Journal of Law Perspectives Review
Volume 2, Nomor 1, 2026, Hal: 9-16
https://doi.org/10.64670/jlpr.v2i1.54

Catalyst Journal

Journal of Law Perspectives Review

journal homepage: journal.catalystindo.org

Cyber Extortion as a Cybercrime in Indonesian Criminal Law: Normative Analysis and Legal Protection for Victims

Rahul Gonzales Sihombing [1], Sachila Fattah [2], Dirga Arya Kesuma Nasution [3], Rosmalinda [4], Annisa Hafizah [5]*

[1,2,3,4,5] Fakultas Hukum, Universitas Sumatera Utara, Sumatera Utara, 20131, Indonesia

ARTICLE INFO

Received: 28 December 2025
Accepted: 19 January 2026
Available Online: 28 January 2026

Keywords:
Cyber Extortion; Cybercrime; Indonesian Criminal Law; Criminal Liability; Victim Protection.

Correspondence
*Nama: Rahul Gonzales Sihombing
Email: rahulgsihombing@gmail.com

ABSTRACT

This study aims to analyze the legal regulation of Cyber Extortion within the Indonesian criminal law system and examine the forms of legal protection and criminal liability applicable to perpetrators and victims. The research employs a juridical-normative method with a descriptive qualitative approach. Primary legal materials include Article 368 of the Criminal Code, Article 45 in conjunction with Article 27B of Law No. 1 of 2024 concerning the Second Amendment to the ITE Law, and Law No. 44 of 2008 concerning Pornography, supported by relevant legal doctrines and court practices. The findings indicate that Indonesian positive law has established a relatively comprehensive normative framework for addressing Cyber Extortion. Judicial interpretation has expanded the concept of "violence or threat of violence" to encompass psychological threats in cyberspace, including threats to disseminate sensitive data that may damage a victim's reputation. Cyber Extortion can be categorized based on the relationship between perpetrators and victims, including both prior face-to-face relationships and purely online interactions. Legal protection mechanisms include the right to report, personal data protection, fair trial guarantees, restitution, and psychological assistance. Criminal liability is grounded in the principle of fault, particularly intentional conduct, with sanctions ranging from six months to twelve years imprisonment. In conclusion, effective implementation still requires stronger inter-agency coordination and increased public awareness to enhance prevention and victim protection.

Introduction

Indonesia is a state of law that places the rule of law as the main foundation in the implementation of the life of the nation and state as affirmed in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia. In the development of modern society, advances in information technology have brought significant changes to social, economic, and legal interaction patterns. The rapid development of digital makes the world seem limitless, thus opening up a wide space of communication while creating the potential for various new forms of crime. One of the consequences of technological advances is the emergence of cybercrime which refers to the misuse of information technology through computerized systems and internet networks. The lack of awareness and digital literacy of the community causes many social media users to be unaware of the various risks of digital crime that lurk (Nurmiati Nurmiati & Harti Winarni, 2025).

Extortion through social media or Cyber Extortion is one form of cybercrime that is increasingly prevalent. This act is expressly prohibited in the provisions of positive Indonesian law, including Article 45 jo. Article 27B Paragraph (2) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions and

Article 368 of the Criminal Code. The provision stipulates that a person can be convicted if he deliberately and without the right distributes, transmits, or makes accessible information or electronic documents that contain threats or extortion through electronic media. This regulation aims to protect the public from unlawful actions that have the potential to cause psychological, financial, and social losses for victims (Hayatinufus, Rizky Awaludin, Amirotunnadia, 2025). Unlike conventional extortion which generally involves physical violence or direct threats, Cyber Extortion is carried out through electronic means such as short messages, social media, and various other digital platforms so that it has special characteristics that require an adaptive legal approach.

Theoretically, Moeljatno explained that criminal acts are unlawful acts accompanied by the threat of criminal sanctions and harm the community (Moeljatno, 2008). This concept is relevant in understanding the phenomenon of Cyber Extortion which not only violates legal norms but also has a wide social impact. The increase in cybercrime shows a change in crime patterns along with globalization and digitalization. Therefore, criminal law is required to be able to respond to these dynamics through effective criminalization policies and law enforcement mechanisms that are adaptive to technological developments.

Law enforcement is a key factor in tackling digital crime. Law enforcement officials are faced with complex challenges that include aspects of law, culture, institutions, community behavior, and legal mindsets. Cybercrime is often committed by perpetrators who use technological devices such as computers, mobile phones, and other means of online communication to commit crimes quickly and anonymously. This condition shows that the development of internet technology has also expanded the space for crime to occur while increasing difficulties in the process of proving and enforcing the law (Fatimah, 2025).

Previous research has shown that studies on cybercrime in Indonesia generally focus on aspects of general regulation and legal protection for victims, including analysis of the application of the Electronic Information and Transaction Law in various types of digital crimes. Several studies highlight the need for regulatory harmonization and capacity building of law enforcement officials in dealing with the development of cybercrime modus operandi. However, research that specifically examines *Cyber Extortion* as a form of digital extortion with a comprehensive criminal law approach is still relatively limited, especially in linking the elements of delicacy, criminal liability, and victim protection in an integrated context in the context of positive Indonesian law.

The novelty of this research lies in an integrative analysis of criminal law regulations related to *Cyber Extortion* with an emphasis on expanding the interpretation of the element of "threat of violence" in the context of cyberspace, the classification of the relationship between perpetrators and victims, and the analysis of legal protection that includes the psychological and social aspects of the victim. This research also seeks to examine the development of judicial practices that have begun to recognize psychological threats as a form of non-physical violence in the crime of digital extortion, thus providing a new perspective in the development of cyber criminal law in Indonesia.

The urgency of this research is even more relevant given the increasing cases of digital extortion that exploit victims' vulnerabilities in cyberspace. One example of a case that reflects this dynamic is the case involving public figures Nikita Mirzani and dr. Reza Gladys, where the court

assessed the threat of the dissemination of personal information and reputation through social media as a form of digital blackmail. The judge interpreted the element of "coercion with the threat of violence" in Article 368 of the Criminal Code broadly to include the threat of psychological violence in cyberspace. The ruling shows the development of legal interpretations that adapt to the realities of modern crime, while confirming that mental distress and reputational damage can be seen as equivalent to physical violence in the context of extortion.

In addition, the urgency of the research is also driven by the need to strengthen legal protection for victims, increase the effectiveness of law enforcement, and strengthen coordination between law enforcement agencies in handling *Cyber Extortion*. The public needs legal certainty that is able to answer the challenges of the digital era while providing a sense of security in using information technology. Based on this description, this study aims to analyze the criminal law regulation of *Cyber Extortion* in Indonesia's positive law, examine the form of criminal responsibility of perpetrators, and assess the effectiveness of legal protection for victims in the context of cybercrime development.

Methods

This study applies juridical-normative methodology as the main approach in studying legal phenomena that are the focus of research (Muhaimin, 2020; Saebani, 2021). This method focuses on the in-depth exploration and analysis of various legal sources, both primary and secondary, that have direct relevance to the research topic, particularly related to Cyber Extortion in the context of criminal acts.

The juridical-normative approach was chosen because this method allows researchers to conduct a systematic review of the entire legal framework in force, identify fundamental principles in law, and analyze legal doctrines that develop in the academic community and legal practitioners.

The analysis technique used in this study is qualitative descriptive analysis, which allows the presentation of information in a holistic and comprehensive manner regarding various aspects of cybercrime, especially Cyber Extortion. Through this approach, the research aims to build a comprehensive overview of Cyber Extortion in the Indonesian criminal law system, especially in the context of cyber crime which is a crime with socio-economic implications. In addition, qualitative descriptive analysis is also used to conduct a critical evaluation of the adequacy of the Cyber Extortion regulation in providing legal certainty to all parties involved in the criminal justice system in Indonesia.

Results and Discussion

Cybercrime, also known as cybercrime, is a type of crime committed online. This crime does not choose the target and does not know the time. It can happen to people or companies wherever they are. The goals of cybercrime are diverse. It may be just a minor crime, to a significant crime that harms the victim financially (Faysal Banua Suwiknyo Harly Stanly Muaja & Tonny Rompi, 2021). One form of cybercrime is Extortion through social media (Cyber Extortion). Cybercrime is carried out by people either individually or in groups who are really experts in hacking, experts in using computers as a means/tool to commit crimes so that according to experts, the form of cybercrime is

generally in the form of identity theft, cyber espionage, cyber extortion, theft of company data, and carding. Meanwhile, according to Law No. 11 of 2008 Jo. Law No. 19 of 2016 concerning Electronic Information and Transactions Jo. Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Information and Electronic Transactions, forms of cyber crime are criminal acts related to illegal activities, criminal acts related to interference, criminal acts facilitating prohibited acts, and criminal acts of falsifying information or electronic documents. It's important to remember that digital extortion is different from conventional extortion that is carried out with physical violence or real threats. Perpetrators of Cyber Extortion use electronic means such as text messages, emails, social media, or other online platforms to extortion. The modus operandi of Cyber Extortion usually involves threats to disseminate the victim's sensitive data, photos, videos, or personal information if the victim does not comply with the perpetrator's request (Napitupulu, 2025) Victims of Cyber Extortion crimes typically suffer varying losses, including psychological trauma, loss of money, reputational damage, and privacy threats (Makhali, 2023).

Cyber Extortion differs from conventional extortion with a few differences. Cyber fraud is carried out through digital communication platforms such as WhatsApp, Telegram, Instagram, Facebook, email, or others. By using this medium, the perpetrator can contact the victim without having to talk directly to him or her and maintain a safe distance from direct recognition. Internet extortion uses psychological, reputational, and social threats, and threat actors to disseminate personal photos or videos, sensitive data, or information that could damage the victim's reputation on the internet. Victims experience immense fear, mental distress and anxiety as a result of these threats (Sudin et al., 2022).

Cyber Extortion may use a wide variety of objects as a means to pose a threat. Personal photos or videos with pornographic or indecent content, screenshots of private conversations or audio or video recordings, as well as information that could harm the victim's reputation or social relationships fall into this category. Fourth, perpetrators of Cyber Extortion can come from various backgrounds and groups, such as professional perpetrators who carry out Cyber Extortion as a business, people who are only known through social media in online relationships, individuals with personal motivations such as revenge or revenge, to organized groups that carry out Cyber Extortion on a large scale. In most cases, the perpetrator's motivation is to gain financial gain, sexual content, sexual services, or other personal information by exploiting the victim's fears (Boby Iskandar, Eren Arif Budiman, 2021).

In Indonesia, regulations related to the crime of Cyber Extortion are regulated in the Criminal Code and the Electronic Information and Transaction Law (ITE Law). Article 368 of the Criminal Code regulates extortion with the element of "coercion with force or threat of violence". A recent court ruling means that violence in this article can be in the form of psychological pressure or reputational threats, as decided in the digital blackmail case involving Nikita Mirzani and dr. Reza Gladys, where the court judged that the threat to spread disgrace through social media included psychological violence equivalent to physical violence in the context of extortion. The court considered that the act threatened to spread disgrace and damage the victim's reputation on social media, including acts of digital extortion. The judge in this case determined that the element of "coercion with the threat of violence" as referred to in Article 368 of the Criminal Code can be

interpreted broadly to include the threat of psychological violence in cyberspace.

Article 45 in conjunction with Article 27B Paragraph (2) in Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Information and Electronic Transactions expressly regulates the criminal penalties for any person who deliberately and without the right to distribute, transmit, or make accessible information containing threats or extortion through electronic media. Criminal sanctions that can be imposed are imprisonment for a maximum of six years and/or a maximum fine of up to one billion rupiah.

Law Number 44 of 2008 concerning Pornography can also be applied in cases of Cyber Extortion involving pornography or sexually explicit content. Article 4 Paragraph (1) of the Pornography Law prohibits everyone from reproducing, disseminating, broadcasting, or trading pornography. If the perpetrator of internet extortion ends up distributing pornographic content to the victim because their request is not fulfilled or as a result of the extortion, this is a violation of the Pornography Act. The perpetrator can face a prison sentence of a minimum of six months and a maximum of twelve years, and/or a fine of at least two hundred and fifty million to a maximum of six billion rupiah. Among all the penalties that can be applied in a case of Cyber Extortion, this is the severe (Afrida et al., 2023).

Cyber Extortion can be classified based on the type of relationship between the perpetrator and the victim. Cyber Extortion is in face-to-face relationships where the perpetrator and the victim have met each other or even established an intimate relationship in the real world. This type generally involves an ex-romantic partner, a person who is known personally and then exploits the victim's trust, or a case that starts with a normal relationship then turns into extortion after a breakup or conflict. Cyber Extortion is in online relationships where the perpetrator and the victim never meet each other in real life and only interact through social media or online platforms. These types include online predators who target victims through social media, scammers who create fake identities to find victims, or organized groups that systematically seek out and exploit targets (An Nisya Nursabilah et al., 2025).

Legal protection for victims of Cyber Extortion in Indonesia includes the right to reporting, the right to personal data protection, the right to fair examination, and the right to restitution, which is compensation for losses experienced by the victim (Ghani & Saefudin, 2024) Victims are also entitled to psychological support and trauma rehabilitation services, considering that the impact of these crimes is not only material but also mental and social. The court ruling is the basis for restitution and compensation, which can include restitution, counseling costs, and rehabilitation of the victim's reputation (Ghani & Saefudin, 2024) Victims of Cyber Extortion have many rights recognized by Indonesia's positive law. In the protection and security section, victims are entitled to protection from retaliation, where the police must protect them if they feel threatened by the perpetrator or related parties after reporting a crime. Victims also have the right to the security of their personal data to prevent further dissemination of their personal data, as well as privacy during the judicial process, where victims of Cyber Extortion involving sensitive data are entitled to protection (Mufidatul Ma'sumah et al., 2024).

Conclusion

Extortion through social media or Cyber Extortion is a form of serious crime in the digital era that threatens the security and welfare of the community. The development of information technology has opened up new spaces for perpetrators to make threats and psychological pressure on victims through electronic means. In response to this phenomenon, Indonesia's positive law has built a normative framework that can be used to take action against perpetrators, especially through Article 368 of the Criminal Code, Article 45 juncto Article 27B of the ITE Law No. 1 of 2024, as well as various other provisions in the ITE Law and the Pornography Law.

Criminal liability for perpetrators of Cyber Extortion is based on the general principles of Indonesian criminal law, namely the existence of mistakes in the form of intentionality and the ability of the perpetrators to account for their actions. The application of criminal sanctions is adjusted to the provisions of the article used and the severity of the criminal act committed. In practice, the criminal threat that can be imposed ranges from six months to twelve years in prison, depending on the proven elements of the crime and the impact it has on the victim.

Acknowledgments

The author would like to express his gratitude to Dr. Rosmalinda, S.H., LLM for his very meaningful direction and input during the preparation of this research. The author also expresses his gratitude to Annisa Hafizhah, S.H., M.H. for the academic support and corrections that helped improve this article. The author also thanked the Faculty of Law, University of North Sumatra for the facilities and academic environment that supported the research process. Not to forget, the author also thanked the group friends who had cooperated, discussed, and contributed during the work of this journal. Such support and collaboration really helped to complete this article well.

Daftar Pustaka

Afrida, D. T., Ismansyah, & Elda, E. (2023). Sekstorsi Sebagai Tindak Pidana Kekerasan Seksual Berbasis Elektronik Dalam Sistem Hukum Di Indonesia. Delicti : Jurnal Hukum Pidana Dan Kriminologi, 1(1), 11–26. Https://Doi.Org/10.25077/Delicti.V.1.1.1.P.11-26.2023

An Nisya Nursabilah, Nazmi Viranha Khurulani, Anggia Prasanti, Dea Aulia Zuhra, Allyah Alicia Hg, & Nabila Nabanurohmah. (2025). Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Scam Serta Dampaknya Bagi Korban Sebagai Bentuk Viktimisasi Sekunder. Hukum Inovatif : Jurnal Ilmu Hukum Sosial Dan Humaniora, 2(3), 168–187. Https://Doi.Org/10.62383/Humif.V2i3.1912

Boby Iskandar,Eren Arif Budiman. (2021). Kebijakan Formulasi Hukum Pidana Tentang Penanggulangantindak Pidana Terorisme Siber (Cyber Terorism) Di Indonesia. Stih Umel Mandiri Jayapura, 2(01), 20.

Fatimah, S. (2025). Penerapan Sanksi Pidana Terhadap Pelaku Tindak Pidana Cyberstalking Di Indonesia. Journal Of Business Law Research, 1(02), 21.

Faysal Banua Suwiknyo Harly Stanly Muaja & Tonny Rompi. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. Journal Of Business Law Research, Ix(4), 192.

Ghani, M. Y. A., & Saefudin, Y. (2024). Perlindungan Hukum Bagi Korban Tindak Pidana Cyber

Sekstorsi Di Indonesia (Studi Kasus Rebecca Klopper). Southeast Asian Journal Of Victimology, 2(2), 162. Https://Doi.Org/10.51825/Sajv.V2i2.27121

Hayatinufus, Rizky Awaludin, Amirotunnadia. (2025). Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing). Journal Of Applied Computing And Digital Information(Jacodi), 01(01), 10–14.

Makhali, I. (2023). Bentuk Pertanggung Jawaban Pidana Bagi Pelaku Tindak Pidana Mayantara. Transparansi Hukum, 6(1). Https://Doi.Org/10.30737/Transparansi.V6i1.4226

Moeljatno. (2008). Asas-Asas Hukum Pidana Edisi Revisi. Rineka Cipta.

Mufidatul Ma'sumah, Halimatus Khalidawati Salmah, & Bellinda Oktovani Bp. (2024). Perlindungan Hukum Terhadap Perempuan Korban Revenge Porn Melalui Konten Pornografi Yang Dibuat Berdasarkan Kesepakatan (Based On Consent). Jurnal Bedah Hukum, 8(1), 1–15. Https://Doi.Org/10.36596/Jbh.V8i1.1320

Muhaimin, M. (2020). Metode penelitian hukum. Dalam S. Dr. Muhaimin, Metode Penelitian Hukum, Mataram-NTB: Mataram.

Napitupulu, O. P. (2025). Pertanggungjawaban Pelaku Penyebar Konten Vulgar Di Platform Media Sosial Dengan Ancaman Dan Pemerasan (Studi Putusan Nomor 74/Pid.Sus/2021/Pn Nga). Universitas Kristen Indonesia, S1 Thesis.

Nurmiati Nurmiati & Harti Winarni. (2025). Penegakan Hukum Terhadap Tindak Pidana Pemerasan Menggunkan Teknologi Media Sosial Di Polresta Yogyakarta. Hukum Inovatif : Jurnal Ilmu Hukum Sosial Dan Humaniora, 2(3), 322–333. Https://Doi.Org/10.62383/Humif.V2i3.2153

Sudin, P. P., Magdalena, R., Priowirjanto, E. S., & Soeikromo, D. (2022). Penyalahgunaan Akun Instagram Perihal Penipuan Jual Beli Secara Online Ditinjau Dari Uu Ite Dan Pasal 378 Kuhp Tentang Penipuan. Journal Of Education, Humaniora And Social Sciences (Jehss), 5(1), 20–26. Https://Doi.Org/10.34007/Jehss.V5i1.842

Saebani, B. A. (2021). Metode Penelitian Hukum Pendekatan Yuridis Normatif. CV Pustaka Setia.