International Journal of Education, Vocational and Social Science
https://e-journal.citakonsulindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS

Cyber Bullying, Hate Speech, and Defamation in Cyberspace

Heri Tahir[1]
[1,2]Faculty of Social Science and Law, Universitas Negeri Makassar, Indonesia
Ririn Nurfaathirany Heri[2]
[1,2]Faculty of Social Science and Law, Universitas Negeri Makassar, Indonesia

Corresponding Author: [1]heri.tahir@unm.ac.id, [2]ririn.nurfaathirany@unm.ac.id

Abstract

The rapid development of information and communication technology has transformed cyberspace into a limitless medium of social interaction. Normatively (das sollen), digital space should function as a platform for freedom of expression while still respecting human dignity, reputation, and individual rights. However, in reality (das sein), cyberspace is frequently exploited for cyber bullying, hate speech, and online defamation, resulting in psychological harm, social conflict, and human rights violations. This study examines the legal boundaries between legitimate criticism and defamation, as well as the distinction between expressions of dislike and hate speech capable of inciting hostility and violence in digital spaces.

This research employs a normative legal research method using statutory, conceptual, and case approaches. Data were obtained through library research involving legislation, legal documents, academic journals, and relevant scholarly literature, which were analyzed descriptively and qualitatively.

The findings demonstrate that Indonesian legal regulations concerning defamation and hate speech in cyberspace have evolved significantly through amendments to the Electronic Information and Transactions Law, particularly Law Number 1 of 2024. The reformulation of these legal provisions seeks to clarify the boundary between freedom of expression and acts that attack personal honor or incite hatred based on ethnicity, religion, race, and intergroup relations (SARA). This study concludes that law enforcement against content-related cybercrimes must be carried out proportionally and cautiously while maintaining the protection of freedom of expression and the right to human dignity and reputation.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Keywords: Cyber Bullying; Hate Speech; Defamation; Cyberspace; Electronic Information and Transactions Law; Freedom of Expression.

INTRODUCTION

The characteristics of cybercrime have become one of the greatest challenges for modern criminal justice systems. Its transnational nature, anonymity of perpetrators, and the existence of digital traces that are easily manipulated or deleted require law enforcement authorities to adopt more sophisticated investigative methods and international cooperation mechanisms (Sitorus, 2022). Legal systems originally designed to handle crimes with clear territorial jurisdiction (locus delicti) are now compelled to adapt to offenses committed across multiple servers and jurisdictions worldwide (Sitorus, 2022).

The history of cybercrime reflects the evolution of technology itself. From the early activities of hackers motivated by intellectual curiosity, society now faces organized cybercrime syndicates operating like multinational corporations (Holt & Bossler, 2020; Miquic & Brewer, 2023). Understanding this historical trajectory provides insight into how criminal motives and methods have evolved alongside technological advancement, ranging from simple computer viruses to ransomware attacks capable of paralyzing a state's critical infrastructure (Holt & Bossler, 2020; Miquic & Brewer, 2023).

Cyberspace has also dramatically shifted the landscape of modern criminality. The internet is no longer merely the target of attacks but has evolved into an ecosystem facilitating various forms of conventional crimes (Holt & Bossler, 2020). Cyberspace now serves as a black market for drugs and weapons, a platform for terrorist recruitment and propaganda dissemination, and a medium for fraud and exploitation against vulnerable individuals. Consequently, cyberspace has become a catalyst that expands the reach and intensity of criminal activities (Miquic & Brewer, 2023).

The evolution of crime into the digital realm can be understood through three major stages. The first stage occurs when computers are used merely as tools to facilitate conventional crimes. For example, an accountant may use spreadsheet software to manipulate financial reports and embezzle company funds. At this stage, the essence of the offense remains conventional, although technology facilitates its execution (Holt & Bossler, 2020). Existing criminal law systems are relatively capable of addressing such crimes because the fundamental elements of the offense remain unchanged.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Another deeply concerning aspect of cybercrime involves offenses directed against human dignity, honor, and social order itself. Words typed on digital devices may seem insignificant, yet legally and psychologically they can inflict harm more severe than physical violence (Astuti, 2019; Febriani, 2021). Cyberspace has become an arena where reputations may be destroyed instantly, collective hatred may be ignited through viral content, and vulnerable individuals, especially children, may be exploited in unimaginable ways (Astuti, 2019; Febriani, 2021). Content-related crimes present unique challenges to legal systems. Unlike hacking or malware dissemination, which are universally condemned, many content-related offenses occupy a gray area intersecting with the fundamental human right to freedom of expression (Ispriyarso & Setya, 2020). Where should the boundary between legitimate criticism and defamation be drawn? At what point does an expression of dislike transform into hate speech capable of inciting violence? Addressing these questions remains a persistent challenge for legislators, law enforcement authorities, and judges worldwide, including in Indonesia (Saragih & Simarmata, 2021; Ispriyarso & Setya, 2020).

RESEARCH METHOD

This study constitutes normative legal research focusing on positive legal norms, legal doctrines, and the synchronization between legislation and developments in cyberspace-related crimes (Sitorus, 2022; Holt & Bossler, 2020). The research aims to analyze the legal boundaries between legitimate criticism and defamation, as well as the distinction between expressions of dislike and hate speech capable of provoking violence in digital spaces (Ispriyarso & Setya, 2020; Saragih & Simarmata, 2021).

The study employs statutory, conceptual, and case approaches. The statutory approach examines regulations concerning cybercrime, particularly the Indonesian Criminal Code (KUHP), Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 1 of 2024, and other regulations related to human rights and freedom of expression (Law Number 11 of 2008 concerning Electronic Information and Transactions; Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law). The conceptual approach is used to understand cyber bullying, hate speech, defamation, freedom of expression, and the protection of human dignity from criminal law and criminological perspectives (Astuti, 2019; Febriani, 2021; Ispriyarso & Setya, 2020; Saragih & Simarmata, 2021). Meanwhile, the case approach analyzes judicial decisions and contemporary phenomena related to content-based crimes in cyberspace (Sari & Wijaya, 2020; Febriani, 2021).

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Legal materials used in this research consist of primary, secondary, and tertiary legal sources. Primary legal materials include statutes and court decisions (Law Number 11 of 2008 concerning Electronic Information and Transactions; Law Number 1 of 2023 concerning the Criminal Code; Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law). Secondary legal materials consist of books, scientific journals, research findings, academic articles, and expert opinions related to cybercrime, hate speech, cyber bullying, and defamation (Holt & Bossler, 2020; Miquic & Brewer, 2023; Astuti, 2019; Febriani, 2021; Ispriyarso & Setya, 2020; Saragih & Simarmata, 2021; Sari & Wijaya, 2020; Sitorus, 2022). Tertiary legal materials include legal dictionaries, encyclopedias, and supporting references explaining relevant legal concepts and terminology.

RESULTS AND DISCUSSION

The internet, with its anonymity and rapid dissemination features, has become an effective medium for amplifying verbal and social aggression (Astuti, 2019; Febriani, 2021). Bullying that was once confined to school environments can now follow victims into their private spaces twenty-four hours a day. Hate speech that might previously have reached only a limited audience can now spread globally within minutes. Likewise, reputations built over decades may be destroyed through a single defamatory post. Cyber bullying, hate speech, and online defamation, although distinct phenomena, share a common characteristic: the use of words and images as weapons to attack individuals or groups (Astuti, 2019; Febriani, 2021; Saragih & Simarmata, 2021).

The psychological consequences of these attacks are profound and often devastating. Victims may experience anxiety, depression, social isolation, and in extreme cases, suicide (Astuti, 2019; Febriani, 2021). Law enforcement in this area is highly complex because it requires balancing victim protection with constitutional guarantees of freedom of speech and expression. Achieving a fair balance constitutes one of the greatest challenges in implementing Indonesia's Electronic Information and Transactions Law (ITE Law) (Sari & Wijaya, 2020; Ispriyarso & Setya, 2020). Imagine a public square. Freedom of expression is the right of everyone to speak at any available podium. However, this right is not absolute. Defamation is like someone climbing onto a podium and falsely shouting that a vendor in the square is a thief, thus damaging his business. Hate speech is when someone on that podium incites a mob to attack another group of people based on their ethnicity. Cyberbullying is when a group of people persistently follow a single individual around the square, shouting insults and threats. The law's role is to stop this destructive behavior without having to dismantle the podium or ban everyone from speaking.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

1. Legal Boundaries of Online Defamation

Online defamation in Indonesia is currently regulated under Article 27A of Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law). This provision replaced the previous formulation, which had long been criticized as a "rubber article" due to its broad interpretation and potential misuse in suppressing criticism (Sari & Wijaya, 2020). Article 27A stipulates:

"Any person who intentionally attacks the honor or reputation of another person by accusing them of a certain matter with the intention that such accusation becomes publicly known through Electronic Information and/or Electronic Documents conducted via an Electronic System."

This reformulation demonstrates legislative efforts to clarify the elements of defamation by referring more explicitly to conventional criminal law concepts, particularly those previously regulated under Article 310 of the Indonesian Criminal Code and later incorporated into Chapter XVII concerning crimes against honor (Law Number 1 of 2023 concerning the Criminal Code; Sari & Wijaya, 2020). Thus, not every criticism or social media comment can automatically be categorized as defamation. Fundamentally, the prohibited act involves making accusations against another person with the intention that such accusations become publicly known and damage that person's honor or reputation (Sari & Wijaya, 2020).

The revision of the ITE Law, through Law No. 19 of 2016, attempts to mitigate the potential negative impacts of this article by lowering the maximum penalty from 6 years to 4 years in prison (Sari & Wijaya, 2020). This change is significant because with a sentence of less than 5 years, suspects cannot be immediately detained during the investigation stage. Furthermore, the government and the Supreme Court have issued various guidelines, such as the Joint Decree of the Three Ministers, to emphasize that this article should not be used to silence criticism or expression based on facts and the public interest (Joint Decree of the Minister of Communication and Informatics, the Attorney General, and the Chief of the Indonesian National Police).

2. Criminal Elements and Legal Sanctions for Hate Speech

Hate speech is specifically regulated in Article 28 paragraph (2) of the ITE Law (Law Number 11 of 2008 concerning Electronic Information and Transactions). This article prohibits the dissemination of information intended to "incite feelings of hatred or hostility towards individuals and/or certain community groups based on ethnicity, religion, race, and inter-group relations

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

(SARA)." Unlike defamation, which attacks individuals, hate speech targets the collective identity of a group and has the potential to trigger broader social conflict (Ispriyarso & Setya, 2020; Saragih & Simarmata, 2021). Proving this offense presents a higher challenge. Prosecutors must not only prove that the information disseminated contains hatred, but also prove the perpetrator's intent (mens rea) that the information was "intended to incite" hatred (Ispriyarso & Setya, 2020). This is a demanding standard of proof. The "based on ethnicity, religion, race, and intergroup relations" element also limits the scope of this article to the protected identity category, and excludes hate speech based on, for example, sexual orientation or disability (Ispriyarso & Setya, 2020).

The sanctions for violating Article 28 paragraph (2) are regulated in Article 45A paragraph (2), namely a maximum prison sentence of 6 years and/or a maximum fine of IDR 1 billion (Law Number 11 of 2008 concerning Electronic Information and Transactions). Due to the serious threat and its serious impact on social harmony, law enforcement against this offense is a priority (Saragih & Simarmata, 2021). However, just like the defamation article, the application of this article must also be carried out very carefully so as not to misdirect the target and instead suppress critical public discussion on sensitive SARA issues (Ispriyarso & Setya, 2020).

3. The Challenge of Proving Malicious Intent in Cyber Bullying Cases

Cyber bullying is a complex phenomenon and does not yet have a single legal definition in Indonesian law (Astuti, 2019; Febriani, 2021). In practice, cyber bullying cases are often prosecuted using a combination of articles, depending on the nature of the act. If the bullying involves insults, Article 27 paragraph (3) concerning defamation can be used. If it involves threats of violence, Article 29 of the ITE Law ("threats of violence or intimidation directed personally") becomes relevant (Law Number 11 of 2008 concerning Electronic Information and Transactions). The main challenge in prosecuting cyberbullying is proving the perpetrator's malicious intent (mens rea). Perpetrators often claim their actions were merely "jokes," "pranks," or "satire." Distinguishing between inappropriate jokes and systematic bullying aimed at psychologically harming the victim is a difficult task for investigators and judges (Febriani, 2021).

Proof often relies on analysis of context, frequency, and the impact on the victim, which requires testimony from expert psychological witnesses (Febriani, 2021). Digital evidence such as screenshots of conversations or posts is crucial, but it also has limitations. Screenshots may not fully convey the context of the conversation or may even be manipulated. Furthermore, the anonymity facilitated by fake accounts makes identifying perpetrators a technical challenge (Holt & Bossler, 2020; Sitorus, 2022). Effectively addressing cyberbullying ultimately requires not only

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

law enforcement but also extensive education about empathy and digital ethics for the public, especially the younger generation (Astuti, 2019; Febriani, 2021).

This regulation protects the right to freedom of expression, as guaranteed by the constitution and human rights instruments (Ispriyarso & Setya, 2020). In recent developments, defamation remains a criminal offense, meaning legal proceedings can only be initiated upon a direct complaint from the aggrieved party (Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law). The nature of this complaint offense is intended to prevent the arbitrary use of the defamation article by parties other than the direct victim.

Another important change is in the criminal aspect. Based on Article 45 paragraph (4) of the 2024 amendment to the ITE Law, the criminal threat for perpetrators of defamation through electronic media is a maximum prison sentence of 2 (two) years and/or a maximum fine of IDR 400,000,000.00 (four hundred million rupiah) (Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law). This reduction in criminal penalties demonstrates a more proportional direction in criminal law policy and prioritizes the principle of ultimum remedium in handling defamation cases in the digital space (Sari & Wijaya, 2020). The latest provisions in Law No. 1 of 2024 have changed the penalty to a maximum of two years' imprisonment and/or a fine of Rp 400,000,000 (Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law).

The government, together with the Supreme Court and law enforcement officials, has also issued various interpretative guidelines, including the Joint Decree (SKB) on Guidelines for the Implementation of the ITE Law, which emphasizes that defamation provisions may not be used to silence criticism, academic opinions, or expressions based on facts and the public interest (Joint Decree of the Minister of Communication and Informatics, the Attorney General, and the Chief of the Indonesian National Police). In practice, law enforcement officials are required to distinguish between legitimate criticism in a democratic society and personal attacks that seriously damage an individual's honor (Sari & Wijaya, 2020).

Thus, the reformulation of defamation provisions in the latest ITE Law reflects the state's efforts to balance two equally important legal interests: protecting an individual's honor and reputation, on the one hand, and protecting freedom of expression and the right to express opinions in the digital space, on the other (Sari & Wijaya, 2020; Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law).

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

CONCLUSION

The development of information technology has given rise to new forms of cybercrime that not only attack electronic systems but also the honor, dignity, and psychological security of individuals and groups. Cyberbullying, hate speech, and defamation are forms of content-based crime that have a broad impact on social life and the order of the digital community.

Legal regulations in Indonesia regarding defamation and hate speech have undergone significant development through amendments to the Electronic Information and Transactions Law, specifically Law Number 1 of 2024. The reformulation of Article 27A of the ITE Law demonstrates the state's efforts to provide a clearer line between legitimate criticism as part of freedom of expression and actions that attack a person's honor or reputation. Similarly, the regulation of hate speech through Article 28 paragraph (2) of the ITE Law aims to protect the public from the spread of hate based on ethnicity, religion, race, and intergroup relations (SARA), which has the potential to trigger social conflict and violence.

Nevertheless, law enforcement against content-based cybercrime still faces various challenges, particularly in proving the element of malicious intent (mens rea), identifying anonymous perpetrators, and defining the boundaries between criticism, satire, insults, and hate speech. Therefore, law enforcement must be carried out carefully and proportionally, while still ensuring the protection of human rights, particularly freedom of expression. Ultimately, combating cyberbullying, hate speech, and defamation cannot rely solely on a penal approach. It also requires digital literacy education, strengthening social media ethics, and raising public awareness to create a healthy, safe, and civilized digital space.

REFERENCES

Astuti, S. I. (2019). A juridical review of cyberbullying behavior among adolescents in relation to Law Number 19 of 2016. *Wawasan Yuridika Journal, 3*(2), 249–266.

Febriani, A. (2021). Legal protection for victims of cyberbullying from the perspective of Indonesian criminal law. *Indonesian Journal of Legal Development, 3*(1), 108–122.

Holt, T. J., & Bossler, A. M. (2020). *Cybercrime and digital forensics: An introduction*. Routledge.

Ispriyarso, B., & Setya, W. (2020). The limitation of hate speech based on ethnicity, religion, race, and intergroup relations (SARA) in Indonesia: A criminal law perspective. *Journal of Indonesian Legal Studies, 5*(2), 349–376.

Miquic, A., & Brewer, G. (2023). Organized cybercrime: A systematic review. *Trauma, Violence, & Abuse, 25*(2).

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Saragih, H. Y., & Simarmata, J. (2021). Criminal law enforcement of hate speech based on Article 28 Paragraph (2) of the Electronic Information and Transactions Law. *Journal of Law Enforcement Studies, 8*(1), 1–13.

Sari, I. P., & Wijaya, A. (2020). The application of Article 27 Paragraph (3) of the Electronic Information and Transactions Law concerning defamation following the Constitutional Court decision. *Kertha Wicaksana Journal, 14*(2), 101–110.

Sitorus, L. (2022). Characteristics of transnational cybercrime and its law enforcement in Indonesia. *Lex Librum: Journal of Legal Studies, 8*(2), 115–128.

Legislation

Joint Decree of the Minister of Communication and Informatics, the Attorney General of the Republic of Indonesia, and the Chief of the Indonesian National Police concerning the Guidelines for the Implementation of Certain Articles of the Law on Electronic Information and Transactions.

Law Number 11 of 2008 on Electronic Information and Transactions.

Law Number 1 of 2023 on the Criminal Code.

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

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License