Progressive Law Review
Volume 8 No. 1 April 2026
University of Bandar Lampung
(e-ISSN) 2716-2141, progrresivelawreview.ubl.ac.id

CROSS-BORDER CYBERBULLYING LAW ENFORCEMENT FROM A CYBER LAW PERSPECTIVE

Received: May 21, 2026; Accepted: June 01, 2026; Online Published: June 05, 2026

Bobby Aldian Praja[1]

[1] *Faculty of Law,* Universitas Malahayati, *bobbyaldianp@malahayati.ac.id*

Abstract: Cross-border cyberbullying is a contemporary legal problem arising from the rapid development of information and communication technology, which increasingly blurs the territorial boundaries of state sovereignty through deterritorialization. Unlike conventional bullying, cyberbullying may be committed anonymously, disseminated instantly, preserved permanently through digital traces, and directed at victims located in different jurisdictions. This article examines the problems of criminal law enforcement against perpetrators of cross-border cyberbullying and evaluates the adequacy of national and international Cyber Law instruments in responding to such conduct. The research applies normative juridical legal research through statutory, comparative, and conceptual approaches. The analysis shows that law enforcement is obstructed by at least four interrelated issues: conflicts between state sovereignty and extraterritorial jurisdiction, differences in criminalization standards among states, the slow and formalistic operation of Mutual Legal Assistance and extradition mechanisms, and dependence on global digital platform providers for access to electronic evidence. These obstacles demonstrate that the borderless nature of cyberspace remains difficult to reconcile with conventional territorial criminal law. The article argues that Cyber Law requires a more functional and effects-based jurisdictional orientation, supported by the principle of reasonableness, international regulatory harmonization, stronger digital forensic capacity, and more responsive cooperation mechanisms. Such reconstruction is necessary to reduce legal loopholes and strengthen protection for victims of transnational cyberbullying.

Keywords: Cross-Border Crime; Cyber Law; Cyberbullying; Jurisdiction; Law Enforcement

I. INTRODUCTION

The development of information and communication technology in the current era of digital transformation has radically changed the landscape of human social interaction. Cyberspace has emerged as a new reality that offers borderless efficiency. However, behind this civilizational leap lies a massive negative consequence in the form of the increasing quantity and complexity of cybercrime. One of the most psychologically and socially destructive manifestations of cybercrime, yet often underestimated, is cyberbullying.[1]

Unlike conventional bullying, which is bound by spatial and temporal dimensions, cyberbullying has more dangerous characteristics: instant dissemination of information, permanent digital traces, perpetrator anonymity, and the ability to penetrate geopolitical borders. When a perpetrator in State A systematically intimidates, harasses, or assassinates the character of a victim in State B through a global social media platform, the conduct immediately transforms into a transnational crime.[2] Although previous studies have often limited this phenomenon to domestic dimensions through victimological or child protection approaches, this article goes further by examining the reconstruction of the classical doctrine of state sovereignty when confronted with the ubiquitous nature of the content layer.

Theoretically, Cyber Law emerged to anticipate this phenomenon of deterritoriality. Cyberspace is characterized by its borderless nature, whereas conventional criminal law rigidly relies on the absolute principle of territoriality. This principle affirms that a state's authority to adjudicate is strictly limited by its geographical boundaries. When cyberbullying occurs across borders, conflict of laws becomes unavoidable.[3]

In Indonesia, domestic law enforcement against cybercrime is primarily based on Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended several times, most recently by Law Number 1 of 2024. Although the Electronic Information and Transactions Law adopts an extraterritorial principle

[1] Barda Nawawi Arief, 2014. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: RajaGrafindo Persada, p. 45.

[2] Maskun, 2018. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana, p. 112.

[3] Dikdik M. Arief Mansur & Elisatris Gultom, 2017. *Cyber Law: Suatu Pengantar*. Bandung: Refika Aditama, p. 89.

under Article 2, its practical implementation against foreign perpetrators located abroad encounters serious obstacles. A state cannot unilaterally enforce its law within the sovereign territory of another state without violating international law.[4]

This problem is aggravated by differences in criminalization standards among states. Conduct that is regarded as defamation or cyberbullying in Indonesia may not necessarily be treated as a crime in countries that provide broad constitutional protection to freedom of expression, such as the United States under the First Amendment.[5] Consequently, the principle of double criminality, which is an essential requirement in extradition and Mutual Legal Assistance, may not be fulfilled.

Previous studies have mostly focused on the psychological impact of cyberbullying or on its enforcement within a domestic legal framework. There remains a gap in legal scholarship concerning how Cyber Law analyzes and resolves jurisdictional disorder in cyberbullying cases involving legal subjects from different jurisdictions. Therefore, this article aims to analyze the problems of law enforcement against perpetrators of cross-border cyberbullying and to formulate an ideal reconstruction of its enforcement in the future.

II. RESEARCH METHODS

This study employs normative juridical legal research, also known as doctrinal legal research. This method examines written law from several aspects, including legal theory, philosophy, comparative analysis, and the structure of statutory provisions.[6] The research uses three approaches.

1. Statutory approach, by examining the Electronic Information and Transactions Law, the New Criminal Code under Law Number 1 of 2023, and international instruments such as the Budapest Convention on Cybercrime.
2. Comparative approach, by comparing doctrines of cyber law enforcement between Civil Law jurisdictions, particularly Indonesia, and Common Law jurisdictions, particularly the United States and the United Kingdom.

---

[4] I Gede Bintang Putrawan, 2018. *Penerapan Asas Ekstrateritorial dalam Undang-Undang Informasi dan Transaksi Elektronik*. Jurnal Magister Hukum Udayana 7, no. 2, p. 192.

[5] Dan Jerker B. Svantesson, 2017. *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Pres, p. 204.

[6] Soerjono Soekanto & Sri Mamudji, 2015. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers, p. 14.

3. Conceptual approach, by analyzing the concepts of jurisdiction, digital sovereignty, and fundamental principles of Cyber Law.

Secondary data were obtained through library research consisting of primary legal materials, including statutes and conventions; secondary legal materials, including books, scholarly journals, and academic manuscripts; and tertiary legal materials, including legal dictionaries and encyclopedias. The data were analyzed qualitatively and normatively using a deductive method to derive specific conclusions from general legal principles.

III. ANALYSIS AND DISCUSSION

a. Characteristics of Cross-Border Cyberbullying in Cyber Claw

In Cyber Law discourse, cyberbullying is no longer viewed merely as digital juvenile misconduct, but rather as a form of computer-related crime that attacks a person's honor, dignity, and psychological integrity, including cyberstalking, harassment, and defamation.[7] The main characteristics that distinguish cross-border cyberbullying from conventional bullying are shown in Table 1.

Table 1: Characterictics of Conventional Bullying and Cross-Border Cyberbullying

Characteristic	Conventional Bullying	Cross-Border Cyberbullying
Locus delicti	Physically clear, with a single crime scene	Virtual and dispersed across several countries at once
Identity of the perpetrator	Generally known directly by the victim	Uses aliases, fake accounts, or VPNs
Impact on the victim	Limited to the physical social environment	Exponential, viral, and permanent
Legal jurisdiction	Subject to one national legal system	Involves multidimensional conflict of laws

Source: Analysed from secondary legal materials

In Cyber Law doctrine, this phenomenon triggers what Svantesson describes as "jurisdictional chaos."[8] When digital data in the form of insulting text is sent by a perpetrator in Singapore, transits through a server in California, and is downloaded

[7] Josua Sitompul, 2012. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, p. 77.

[8] Dan Jerker B. Svantesson, 2017. *Op Cit*. p. 56.

by a victim in Jakarta, causing acute psychological harm, the elements of action and effect become legally fragmented.

Cyber Law analyzes this situation by dividing cyberspace into three layers: the physical layer, consisting of physical servers; the logical layer, consisting of codes and protocols; and the content layer, consisting of digital information.[9] Cyberbullying operates at the content layer, yet its enforcement requires access to the physical and logical layers, which are often located outside the territorial jurisdiction of the victim's state. The content is global, but the reach of law enforcement remains local.

b. Main Problems in Cross-Border Law Enforcement

Criminal law enforcement against perpetrators of transnational cyberbullying faces several major barriers. These barriers are not only procedural but also substantive, technical, and political. They indicate that the conventional architecture of criminal law has not fully adapted to the transnational nature of digital harm.

1. Conflict Between Sovereignty and Jurisdictional Claims

A fundamental principle of international law provides that the sovereignty of a state is exclusive within its own territory under the principle of non-intervention.[10] Indonesia adopts an extraterritorial principle through Article 2 of the Electronic Information and Transactions Law, which provides that the law applies to legal acts committed both within and outside Indonesian territory, as long as such acts have legal consequences within Indonesia.

However, in public law, this extraterritorial principle is largely passive and declaratory. Indonesia does not possess enforcement jurisdiction to arrest a foreign national located in another state merely on the basis of domestic cyber law.[11] If Indonesian law enforcement authorities conducted police action abroad without the permission of the host state, such action would constitute a serious infringement of another state's sovereignty.

---

[9] Edmon Makarim, 2018. *Tantangan Hukum Mayantara dalam Menghadapi Kedaulatan Digital Negara*. Jurnal Hukum Pembangunan 48, no. 3, p. 455.

[10] Malcolm N. Shawm 2017. *International Law: 8th ed*. Cambridge: Cambridge University Press, p. 480.

[11] Edmon Makarim, 2018. *Op Cit*. p. 461.

2. Differences in Criminalization Standards and Dual Criminality

The most crucial substantive obstacle is the absence of uniform international standards concerning the limits of cyberbullying. In Indonesia, insult, defamation, and cyber-based attacks on personal honor are regulated under Articles 27A and 27B of the Electronic Information and Transactions Law, as amended in 2024. Distribution of content attacking a person's dignity may result in criminal liability.

By contrast, several Western jurisdictions, particularly the United States, adopt a broader conception of freedom of expression under constitutional protection.[12] In such jurisdictions, cyberbullying against adults may be treated as part of free speech unless it satisfies the element of a real and factual threat of violence. This legal difference has serious implications for international cooperation because double criminality requires that the act constitute a crime in both states. When Indonesia requests assistance from a state where the act is not criminalized, the request may be refused.[13]

3. Ineffectiveness of Mutual Legal Assistance and Extradition

Formal cooperation among states through Mutual Legal Assistance in cybercrime cases is widely known to be slow and bureaucratic. The process may take months or years, moving through several governmental channels before reaching the central authority of the requested state.[14]

This creates a structural contradiction between legal procedure and digital evidence. Electronic evidence is volatile and can be deleted, altered, or modified within seconds. By the time MLA documents are processed, log data or digital traces stored by foreign Internet Service Providers may have expired or been deleted because of short data-retention policies.[15] Extradition is also rarely effective in cyberbullying cases because the economic and political costs of cross-border extradition are often disproportionate to the weight of the criminal sanction.

---

[12] Dan Jerker B. Svantesson, 2017. *Op Cit*. p. 208.

[13] Agus Sukarno, 2021. *Mutual Legal Assistance (MLA) sebagai Instrumen Penegakan Hukum Cybercrime Transnasional*. Jurnal Hukum Siber Indonesia 4, no. 1, p. 25.

[14] Agus Sukarno, 2021. *Op Cit*. p. 29.

[15] United Nations Office on Drugs and Crime (UNODC). *Cybercrime Module 7: International Cooperation in Cybercrime Matters*. accessed May 15, 2026, https://www.unodc.org/e4j/en/cybercrime/module-7/index.html.

4. Dependece on Global Platform Providers

Most large-scale cyberbullying cases occur on global platforms such as Meta, X, TikTok, and Google. These technology companies are generally subject to the laws of the states in which they are incorporated, many of which are located in the United States.[16]

Indonesian law enforcement authorities frequently encounter difficulties in requesting personal data of perpetrators, including IP addresses and registered telephone numbers. Platform providers apply strict data privacy rules and often refuse to disclose user data unless there is a valid court order from the relevant jurisdiction or the case involves priority offences such as terrorism or child sexual exploitation.[17] As a result, cyberbullying and defamation cases under Indonesian law may receive limited cooperation, even when the conduct causes serious and long-term psychological harm to victims.

c. Comparative Analysis of the Budapest Convention on Cybercrime

In the search for a global solution, the most comprehensive international legal instrument currently available is the Convention on Cybercrime, commonly known as the Budapest Convention of 2001. This convention coordinates national criminal laws, investigative techniques, and international cooperation.[18]

One of the major strengths of the Budapest Convention is its regulation of expedited preservation of stored computer data under Articles 16 and 17. This mechanism requires member states to immediately preserve vulnerable cyber data before the formal Mutual Legal Assistance process is completed.[19] The problem for Indonesia is that, as of 2026, Indonesia has not ratified the Budapest Convention.

The delay in ratification is rooted in domestic legal-political concerns regarding intervention in digital sovereignty and the insufficient readiness of national law enforcement infrastructure.[20] Because Indonesia remains outside the convention system, its law enforcement authorities lose access to the 24/7 contact point

[16] Josua Sitompul, 2012. *Op Cit*. p. 143.
[17] Agus Sukarno, 2021. *Op Cit*. p. 32.
[18] Council of Europe, 2001. Convention on Cybercrime (Budapest Convention), ETS No. 185, Preamble.
[19] Council of Europe, 2001. Convention on Cybercrime (Budapest Convention), ETS No. 185, Article 16.
[20] Maskun, 2018. *Op Cit*. p. 201.

network, which is crucial for tracking perpetrators of cross-border cybercrime in real time.

d. Theoretical Reconstruction of Cyber Law Jurisdiction

To address the problems above, international law and Cyber Law have developed several theories to expand the reach of jurisdiction. The first is the objective territorial theory, or the Effect Doctrine, which provides that a state may exercise jurisdiction over acts initiated abroad when they produce substantial and essential harmful effects within its territory.[21] This theory has been adopted by Indonesia through the Electronic Information and Transactions Law.

The second is the subjective territorial theory, which emphasizes jurisdiction based on the place where the act was initiated or planned. The third is the ubiquity theory, which regards a crime as occurring both where the act was committed and where its consequences arose. This theory is particularly relevant to Cyber Law because it combines the place of conduct and the place of harm.[22]

Nevertheless, in cyberbullying cases, the Effect Doctrine must be applied together with the principle of reasonableness. A state should not claim jurisdiction over a foreign perpetrator if the impact within its territory is merely incidental or unintended.[23] There must be minimum contacts or proof of intent showing that the perpetrator deliberately directed the harmful digital conduct toward a victim located in the forum state.

IV. CONCLUSION

Law enforcement against perpetrators of cross-border cyberbullying from the perspective of Cyber Law continues to face complex structural and conceptual obstacles. The borderless character of cyberspace conflicts with the conventional conception of state sovereignty, which is based on physical geographical boundaries. The main barriers arise from the limited ability to exercise enforcement jurisdiction outside national territory, differences in substantive criminal law standards among states, the slow operation of Mutual Legal Assistance mechanisms,

[21] Dikdik M. Arief Mansur & Elisatris Gultom, 2017. *Op Cit*. p. 103.
[22] Barda Nawawi Arief, 2014. *Op Cit*. p. 92.
[23] Dan Jerker B. Svantesson, 2017. *Op Cit*. p. 312.

and the dependence of investigators on global platform providers for access to electronic evidence.

These findings show that conventional territorial criminal law is insufficient to respond to digital harm that is transnational, anonymous, and rapidly disseminated. Future Cyber Law therefore requires a reorientation from rigid physical sovereignty toward functional digital sovereignty. Jurisdiction should not be determined solely by the physical place where a perpetrator initiates data transmission, but also by the jurisdiction where substantial and intentional harm materializes. This orientation should be supported by the principle of reasonableness so that jurisdictional claims remain legitimate under international law.

Several recommendations follow from this analysis. First, Indonesia should accelerate the ratification of the Budapest Convention on Cybercrime or, at minimum, establish cyber-specific bilateral cooperation agreements with states that host major digital platforms. Second, the government should build formal cooperation with Over-the-Top platform providers to accelerate lawful access to data in severe cyberbullying cases. Third, law enforcement authorities should strengthen indictments through the ubiquity theory and a measurable Effect Doctrine supported by digital forensic evidence. Fourth, the state should invest in the technical capacity of cyber investigators so that electronic evidence collected in cross-border cases can satisfy international standards of admissibility.

REFERENCES

Arief, Barda Nawawi, 2014. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: RajaGrafindo Persada.

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

https://www.unodc.org/e4j/en/cybercrime/module-7/index.html.

Makarim, Edmon, 2018. *Tantangan Hukum Mayantara dalam Menghadapi Kedaulatan Digital Negara*. Jurnal Hukum Pembangunan 48, no. 3.

Mansur, Dikdik M. Arief & Elisatris Gultom, 2017. *Cyber Law: Suatu Pengantar*. Bandung: Refika Aditama.

Maskun, 2018. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana.

Putrawan, I Gede Bintang, 2018. *Penerapan Asas Ekstrateritorial dalam Undang-Undang Informasi dan Transaksi Elektronik*. Jurnal Magister Hukum Udayana 7, no. 2.

Republic of Indonesia, 2008. Law Number 11 of 2008 concerning Electronic Information and Transactions. State Gazette of the Republic of Indonesia Year 2008 Number 58.

Republic of Indonesia, 2024. Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. State Gazette of the Republic of Indonesia Year 2024 Number 3.

Shawn, Malcolm N., 2017. *International Law: 8th ed*. Cambridge: Cambridge University Press.

Sitompul, Josua, 2012. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.

Soekanto, Soerjono & Sri Mamudji, 2015. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers.

Sukarno, Agus, 2021. *Mutual Legal Assistance (MLA) sebagai Instrumen Penegakan Hukum Cybercrime Transnasional*. Jurnal Hukum Siber Indonesia 4, no. 1.

Svantesson, Dan Jerker B., 2017. *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Pres.