Law Enforcement Against Criminal Acts of Intimidation Through Social Media

Ahmad Irham Thaji, Sumarno, Rahmayanti

Abstract

Threats through social media have developed into a cybercrime phenomenon that has a serious psychological impact on victims while presenting complex challenges for Indonesia's criminal law enforcement system. This study aims to analyze two main issues: first, how the normative construction of the crime of intimidation in Indonesian criminal law regulates acts committed through social media; and second, how law enforcement is carried out in practice and the structural obstacles faced. The research uses normative legal methods with a statutory and conceptual approach, sourced from primary legal materials in the form of laws and regulations, especially Law Number 1 of 2023 concerning the new Criminal Code, the ITE Law and its amendments, and selected jurisprudence, as well as secondary legal materials in the form of up-to-date academic literature. The results of the study show that Indonesia's normative framework contains layers of regulations that overlap between the threat offenses in the Criminal Code and Article 29 of the ITE Law, resulting in uncertainty in determining the basis for appropriate prosecution. Meanwhile, law enforcement faces multiple obstacles ranging from the complexity of forensic digital, the anonymity of perpetrators, limited coordination with foreign digital platforms, to the disparity of court decisions that reflect the absence of uniform criminal guidelines. This research emphasizes the urgency of regulatory reform that clearly separates conventional threats from digital threats, accompanied by measurable law enforcement guidelines and more substantial victim protection.

Keywords: *criminal intimidation, social media, criminal law enforcement, ITE Law, cybercrime*

Ahmad Irham Thaji
[1] Master of Laws, Panca Budi University, Indonesia
E-mail: ahmadirhamthaji123@gmail.com

Sumarno, Rahmayanti
[2,3] Master of Laws, Panca Budi University, Indonesia
Email: sumarno@dosen.pancabudi.ac.id, rahmayanti@dosen.pancabudi.ac.id.
3rd International Conference Epicentrum of Economic Global Framework (ICEEGLOF)
Theme: Cross-Sector and Cross-Disciplinary Strategies for Achieving the SDGS
https://proceeding.pancabudi.ac.id/index.php/ICEEGLOF

Introduction

The transformation of human communication that has taken place in the last two decades has brought about a fundamental shift in the way crimes are committed. Social media, originally designed as an infrastructure for social interaction and information exchange, is now often a medium used to commit various criminal acts, including threats [1]. This phenomenon is not just a shift in mode from the physical world to the digital space, but presents a new dimension that is qualitatively different: threats can be spread instantly to a wide audience, perpetrators can operate behind relatively easy anonymity to build, and the psychological impact on victims often goes far beyond the threats conveyed directly.

Data from the Cyber Crime Directorate of the National Police Criminal Investigation Agency shows an increasing trend of reports related to cybercrime, including online threats and intimidation, in recent years. This increase cannot be separated from the acceleration of internet penetration in Indonesia, which by 2024 will reach more than 221 million users, making Indonesia one of the countries with the largest population of social media users in the world [2].

From a criminal law perspective, threats through social media present normative issues that are not simple. Indonesia has several legal instruments that can simultaneously be applied to this act: the threat provisions in the old Criminal Code (KUHP) inherited from the colonial Wetboek van Strafrecht, similar provisions in Law Number 1 of 2023 concerning the new Criminal Code [3], and Article 29 of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) as amended by Law Number 1 of 2024 [4]. This regulatory pluralism, instead of providing more comprehensive protection, often creates legal uncertainty in the practice of prosecution and punishment.

A review of the existing academic literature shows that there is a significant research gap. Most legal studies on cybercrime in Indonesia focus on hate speech, the spread of fake news (disinformation), digital defamation, and privacy violations [5]. Meanwhile, threats through social media as a crime that have its own characteristics and dynamics have not received adequate and systematic academic attention. Existing studies generally discuss threats in a broader context, without delving into specific issues regarding the construction of criminal elements in digital contexts, the challenges of proof based on electronic evidence, and disparities in the application of the law at the judicial level.

Based on these gaps, this research is formulated to answer two main questions. First, how does the normative construction of criminal acts of intimidation in Indonesian criminal law accommodate acts committed through social media? Second, how is law enforcement against criminal acts of intimidation through social media carried out in practice, and what structural barriers are faced? The answers to these two questions are expected to provide academic contributions as well as policy recommendations needed to strengthen the criminal law enforcement system in dealing with cybercrime in Indonesia.

Literature Review

2.1 Conceptual Framework of Threat Delik

The delusion of threats in Indonesian criminal law is rooted in the provisions of extortion and threats in the Criminal Code, especially Article 368 and Article 369, the formulation and elements of which are outlined in the article-by-article commentary on the Criminal Code [6]. These provisions stand on broader criminal law principles, such as criminal liability and the element of error (mens rea), which are discussed in the basic criminal law literature [7]. This delik protects a person's psychological freedom and sense of security from pressure exerted through threats.

When several norms can be applied to a single act, the principle of lex specialis derogat legi generali becomes a reference for determining the norm that takes precedence. Theoretically, the special norms in the ITE Law override the general norms in the Criminal

Code. For technology-based crimes, the comparative study of cyber law provides a perspective on how various legal systems regulate acts in the digital space [8].

2.2 Previous Research on Threats through Social Media

Research that specifically raises threats through social media is generally applied. Andrian et al. examined law enforcement against perpetrators of threats with violence through social media [9]. Putri et al. examined the causes of threats of violence and murder through social media and their law enforcement, referring to Article 335 paragraph (1) and Article 369 paragraph (1) of the Criminal Code and Article 45B OF THE ITE LAW [10]. Maulana et al. discussed legal protection for victims of threats in debt collection through social media. They concluded that protection can be provided through the Criminal Code and the ITE Law, that such threats can be qualified as cybercrime if they cause fear or harm to the victim, and that strict law enforcement and public legal awareness play an important role [11]. The three studies focused on specific forms of threats, such as threats of violence, murder, and debt collection.

2.3 Research Position

Based on the literature reviewed, studies on threats through social media tend to focus on the application of the law to certain forms of threats or on victim protection in certain contexts. There has not been a study that has integrated the normative construction of threats in the digital space, the overlap between the Criminal Code and Article 29 of the ITE Law, as well as the structural obstacles to its enforcement, including digital forensic, coordination with foreign platforms, and disparity in verdicts. This study fills this gap by analyzing the two dimensions in one framework.

Research Methodology

This study uses a normative legal research method, which is research that focuses on positive legal norms, legal principles, legal concepts, and relevant doctrines [12]. The choice of this method is based on the character of the problem formulated, namely normative problems regarding the construction of regulations and applied problems regarding law enforcement, both of which require an analysis of legal norms as a starting point.

The approach used includes two types [13]. First, the statute approach, which is carried out by examining relevant laws and regulations in a systematic and hierarchical manner. The legal instruments studied include the old Criminal Code, Law Number 1 of 2023 concerning the new Criminal Code, Law Number 11 of 2008 concerning ITE as amended by Law Number 1 of 2024, as well as related implementing regulations. Second, the conceptual approach, which is used to analyze fundamental concepts such as mens rea in the crime of threats, standards for proving electronic evidence, the principle of lex specialis derogat legi generali in the context of norm competition, and victim protection theory in modern criminal law.

The legal materials used consist of three layers. Primary legal materials include the aforementioned laws and regulations as well as court decisions that are purposively selected based on their relevance to the research issue. Secondary legal materials include scientific journal articles published between 2021 and 2025 obtained from Scopus, DOAJ, and Google Scholar databases, as well as relevant criminal law and cyber law textbooks. Tertiary legal materials include legal dictionaries and legislative glossaries. All legal materials are analyzed using qualitative analysis methods with grammatical, systematic, and teleological interpretation techniques, which are then synthesized into coherent scientific arguments.

Results

4.1 Normative Construction of Criminal Acts of Intimidation in Indonesian Criminal Law

Understanding the normative construction of the crime of threat in Indonesian criminal law requires a reading that is not only horizontal to a single legal instrument, but also vertical and comparative between the various layers of regulation that are simultaneously in effect or are in the process of transition. This complexity is not just a technical issue of legislation, but reflects the fundamental tension between the legacy of the continental criminal law tradition that is general in nature and the regulatory needs that are increasingly specific to the phenomenon of technology-based crime [14].

In the Criminal Code that was in force until before Law Number 1 of 2023 was fully enacted, the offense of threats is regulated, mainly in Article 368 and Article 369. Article 368 of the Criminal Code regulates extortion with violence or threats of violence, while Article 369 of the Criminal Code regulates threats with the intention of benefiting oneself or others unlawfully. The difference between the two lies in the element of economic gain: Article 368 requires the intention to force the surrender of objects, while Article 369 regulates threats with the intention of forcing people to do, not do, or allow something that is not always directly economically charged [15]. These two articles are formulated in the context of physical interaction between people, so they do not explicitly anticipate digital media as a means of conveying threats.

Law Number 1 of 2023 on the new Criminal Code is a significant step forward, although not without its weaknesses. The new Criminal Code retains the construction of the threat offense in a substance that is not much different from its predecessor, but refines the formulation with a more systematic approach. The articles regulating threats are placed in a more coherent context with the overall architecture of the new Criminal Code. However, an academic criticism that deserves attention is that the new Criminal Code still does not explicitly formulate threats through electronic media or social media as a crime that has its own characteristics. Digital threats are still implicitly expected to be covered through an extensive interpretation of general provisions, which in practice results in inconsistencies [16].

Article 29 of the ITE Law is present as a special norm that directly responds to information technology-based crimes. The article prohibits everyone from intentionally and without the right to send electronic information and/or electronic documents containing threats of violence or intimidation aimed at a person. On the surface, this provision seems to be on point. However, a closer study reveals some serious normative problems. First, the phrase "personally directed scares" creates an ambiguity of interpretation: does a threat posted publicly on social media timelines and directed at a particular person still meet the "personal" element, or should it be sent via direct message? This debate over interpretation is not only theoretical, but has led to a real difference of opinion between law enforcement officials and judges.

Second, the ITE Law does not adequately define what constitutes a "threat of violence" in the digital context. An important question that arises is: does a threat that is not accompanied by a concrete indication of the perpetrator's ability to carry it out still meet the element of delicacy? In comparative criminal law, some jurisdictions such as Germany through Strafgesetzbuch §241 require that the threat must be "serious" (ernst gemeint) and have the ability to instill a reasonable fear in a rational victim. This kind of standard has not been explicitly articulated in Indonesia's ITE Law, leaving a wide interpretive gap for law enforcement.

Third, the issue of lex specialis between the Criminal Code and the ITE Law presents its own complications. The principle of lex specialis derogat legi generali theoretically requires that the ITE Law, as a special norm, take precedence in the prosecution of threats through digital media. However, practice shows that public prosecutors often use both instruments simultaneously in a single indictment, either alternatively or cumulatively, which raises

questions about the legal certainty and proportionality of the punishment [17]. This practice of layered indictments reflects the absence of clear guidelines on when the Criminal Code should be used and when the ITE Law should be the sole basis for prosecution.

The amendment to the ITE Law through Law Number 1 of 2024 does bring some adjustments, but it does not fundamentally solve the above normative problems. The changes focus more on adjusting terminology and adding provisions related to digital content in general, without providing a more precise operational definition of the elements of digital threat crimes [18].

One normative dimension that often goes unnoticed is the relationship between the crime of intimidation and the protection of victims' rights. The Criminal Code and the ITE Law basically formulate the crime of intimidation as a crime that attacks the legal interests of individuals in the form of psychological freedom and a sense of security. However, both do not adequately integrate proactive victim protection provisions, such as the emergency protection order mechanism that can be immediately granted by the court even before the case is decided [19].

A comparative analysis of the regulations of other countries provides a useful perspective. Singapore through the Protection from Harassment Act (POHA) has developed a legal framework that specifically regulates harassment, intimidation, and threats through digital media with more responsive victim protection mechanisms, including the possibility of expeditionary application for protection orders [20]. Malaysia through the amendments of the Communications and Multimedia Act 1998 has also strengthened provisions on online threatening content. The experience of these two neighboring countries shows that regulatory reforms that focus on the specific characteristics of digital crime are more effective than approaches that only marginally modify conventional norms. Indonesia has not moved towards this kind of approach consistently.

From the normative construction described above, several analytical conclusions can be drawn. Indonesia's criminal law system faces what can be termed as a "layered regulatory paradox": on the one hand there are many legal instruments that formally cover digital threats, but on the other hand there is no single instrument that formulates them with sufficient precision for the needs of law enforcement in the age of social media.

4.2 Law Enforcement against Criminal Acts of Threats Through Social Media: Between Norms and Practices

The distance between written norms and law enforcement practices is one of the classic issues in legal science, but in the context of cybercrime, this distance has a deeper and more complex dimension. Law enforcement against criminal acts of intimidation through social media not only faces the juridical challenges discussed in the previous subsection, but also faces technical, institutional, and structural obstacles that interact with each other to form a non-optimal law enforcement ecosystem [21].

At the institutional level, the National Police has established the Directorate of Cyber Crime (Dittipidsiber) of the Criminal Investigation Branch as a special unit that handles information technology-based crimes. The existence of this unit is an important institutional step, considering that cybercrime investigations require technical expertise that is fundamentally different from conventional crime investigations. However, the distribution of digital investigative capacity at the police and police levels is still very uneven. Public reports about threats through social media submitted to police units in the regions are often not handled adequately due to the limited number of human resources who have digital forensic expertise [22].

The challenge of digital forensics is the most significant technical obstacle in the enforcement of the law of threats through social media. Proving this case requires the acquisition, security, analysis, and presentation of electronic evidence that meets the standards

of authenticity and integrity required by procedural law. In practice, problems arise at every stage. At the acquisition stage, investigators must immediately secure threatening content before the perpetrator deletes it, considering that digital content can be removed in seconds.

At the analysis stage, the issue of anonymity and pseudonymity of perpetrators is an obstacle that is often difficult to overcome. Social media allows users to create accounts with fake identities, use IP addresses disguised through Virtual Private Networks (VPNs), or operate through various layers of technical anonymization. Identifying the real perpetrators behind anonymous accounts requires the cooperation of digital platforms to disclose user data [23].

Coordination between Indonesian law enforcement officials and foreign social media platforms is one of the most critical weak points in the law enforcement chain. Most of the social media platforms that are predominantly used in Indonesia, such as Meta (Facebook and Instagram), X (Twitter), and TikTok, have legal status outside of Indonesian jurisdiction. Requests for user data from these platforms must go through the Mutual Legal Assistance (MLA) mechanism or a special channel provided by the platform through the legal request process. In practice, the MLA process takes a very long time, often months to exceed the deadline for investigations.

The issue of cross-border jurisdiction is even more complex when the perpetrator and the victim are in different countries. Indonesian criminal law in principle applies based on the territorial principle and the principle of active-passive personality as stipulated in the Criminal Code, but the application of these principles in the cyber context faces real practical obstacles due to the absence of comprehensive bilateral agreements and effective extradition mechanisms for minor cybercrimes such as individual threats. As a result, perpetrators operating from abroad are practically difficult to reach by Indonesian criminal law.

In the judicial system, the disparity in court decisions in cases of threats through social media is a symptom that reflects deeper normative issues. An analysis of a number of court decisions in the period 2021 to 2024 reveals quite striking differences in terms of: the choice of legal basis between the Criminal Code and the ITE Law, the interpretation of the "deliberate" element in digital threat offenses, and the amount of sanctions imposed for cases with substantially similar facts. For example, threats through short messages on the WhatsApp application have been decided by various courts using different legal bases: some use Article 29 of the ITE Law, others use Article 368 or 369 of the Criminal Code, and some use layered indictments of both instruments.

This disparity does not merely reflect the freedom of judges to interpret the law, but is a systemic symptom of the absence of sentencing guidelines specifically designed for cybercrime. The Supreme Court has not issued a Supreme Court Regulation (Perma) or Circular Letter (SEMA) that specifically provides guidance for judges in deciding cases of digital crimes, including threats through social media.

From the perspective of criminal theory, this kind of disparity has the potential to weaken the effect of general deterrence, which should be one of the criminal functions in organized crime and opportunistic crimes such as digital threats.

The victim protection dimension in law enforcement practice also reveals structural weaknesses that deserve serious attention. Victims of threats through social media face a disproportionate burden in the legal process. The Witness and Victim Protection Agency (LPSK) has a mandate to provide protection, but access mechanisms for victims of cybercrime, including digital threats, have not been adequately standardized and socialized [24].

One aspect that is often overlooked in academic discourse on digital threat law enforcement is the gender dimension. Criminological research shows that women are significantly more likely to be victims of online threats and harassment than men, with threat patterns that are often sexually charged or gender-based. However, Indonesian criminal law does not integrate a gender perspective into the construction of digital threat offenses, nor does

it provide explicit sanctions for gender-based threats [25]. This is a normative gap as well as a mutually reinforcing law enforcement loophole.

From the overall analysis of law enforcement practices, four structural obstacles can be identified that interact with each other to form a system that is not optimal. First, technical capacity obstacles that are asymmetrical between the central and regional governments in terms of forensic digital mastery. Second, coordination obstacles between law enforcement officials and foreign digital platforms operating under different jurisdictions. Third, normative obstacles in the form of the absence of standardized law enforcement guidelines for cybercrime. Fourth, institutional obstacles in the form of institutional response fragmentation that have not been effectively integrated.

Conclusion

This research has analyzed two main dimensions of law enforcement issues against the crime of threats through social media in the Indonesian criminal law system. From a normative perspective, the existing regulatory framework contains a multi-layered regulatory paradox: formally there is legal coverage through the Criminal Code and the ITE Law, but substantively there is no single instrument that formulates digital threats with adequate precision. The ambiguity of interpretation of Article 29 of the ITE Law, the absence of a measurable "serious threat" standard, and the unclear application of the lex specialis principle between the Criminal Code and the ITE Law are normative weaknesses that directly affect the quality of law enforcement.

From a practical perspective, law enforcement faces four mutually reinforcing structural barriers: asymmetry of technical capacity between central and regional governments, coordination constraints with foreign digital platforms, the absence of standardized penal guidelines, and fragmentation of institutional responses. The most concrete manifestation of these obstacles is the disparity in court rulings that point to inconsistent application of the law, as well as weak protection of victims during legal proceedings.

Based on these findings, this study recommends three urgent reform steps. First, legislative reform that expressly separates conventional threat offenses and digital threats, by introducing a precise operational definition of the elements of digital threat offenses, including measurable threat seriousness standards. Second, the issuance of criminal guidelines by the Supreme Court that specifically regulates cybercrime cases, including digital threats, in order to reduce disparities in verdicts and strengthen the general prevention function of criminal law. Third, strengthening coordination mechanisms between law enforcement officials and digital platforms through more comprehensive bilateral agreements and more responsive legal request mechanisms, accompanied by equitable distribution of digital forensic capacity to the police and police levels.

References

[1] N. Syaharani, R. Rahmayanti, C. Nurdiana, D. D. Saputra, and R. N. F. Harahap, "Perlindungan hukum bagi remaja perempuan dari kekerasan seksual via media sosial," Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, vol. 5, no. 2, pp. 1036–1047, 2025.

[2] Asosiasi Penyelenggara Jasa Internet Indonesia, Laporan Penetrasi Internet Indonesia 2024. Jakarta, Indonesia: APJII, 2024.

[3] Republik Indonesia, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, 2023.

[4] Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024, 2024.

[5] C. Nasution, "Kajian hukum model literasi media dalam menganalisa informasi berita palsu (hoax) pada media sosial," Jurnal Hukum Responsif, vol. 7, no. 2, pp. 157–170, 2019.
[6] R. Soesilo, Kitab Undang-Undang Hukum Pidana (KUHP) serta Komentar-Komentarnya Lengkap Pasal demi Pasal. Bogor, Indonesia: Politeia, 2020.
[7] M. Ali, Dasar-Dasar Hukum Pidana. Jakarta, Indonesia: Sinar Grafika, 2022.
[8] R. Arifin and F. Maulana, Hukum Siber di Indonesia: Perspektif Komparatif. Yogyakarta, Indonesia: Pustaka Pelajar, 2023.
[9] K. Andrian, I. P. Hapsari, and D. J. Wardana, "Penegakan hukum terhadap pelaku tindak pidana pengancaman dengan kekerasan melalui media sosial," Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-Undangan dan Pranata Sosial, vol. 7, no. 1, pp. 268–289, 2022.
[10] P. D. P. Putri, I. N. G. Sugiartha, and D. G. Sudibya, "Penegakan hukum terhadap pelaku tindak pidana pengancaman kekerasan dan pembunuhan melalui media sosial," Jurnal Preferensi Hukum, vol. 3, no. 1, pp. 208–212, 2022.
[11] M. I. A. Maulana, N. P. R. Yuliartini, and D. G. S. Mangku, "Perlindungan hukum terhadap korban tindak pidana pengancaman pembayaran utang melalui media sosial sebagai bentuk kejahatan cybercrime," Al-Zayn: Jurnal Ilmu Sosial & Hukum, vol. 4, no. 2, pp. 6282–6293, 2026.
[12] Sumarno, "Metode penelitian hukum normatif dan empiris sebagai strategi penguatan perspektif kajian ilmu hukum," Notary Law Journal, vol. 4, no. 3, pp. 114–128, 2025.
[13] P. M. Marzuki, Penelitian Hukum, edisi revisi. Jakarta, Indonesia: Kencana Prenada Media, 2021.
[14] Budiyanto, Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia. Sada Kurnia Pustaka, 2025.
[15] A. R. H. Hasibuan, I. U. Tanjung, and K. P. Q. B. Panjaitan, Pidana dalam Ulasan Produk di Media Sosial. Serasi Media Teknologi, 2024.
[16] D. M. Rolando, H. H. Aulia, and M. T. Andini, "Transformasi digital dan ancaman cybercrime," Siyasah, vol. 3, no. 1, pp. 68–84, 2023.
[17] L. I. C. Dharani, S. Idayanti, and K. Rahayu, Perlindungan Hukum terhadap Tindakan Phishing di Media Sosial. Penerbit NEM, 2024.
[18] E. A. Budiman, "Literasi hukum digital di tingkat masyarakat," Transformasi Hukum, p. 47, 2025.
[19] B. Waluyo, Viktimologi: Perlindungan Korban dan Saksi. Sinar Grafika, 2022.
[20] S. Yulianingsih, R. K. Putra, and T. Christiana, "Aspek hukum penanganan kekerasan berbasis gender di ruang digital: Studi perbandingan antara Indonesia dan negara-negara di ASEAN," Jaksa: Jurnal Kajian Ilmu Hukum dan Politik, vol. 2, no. 4, pp. 19–30, 2024.
[21] S. T. Cahyono, W. Erni, and T. Hidayat, "Rekonstruksi hukum pidana terhadap kejahatan siber (cyber crime) dalam sistem peradilan pidana Indonesia," Dame Journal of Law, vol. 1, no. 1, pp. 111–133, 2025.
[22] G. B. A. Bagaskara, "Tindak pidana pengancaman melalui media sosial: Tinjauan hukum pidana terhadap penanganan oleh penyidik Polres Tomohon," Menulis: Jurnal Penelitian Nusantara, vol. 1, no. 10, pp. 297–308, 2025.
[23] M. Nasrullah and R. Ramadhan, Dasar-Dasar Keamanan Informasi dan Siber: Teori dan Praktik. Deepublish, 2025.
[24] A. M. Rusdi, "Lembaga Perlindungan Saksi dan Korban sebagai garda terdepan melindungi saksi dan korban dalam menjamin keamanan dan keadilan," Constitutum: Jurnal Ilmiah Hukum, vol. 3, no. 2, pp. 40–52, 2025.
[25] S. Arifin, A. Mudatsir, and A. D. Anam, "Tindak pidana pemerasan seksual berbasis gender siber melalui elektronik dalam sistem hukum pidana di Indonesia," An-Nawazil: Jurnal Hukum dan Syariah Kontemporer, vol. 6, no. 1, pp. 69–90, 2024.