

Law Enforcement Against Perpetrators of Hate Speech Crimes on Social Media Within the Jurisdiction of the Riau Regional Police

Rudi Hidayat⁽¹⁾ M.Musa⁽²⁾ Zulkarnain.S⁽³⁾

^{1,2,3} Universitas Islam Riau

¹rudihidayatpps@student.uir.ac.id, ²musa@law.uir.ac.id, ³zulkarnains@law.uir.ac.id

Article Info

Received: 2026-05-10

Revised: 2026-10-16

Accepted: 2026-10-21

Keywords:

*hate speech; social media;
law enforcement; electronic
evidence;*

Abstract

The growth of social media has expanded the scope of freedom of expression while simultaneously increasing the risk of hate speech spreading potentially leading to hostility, discrimination, and disruptions to social order. This study aims to analyze law enforcement actions against perpetrators of hate speech crimes via social media within the jurisdiction of the Riau Regional Police (Polda Riau), as well as the factors hindering such enforcement. The study employs an empirical juridical (or sociological) method with a descriptive approach. Primary data were obtained through interviews with one Head of the Special Criminal Investigation Unit and two investigators. The data were analyzed qualitatively using Soerjono Soekanto's law enforcement theory and the theory of legal certainty. The analysis reveals that ideal law enforcement involves receiving reports, conducting preliminary inquiries, identifying criminal elements, securing electronic evidence, carrying out formal investigations, and coordinating with relevant parties. Key obstacles include account anonymity, content deletion, difficulties in obtaining digital data, limitations in facilities and technical expertise, and the challenge of distinguishing between freedom of opinion and hate speech. Consequently, the effectiveness of law enforcement is determined not merely by the existence of legal norms, but also by the quality of law enforcement personnel, digital infrastructure, public participation, and legal culture.

I. Introduction

Indonesia is a state governed by the rule of law, utilizing law as an instrument to ensure order, justice, and the protection of citizens' rights. Advances in information technology have transformed patterns of public communication. Social media enables individuals to rapidly convey their opinions to a wide audience. However, this open communication space can also be exploited to disseminate insults, provocations, hostility, discrimination, and hate speech. These issues are further complicated by the fact that digital content can be copied, shared, and disseminated in a very short time.

In the context of Indonesian law, the regulation of hate speech via electronic media cannot be separated from the Electronic Information and Transactions (ITE) Law and its amendments, criminal law provisions, and the hate speech handling policies of the Indonesian National Police. The second amendment, enacted via Law Number 1 of 2024, updated several provisions of the ITE Law, including the penal regime concerning the dissemination of electronic information containing hate or hostility based on specific identities. The primary issue in practice is not merely the absence of legal norms, but rather how those norms are applied in a manner that is precise, proportionate, and capable of being substantiated.

Recent literature indicates that the boundary between freedom of expression and hate speech is a central issue in digital law enforcement. An analysis of Indonesian court rulings reveals that hate speech provisions are open to broad interpretation due to the lack of sufficiently detailed objective thresholds; consequently, considering context, content, dissemination, and the link between the speech and resulting harm becomes crucial (Mathias, 2023). Other research

suggests that classifying hate speech cannot rely solely on specific words or lexical meanings but must also take into account context, intent, and implicature (Puspawati, 2026).

Research relevant to the Riau region also indicates that the issue of hate speech possesses significant local dimensions. A study of a case at the Tembilahan District Court in Indragiri Hilir, for instance, analyzed social media posts containing ill-wishes directed at the president during an election period; it highlighted the importance of semantic, sociolinguistic, and pragmatic analyses in understanding the speech elements subject to legal scrutiny (Surahmat et al., 2025). These findings demonstrate that addressing hate speech in Riau requires consideration of the digital communication context, rather than focusing solely on sentence structure.

Beyond issues of interpretation, electronic evidence constitutes a crucial element. While electronic information and documents hold legal status as evidence, the processes of collection, authentication, integrity preservation, and maintaining the chain of custody still face challenges. Literature on digital evidence in Indonesia highlights that the evidentiary framework suffers from fragmented standards and lacks fully integrated procedures (Santosa & Kamali, 2022; Samudra et al., 2026). Consequently, investigators are required to possess adequate technical skills and an understanding of the relationship between digital facts and the construction of criminal law.

This study focuses on the Riau Regional Police as the research site, as law enforcement regarding hate speech on social media requires an empirical examination of the handling process and the factors that impede it. The planned study population comprises one Head of the Special Criminal Investigation Unit

and two investigators, thereby aiming to obtain direct perspectives from the officers handling the cases.

The novelty of this article lies in its integration of an empirical policing perspective with Soerjono Soekanto's theory of law enforcement factors and the theory of legal certainty; specifically, it examines how issues such as anonymous accounts, electronic evidence, investigator capacity, facilities, and public participation affect the effectiveness of handling hate speech within the jurisdiction of the Riau Regional Police. This study addresses two primary questions: how law enforcement against perpetrators of hate speech via social media is conducted within the Riau Regional Police's jurisdiction, and what factors hinder such enforcement.

2. Research Method

This study employs an empirical or sociological legal research method with a descriptive nature. The research aims to examine the law in practice, specifically the enforcement of laws regarding hate speech on social media. The study is conducted at the Riau Regional Police (Polda Riau), an institution selected for its relevance to the study of information technology based criminal law enforcement. The study population comprises one Head of the Special Criminal Investigation Unit and two investigators, resulting in a total of three respondents. Primary data collection is designed to be carried out through interviews, while secondary data is derived from legislation, books, scholarly articles, and other relevant literature. Analysis is conducted using a qualitative-descriptive approach by evaluating respondents' answers against the research focus and subsequently relating them to theories of law enforcement and legal certainty.

3. Results and Discussion

3.1 Interview Results

The interviews were structured based on the respondents' three respective roles. The first respondent was the Head of the Special Criminal Investigation Unit, while the second and third respondents were investigators. The substance of the responses focused on stages of law enforcement, digital evidence, challenges in identifying perpetrators, and prevention efforts.

Respondent 1, the Head of the Special Criminal Investigation Unit, explained that case handling begins with a report or information from the public, followed by a preliminary inquiry to determine whether the incident shows indications of a criminal offense. If sufficient preliminary evidence exists, the process proceeds to a formal investigation, involving witness questioning, the examination of electronic devices or data, and other investigative actions as required by the case. Based on the interview, investigators must assess the context of a post before concluding that a crime has occurred, as not every statement that offends another party automatically constitutes hate speech.

Respondent 1 also outlined that forms of speech requiring attention include provocation, insults, the incitement of hostility, and content targeting specific groups based on identity. In practice, difficulties arise when perpetrators use false identities or anonymous accounts, delete content, or utilize digital communication platforms where data is stored outside Indonesian jurisdiction. Preventive measures are implemented through public education and appeals for responsible social media use.

Respondent 2, an investigator, emphasized the importance of electronic evidence. Reported content must be documented and traced, including accounts, posts, comments, images, videos, links, and other relevant electronic

communications. Screenshots alone are not always sufficient to build a case; investigators need to link them to data sources, account identities, communication contexts, and other evidence. This aligns with literature identifying authentication and integrity as crucial aspects of electronic evidence (Wiarti, 2024; Wulandari, 2024).

Respondent 2 also noted that the public does not yet fully grasp the limits of freedom of speech. Some social media users believe that any statement falls under the right to freedom of opinion; however, this freedom is constrained when a statement meets the elements of a criminal offense as defined by law. This finding aligns with research on freedom of speech on social media, which emphasizes the need for a balance between freedom of expression and the protection of the legal interests of other individuals or groups (Mathias & Silliman, 2022).

Investigators have also identified five categories of obstacles: legal factors, law enforcement personnel, facilities and infrastructure, the public, and legal culture. From a technical standpoint, technological advancements cause the patterns of perpetrators' actions to shift rapidly. Content deletion can erase parts of the digital footprint, while the use of fake accounts complicates perpetrator identification. Furthermore, when data is held by platform providers based outside Indonesia, investigators face challenges regarding coordination and jurisdiction.

The three interviews reveal a consistent pattern: effective law enforcement requires a combination of legal expertise and technological proficiency. Handling these cases goes beyond merely determining whether language is abusive; it requires an examination of criminal elements, context, the target's identity, intent, distribution, and the relationship between the content and the protected legal interests.

3.2 Law Enforcement Against Hate Speech on Social Media

Law enforcement can be understood as the process of translating legal norms into reality. From Soerjono Soekanto's perspective, the effectiveness of law enforcement is influenced by factors such as the law itself, law enforcement officials, facilities and resources, the public, and culture. This framework is relevant for analyzing hate speech, as digital cases involve the intersection of criminal regulations with rapidly evolving technology.

The process begins with information regarding content suspected of violating the law. Such information may originate from victim reports, public reports, monitoring activities, or findings by authorities. The subsequent stage involves an investigation to ascertain the nature of the incident. In hate speech cases, investigators must avoid approaches based solely on personal dislike of the statement's content; instead, assessments must focus on the specific elements defined in criminal statutes.

An analysis of 27 Indonesian court rulings reveals that the primary issue lies in the absence of a uniform, objective threshold for defining hate speech. Assessments regarding protected groups, dissemination, the content of the speech, and the link between the speech and resulting harm can lead to varying legal interpretations. This situation underscores the need for consistent interpretation to prevent law enforcement from devolving into the criminalization of expressions that should be protected (Mathias, 2023).

The next stage involves the collection and securing of evidence. Digital evidence may encompass electronic information, electronic documents, devices, metadata, communications, and forensic examination results. Recent literature indicates that while Indonesia has normatively recognized electronic evidence,

procedures regarding authentication, preservation, and the chain of custody still require more robust standardization (Aji Putra, 2026; Agatha & Rahaditya, 2026).

Once evidence has been gathered, investigators must establish the connections between the account, the content, the device, and the suspected perpetrator. This stage distinguishes digital cases from conventional ones. An account's identity is not necessarily identical to the identity of the person operating it; therefore, account information must be corroborated by other evidence. In this context, digital forensics serves as a bridge between technical facts and legal constructs.

Law enforcement must also uphold the principle of legal certainty. Legal certainty entails not only the existence of written rules but also their consistent, predictable, and non-discriminatory application. If two substantially similar pieces of content are treated differently without a justifiable legal basis, public confidence in the law may be undermined.

3.3 Analysis of Inhibiting Factors Based on Soerjono Soekanto's Theory

3.3.1 Legal Factors

Legal factors pertain to the quality and clarity of legal norms. Hate speech is multidimensional in nature; consequently, certain acts may overlap with defamation, slander, incitement, discrimination, or other criminal offenses. While amendments to the ITE Law have introduced normative updates, interpreting the context and the boundary between legitimate expression and criminalizable speech still requires caution.

Literature indicates that the primary issue is not necessarily an absence of regulations, but rather the gap between legal provisions and their application. Therefore, internal guidelines, consistency in interpretation, and the rigorous

assessment of criminal elements are crucial. Law enforcement must avoid the excessive use of legal provisions simply because the content in question sparks controversy.

3.3.2 Law Enforcement Factors

Law enforcement personnel are a central factor because digital cases require a combination of competencies in criminal law, procedural law, information technology, and the analysis of electronic evidence. Investigators must understand how to lawfully obtain evidence, maintain data integrity, assess the context of content, and establish a link between digital evidence and the suspect.

Limited competence can lead to two risks. First, it may be difficult to prove cases that actually meet the elements of a criminal offense. Second, cases requiring contextual assessment might be processed too hastily. Therefore, enhancing investigator capacity through training in digital forensics, social media analysis, and an understanding of freedom of expression is essential.

3.3.3 Facilities and Infrastructure Factors

Handling digital evidence requires examination tools, forensic software, secure storage systems, and access to experts. Recent literature emphasizes that the fragmentation of digital forensic standards can affect the authentication and reliability of evidence (Agatha & Rahaditya, 2026). Limited facilities can also prolong the investigation process. The situation becomes increasingly complex when data resides on digital platforms operating across national borders. Investigators require mechanisms for cooperation and procedurally sound data requests. These conditions demonstrate that internal technical capabilities must go hand-in-hand with inter-agency and cross-jurisdictional cooperation

capabilities.

3.3.4 The Role of the Public

The public is not merely the object of law enforcement but also a source of information. Reports from the public can serve as a starting point for uncovering hate speech content. However, reports that are incomplete or based solely on perception can hinder investigators. Therefore, digital legal literacy needs to be improved so that the public can distinguish between criticism, opinion, insults, provocation, and hate speech. Enhancing literacy is also crucial to prevent the public from engaging in vigilantism such as resharing problematic content under the guise of condemning it as such actions can actually amplify the content's impact.

3.3.5 Cultural Factors

Digital communication culture influences patterns of hate speech. Social media fosters communication that is rapid, brief, emotional, and often reactive. Content distribution algorithms can also amplify controversial posts. Research on hate speech dynamics in Indonesia reveals a link between identity, politics, ethnicity, and the tendency to generate expressions of hate (Saputra et al., 2026). Therefore, law enforcement must be accompanied by a preventive approach. Digital ethics education, campaigns promoting responsible social media use, and the strengthening of a culture of dialogue can alleviate the burden on repressive law enforcement measures.

3.4 Legal Certainty and the Protection of Freedom of Expression

Hate speech law enforcement must strike a balance between public protection and freedom of expression. Freedom of opinion is a constitutional right, yet its exercise is not absolute. Restrictions may be imposed by law to protect the rights of

others and legitimate interests. The challenge for law enforcement officials is to ensure that such restrictions are genuinely grounded in criminal elements, rather than merely because an opinion is deemed unpleasant.

Legal certainty in hate speech cases implies that suspects, victims, and the public can understand the grounds for whether or not an act is prosecuted. Research on court rulings reveals variations in the assessment of harm and the elements constituting hate speech. This underscores the importance for officials to construct cases transparently and based on evidence (Mathias, 2023).

In the context of digital evidence, legal certainty also relates to how data is obtained and preserved. Volatile evidence requires procedures that guarantee authenticity. Consequently, digital forensics serves not only to uncover evidence but also to provide a basis for accounting for the acquisition process. Strengthening the chain of custody is a critical requirement within the digital criminal evidentiary system (Aji Putra, 2026).

3.5 Strategies to Enhance the Effectiveness of Law Enforcement

First, the competence of investigators must be continuously enhanced. Training should cover the identification of hate speech, analysis of linguistic context, collection of electronic evidence, fundamentals of digital forensics, and the protection of human rights. Second, digital forensic facilities and laboratories need to be strengthened so that examinations do not constantly rely on external facilities.

Third, more detailed operational procedures are required for the preservation of social media evidence. Every content-securing process must document the source, time, method of acquisition, devices used, and any changes made to the data. Fourth, coordination with relevant platforms and agencies needs to be improved to handle cases involving anonymous accounts or cross-jurisdictional data.

Fifth, preventive efforts must be expanded. Police can collaborate with schools, universities, local governments, digital communities, and civil society organizations to raise legal awareness. Research on hate speech law enforcement in Indonesia also emphasizes the importance of cyber patrols, specialized units, and public reporting services as part of the handling strategy (Situngkir & Istinah, 2021).

Thus, the ideal law enforcement model is not merely repressive. It combines prevention, detection, professional investigation, accountable digital evidence gathering, and public education. Such an approach is better suited to the nature of criminal offenses in the digital space, which are fast-moving and cross-border in scope.

4. Conclusion

Law enforcement against perpetrators of hate speech via social media within the jurisdiction of the Riau Regional Police requires, in principle, a measured, step by step process ranging from the receipt of reports or information, preliminary inquiry, and identification of criminal elements, to the securing and examination of electronic evidence, formal investigation, and subsequent legal proceedings. The effectiveness of law enforcement depends not only on criminal statutes but also on the ability of officers to grasp the context of digital communication and distinguish hate speech from expression that remains legally protected.

Obstacles to enforcement can be analyzed through Soerjono Soekanto's five factors: the law itself, law enforcement officials, facilities and infrastructure, the community, and culture. In digital cases, prominent challenges include anonymous accounts, content deletion, difficulties in data acquisition, the need for digital forensics, limited technical competence, and low digital legal literacy. Consequently,

necessary measures include enhancing investigator capacity, strengthening digital forensic facilities, standardizing evidence management, fostering inter-agency cooperation, and promoting public education.

At the same time, law enforcement must ensure legal certainty and the protection of freedom of expression. Criminal proceedings must be grounded in legal elements and sufficient evidence, rather than merely the controversial nature of an opinion. Through an objective, proportionate, and evidence-based approach, law enforcement regarding hate speech can protect the public while preventing the criminalization of legitimate expression.

References

- Aji Putra, G. R. (2026). Kedudukan bukti digital dalam sistem peradilan pidana Indonesia: Rekonsepsi pengaturan dan penguatan chain of custody di era cyber-enabled crime. *BULETIN ADALAH*, 8(7). <https://doi.org/10.15408/adalah.v8i7.51879>
- Agatha, C., & Rahaditya, R. (2026). Fragmented digital forensic standards in Indonesian criminal evidence. *Indonesian Journal of Law and Economics Review*, 21(2). <https://doi.org/10.21070/ijler.v21i2.1558>
- Arianto, D., Rindiani, A., & Yuliana, S. (2026). Analisis penegakan hukum pidana dalam menangani ujaran kebencian berbasis SARA di platform media sosial. *Legal Standing: Jurnal Ilmu Hukum*, 10(1), 1–17. <https://doi.org/10.24269/lis.v10i1.12589>
- Dhumillah, D. S. R. (2024). The stand of electronic evidence in cyber crime law enforcement in Indonesia. *Journal Eduvest*, 4(9). <https://doi.org/10.59188/eduvest.v4i9.1812>
- Ilham, A. I., Shuhufi, M., & Amin, A. R. M. (2024). Kedudukan alat bukti elektronik dalam pembuktian tindak pidana. *Media Hukum Indonesia*, 2(2).

- Mathias, J. (2023). Hate speech and the harm in Indonesian judicial decisions. *Cogent Social Sciences*, 9. <https://doi.org/10.1080/23311886.2023.2274430>
- Mathias, J., & Silliman, R. B. (2022). Hate speech and the freedom discourse. *Indonesia Media Law Review*, 1(1), 1–22. <https://doi.org/10.15294/imrev.v1i1.21729>
- Musa, A. A., Mandey, M., & Goni, C. J. J. G. (2025). Tinjauan yuridis penegakan hukum terhadap pelaku ujaran kebencian (hate speech) di media sosial dalam perspektif hukum pidana. *Jurnal Tana Mana*, 6(3). <https://doi.org/10.33648/jtm.v6i3.1301>
- Numani, A. N. (2021). Hate speech and hoaxes in social medias: The dark portrait of uncertainty in law enforcement. *Law Research Review Quarterly*, 7(1). <https://doi.org/10.15294/lrrq.v7i1.43166>
- Putra, V. G. R., Febriyatko, A., & Busri, H. (2024). Hate speech in Instagram comments of DPR RI: A forensic linguistic analysis. *KEMBARA*, 10(1). <https://doi.org/10.22219/kembara.v10i1.28128>
- Puspawati, A. (2026). Hate speech on social media: An integrated analysis of forensic linguistics and Indonesian criminal law. *Jurnal Ilmu Sosial dan Humaniora*, 4(3), 997–1015. <https://doi.org/10.58540/isihumor.v4i3.2127>
- Roziqin, M. C., Cornelis, V. I., & Taufik, M. (2025). Penegakan hukum ujaran kebencian yang mengandung diskriminasi ras dan etnis melalui sosial media. *Journal of Sharia Economics*, 4(2). <https://doi.org/10.35896/jse.v4i2.1144>
- Samudra, A. H., Basu, S., & Saenz Perez, C. (2026). Digital challenge, analogue mind-set: Assessing Indonesia's electronic criminal evidence framework. *Journal of Indonesian Legal Studies*, 11(1). <https://doi.org/10.15294/jils.v11i1.35378>
- Santosa, D. G. G., & Kamali, K. M. I. (2022). Acquisition and presentation of digital evidence in criminal trial in Indonesia. *Jurnal Hukum dan Peradilan*, 11(2), 195–218. <https://doi.org/10.25216/jhp.11.2.2022.195-218>

- Saputra, G. B. R., Abdul Azis Lamadjido, N., Wulandari, D. R., Sari, D. F. K., & Kudratullah. (2026). Examining hate speech and social media in Indonesia: A systematic literature review. *Jurnal Audience*, 9(2). <https://doi.org/10.33633/ja.v9i2.17621>
- Setiadi, A. S. (2026). Navigating freedom of speech in social media: Reconstruction of the crime of defamation in the era of the New Criminal Code. *Jurnal Hukum dan Peradilan*, 15(2), 233–260. <https://doi.org/10.25216/jhp.15.2.2026.233-260>
- Situngkir, F. V., & Istinah, S. R. D. (2021). The enforcement of criminal laws of hate speech in social media. *Law Development Journal*, 2(4), 542–548. <https://doi.org/10.30659/ldj.2.4.542-548>
- Surahmat, S., Arimi, S., Susilowati, N. E., & Imamah, F. M. (2025). From invocation to indictment: Analyzing hate speech elements in a social media prayer. *Rainbow*, 14(1). <https://doi.org/10.15294/rainbow.v14i1.23626>
- Wiarti, J. (2024). Legality of electronic evidence in cyber crime cases. *Ahmad Dahlan Indonesian Law Journal*, 1(2), 11–19. <https://doi.org/10.12928/adil.v1i1.572>
- Wulandari, L. (2024). Kekuatan pembuktian alat bukti elektronik dalam perkara pidana di Indonesia. *RETORIKA: Journal of Law, Social, and Humanities*, 3(1), 33–46. <https://doi.org/10.69503/retorika.v3i1.1572>
- Sabila, S. P., & Siswanto, A. H. (2026). Legal review of criminal hate speech related to blasphemy through social media based on the ITE Law. *International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy*, 1(2). <https://doi.org/10.56861/nalarnagara.v1i2.270>
- Satriani, N. K. (2026). Law enforcement against cybercrime in Indonesia: Analysis of regulatory effectiveness and digital forensic challenges. *Journal of Legal Studies Judex Praetor*, 2(1), 20–29. <https://doi.org/10.35671/judex.v2i1.175>

- Sukawati, T. G. P. M., Dewi, C. I. D. L., & Dewi, K. A. P. (2025). Effectiveness of law enforcement against hate speech and the spread of fake news on social media based on Indonesian positive law. *VERITAS*, 11(2). <https://doi.org/10.34005/veritas.v11i2.4810>
- Alim, N. (2025). Tinjauan hukum pidana terhadap pelaku ujaran kebencian (hate speech) dalam masa kampanye di Indonesia. *Datuk Sulaiman Law Review*, 6(1), 54–61. <https://doi.org/10.24256/dalrev.v6i1.6591>
- Marsanabila, A., Waluyo, D., Pradesti, A., Kusuma, R. P., & Hikmat. (2023). Analisis yuridis tindak pidana ujaran kebencian (hate speech) dalam media. *Lex Veritatis*, 2(2), 110–121. <https://doi.org/10.33592/jlv.v2i02.3921>
- Permana, I. M. A. S., Dewi, A. A. S. L., & Karma, N. M. S. (2022). Tinjauan yuridis pertanggungjawaban pidana terhadap ujaran kebencian (hate speech) di media sosial. *Jurnal Konstruksi Hukum*, 3(1), 130–134. <https://doi.org/10.22225/jkh.3.1.4247.130-134>
- Saputra, R., Setiodjati, J. P., & Barkhuizen, J. (2023). Under-legislation in electronic trials and renewing criminal law enforcement in Indonesia. *Journal of Indonesian Legal Studies*, 8(1), 243–288. <https://doi.org/10.15294/jils.v8i1.67632>
- Sumardiana, B., Pujiyono, P., Cahyaningtyas, I., & Wulandari, C. (2024). Evaluation of electronic evidence in criminal justice in the era of advanced artificial intelligence technology. *Indonesian Journal of Criminal Law Studies*, 9(2), 309–332. <https://doi.org/10.15294/ijcls.v9i2.36634>