JURNAL HUKUM SEHASEN
p-ISSN : 2528-5025
e-ISSN : 2746-6485

Legal Policy On The Criminal Acts Of Extortion And Threast Via Social Media

Kebijakan Hukum Terhadap Tindak Pidana Pemerasan Dan Pengancaman Melalui Media Sosial

Andini Puspita Sari [1]; Muhammad Ruhly Kesuma Dinata [2]; Noveka Wati [3]
[1,2,3] Universitas Muhammadiyah Kotabumi
Email: [1] andinipuspitasari751@gmail.com ;[2] muhammadruhlykesumadinata@gmail.com ;[3] novekawati@umko.ac.id

ARTICLE HISTORY
Received [17 Februari 2025]
Revised [19 Maret 2025]
Accepted [24 Maret 2025]

KEYWORDS
ITE Law, Extortion and Threats, Social Media.

ABSTRAK

Kebijakan hukum mengenai tindakan pemerasan dan pengancaman melalui media sosial semakin menjadi fokus utama seiring meningkatnya jumlah kejahatan siber. Media sosial, yang merupakan alat komunikasi yang mudah diakses, seringkali disalahgunakan untuk melakukan tindakan kriminal yang merugikan pihak korban, baik dari segi materiil maupun immateriil. Penelitian ini bertujuan untuk mengkaji kebijakan hukum mengenai tindakan pemerasan dan pengancaman yang terjadi di media sosial di Indonesia. Metode yang digunakan dalam penelitian ini adalah yuridis normatif, yang berfokus pada peraturan perundang-undangan serta sumber hukum sekunder yang diperoleh dari buku dan jurnal hukum. Hasil penelitian menunjukkan bahwa meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah menyusun ketentuan yang jelas mengenai tindakan pemerasan dan ancaman di media sosial, masih terdapat celah dalam penerapan serta penegakan hukum yang efisien. Oleh karena itu, dianjurkan untuk memperkuat regulasi, meningkatkan pemahaman digital di masyarakat, dan memberikan pelatihan kepada penegak hukum agar lebih efektif dalam mengidentifikasi dan menangani kasus pemerasan serta pengancaman di dunia maya.

ABSTRACT

Legal policies regarding extortion and threats through social media are increasingly in primary focus as the number of cybercrimes increases. Social media, which is an easily accessible communication tool, is often misused to commit criminal acts that harm the victim, both in terms of material and immaterial. This study aims to examine legal policies regarding extortion and threats that occur on social media in Indonesia. The method used in this study is normative juridical, which focuses on laws and regulations as well as secondary legal sources obtained from legal books and journals. The results of the study show that although the Electronic Information and Transaction Law (UU ITE) has drafted clear provisions regarding extortion and threat on social media, there are still gaps in the efficient implementation and enforcement of the law. Therefore, it is recommended to strengthen regulations, increase digital understanding in society, and provide training to law enforcement to be more effective in identifying and handling cases of extortion and threats in cyberspace.

INTRODUCTION

The developments of information and technology in the era of globalization has made very rapid progress. Humans continue to innovate to develop and perfect various types of technology as tools that can support various aspects of daily life (Durham, 2022). The rapid developments of information technology has led to changes in the patterns of human activity and life, which in turn has a direct impact on the emergence of new types of legal acts and events (Asmadi, 2020). The developments of Information and Communication Technology has indeed made it easier for humans to carry out their daily activities. However, as it develops, the presence of technology can also tempt parties who have malicious intentions or want to abuse it. Therefore, technology can be considered a criminogenic factor, which is a factor that encourages the emergence of a person's intention to commit evil deeds or facilitate the execution of crimes (Idris & Supandi, 2024).

There are many cases of crimes committed by irresponsible people for their personal satisfaction in committing criminal acts. Technology is often considered a criminogenic factor, which is a factor that can trigger the onset of a person's intention to do evil or make it easier for someone to commit crimes, such as extortion and threats. Extortion and threats are forms of crime that in practice have evolved along with the advancement of information technology (Ningrum, 2020).

Some of the reasons why a person commits a criminal act of intimidation are due to individual internal factors that play an important role in the occurrence of threats, especially the psychological state of the individual, namely uncontrolled emotional power due to a stressful situation in the family environment and also a sense of disappointment, sentiment and encouragement along with weak faith. Economic factors are also one of the important issues in human activities, the economic pressure that squeezes and the increasing human needs that must be met so that demanding high expenses are often the reason for someone to commit these criminal acts.

With the developments of information technology, it can give rise to new problems that have a relationship with the crime of extortion and online threats (Udayana et al., 2022). Although the ITE Law has provided regulations on this, it is increasingly happening. The emergence of legal problems that contain elements of extortion and threats through social media is a type of extortion in which the perpetrator threatens to spread personal content, such as photos or videos, if the victim does not provide money or certain items (Kadir Ainun Jariyah, Pawennei Mulyanti, 2024).

Another term for social media crime is Cybercrime. Cybercrime or cybercrime is a criminal act committed by utilizing information technology or computer devices, internet networks, and other digital systems. These crimes can be in the form of various illegal activities such as hacking, theft of personal data, online fraud, spread of viruses, as well as crimes related to the misuse of technology to harm individuals, organizations, or countries. Other terms that are also applied are Information Technology Law (*Information Technology Law), Cyber Law and Virtual Law*. These terms were born by paying attention to internet activities and the use of virtual-based information technology, for example in the criminal act of extortion and threats (Matheus, 2021).

LITERATURE RIVIEW

The theoretical basis in research on legal policy against the crime of extortion and threats through social media needs to be based on several basic legal concepts as well as theories relevant to aspects of criminal law, cyber law, and legal policy. Some theoretical foundations that can be used to study this topic include:

1. Criminal Law Theory. Criminal law theory is the main basis for analyzing criminal acts, including extortion and threats. Criminal law serves to regulate behavior that is considered detrimental to society and provide sanctions for criminals. Extortion and threats through social media are included in the category of criminal acts that require clear law enforcement to provide protection to victims.
2. Cyber Law Theory. Cyber law refers to the laws that govern the use of information and communication technology, including social media. In this context, cyber legal theory is needed to understand how social media can be misused to commit criminal acts and how legal policies should be adapted to the developments of information technology.
3. Legal Policy Theory. Legal policy is concerned with the formation, implementation, and evaluation of existing policies in the legal system to achieve certain goals, such as justice and legal certainty. In the context of extortion and threats through social media, legal policies must include prevention, strict law enforcement, and protection of victims.

METHODS

This research uses a normative juridical research method, which is research conducted with a literature study approach or document study, which aims to analyze the rules, norms, and rules related to the problem to be discussed. This method focuses more on the study of existing legal texts without using field data or empirical experiments. The data collection method used in this study is to use secondary legal materials that include various sources that have existed before and are relevant to the research topic. That is, to study relevant legal texts, such as laws, regulations, legal textbooks, and scientific articles.

RESULTS AND DISCUSSION

Definition And Concept Of Extortion And Threats Through Social Media

The term criminal act is the most common translation of the term strafbaar feit in Dutch. The term strafbaar feit in Indonesian is translated with various terms, such as criminal acts, delicacies, criminal events, punishable acts, or criminal acts. According to Pompe, strafbaar feit can theoretically be defined as a violation of norms (disturbance of the rule of law) committed intentionally or unintentionally by a person, where the punishment of the perpetrator is necessary to maintain law and order and ensure the public interest (Wahyuni & Marwenny, 2020).

Criminal acts are actions that are prohibited by law and are associated with certain punishments or impacts. In the realm of criminal law, this violation includes behavior that violates existing legal standards and can lead to sanctions from government authorities. Usually, these violations are governed by certain laws and regulations, such as the Criminal Code (KUHP) in Indonesia. In today's cyberspace, different types of offenses are committed, and these crimes are not limited to direct interactions; Many individuals are now engaging in criminal behavior through social media platforms. An example presented in this paper is the issue of extortion and threats carried out through social media channels.

The definition of extortion is an act that benefits a certain party (extortionist) and harms another party (extortionist). In legal terms, extortion has a criminal formulation that is listed in positive law. Etymologically, the word “exortions” in Indonesian comes from the root word “squeezes”, which lexically means to ask for money or other objects with threats (Alweni, 2019). Extortion can occur in many forms, either in person (face-to-face) or through social media or other information technology. The Concept of Extortion on Social Media is:

1. Threats, perpetrators can threaten to disseminate the victim's personal data, sensitive photos or videos, or reveal information that could damage the victim's reputation.
2. The prosecution demanded that the perpetrator ask for something from the victim, either in the form of money, goods, or certain actions.
3. Coercion: Extortion is carried out by coercing the victim, which can be through intimidating threats or pressure.

According to the provisions of the Criminal Code, the crime of extortion not only has a general formula, but also includes its specific forms.According to the formulation of Article 368 paragraph (1), the definition of extortion includes several elements as follows:

a. Objective elements:
   2) Coercive Actions
   3) The Corced Party: a person
   4) Coercion is carried out by force, or the threat of violence
   5) The goal is the result of coercive actions that use violence or threats of violence
b. Subjective elements
   1) Intent to benefit oneself or others
   2) It is against the law

The four objective elements in the act of extortion include the first, the act of coercion (dwingen). Although the law does not explain in detail what coercion is, it refers to an attempt (active, in this case involving violence or threat of violence) that suppresses a person's will or intention, so that the person is forced to do something against his or her will.

Furthermore, the definition of Threatening is the act of threatening someone with the aim of scaring or forcing the victim to do something or not do something (Agam, 2021). In the context of social media, threats are often carried out by spreading messages or uploads that contain threats to the physical safety, reputation, or welfare of the victim. The Great Dictionary of the Indonesian Language (KBBI) defines threats as a threatening process, method, or action. Threatening means expressing an intention or plan to do something that could harm, difficult, inconvenience, or harm the other party. Threats are a type of wrongdoing that can indirectly cause fear, anxiety, stress, or confusion in a person. Threats are included in illegal acts that are considered a violation of the law (Andrian, 2022). The concept of threat on social media is :

1. Physical or Psychological Threats, physical threats can be in the from of threats to hurt the victim, while psychological threats can be in the form of threats to demage the victim’s good name.
2. Social Media as a means of perpetrators using platforms such as Instagram, Twitter, Facebook, or other messaging applications to spread threats.
3. Intimidation, the purpose of threats is to scare the victim into doing something the perpetrator asks or to limit the victim's freedom.

The crime of extortion and threats through social media is an unlawful act. There are many regulations that regulate the crime of extortion and threats in the digital world, but this is often caused by a lack of public understanding due to low interest in reading. Therefore, the government and law enforcement officials need to conduct socialization to increase public awareness about the existence of regulations that regulate the legal impact for perpetrators of extortion and threats through electronic media, which are listed in the Law (Akmal, 2020).

Crimes Of Extortion And Threats In The ITE Law

The Electronic Information and Transaction Law (ITE Law) functions to regulate various public activities in interacting on social media platforms. In addition to fulfilling the sociological aspect, the ITE Law has also fulfilled the philosophical aspect. Philosophically, the presence of the ITE Law is based on Article 28F of the 1945 Constitution of the Republic of Indonesia which states, “Every individual has the right to seesk, obtains, posses, stores, proces, and convey informations through various availables means”.

Along with the progress of the times, in regulating criminal cases through electronic media, regulations have been issued specifically regulating information technology crimes listed in Law Number 1 of 2024 concerning the Second Amendment to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (hereinafter abbreviated as the ITE Law). The ITE Law is expected to be a tool for controlling and enforcing order in the use of information technology. Sociologically, society does need clear and concrete legal regulations regarding information technology. Before the ITE Law was issued, existing regulations were limited to regulating certain aspects related to information technology, without providing a more direct and detailed explanation.

According to the author, the provisions regarding extortion regulated in laws and regulations can be implemented based on the Criminal Code and also the ITE Law, in the Criminal Code Article 368 states that "Whoever with the intention of unlawfully benefiting himself or others, forces a person by violence or threat of violence, to give away something, which wholly or partially belongs to that person or another person, or to give a debt or write off receivable, threateneds, for extortiosn with a maximum prison sentence of nine years", while in the ITE Law Article 27B (2):

"Every Person deliberately and without rights distributes and/or transmits Electronic Information and/or Electronic Documents, with the intention to benefit themselves or others unlawfully, with the threat of pollution or with the threat of revealing secrets, compel a person to: a. give an item that belongs in part or wholly to that person or to another person; or b. indebtedness, making an acknowledgment of a debt, or writing off receivables.", and the relevant sanctions are provided for in Article 45 (10): "Any person who intentionally and without rights distributor and/or transmits Electronic information and/or Electronics documents with the intention to unlawfully, with the threat of defamation or with the threat of disclosure of confidentiality, compel a person to: a. give an item that belongs in part or wholly to that person or to another person; or b. giving debts, making a debt confession or writing off receivables, as intended in article 27B (2) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp 1000,000,000.00 (one billion rupiah).

Based on these two articles, both regulate the crime of extortion, but the Criminal Code only regulates the crime of extortion in general (lex generali), while the ITE Law regulates the crime of extortion more specifically (lex specialis). When referring to Article 63 paragraph 2 of the Criminal Code which states that "If an act is included in a general criminal law, it is also regulator in a special criminal law, then that special one is applied. According to the rules based on Article 63 paragraph 2 of the Criminal Code, the crime of extortion in the digital (electronic) world, the rules that can be implemented are in Article 27B paragraph (2) and Article 45 paragraph (10) of the ITE Law. Therefore, in an effort to implement the ITE Law as a form of eradicating the crime of extortion in the digital world, cooperation and support with various parties are needed, both from law enforcement officials and also from the legal community. And to implement the eradication of extortion in the digital world as well as electronic media and social media, repressive efforts and preventif efforts are needed.

Law Enforcement Policy On Extortion And Threat On Social Media

Law enforcement is one of the strategies to deal with offences effectively, and fulfil a sense of justice. Related to the management of various means as options that can be given to criminal offenders, both as criminal and non-criminal means, which can be integrated with each other. Law enforcement needs to be understood in three aspects; First, the aspect of law enforcement as a whole (total enforcement concept) which requires all values underlying legal norms to be enforced without exception. Second, the full enforcement aspect which recognises that the total concept must be limited by procedural law and the like to protect individual interests. Third, the actual enforcement concept arises when there is a recognition of discretion in the application of law due to various limitations, whether related to infrastructure, quality of human resources, quality of legislation, or low public participation.

Law enforcement carried out to respond to cases of extortion and threats via social media can be implemented through two methods, namely repressive law enforcement and preventive law enforcement. Repressive enforcement involves the application of criminal law that focuses on follow-up actions after a criminal act has occurred, where an investigation process is carried out, action against the perpetrator is taken, and a report on the outcome of the case file is prepared. On the other hand, preventive enforcement can be pursued through socialization or counseling to the public about the negative effects of social media deviations.

Law enforcement policies against extortion and intimidation in Indonesia aim to protect individual rights and ensure the creation of public security and order. Criminal liability is a process to determine whether a person can be convicted of a criminal act that has been committed. In this case, to declare that a person has criminal responsibility, there are several elements that must be met, namely the existence of a criminal act, an element of guilt, and no excuse for forgiveness (Geraldo & Waluyo, 2023). Law

enforcement in Indonesia faces significant challenges in dealing with the rise of cybercrime. This is due to the limitations of law enforcement officials who have a deep understanding of information technology (internet). In addition, many law enforcement officials in the region are not ready to face the developments of this crime because many of them are still less skilled in technology (gaptek). This problem is exacerbated by the lack of infrastructure support, such as internet networks, in many law enforcement institutions in the region (Akmal, 2020). Without adequate facilities and facilities, law enforcement will not run effectively. These facilities and facilities include an educated and skilled workforce, a well-structured organization, adequate equipment, and adequate financial support. If these things are not available, then law enforcement will find it difficult to achieve its goals.

In the concept of modern social security, the security system is not only the responsibility of law enforcement, but also the shared responsibility of all elements of society. In this case, society functions not only as an object, but also as a subject. As subjects, people are involved in communication between individuals as well as utilizing internet services and other media. As objects, people are targets and victims of various criminal activities that occur in cyberspace.The law enforcement policy for extortion that violates the ITE Law is to ensnare the perpetrator with Article 27B paragraph (2). And the criminal threat of perpetrators who are proven to violate this article, namely in Article 45 paragraph (10), can be sentenced to a maximum of 6 years in prison and/or a maximum fine of Rp 1,000,000,000 (one billion rupiah). The ITE Law is one of the efforts to tackle crimes related to technology. Conventional criminal acts regulated in the Criminal Code are reformulated in the ITE Law by adding elements of scope and acts in the realm of technology.To implement the ITE Law in eradicating extortion in the digital world, cooperation and support from various parties, both law enforcement officials and the legal community are needed. In addition, in an effort to eradicate the crime of extortion in the digital world, electronic media, and social media, repressive measures and preventive measures are needed.

Repressive enforcement is achieved through the application of criminal law that prioritizes eradication after the occurrence of criminal acts, by conducting investigations, taking steps against perpetrators, conducting analysis, and compiling case file documents. On the other hand, preventive enforcement can be carried out by providing education or counseling to the public about the consequences of misusing social media (Putri et al., 2022).Overall, the existence of the ITE Law has a number of benefits if implemented correctly. Some of the benefits resulting from the ITE Law are:

1) Legal certainty in online transaction activities
2) Stimulating economic developments in Indonesia.
3) Role in reducing cybercrime
4) Protect the community.

CONCLUSIONS AND SUGGESTIONS

Conclusion

The crime of extortion and threats through social media is an unlawful act. There are many regulations governing such crimes in the digital world, but often public ignorance is the main factor, mainly due to a lack of interest in reading. Therefore, the government and law enforcement officials need to hold socialization so that the public understands that there are regulations that regulate the legal impact of the crime of extortion and threats through electronic media in accordance with the Law. The implementation of the ITE Law also aims to provide legal protection to victims who can suffer emotional and financial losses. In addition, the ITE Law provides room for preventive and legal measures to prevent the misuse of social media for unlawful purposes. Overall, legal policy on the misuse of social media for the crime of extortion and threats must prioritize a comprehensive approach, including strict law enforcement, protection for victims, public education, and cooperation between related parties.

Suggestion

1. Increasing Digital Literacy to the Community
   To reduce the crime of extortion and threats through social media, it is very important for the government to increase digital literacy among the public. Education on how to protect personal data, recognize forms of threats in cyberspace, and understand the risks of misuse of social media will help individuals become more vigilant and make wiser decisions when interacting in the digital world.
2. Socialization about Legal Sanctions for Perpetrators
   Socialization of the threat of clear and firm legal sanctions against extortionists and threats through social media needs to be carried out. By increasing public understanding of the legal consequences of this criminal act, it is hoped that it can reduce the malicious intentions of the perpetrators and encourage them to be more compliant with existing regulations.
3. Law Enforcement Capacity Building

Law enforcement officials, such as police and prosecutors, must have a good understanding and adequate technical skills to handle extortion and intimidation cases involving social media. This includes the ability to track perpetrators through digital footprints left on social media platforms.

REFERENCES

Agam, G. (2021). TINJAUAN YURIDIS TERHADAP TINDAKAN PENGANCAMAN MELALUI MEDIA ELEKTRONIK BERUPA PESAN SINGKAT. *Jurnal Of Law*, *7*, 8.

Akmal, D. A. & A. (2020). Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi InformasiNo Title. *Journal Of Sciencs and Social REASEARC*, *2*(2), 39–46.

Alweni, M. K. (2019). Kajian Tindak Pidana Pemerasan Berdasarkan Pasal 368 KUHP. *Jurnal Lex Crimen*, *8*(3), 47–54.

Andrian, K. (2022). *Penegakan Hukum Terhadap Pelaku Tindak Pidana Pengancaman Dengan Kekerasan Melalui Media Sosial*. *1*, 268–289.

Asmadi, E. (2020). Rumusan Delik Dan Pemidanaan Bagi Tindak Pidana Pencemaran Nama Baik Di Media Sosial. *De Lega Lata: Jurnal Ilmu Hukum*, *6*(1), 16–33. https://kumparan.com/kumparannews/polri-kasus-uu0ite-terbanyak-terkait-pencemaran-nama-baik-ada-1-794-laporan-1vKQXFs6cNx

Durham, C. (2022). Amicus Curiae. *Revista Latinoamericana de Derecho y Religión*, *1*(NE), 1272–1284. https://doi.org/10.7764/rldr.ne01.009

Geraldo, H., & Waluyo, B. (2023). Pertanggungjawaban Pidana Pelaku Tindak Pidana Pengancaman Secara Elektronik. *Jurnal Yuridis*, *10*(2), 33–51. https://doi.org/10.35586/jyur.v10i2.7097

Idris, J. I., & Supandi, A. (2024). Evaluasi Kebijakan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia; Potret Bibliometric Analysis. *Transparansi : Jurnal Ilmiah Ilmu Administrasi*, *7*(1), 149–162. https://doi.org/10.31334/transparansi.v7i1.3709

Kadir Ainun Jariyah, Pawennei Mulyanti, A. (2024). Journal of Lex Philosophy (JLP). *Journal of Lex Philosophy (JLP)*, *5*(1), 260–275.

Matheus, J. S. (2021). PERTANGGUNGJAWABAN PIDANA PELAKU PEMERASAN DAN/ATAU PENGANCAMAN YANG DILAKUKAN MELALUI MEDIA ELEKTRONIK. *Repository Universitas HKBP Nommensen*, 14.

Ningrum, P. A. P. (2020). *Penegakan Hukum Terhadap Pelaku Tindak Pidana Pengancaman Yang Ditujukkan Dengan Ucapan Dan Hinaan Oleh: Putu Ary Prasetya Ningrum, M.H*. 39–45.

Putri, P. D. P., Sugiartha, I. N. G., Sudibya, D. G., & Sudibya, D. G. (2022). Penegakan Hukum Terhadap Pelaku Tindak Pidana Pengancaman Kekerasan dan Pembunuhan Melalui Media Sosial. *Jurnal Preferensi Hukum*, *3*(1), 208–212. https://doi.org/10.22225/jph.3.1.4685.208-212

Udayana, I. G. P., I Made Minggu Widyantara, & Ni Made Sukaryati Karma. (2022). Penyalahgunaan Aplikasi Media Sosial sebagai Eksploitasi dalam Tindak Pidana Pornografi. *Jurnal Konstruksi Hukum*, *3*(2), 438–443. https://doi.org/10.55637/jkh.3.2.4852.438-443

Wahyuni, S., & Marwenny, E. (2020). Tinjauan Yuridis Terhadap Tindak Pidana Pengancaman dalam Undang-Undang Informasi dan Transaksi Elektronik. *UIR Law Review*, *4*(2), 51–58. https://doi.org/10.25299/uirlrev.2020.vol4(2).6468