CC BY-NC](#) license



**Corresponding Author:**

Fadilla Dwi Maharani  
Universitas Putera Batam  
pb220710025@upbatam.ac.id

---

## 1. Introduction

The development of information and communication technology has brought significant changes to various aspects of people's lives, particularly in social interaction patterns. The digitalization of communication through social media, instant messaging applications, and various online platforms has created new spaces for people to interact without the constraints of time and space. According to Castells (2020), society has now entered the era of the network society, where social relations increasingly rely on open, fast, and massive digital networks. While providing many benefits, this development has also given rise to various new social risks, one of which is the increase in information technology-based crime.

One form of crime that is increasingly prominent in the digital space is cyberbullying. Cyberbullying is an act of intimidation, insults, threats, or harassment carried out repeatedly through electronic media, such as social media, text messages, or other online platforms. According to Kowalski et al. (2021), cyberbullying has a more severe psychological impact than conventional bullying because attacks can occur at any time, are permanent, and can be witnessed by a wide audience. These impacts include stress, anxiety, depression, reduced self-confidence, and even social and economic disruption for victims.

Unlike conventional bullying, which generally occurs in person and is confined to a specific space, cyberbullying has unique characteristics, including the anonymity of the perpetrator, the wide reach of the

victim, and the speed at which content spreads, making it difficult to control. According to Hinduja and Patchin (2022), anonymity online often encourages perpetrators to act more aggressively because they feel protected from their true identities. Furthermore, insulting or defamatory content that has spread online is very difficult to completely remove, so the victim's suffering can last for a long time.

This cyberbullying phenomenon poses serious challenges to criminal law, particularly in terms of establishing evidence, determining criminal liability, and legal protection for victims. In the context of modern criminal law, criminal liability not only requires the existence of an unlawful act but must also consider the elements of culpability and the perpetrator's capacity to take responsibility. According to Muladi (2021), the development of cybercrime requires adjustments to the concept of criminal liability to remain relevant to the cross-border, technology-based nature of digital crime.

In Indonesia, regulations regarding cyberbullying are still scattered and have not been specifically regulated in a single regulation. Law enforcement against cyberbullying generally relies on Law Number 11 of 2008 concerning Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024, and several provisions in the Criminal Code. However, the application of these provisions in practice often sparks debate, particularly regarding the interpretation of loose provisions, the boundary between criticism and insult, and the protection of freedom of expression. According to Marzuki (2023), unclear norms in handling cybercrime have the potential to create legal uncertainty for both victims and perpetrators.

Furthermore, legal protection for cyberbullying victims still faces various obstacles, both from regulatory aspects, law enforcement officials, and public awareness. Many victims are reluctant to report cyberbullying incidents due to fear of social stigma, complicated legal processes, or a lack of understanding of available legal protection mechanisms. According to Wibowo and Rahmawati (2022), the cybercrime victim protection system in Indonesia still needs strengthening, particularly in terms of legal assistance and psychological recovery for victims.

Based on this description, this research is crucial for in-depth examination of the regulation and implementation of criminal liability for cyberbullying perpetrators in Indonesian criminal law, as well as identifying the obstacles faced in providing effective legal protection for victims. The results of this research are expected to contribute to the development of a national criminal law that is more responsive to the development of crime in the digital era.

Based on the above background, this research aims to: (1) Determine the form of criminal liability for cyberbullying perpetrators in Indonesian criminal law. (2) Identify the obstacles to law enforcement in providing protection for cyberbullying victims.

## 2. Method

This research employs a normative juridical method, namely legal research that focuses on the study of applicable positive legal norms and legal principles and doctrines relevant to the problem under study. The approaches employed in this research include a statute approach and a conceptual approach. The statutory approach is carried out by systematically examining various legal provisions governing cyberbullying, particularly the Electronic Information and Transactions Law, the Criminal Code, and other laws and regulations related to criminal liability and victim protection. Meanwhile, the conceptual approach is used to examine the concepts, doctrines, and views of legal experts regarding criminal liability, cybercrime, and legal protection for victims.

The type of data used in this research is secondary data obtained through library research. The legal materials analyzed consist of primary legal materials, namely relevant laws and court decisions; secondary

legal materials, in the form of legal literature such as textbooks, scientific journals, research results, and legal articles discussing cyberbullying and criminal law; and secondary legal materials, in the form of legal literature such as textbooks, scientific journals, research results, and legal articles discussing cyberbullying and criminal law. and tertiary legal materials, such as legal dictionaries, encyclopedias, and other supporting sources that assist in understanding the legal terms and concepts used.

Data collection was conducted through an inventory, classification, and systematization of legal materials in accordance with the research problem. Next, the data was analyzed qualitatively using legal interpretation methods, such as grammatical, systematic, and teleological interpretation, to gain a deep and comprehensive understanding of applicable legal norms. The results of the analysis were then presented descriptively and analytically to provide a comprehensive picture of the forms of criminal liability for cyberbullying perpetrators and legal protection efforts for victims within the Indonesian criminal law system.

### 3. Results and Discussion

#### Criminal Liability for Cyberbullying Perpetrators in Indonesia

Cyberbullying, as a form of technology-based crime, has distinct characteristics from conventional bullying. The anonymity of the perpetrator, the widespread reach of digital media, and the speed of information dissemination make this crime have serious psychological, social, and even economic impacts on victims. In the context of Indonesian criminal law, the basis for perpetrator liability can be found in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments in Law Number 19 of 2016, as well as several articles in the Criminal Code. The ITE Law provides a more specific legal basis for acts of insult, defamation, and intimidation in the digital realm. Articles in the ITE Law, such as Article 27 paragraph (3) concerning insult/defamation and Article 29 concerning threats of violence, can be used as a basis for prosecuting cyberbullying perpetrators. In addition, general provisions in the Criminal Code, such as Articles 310 and 311 concerning defamation, can also be applied. Thus, criminal liability for cyberbullying perpetrators essentially has a legal basis, although in practice, challenges remain.

Several legal studies also confirm that although cyberbullying is not expressly mentioned in a specific article in the Criminal Code, such acts can still be classified as criminal acts based on existing norms, such as insults, defamation, and threats of violence in the digital space. This research explains that the Electronic Information and Transactions Law (ITE) and the Criminal Code serve as alternative legal bases for prosecuting cyberbullying perpetrators, but their implementation often encounters obstacles such as difficult perpetrator identification and a normative framework that is not specific enough to address the complexity of information technology-based crimes. Therefore, although the basis for criminal liability is already available in Indonesian positive law, the clarity of the definition and application of these articles still requires legal consolidation to optimize protection for victims and legal certainty for perpetrators.

In addition to fulfilling the normative legal basis, criminal liability for cyberbullying perpetrators must also be analyzed through the theory of criminal liability in Indonesian criminal law. Criminal liability requires the perpetrator to be guilty, whether intentional or negligent, and the perpetrator's ability to be legally accountable for their actions. This principle aligns with the principle of "geen straf zonder schuld," which asserts that criminal penalties can only be imposed if there is a spiritual connection between the perpetrator and the act. In the context of cyberbullying, even though the act is committed through digital media and often with anonymity, the element of guilt can still be proven through digital traces, communication patterns, and electronic content that indicate the perpetrator's intent or awareness of committing an act that harms

the victim. Thus, electronic media does not eliminate criminal liability but rather serves as a means to expand the range of criminal acts for which legal accountability is available.

In addition to the normative legal basis and theory of criminal liability, several juridical studies emphasize that the regulation of cyberbullying in Indonesian law still faces significant challenges, primarily due to the lack of regulations specifically designating cyberbullying as a separate offense. Research shows that although the ITE Law and the Criminal Code can be used to prosecute cyberbullying perpetrators for offenses such as insult, defamation, or threats of violence, their implementation in practice is still considered ineffective due to the lack of explicit definitions and categorizations in the applicable regulations. This creates legal uncertainty and difficulties in consistently enforcing criminal accountability, including in identifying and proving elements of perpetrators' culpability in the digital realm. Therefore, normative consolidation is needed to clarify the scope of cyberbullying crimes and improve law enforcement officials' understanding of electronic evidence to optimize legal protection for victims.

In addition to normative aspects and theories of criminal responsibility, various legal studies indicate that one of the main obstacles in addressing cyberbullying is the unclear status of the crime of cyberbullying itself in Indonesian criminal law, necessitating interpretation across existing articles. Although the Electronic Information and Transactions Law (ITE Law) and the Criminal Code (KUHP) are often used as references to prosecute perpetrators because they can accommodate acts of harassment, insults, or the distribution of harmful content electronically, these regulations do not explicitly address cyberbullying as a specific offense. Therefore, law enforcement officials often face challenges in consistently applying the provisions, particularly in proving the perpetrator's identity and elements of their culpability in the digital space. Consequently, while a legal framework exists that can be used to prosecute perpetrators, its lack of specificity regarding the phenomenon of cyberbullying creates legal uncertainty and requires further synchronization between existing regulations and law enforcement practices in the field. Therefore, in addition to strengthening the understanding of law enforcement officials, updating regulations that are more specific to information technology-based crimes is considered crucial to ensure legal certainty and effective protection for victims.

### **Barriers to Law Enforcement Against Cyberbullying**

Despite the availability of legal instruments, law enforcement against cyberbullying cases in Indonesia faces several major obstacles. First, law enforcement officials' lack of understanding of the various forms of digital crime often results in suboptimal investigation and prosecution processes. Second, difficulties in obtaining digital evidence, such as tracing the identities of perpetrators who frequently use anonymous accounts, slow down case handling. Third, rapid technological developments often outpace regulatory updates, making it difficult for authorities to adapt to new modes of cybercrime. Another obstacle lies in low public awareness of the importance of personal data protection and ethics in social media. Many victims are reluctant to report their experiences due to feelings of shame, fear, or distrust of law enforcement officials. This exacerbates the situation and has the potential to increase the psychological impact on victims.

### **Law Enforcement and Victim Protection**

To strengthen legal protection for victims of cyberbullying, concrete steps are needed, both in terms of regulations and law enforcement practices. From a regulatory perspective, policymakers need to update legal instruments to be more responsive to developments in digital crime. Drafting specific regulations regarding cyberbullying can be a solution to clarify its definition, forms, and criminal sanctions. From a law enforcement perspective, increasing the capacity of officers through training in cybercrime investigation is a crucial step. Authorities must be equipped with the technical skills to identify digital evidence, trace perpetrators, and understand relevant regulations. Furthermore, cooperation between institutions, both

national and international, is necessary, given that cybercrime often transcends national jurisdictions. Furthermore, preventive measures are also crucial through educating the public, especially the younger generation, about the dangers and impacts of cyberbullying. Digital literacy and anti-cyberbullying campaigns can reduce the potential for incidents and encourage victims to be more willing to report them.

#### 4. Conclusion

Cyberbullying, as a technology-based crime, has characteristics that differ from conventional bullying because it is carried out through digital media with wide reach, high speed of distribution, and anonymity of the perpetrator, resulting in serious psychological, social, and economic impacts for the victim. Indonesia actually has a legal basis for ensnaring perpetrators, namely through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was amended by Law Number 19 of 2016, as well as several provisions in the Criminal Code such as Articles 310 and 311 concerning defamation. However, law enforcement practices still face obstacles such as a lack of understanding by officials, the difficulty of digital evidence, rapid technological developments that are not balanced with regulatory updates, and low public awareness in reporting cases. Therefore, legal protection for victims of cyberbullying requires more comprehensive measures, both through more specific regulatory updates, increasing the capacity of law enforcement officials, cross-institutional cooperation, including international ones, as well as preventive efforts in the form of digital literacy and anti-cyberbullying campaigns to create a safe and healthy digital environment.

#### 5. Reference

- Arief, B. N. (2018). *Bunga rampai kebijakan hukum pidana*. Kencana Prenadamedia Group.
- Castells, M. (2020). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
- Cyberbullying sebagai bentuk kejahatan siber dan tantangan penegakan hukumnya di Indonesia. (2019). *Jurnal Ilmu Hukum*, 10(2).
- Hinduja, S., & Patchin, J. W. (2015). Bullying beyond the schoolyard: Preventing and responding to cyberbullying. *Aggression and Violent Behavior*, 23, 69–74.
- Hinduja, S., & Patchin, J. W. (2022). *Cyberbullying: Identification, prevention, and response*. Cyberbullying Research Center.
- Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Kowalski, R. M., Limber, S. P., & McCord, A. (2021). A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*, 57, 101428. <https://doi.org/10.1016/j.avb.2020.101428>
- Makarim, E. (2015). Kerangka kebijakan dan reformasi hukum cyber law di Indonesia. *Jurnal Hukum dan Pembangunan*, 45(2), 235–256.
- Marzuki, P. M. (2023). *Penelitian hukum: Edisi revisi*. Kencana Prenadamedia Group.
- Muladi. (2021). Pertanggungjawaban pidana dalam tindak pidana berbasis teknologi informasi. *Jurnal Hukum & Pembangunan*, 51(2), 245–260. <https://doi.org/10.21143/jhp.vol51.no2>
- Rahardjo, S. (2014). *Penegakan hukum: Suatu tinjauan sosiologis*. Citra Aditya Bakti.
- Raharjo, A. (2018). Tantangan penegakan hukum terhadap kejahatan siber di Indonesia. *Jurnal RechtsVinding*, 7(2), 245–260.

- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376–385.
- Soekanto, S. (2015). *Faktor-faktor yang mempengaruhi penegakan hukum*. RajaGrafindo Persada.
- Tokunaga, R. S. (2010). Following you home from school: A critical review of cyberbullying research. *Computers in Human Behavior*, 26(3), 277–287.
- Wibowo, A., & Rahmawati, N. (2022). Perlindungan hukum terhadap korban kejahatan siber di Indonesia. *Jurnal RechtsVinding*, 11(3), 421–436.