Journal Social Sciences and Humanioran Review (JSSHR)
P-ISSN : 3032-6176, E-ISSN : 3032-5848
Volume 02 Issue 01 January 2025
DOI: 10.64578/jsshr.v2i01.153
Page Number 9-18

OPTIMIZING LEGAL REGULATIONS FOR THE PROTECTION OF CYBERSTALKING VICTIMS IN INDONESIA

Rafhael Roberto[a], Balqis Tsabitah Azzahrah[b], Khoirunnisa Putri Diksy[c], Nadia Marsya Ramdhani[d], Atik Winanti[e]
Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta
e-mail: 2310611147@mahasiswa.upnvj.ac.id

Keywords: *Cyberstalking; Legal Protection; Regulation*

Abstract

Cyberstalking involves stalking, monitoring, or harassing someone continuously through digital media, which can threaten an individual's privacy and cause psychological distress to the victim, including anxiety, trauma, and insecurity. Although there are laws regulating cyberstalking, legal protection for victims of cyberstalking is still inadequate due to limitations in handling cyberstalking cases. This study examines legal protections for victims of cyberstalking in Indonesia and identifies efforts to optimize cyberstalking regulations in the country. This study uses a normative legal approach (doctrinal research) with a statutory approach and a conceptual approach. The results of this analysis show that legal protection for victims of cyberstalking in Indonesia still faces challenges. Although there are regulations to handle cyberstalking cases, law enforcement remains ineffective and incomplete, and there are no specific regulations addressing cyberstalking. Additionally, legal loopholes indicate legal weaknesses in the regulation of cyberstalking in Indonesia. Therefore, it is necessary to establish a specific law that specifically regulates cyberstalking and revise existing regulations to strengthen the legal framework governing cyberstalking. Furthermore, it's important to raise awareness about cyberstalking and strengthen technological infrastructure in digital investigations so that the law can be enforced effectively and comprehensively, thereby protecting victims of cyberstalking in Indonesia.

Submit : 2025-06-16
Review : 2025-06-29
Diterima : 2025-12-24

A. Introduction

The development of information technology has had a significant impact on various aspects of life, including communication, economics, and social interaction. However, behind the convenience it offers, the digital era also presents new challenges in

How to cite Roberto, R., et al., Optimizing Legal Regulations for the Protection of Cycberstalking Victims in Indonesa, Volume 02 Issue 01 January 2025
Published by Zhata Institut

the form of cybercrimes one of which is cyberstalking, defined as the act of persistently stalking, monitoring, or harassing someone through digital media. This phenomenon not only threatens individual privacy but also has serious psychological effects on victims, such as anxiety, trauma, and a sense of insecurity in everyday life (Smith, 2023). Alongside rapid technological advancements and increasing internet penetration, cyberstalking cases have shown an alarming upward trend in Indonesia.

Although Indonesia has several relevant laws, such as Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) as amended by Law Number 19 of 2016, and criminal provisions under the Indonesian Penal Code (KUHP), legal protection for victims of cyberstalking is still considered suboptimal (Setiawan, 2022). Various limitations have emerged, including the lack of a comprehensive definition, difficulties in proving cases, and insufficient understanding by law enforcement officers regarding the unique characteristics of this cybercrime. Moreover, law enforcement tends to be reactive, and the lack of understanding of cyberstalking often results in victims not receiving proper justice.

Therefore, optimizing the legal framework for protecting cyberstalking victims in Indonesia has become crucial. Such optimization may include the reformulation of criminal law norms, capacity building for law enforcement, and strengthening the role of victim protection institutions in the digital realm. These efforts are essential to ensure victims' rights, uphold justice, and maintain digital security for society as a whole (Farisa, 2022). Consequently, it is hoped that a more effective and responsive protection system can be established, one that aligns with the evolving dynamics of cyberstalking crimes and contributes to a safer cyberspace.

B. Method

This study employs a normative juridical method (doctrinal research), which specifically focuses on examining the applicable legal rules and doctrines related to the legal protection of cyberstalking victims in Indonesia. The selection of this method is based on the research objective, which emphasizes the analysis of laws and existing legal concepts. In this study, two main approaches are applied. First, the statute approach, which involves a comprehensive review of various relevant legislations, including Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) as amended by Law Number 19 of 2016, as well as the Indonesian Penal Code (KUHP). Second, the conceptual approach, which aims to analyze various legal concepts and principles underlying the protection of cybercrime victims, such as human rights in the digital realm and privacy protection.

The data used in this research is secondary data, specifically consisting of primary legal materials, such as laws and court decisions directly related to cyberstalking cases. Additionally, secondary legal materials are utilized, including books, scientific articles,

journals, and research findings that discuss legal protection and cybercrime. To enhance understanding, tertiary legal materials, such as legal dictionaries, encyclopedias, and indexes, are also used as references. Data collection was carried out through library research, by identifying, selecting, and systematically analyzing legal documents and supporting literature. Once the data is collected, the analysis is conducted using a descriptive-prescriptive analysis. The descriptive stage outlines the current regulatory conditions, while the prescriptive stage formulates recommendations to optimize these regulations, so that the legal protection for cyberstalking victims can become more comprehensive and effective.

C. Result & Discussion

1. Legal Protection for Victims of Cyberstalking in Indonesia

Cyberspace is a boundless world, often referred to as a borderless world or an invisible world. This has a significant impact on cyberspace security, which has no boundaries. The lack of security in cyberspace can be linked to cybercrime. As the dynamics of change and development in the world of digital technology evolve, so too does the increase and development of crime in cyberspace. One of the most fundamental cybercrimes affecting an individual's privacy is cyberstalking (Cindy et al., 2025). Cyberstalking is an anonymous act of stalking carried out through digital media with the aim of harassing, threatening, or humiliating an individual, or with a specific intent. Such cyberstalking actions can have serious consequences for victims, ranging from privacy violations to psychological impacts such as anxiety, stress, and trauma. Fundamentally, the consequences of cyberstalking include the destruction of the victim's dignity, social reputation, and even direct physical safety if the cyberstalking escalates to real-world threats (Ketut, 2025). The issues surrounding cyberstalking are closely intertwined with data privacy protection, which is fundamentally rooted in the concept of privacy. The concept of privacy encompasses the idea of protecting the integrity and dignity of individuals. Personal privacy involves an individual's efforts to establish boundaries regarding who can access their information and how that information is used (Regita & Hadi, 2024).

To date, Indonesia does not yet have specific regulations that effectively govern privacy and digital data protection related to cyberstalking. It is known that before the ITE Law came into effect in Indonesia, cybercrime in Indonesia was still prosecuted using provisions of the Criminal Code, which were considered to contain relevant and appropriate elements for the punishment of cybercriminals (Regita & Hadi, 2024). Regulations related to cyberstalking still adopt the provisions of the ITE Law No. 19 of 2016 amending the ITE Law No. 11 of 2008. Under Articles 27(1) to (4) of the ITE Law No. 19 of 2016, prohibited acts include intentionally and without authorisation disseminating, transmitting, or making available electronic information and electronic

documents containing content that violates public morality, gambling, defamation or slander, extortion, and threats (Nadya et al., 2024).

The dissemination, transmission, or accessibility of electronic materials containing extortion or threats is the primary focus of law enforcement under the ITE Law. This demonstrates that the perpetrator's intent to obtain financial gain is a key aspect in determining the criminal offence of cyberstalking. Perpetrators may also be prosecuted under the Criminal Code (KUHP), specifically Articles 368 or 335 (Nabih et al., 2024). There is research using data from an analysis of cyberstalking factors in Indonesia, known as Confirmatory Factor Analysis (CFA), to obtain evidence regarding the internal structure of cyberstalking scale items. The study concluded that cyberstalking in Indonesia has a validated cyberstalking scale consisting of three aspects: romantic relationships (past, present, and desired), abuse of acquaintances, and individuals suspected or disliked by the perpetrator (Rerepih & Ratri, 2024). There is also a discussion on cyberstalking in Malaysia, which is perceived to be similar to the current cyberstalking situation in Indonesia. The study examines traditional stalking and cyberstalking, showing that women are more frequently victims of stalking than men, indicating that such crimes are motivated by specific interactive factors (Wan et al., 2021).

Singapore, which followed in the footsteps of England and Wales regarding cyberstalking, has a system of criminalising cyberstalking and created the Protection from Harassment Act in 2014. This was followed by literature showing that anti-stalking laws in England and Wales, Singapore, and the United States offer various protections for victims of stalking, such as protection orders, court orders, compensation, and detention orders. In the context of national law on cyberstalking, especially protection for victims of cyberstalking itself, this has not yet been clearly articulated (Wan et al., 2021). Although there are regulations that can serve as a basis for addressing cyberstalking, there are still gaps in protection for victims. One of the main challenges is the difficulty in identifying and apprehending cyberstalkers, particularly due to the anonymous nature of such cybercrimes. As a result, victims often struggle to obtain adequate protection from the authorities. Therefore, further steps are needed to enhance the effectiveness of law enforcement, as well as revisions and clarifications to existing regulations to strengthen protection for victims of cyberstalking in the current digital age (Hera, 2024).

Essentially, the elements of cyberstalking collectively contribute to the widespread disclosure of individual identity, which is directly related to identity theft and requires serious attention. Article 30 paragraph 3 of the ITE Law provides an explanation of security systems, which are defined as mechanisms that restrict or prohibit computer access based on user categorisation, accompanied by a set level of authority. This legal provision emphasises that intentional access to computer or electronic systems by ignoring or violating security measures set by the owner or user is a criminal act known as ‘cracking’. The 1945 Constitution of the Republic of Indonesia, or UUD 1945, regulates

the protection of personal identity. This legal framework is enshrined in Article 28G paragraph (1) of the 1945 Constitution, which explicitly states that 'Every person has the right to protection of themselves, their family, their honour, their dignity, and their property under their control, as well as the right to feel safe and protected from threats of fear to do or not do something that is a human right.' The principle of data collection restrictions and identity privacy emphasises that data collection must be conducted through legally valid, fair, and necessary methods, based on the knowledge and consent of the individual concerned. Provisions regarding the protection of personal data, especially in electronic form, are also related to Article 26 of the ITE Law, which broadly states that any use of a person's personal data through electronic media must be with the consent of the person concerned, unless there are other provisions that regulate it (Umi et al., 2024).

Law No. 31 of 2014 on the Protection of Witnesses and Victims, Article 5, only regulates the rights of witnesses or victims, such as: obtaining protection for their personal safety, family, and property. It is stated that victims also have the right to participate in the process of selecting and determining the form of protection and security support because victims are the most affected parties (Yan et al., 2024). Furthermore, with the enactment of the Personal Data Protection Law (PDP Law), cyberstalking has become a criminal offence, as defined in Article 65 of the PDP Law as 'collecting and disseminating another person's personal data,' with criminal penalties under Article 67 of the PDP Law, including a maximum prison sentence of five years and/or a fine of IDR 5 billion. Cyberstalking can be categorised as a criminal offence when there is forced interaction by the perpetrator towards the victim, causing feelings of fear and insecurity in the victim (Leli et al., 2024).

Legal protection for victims of cyberstalking currently consists of two aspects, namely the substantive aspect of law as a preventive measure and the structural aspect of law as a repressive measure. Preventive legal protection means giving legal subjects the opportunity to raise objections or opinions before the government makes a final decision. This aims to avoid disputes. Repressive legal protection is carried out after a problem has occurred. Repressive legal protection seeks to resolve problems so that the rights of every individual can be protected. For now, both of these can be seen as manifestations of the objectives of law, namely to uphold justice, certainty, order, benefit, and peace. There is a continuation of the same research discussion which states that, in general, there are two models for providing legal protection to victims of cybercrime, namely the procedural rights model and the service model. The procedural rights model explicitly gives cybercrime victims the ability to 'retaliate' against those who have harmed them by giving them the ability to report crimes, cooperate with law enforcement, and attend all trials where their testimony is required. Then, according to the service model, cybercrime victims are people who need to be served by the police and other law enforcement officers (Leli et al., 2024).

2. Efforts to Optimise Cyberstalking Regulations in Indonesia

Cases of cyberstalking have been increasing in recent times, and this phenomenon does not only occur in Indonesia but also across the world. This means that it has reached a global scope and indicates an urgent need to be addressed. As previously explained, the term "cyberstalking" actually originates from two different root words. First, "cyber," which means something that is done online using technology. Second, "stalking," which means an act such as spying on or following someone. Thus, seen from its general definition, cyberstalking is the act of spying on someone on the internet with the intention of collecting personal data, spreading threats, or committing harassment against them (Anggraini, 2022). The problem that arises in cases such as cyberstalking is that someone who is being stalked online most likely does not realize that they are being watched.

In Indonesia, the act of online stalking is regulated under the Electronic Information and Transactions Law (ITE Law). However, the issue is that the regulation stipulated in the ITE Law is still limited to the element of threat, meaning the application of criminal sanctions against cybercrime perpetrators is considered not yet optimal in creating a deterrent effect (Juharwati, 2024). Furthermore, the regulation regarding this criminal act is not yet specifically stipulated in the Criminal Code (KUHP). What makes it even more complex is the fact that this act is committed online, so often the perpetrator of online stalking is not detected by law enforcement, which of course makes it difficult to identify and apprehend the perpetrator. This is the core problem that often causes many victims to feel that they do not receive adequate protection.

Looking at the current regulation, it can be seen that the regulation regarding cyberstalking requires an action that only fulfills the elements of a crime if it is accompanied by a threat to the victim. Meanwhile, disturbing behavior or harassment has not yet received special regulation in the ITE Law (Partisya & Reza, 2024). This clearly shows a legal weakness that opens opportunities or loopholes for someone to commit cyberstalking without fear of being punished. To optimize the current regulation, in the author's view, there are two things that can be done. First, a specific law can be created that concretely regulates cyberstalking. Second, a revision can be carried out to strengthen the regulation that governs cyberstalking. More concretely, we must look at both current regulations that govern cyberstalking, namely the KUHP and the ITE Law.

Referring to the ITE Law as amended by Law No. 1 of 2024, first, in terms of the phrase “threat of violence,” the interpretation of that phrase in an electronic context still requires clearer elaboration, because it greatly depends on the situation and the perception of the individual receiving the message (Ardhianti et al., 2023). Therefore, the law must clearly regulate what types of messages qualify as threats of violence to prevent misuse in legal practice. Second, it is necessary to conduct a deeper review of the comparison between Article 27B paragraph (1) of Law 1/2024 and Article 368 of the KUHP which regulates extortion. Although both emphasize the element of threat for

personal gain, cases in the digital realm present new challenges that are not yet fully covered by the KUHP. As an old regulation, the KUHP is not necessarily relevant in handling crimes that occur in the vast and often anonymous digital world (Mathilda, 2012). Lastly, in practice, law enforcement based on the ITE Law often encounters obstacles in terms of evidence. This is because digital evidence from electronic transactions is very easy to modify or even delete (Najwa, 2024). Therefore, it is important to strengthen methods of collecting evidence and ensure the authenticity of digital data so that the law can be enforced effectively, especially in cyberstalking cases.

D. Conclusion

Legal protection for victims of cyberstalking in Indonesia currently faces a number of significant challenges. Although there are several regulations that can be used as a basis for handling cyberstalking cases, these regulations are considered to be insufficiently specific and comprehensive in their handling. For example, cyberstalking is indirectly regulated under the ITE Law, specifically Articles 27 and 29, as well as Articles 335 and 368 of the Criminal Code. While these regulations can be linked to cyberstalking, they do not explicitly refer to it, which could lead to multiple interpretations and demonstrate the ineffectiveness of protecting victims. Furthermore, cyberstalking, which is closely related to personal data, can also be linked to the Personal Data Protection Law (PDP Law), which strengthens penalties for data misuse as stated in Article 67. However, despite efforts to strengthen penalties for perpetrators, this law does not provide detailed mechanisms for protecting victims of cyberstalking.

The challenges in enforcing the law regarding victim protection stem from the anomalous nature of perpetrators and the cross-border nature of cyberstalking, which can complicate the identification and apprehension of perpetrators. Additionally, the lack of awareness regarding cyberstalking, coupled with weak technological infrastructure in digital investigations, also plays a role. In terms of victim protection, victims can only rely on the Witness and Victim Protection Act, specifically Article 5, as a form of physical and psychological protection; however, this mechanism has not been integrated into the handling of cyberstalking cases. In essence, although Indonesia has a basis for handling cyberstalking, protection for victims is still limited due to unspecified regulations and weak law enforcement. Therefore, policy revisions, increased law enforcement capacity, and increased public education are needed as preventive measures.

E. Recommendation

Based on the discussion above, it is necessary to propose several concrete steps to optimize the regulation of cyberstalking in Indonesia. First and foremost, there should be a specific law that comprehensively regulates cyberstalking, including a clear definition, forms of behavior that fall under this offense, and proportional criminal sanctions. The current legal instruments, namely the ITE Law and the Criminal Code (KUHP), should also be revised to accommodate the evolving nature of cyber crimes, particularly by

expanding the interpretation of terms such as "threat" and "harassment" in digital contexts. In addition, the capacity of law enforcement agencies must be enhanced, especially in the field of digital forensics, to ensure that cyberstalking perpetrators—who often operate anonymously—can be identified and prosecuted effectively. To support this, procedures for collecting and authenticating digital evidence must be strengthened to ensure that such evidence can be used reliably in legal proceedings. Furthermore, public awareness regarding cyberstalking should be increased through education and campaigns, empowering individuals to recognize, report, and protect themselves from online threats. Finally, there must be structured support mechanisms for victims, including psychological assistance and accessible legal aid, so that victims of cyberstalking receive proper protection and justice.

F. Acknowledgments

We would like to express our deepest gratitude to our lecturer for their invaluable guidance, encouragement, and insightful feedback throughout the completion of this group project. The expertise and support provided have been instrumental in shaping the direction and depth of our research on "Optimizing Legal Regulations for the Protection of Cyberstalking Victims in Indonesia." Expressions of gratitude are extended to all members of the group for their dedication, collaboration, and commitment, which were instrumental in the success of this journal. In addition, the authors whose works have been cited in this journal are to be sincerely thanked; their valuable research and insights have significantly enriched the study.

Bibliography

Anggraini, H. (2022). *Cyberstalking: Pengertian, dampak, & bantuan yang dibutuhkan*. DW Indonesia. https://www.dw.com/id/cyberstalking-pengertian-dampak-bantuan-yang-dibutuhkan/a-63423233

Ardhianti, M., Prawoto, E. C., Pujiastuti, R., & Risaldi, A. (2023). *Semiotika kritis pendekatan dalam teks kejahatan siber*. Purwokerto: Pena Persada Kerta Utama.

Cindy, et al. (2025). *Kejahatan Cyberstalking Dalam Perspektif Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik*. Lex Administratum, 13(1).

Hera. (2024). *Strategi Pencegahan Cyberstalking dan Upaya Perlindungan Hukum.* Jurnal BATAVIA, 1(3).

Juharwati. (2024). Jerat hukum pelaku cyberstalking dalam UU ITE 2024 dan KUHP (KUHP saat ini dan masa mendatang/ UU 1/2023). *Selisik: Jurnal Hukum dan Sosial*, 10(1), 124–142.

Ketut. (2025). *Cyberstalking sebagai Kejahatan Multidimensional. Jurnal Hukum, Administrasi Publik dan Negara,* 2(3). https://doi.org/10.62383/hukum.v2i3.273.

Leli, et al. (2024). Legal Protection for Victims of Cyberstalking According to Indonesia's Law. International Journal of Social and Human Research, 7(6). https://doi.org/10.47191/ijsshr/v7-i06-23.

Mathilda, F. (2012). Cyber crime dalam sistem hukum Indonesia. *Sigma-Mu*, 4(2), 43–53.

Najwa, F. R. (2024). Analisis hukum terhadap tantangan keamanan siber: Studi kasus penegakan hukum siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, 2(1), 13–25.

Nabih, et al. (2024). Cyberstalking Crime and Application of Criminal Law in Indonesia. Journal of Law Science, 6(1).

Nadya, et al. (2024). Cyberstalking Among Adolescents: Looking at Responses, PrivacyConsequences, and Prevention Strategies. Dicoment, 1(1). https://orcid.org/0000-0002-3472-140X.

Partisya, R. (2024). *Pertanggungjawaban pelaku cyberstalking sebagai perbuatan melawan hukum pidana Indonesia* (Tesis Magister Ilmu Hukum, Universitas Jambi).

Regita & Hudi Yusuf. (2024). *Pencurian Data Pribadi Di Internet Dari Sudut Pandang Kriminologi*. JICN, 1(2).

Rerepih & Ratri Pratiwi. (2024). The Indonesian Cyberstalking Scale: Adaptation and Psychometric Properties. ICoP.

Umi, et al. (2024). Legal Safeguards For Victims of Data Dissemination Crimes and Cybercrime Protection. *Jurnal Hukum Fakultas Hukum Unissula,* 40(2). http://dx.doi.org/10.26532/jh.v40i2.39974.

Wan, et al. (2021). Non-Criminalisation of Cyberstalking and Its Impact on Justice for Victims: Some Evidence from Malaysia. INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS AND SOCIAL SCIENCES, 11(6).

Yan, et al. (2024). *Cyberstalking sebagai Perbuatan Melawan Hukum dalam Hukum Pidana Indonesia.* Halu Oleo Legal Research, 6(1).

Laws and Regulations

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Republik Indonesia, Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 1 tahun 2023 Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842.

Republik Indonesia, Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 1 tahun 2024 Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

Republik Indonesia, Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Undang-Undang Nomor 19 tahun 2016 Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Republik Indonesia, Perubahan atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban, Undang-Undang Nomor 31 tahun 2014 Lembaran Negara Republik Indonesia Tahun 2014 Nomor 293, Tambahan Lembaran Negara Republik Indonesia Nomor 5602.

Republik Indonesia, Undang-Undang Pelindungan Data Pribadi, Undang-Undang Nomor 27 tahun 2022 Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.