

Extraterritoriality of Hate Speech in Cyberspace from The Perspective of Jurisdictional Limits of The Electronic Information and Transaction Law

Rivana ¹⁾, Agus Mulyawan ²⁾, Rizki Setyobowo Sangalang ³⁾ & Heriamariaty ⁴⁾

¹⁾ Faculty of Law, Universitas Palangka Raya, Indonesia, E-mail: rivanaydr@gmail.com

²⁾ Faculty of Law, Universitas Palangka Raya, Indonesia, E-mail: agus.mulyawan@law.upr.ac.id

³⁾ Faculty of Law, Universitas Palangka Raya, Indonesia, E-mail: rizkisetayobowo@law.upr.ac.id

⁴⁾ Faculty of Law, Universitas Palangka Raya, Indonesia, E-mail: heriamariaty@law.upr.ac.id

Abstract. *The advancement of information and communication technology has created a new sphere of interaction known as cyberspace, where information can be disseminated without geographical boundaries. This condition not only facilitates the exchange of information but also gives rise to complex legal challenges, particularly concerning hate speech offenses. In Indonesia, the regulation of online hate speech is stipulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law Number 19 of 2016. The problem arises when perpetrators of hate speech reside outside Indonesia, yet their actions have legal impacts within the country. This situation relates to the application of the principle of extraterritoriality as regulated in Article 2 of the ITE Law, which extends Indonesia's jurisdiction to acts committed abroad that have legal consequences domestically. However, the application of this principle raises debate due to its potential conflict with the principle of territoriality in Indonesian criminal law as regulated in the Criminal Code (KUHP). This study aims to analyze the criminal law regulation of extraterritoriality within the ITE Law regarding hate speech in cyberspace and to examine the limits of Indonesia's jurisdiction in enforcing the law against cross-border cyber offenses. The research employs a normative legal method with statutory and conceptual approaches. The findings are expected to provide insight into the extent to which the principle of extraterritoriality in the ITE Law can be effectively applied in harmony with the general principles of Indonesian criminal law.*

Keywords: *Cyberspace; Extraterritoriality; Hate Speech; ITE Law; Jurisdiction.*

1. Introduction

The development of information and communication technology continues to lead humans towards the development of a new space for communication or interaction called cyberspace.

This space facilitates the process of disseminating and exchanging information without geographical boundaries, but on the other hand also gives rise to quite complex legal issues, especially related to criminal acts of hate speech. In this condition, provisions in Indonesia regarding hate speech carried out in cyberspace are regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) which has been amended by Law Number 19 of 2016. Article 27 paragraph (3) and Article 28 paragraph (2) of the ITE Law are the main legal basis for prohibiting acts that harm other parties through electronic media, including hate speech containing elements of SARA.

The increase in hate speech in cyberspace is accompanied by weak technical regulations for digital evidence in the Indonesian legal system (Azhar & Soponyono, 2020). The problem becomes more complex when the perpetrator of hate speech is located outside of Indonesia, but their actions have legal implications domestically. This relates to the application of the extraterritorial principle as stipulated in Article 2 of the ITE Law, which emphasizes that the law applies to anyone who commits a legal act, whether within or outside Indonesia, as long as the act has legal implications in Indonesia. With this provision, the ITE Law clearly recognizes the applicability of extraterritorial jurisdiction. However, debate has arisen regarding the limits of the application of this jurisdiction because the principle of territoriality in Indonesian criminal law, as stipulated in Article 2 of the Criminal Code, essentially only covers the territory of the state. Although Articles 4 to 9 of the Criminal Code also regulate the principle of extraterritoriality, its scope is still limited to the interests of a particular state. Therefore, the regulation of extraterritorial jurisdiction in the ITE Law raises questions about how it can be effectively implemented, particularly in cases of transnational hate speech.

Thus, this study focuses on examining the extent to which the application of the extraterritorial principle in the ITE Law is able to answer the challenges of law enforcement against hate speech in cyberspace that goes beyond national jurisdiction, and how it aligns with the general principles of criminal law applicable in Indonesia.

2. Research Methods

This study employs a normative legal research method with a statute approach and a conceptual approach. This method was chosen because the problem under study focuses on the analysis of positive legal norms contained in the Electronic Information and Transactions Law, the Criminal Code, and other relevant criminal law provisions. The data used consists of primary, secondary, and tertiary legal materials, which are then analyzed qualitatively to interpret and assess the consistency, harmonization, and effectiveness of extraterritoriality regulations in the context of hate speech in cyberspace.

3. Results and Discussion

3.1. Criminal Law Regulations Regarding Extraterritoriality in the Electronic Information and Transactions Law Regarding Hate Speech in Cyberspace

The development of computer and internet technology has had significant implications and impacts on the regulation and formation of cyberspace and cyber law, as well as on the development of cybercrime. Although internet use is now widespread, bringing positive changes to various aspects of life, including politics, social issues, and economics, it has also created a paradigm shift in the study of crime, particularly technology-related crimes. The criminal law provisions regarding extraterritoriality in the Electronic Information and Transactions Law (UU ITE) regarding hate speech in cyberspace refer to the principle of jurisdiction that covers territorial and extraterritorial aspects. Article 28 paragraph (2) of the ITE Law together with Article 45 paragraph (2) stipulates that the dissemination of information that incites hatred or hostility based on SARA (Ethnicity, Religion, Race, and Inter-group) can be punished with a maximum prison sentence of 6 years and/or a maximum fine of IDR 1 billion.

The extraterritoriality principle in the ITE Law allows for law enforcement of hate speech crimes committed by perpetrators outside Indonesia, provided the impact is felt within Indonesia. In the context of cybercrime, the ITE Law adopts the concept of extraterritoriality, as affirmed in Article 2 of the ITE Law. This provision reflects the application of the effects doctrine, a doctrine that authorizes a country to enforce its laws if the consequences of an act are felt within its territory (where the effect is felt), even if the act is committed abroad (Evelyn Julian Halim. (2022)). This law provides a legal basis for Indonesian law enforcement officials to take action against perpetrators of hate speech who utilize cyberspace even if the actions are carried out extraterritorially, that is, outside the country's borders (Evi Retno Wulan, (2015)). Although the principle of extraterritoriality is normatively stipulated in legislation, the application of this provision cannot be separated from the concept of criminal jurisdiction, namely the state's authority to establish and enforce criminal law against an act. According to Andi Hamzah, criminal jurisdiction is the basis of the state's legitimacy in exercising its criminal powers, both for acts committed within and outside the state's territory (Hijir Ismail Edhar. (2024)). However, in practice, several obstacles remain, primarily the differences in legal systems between countries and the limitations of extradition treaties, which complicate law enforcement efforts against transnational cybercriminals. Furthermore, difficulties in establishing evidence pose a challenge, given that digital data is often stored on servers outside Indonesia and can easily be deleted or manipulated. This situation demands strong international cooperation through mutual legal assistance mechanisms, extradition treaties, and enhanced digital forensic capabilities of law enforcement officials (Lilik Mulyadi, 2020). Without this mechanism, the legal process becomes difficult to carry out, especially if the country where the perpetrator is located does not have a treaty relationship with Indonesia.

Second, there are differences in legal standards and definitions of cybercrime between countries. Not all countries categorize hate speech as a crime, especially those that uphold

absolute freedom of expression. As a result, law enforcement against perpetrators in these jurisdictions is difficult due to differences in fundamental legal principles. Third, the aspect of providing evidence and identifying perpetrators in cyberspace also presents its own challenges. Cybercrime is also related to the concept of digital locus delicti, which determines the place of occurrence of a crime based on the location where the legal consequences arise, not solely the physical location of the perpetrator. The use of virtual private networks (VPNs), fake identities, or anonymous accounts makes it difficult for law enforcement officials to track down the actual perpetrators. Furthermore, digital evidence is easily altered and deleted, requiring specialized expertise and cross-border cooperation in the collection of electronic evidence (M. Yahya Harahap, 2017). To strengthen the implementation of the principle of extraterritoriality in law enforcement against hate speech in cyberspace, synchronization is needed between the Criminal Code, the ITE Law, and relevant international legal instruments.

This legal synchronization is crucial to avoid overlapping regulations and ensure effective law enforcement. Furthermore, increasing the capacity of law enforcement officials to understand the characteristics of cybercrime and the use of digital forensic technology are also crucial steps in supporting an accurate and efficient evidence-gathering process (R. Wiyono, 2021). Thus, the criminal law regulation of the extraterritoriality principle in the ITE Law represents an adaptation of national law to the challenges of globalization in information technology. The application of this principle is expected to protect national interests and ensure legal justice for the Indonesian people from the negative impacts of information technology misuse, particularly regarding the spread of hate speech in cyberspace, which can threaten unity, security, and public order (Teguh Prasetyo, 2017).

3.2. Jurisdictional Limits of the Electronic Information and Transactions Law in Enforcing the Law Against Online Hate Speech Carried Out Across Countries

Extraterritorial jurisdiction is the legal authority of a country to prosecute acts occurring outside its territory. However, the implementation of this principle faces various obstacles, primarily due to the limitations of the state in exercising power within the territory of another country, despite having jurisdiction over certain acts and legal interests. In the context of law enforcement in Indonesia, the ITE Law and the Criminal Code are the national legal instruments used to address cybercrimes. The provisions regarding criminal jurisdiction in Book I of the Criminal Code, specifically Articles 4 to 9, and Articles 2 and 37 of the Electronic Information and Transactions Law, remain limited in scope. This situation has the potential to create legal loopholes that prevent cybercrimes from being prosecuted or tried, thus contradicting the no-safe-haven principle, which emphasizes that there should be no safe haven for perpetrators of cybercrimes. The provisions on criminal jurisdiction over cybercrimes in Indonesian laws and regulations should be based on the application of the principle of extraterritorial jurisdiction. Therefore, strengthening criminal jurisdiction regulations in national criminal law is necessary to cover cybercrimes committed outside the country's territory, whether within the jurisdiction of another country or occurring outside the jurisdiction of any country (Rusdianto, & Muh. Risnain, (2023). Theoretically, the limits of a country's jurisdiction in criminal law are determined by several principles, namely the

principles of territoriality, active nationality, passive nationality, protection, and universality (Andi Hamzah, 2008). In addition, the concept of prescriptive jurisdiction has also developed, namely the authority of a state to establish legal norms regarding certain actions even if they are carried out outside its territory, as long as these actions threaten national legal interests.

This concept aligns with the principle of protection, which justifies the state's actions to maintain national order and security. However, the development of cybercrime necessitates an expansion of this territorial principle, as cybercrime is often committed without geographical boundaries. In a global context, jurisdiction over transnational crimes is governed by several principles of international law, including the objective territorial principle (jurisdiction applies if the consequences of the act are felt within the state's territory), the protective principle (if the act threatens the vital interests of the state), and the universality principle (if the crime is deemed to threaten the public interest worldwide, such as terrorism and war crimes). This objective territoriality principle underpins the application of the ITE Law to transnational online hate speech, as its legal consequences are felt in Indonesia.

For example, when perpetrators of hate speech against Indonesian state symbols carry out their actions from abroad via global social media platforms such as X (Twitter) or Facebook, Indonesian law enforcement officials need to cooperate with the authorities of the country where the perpetrator or the platform server is located to obtain digital evidence and carry out legal summons (Budi Suhariyanto, 2013).

Without an effective cooperation mechanism, law enforcement will be hampered and perpetrators will likely act without fear of legal consequences. In addition to legal and technical constraints, there are also issues of legal substance. The ITE Law does not yet provide a clear definition of the scope of "legal consequences in Indonesia," which forms the basis for the application of extraterritorial jurisdiction. This opens the door to diverse interpretations and has the potential to create legal uncertainty. Therefore, efforts are needed to synchronize the ITE Law with international legal provisions, particularly the 2001 Budapest Convention on Cybercrime, which regulates international cooperation mechanisms in the investigation and prosecution of cybercrimes (Riri Fitria, (2019). From a legal policy perspective, the Indonesian government needs to strengthen its national legal standing by establishing international digital cooperation instruments and amending the Electronic Information and Transactions (ITE) Law, which explicitly regulates jurisdictional boundaries and cross-border law enforcement mechanisms. These steps are crucial to ensure legal certainty, effective enforcement, and protection of the legal interests of Indonesian citizens in cyberspace.

Thus, the jurisdictional limits of the ITE Law in enforcing the law against transnational online hate speech can be said to be extraterritorial but limited. Normatively, Indonesia has the authority to enforce the law against acts that have consequences within its territory, but in practice, it relies on international cooperation and recognition of the principle of sovereignty of other states. Therefore, strengthening global cooperation mechanisms and harmonizing national laws with international law is imperative to ensure the effectiveness of cyber law enforcement in the future.

4. Conclusion

The conclusions that can be drawn from the Scientific Article/Journal entitled "Extraterritoriality of Hate Speech in Cyberspace from the Perspective of the Jurisdictional Boundaries of the Electronic Information and Transactions Law" are as follows: 1. The development of information technology demands adaptation of criminal law, particularly in addressing hate speech in cyberspace. The ITE Law stipulates the principle of extraterritoriality, allowing law enforcement against perpetrators outside Indonesia as long as the impact is felt domestically. However, its implementation still faces various obstacles, such as differences in legal systems between countries, limitations on extradition, and difficulties in obtaining digital evidence. Therefore, synchronization of national regulations with international law, strengthening cross-border cooperation, and increasing the capacity of law enforcement officials are necessary to ensure effective cyber law enforcement and provide legal protection for the public. 2. Extraterritorial jurisdiction provides Indonesia with the basis for prosecuting cybercrimes committed from abroad, but its application is limited by the need to respect the sovereignty of other countries. The Criminal Code and the Electronic Information and Transactions (ITE) Law are not yet fully adequate to cover all cross-border cybercrimes, primarily due to limited jurisdictional rules, the difficulty of obtaining digital evidence, and the need for international cooperation. The principle of objective territoriality underpins the application of the ITE Law to transnational hate speech, as long as the consequences are felt in Indonesia. However, the unclear boundaries of "legal consequences in Indonesia" and weak international cooperation mechanisms often hinder law enforcement. Therefore, Indonesia needs to align the ITE Law with international law such as the Budapest Convention, strengthen global cooperation, and clarify jurisdictional rules in national law to ensure effective cyber law enforcement.

5. References

Journals:

- Azhar, A. F., & Soponyono, E. (2020). Kebijakan Hukum Pidana dalam Pengaturan dan Penanggulangan Ujaran Kebencian (Hate Speech) di Media Sosial. *Jurnal Pembangunan Hukum Indonesia*, Vol 2, No. 2. <https://ejournal2.undip.ac.id/index.php/jphi/article/view/8470>.
- Fitria, R. (2019). Sinkronisasi Hukum Nasional dengan Hukum Internasional dalam Penegakan Hukum Siber. *Jurnal Hukum dan Pembangunan*, Vol 29, No. 3.
- Rusdianto, & Risnain, M. (2023). Penerapan Prinsip Extraterritorial Jurisdiction Dalam Memerangi Tindak Pidana Siber. *Mataram Journal of International Law*, Vol 1, No. 1. <https://journal.unram.ac.id/index.php/majil/index>.
- Wulan, E. R. (2015). Pertanggung-Jawaban Kejahatan Yang Dilakukan Dalam Layanan Free Wifi Menurut Uu No 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *e-Jurnal THE SPIRIT OF LOW*, Vol 1, No. 1.



<http://repository.narotama.ac.id/1663/15/7.%20Jurnal%20Nasional.pdf>.

Books:

- Hamzah, A. (2008). Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.
- Harahap, M. Y. (2017). Hukum Acara Pidana Indonesia. Jakarta: Sinar Grafika.
- Mulyadi, L. (2020). Kejahatan Teknologi Informasi: Cybercrime dalam Perspektif Hukum Pidana Indonesia. Bandung: Alumni.
- Prasetyo, T. (2017). Politik Hukum Pidana di Indonesia. Yogyakarta: Pustaka Pelajar.
- Suhariyanto, B. (2013). Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya di Indonesia. Jakarta: Rajawali Pers.
- Wiyono, R. (2021). Hukum Pidana di Era Digital. Yogyakarta: Deepublish.

Regulations:

Law Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of Indonesia 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843)

Internet:

- Edhar, H. I. (2024). Kajian Tentang Yurisdiksi Dalam Penerapan UU ITE. AkarBerita.Com. <https://akarberita.com/kajian-tentang-yurisdiksi-dalam-penerapan-uu-ite/>.
- Halim, E. J. (2022). Prinsip Ekstrateritorial dalam UU PDP: Tantangan dan Implikasinya. HukumOnline.Com. <https://www.hukumonline.com/berita/a/prinsip-ekstrateritorial-dalam-uu-pdp--tantangan-dan-implikasinya-lt6390111b768aa/>.