

Legal Vacuity Regarding Legal Protection for Victims of Criminal Acts of Defamation in Electronic Media

Wieke Dewi Suryandari

Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia

wieke@undaris.ac.id

Address: Jl. Tentara Pelajar, Paren, Sidomulyo, Ungaran Tim. District, Semarang Regency, Central Java 50519

Author correspondence: wieke@undaris.ac.id

Abstract. *This study aims to analyze the legal gap in legal protection for victims of criminal acts of defamation in electronic media and the challenges and efforts to protect them. Although the Electronic Information and Transactions Law (UU ITE) has regulated criminal acts of libel, there is still a legal gap in terms of victim protection, especially in enforcing victims' rights and resolving cases through clear legal mechanisms. This study uses a normative legal research method with a legislative approach and a conceptual approach to explore existing legal regulations and analyze the challenges in their implementation practices. The study results indicate that the lack of clarity in the definition and application of the law between the Criminal Code and the ITE Law confuses perpetrators and victims in accessing justice. Therefore, this study proposes the need for legal harmonization, as well as strengthening the legal protection mechanism for victims through clearer regulations and consistent application.*

Keywords: *Legal gap, legal protection, criminal acts of defamation, electronic media*

1 INTRODUCTION

We live in an information age, where significant changes in various aspects of life, such as social, political, economic, spatial, and cultural, occur as a result of advancements in information technology. [1] This technology has created a high-tech industry that fundamentally alters how humans communicate and interact. Generally, information technology encompasses tools used for storing, processing, distributing, or generating information. The data or information managed through this technology is highly diverse, without limitations on specific types or formats. Information technology operates based on fundamental principles that process data into usable information across various life aspects [2]. From message exchange through social media to the emergence of more sophisticated technological innovations, its application has become an integral part of modern life, highlighting the central role of technology in shaping new communication patterns in society.

The development of information technology also significantly impacts social attitudes and public expectations regarding information. Nowadays, people not only expect easy access to information but also demand more transparent and relevant information for decision-making in various life aspects [3]. This change creates a growing need for obtaining accurate data about specific products, services, or organizations, enabling people to make more precise and strategic decisions in their interactions. [4] The presence of smartphones not only simplifies

internet access but also offers a wider range of communication facilities, such as chatting services, emails, SMS, MMS, browsing, and social media. With these features, communication becomes more practical and faster, allowing individuals to interact anytime and anywhere without the constraints of space and time. [5] This technology also expands the reach of communication in unprecedented ways.

Social media, as one of the internet-based innovations, provides a platform for individuals to represent themselves, share information, and form social relationships virtually. Social media is not limited to personal communication; it enables large-scale collaboration for business, education, and other social activities. Through social media, people can connect with others from various parts of the world, expanding networks and creating new social bonds. Thus, technology has transformed communication patterns to be faster, more efficient, and broader, supporting the needs of the increasingly dynamic and connected modern society. [6] However, this convenience also brings risks, where users can become entangled in criminal activities conducted through social media. As times change, methods for committing crimes have also evolved, utilizing platforms like Twitter, Facebook, Instagram, YouTube, and email. The use of the Internet has become an inseparable part of daily human activities, whether in national or international business, governmental affairs, or personal life. Although it offers various benefits, this transformation presents new challenges, including the potential misuse of technology for unlawful activities. [7]

The internet has had a profound impact on the global community through the concept of the Global Village, where individuals can connect without the limitations of space and time. However, social media also has the potential to become a tool for crime as offenses continue to evolve alongside societal dynamics. [8] The advancement of information technology has increased both the number and types of crimes, including cybercrimes that differ from conventional offenses. These crimes require a specific legal approach regarding substance, culture, and procedures. For this reason, Law Number 19 of 2016 was enacted as a revision of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), aimed at addressing technology-based crimes more effectively. One negative impact of this technological development is the occurrence of defamation, which is categorized in the Penal Code into several types, such as slander, defamation, light insults, defamatory complaints, and false presumptions. [9] However, the ITE Law consolidates all forms of insult and defamation into one criminal act under Article 27, paragraph (3), without differentiating based on object, type, or the severity of penalties. This article also does not include essential requirements such

as proof of truth for public interest and removes the complaint requirement, which was previously a crucial element in defamation offenses. [10]

Furthermore, the vagueness in defining what constitutes defamation creates legal uncertainty and opens the possibility for arbitrary actions by law enforcement or others in interpreting these provisions. It indicates that the ITE Law often fails to adequately accommodate protections for victims, especially in the digital era where technology evolves far more rapidly than regulation. This legal gap becomes a serious challenge that must be addressed to create an adaptive legal system that fairly protects the rights of all parties. Therefore, based on this brief overview, this study will discuss the legal vacuum regarding the legal protection of victims of defamation in electronic media. Additionally, this research will analyze the challenges and efforts for the legal protection of defamation victims in electronic media.

2 METHOD

The normative legal research method is a method used in legal studies that focuses on the analysis of documents and legal norms. This method aims to analyze applicable legal rules and how these rules are implemented or interpreted within a specific framework. In normative legal research, the primary sources used are statutes and other legal literature. This approach is particularly relevant when investigating theoretical and conceptual legal issues, such as discussing the legal vacuum concerning the protection of victims of defamation in electronic media. Additionally, in this study, the author will analyze the challenges and efforts for the legal protection of defamation victims in electronic media. One of the approaches used in this method is the statute approach and the conceptual approach. [11] The statute approach involves examining and analyzing various regulations governing specific issues, such as the Republic of Indonesia Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions and related regulations. Through this approach, researchers can discuss the legal vacuum related to the protection of victims of defamation in electronic media, as well as analyze the challenges and efforts for the legal protection of these victims.

3 RESULT AND DISCUSSION

Legal Vacuity Regarding Legal Protection for Victims of Criminal Acts of Defamation in Electronic Media

Legal protection in Indonesia is manifested through various laws and regulations encompassing different categories, such as civil legal protection, consumer protection, child protection, and protection against defamation through electronic media. Defamation, also commonly referred to as slander, essentially constitutes an act that attacks an individual's good name and honor outside the sexual context, causing harm to the individual. Good name and honor have different meanings but are interconnected, where attacking one can tarnish both. Therefore, actions targeting good name or honor are sufficient to fulfill the elements of slander according to the law. However, Indonesia lacks a specific law that explicitly regulates defamation. The handling of such cases thus far refers to the provisions of Articles 310 to 321 of the Criminal Code (KUHP) and Article 27, paragraph (3) of Law No. 19 of 2016 regarding Amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law). These legal instruments serve as a basis for prosecuting offenders of slander or defamation, but they do not provide comprehensive protection. The absence of specific regulations poses a challenge in delivering a legal system capable of addressing the complexities of slander in the digital era.

With technological advancements, defamation has become increasingly prevalent in society, especially through various electronic media. This global development is known as defamation, referring to behaviors that harm an individual's reputation through false statements. Such actions are simple to execute, spread quickly, and can have profound effects, including the ability to shape public opinion in a way that is harmful to the victim. Social media and various online platforms facilitate the easy commission of slander, highlighting the need for more adaptive and targeted regulations to embark this issue.

In Article 27, paragraph (3) of the ITE Law, the definitions of slander and defamation are not explicitly stated; however, it can be systematically concluded that defamation refers to the definitions in Article 310, paragraph (1) of the KUHP, which relates to defamation and slander. This article states that anyone who intentionally distributes, transmits, or creates electronic information containing slander or defamation can face a prison sentence of up to six years and/or a fine of up to IDR 1 billion. This indicates that Article 27, paragraph (3) of the ITE Law refers to the same provisions governed by the KUHP, making it a part of the broader Indonesian criminal law system.

In practice, Article 27, paragraph (3) of the ITE Law may create a legal vacuum, particularly due to the lack of detailed explanations regarding what constitutes slander or defamation conducted via electronic media. Although this article refers to articles within the KUHP, which provide clearer definitions regarding defamation, criminal law in cyberspace has its own complexities. This vagueness can lead to confusion in legal practice, where law enforcement must determine whether certain electronic information defames someone, which often relies on subjective interpretation, raising questions about whether the information violates prevailing social norms.

Furthermore, to enforce Article 27, paragraph (3), there are two crucial elements that law enforcement must prove: subjective and objective elements. The subjective element relates to the intent of the perpetrator, whether the act of distributing or transmitting such electronic information was indeed intended to slander or defame. However, the objective element must also be examined, determining whether the disseminated information genuinely contains slanderous content and whether it contradicts prevailing social norms in society. This process not only requires evidence of facts but also assessments of existing social values, which are often subjective and susceptible to abuse. It can lead to Article 27, paragraph (3) being used as a tool to suppress freedom of expression, thereby posing challenges in ensuring fair and impartial legal protection.

Regarding the Constitutional Court ruling No. 2/PUU-VII/2009, Article 27, paragraph (3) of the ITE Law cannot fundamentally be regarded as a violation of the rights of individual citizens, as human rights (HAM) themselves must be understood as respecting the rights of others. Thus, in exercising their rights, every citizen has an obligation not to infringe upon the rights of others, thereby creating a balance in the implementation and respect for human rights. When the state limits individual rights through criminal law, it does not automatically reject democratic values. True democracy must be practiced with attention to humanitarian values; otherwise, the quality of democracy itself will decline. The Indonesian Constitution guarantees protection for individual rights, such as the right to dignity, honor, and security, as well as the right to be free from threats.

However, although Article 27, paragraph (3) of the ITE Law serves as a legal foundation for addressing defamation in cyberspace, petitioners argue that this article contradicts the right to freedom of expression guaranteed by the 1945 Constitution, specifically Article 28E, paragraph (3), which governs the right to express opinions. Freedom of expression, whether orally, in writing, or through various media, is a broad human right that encompasses the right to seek, receive, and disseminate information. However, this freedom is not absolute and must

be limited by other legal norms to protect the rights of others. Therefore, although freedom of expression is a constitutional right, its application must consider the principle of caution so as not to harm or violate the rights of others, especially concerning personal honor and reputation.

Article 27, paragraph (3) of the ITE Law is not intended to be a repressive tool that limits freedom of expression, speech, or the expression of opinions, but rather as an effort to ensure that this freedom does not exceed its bounds and lead to abuses that can cause harm to others. Freedom of expression must be understood within the principle of balance, where an individual's right to express opinions must not harm others or create unrestrained power that can disrupt social order. Article 27, paragraph (3) aims to ensure that this freedom does not violate legal norms and is not used as a means to harm or destroy an individual's reputation through the dissemination of false information.

The characteristics of electronic media, or cyberspace, underscore the necessity of Article 27, paragraph (3) of the ITE Law. Firstly, information in cyberspace can be easily uploaded and disseminated with just the push of a button, making it widely accessible to a broad audience compared to traditional media. Secondly, this information can spread rapidly and extensively, transcending national borders without the burden of additional costs like purchases or subscriptions. Lastly, the potential harm caused by defamatory content in electronic media is significant, given its ability to reach numerous individuals in a short time and across various locations, far surpassing the impact of conventional media, which is typically confined to specific audiences or regions. However, even though Article 27, paragraph (3) has legitimate purposes, its application must be conducted carefully and selectively. Law enforcement agencies must ensure that the two critical subjective and objective elements are clearly proven before taking legal action. Moreover, the malicious intent of the perpetrator must also be considered. Merely proving the subjective element is insufficient to prosecute the perpetrator, as this may potentially be misused to suppress freedom of opinion. The criminal sanctions imposed serve to protect individuals from defamation, but if applied without proper consideration, they can threaten individual freedoms. Thus, criminal law in this context must be used wisely to remain a protective tool, not a means of repression.

The ambiguity of the boundaries of slander and defamation in Article 27, paragraph (3) of the ITE Law is one significant obstacle to its implementation. Although this article refers to provisions in the KUHP concerning slander and defamation, there is no clear explanation regarding the definition and scope of slander in electronic media. Lack of precision in formulating these boundaries results in differing interpretations among law enforcement officials, often leading to subjective and inconsistent decisions. In practice, it is frequently

challenging to distinguish between the legitimate expression of opinions and actions that can be categorized as slander or defamation, creating legal uncertainty for individuals and legal practitioners involved. It establishes space for abuse of this article that could restrict freedom of expression.

The dualism of interpretation between the KUHP and the ITE Law is also one of the main obstacles to implementing Article 27, paragraph (3) of the ITE Law. On the one hand, KUHP provides a clearer definition of slander and defamation, while the ITE Law focuses more on the digital context without detailing the elements that constitute these offenses. This difference creates uncertainty in legal practice due to the absence of clear consensus between the applicable articles in these two regulations. Law enforcement officials referring to either of these laws may find themselves confused when identifying and proving cases of defamation, particularly those occurring on social media and in cyberspace, which require a more specific and adaptive legal approach. This uncertainty can harm both victims and perpetrators, who may become ensnared in legal interpretations that do not align with the context of electronic media.

Legal protection for victims of defamation through electronic media can be divided into two main aspects: preventive protection and repressive protection. Preventive protection focuses on efforts to prevent defamation from occurring early on. One primary challenge in this aspect is the lack of public understanding regarding the responsible and wise use of technology. Low digital literacy leads to abuse of social media and other online platforms, which are often used to disseminate information that can harm an individual's reputation. To tackle this challenge, systematic efforts must be made to enhance public understanding of ethical communication in cyberspace, including recognizing and avoiding the spread of hoaxes, hate speech, or false information that can damage someone's good name.

On the other hand, repressive protection relates to law enforcement against perpetrators of defamation who have harmed victims. The main challenge in this aspect is the difficulty in proving the necessary elements for the crime of defamation, especially in an anonymous internet environment. Perpetrators who spread harmful information often utilize platforms that allow them to remain anonymous, making it challenging for law enforcement to trace their identities and impose appropriate sanctions. It can hinder the enforcement of justice and create a sense of injustice for the victims.

Challenges and Efforts for Legal Protection for Victims of Defamation in Electronic Media

Defamation through electronic media has emerged as an increasingly pressing legal issue in the digital era. With the advancement of information and communication technology, false information that harms someone's reputation can occur swiftly and broadly, making its impact significantly more profound than traditional media. Social media, online platforms, and instant messaging applications facilitate perpetrators in spreading hate speech or defamatory information with minimal barriers. On the other hand, victims of online defamation often face challenges in obtaining adequate protection, both in terms of prevention and law enforcement.

Legal protection for victims of online defamation encompasses two main aspects: preventive and repressive protection. The preventive aspect focuses on educational efforts and enhancing the digital literacy of the public to use electronic media responsibly, as well as strengthening regulations to ensure a clear legal foundation for addressing such cases. Conversely, the repressive aspect involves legal actions against offenders who commit defamation, which are often hindered by various challenges such as the anonymity of perpetrators, difficulties in proving allegations, and the rapid spread of information that complicates the retrieval of digital footprints that have already circulated.

To address these challenges, various efforts are needed to strengthen the legal protection system for victims of defamation. These efforts should involve not only strict law enforcement but also adjustments to regulations that are more responsive to technological advancements, along with the implementation of fair and proportional sanctions. Only through a holistic approach and collaboration among various parties—government, society, and providers of electronic media platforms—can effective legal protection for victims of online defamation be achieved.

One of the biggest challenges in handling online defamation cases is the anonymity provided by the digital world. Many perpetrators can easily conceal their identities behind pseudonyms or fake accounts, making it difficult for law enforcement to track and effectively address them. This anonymity gives perpetrators a sense of security to commit defamation without fear of legal consequences or social sanctions. Even with clear evidence, identifying and bringing perpetrators to court often faces significant technical obstacles. It leaves victims to bear substantial reputational harm while perpetrators remain free from appropriate punishment. Solutions to this challenge require increased cooperation between electronic media platform providers and authorities to facilitate more transparent and accurate identification of cybercriminals.

Electronic media, particularly the Internet and social media platforms, exhibit characteristics of rapid and extensive information dissemination. Once negative or defamatory information is spread—intentionally or otherwise—it can reach thousands or even millions of people in a short time, crossing geographical boundaries and being untethered by time constraints. Even if the information is later deleted, the already widespread digital footprint is often difficult to erase. This makes it problematic for victims of online defamation to mitigate its negative impact. A tarnished reputation in the digital space is difficult to restore, even if the harmful content is no longer publicly available. The speed and extent of this dissemination pose a significant challenge in addressing defamation cases, as their effects are much broader and longer-lasting compared to traditional media.

A significant factor exacerbating the issue of online defamation is the low level of digital literacy among the public. Many individuals do not fully understand how to use electronic media and the internet wisely and responsibly. Ignorance regarding the legal consequences of spreading false information often drives individuals to engage in actions that could harm others, unaware of the legal consequences they could incur. Furthermore, a lack of understanding of ethical communication in the digital realm leads to widespread dissemination of hate speech, slander, or false information that damages the reputation of individuals or groups. Therefore, enhancing digital literacy is crucial in raising public awareness about the importance of responsibility when using electronic media platforms, so individuals do not unintentionally engage in unlawful actions that harm others.

Although Indonesia has enacted the ITE Law to address defamation cases, uncertainties in the law hinder effective law enforcement. One of the primary obstacles is the lack of clarity in the interpretation and application of this law, particularly concerning the subjective and objective elements of online defamation. The difficulty of proving cases—especially when available evidence is limited to hard-to-trace digital footprints—renders the legal process ineffective. This ambiguity in regulations also opens opportunities for legal abuse, which can result in injustice for both victims and offenders. Thus, updates and refinements to existing regulations are necessary to make the law more responsive and adaptive to technological developments, ensuring better protection for victims.

Another complex challenge in defamation cases in electronic media is the differing perspectives on freedom of expression and the protection of an individual's reputation. On one hand, freedom of speech is regarded as a fundamental right guaranteed by the Constitution, allowing individuals to express their opinions without fear of retaliation. On the other hand, the right to protect one's reputation is also recognized as equally important, as defamation can

have detrimental social and economic effects on victims. When these two rights intersect, conflicts often arise between freedom of expression and the need to protect individuals from the spread of false information. This divergence of views poses challenges in law enforcement, as there is often no agreement on how far freedom of expression can be limited without violating broader constitutional rights.

Consequently, a crucial preventive effort in the legal protection of victims of online defamation is enhancing digital literacy within the community. With rapid technological advancements, the public needs to be equipped with a better understanding of ethics and responsibilities in communicating in the digital space. This education can be conducted through various channels, such as public campaigns, school training programs, and social initiatives that emphasize the importance of responsible social media use. The goal is to raise awareness that the irresponsible dissemination of information can damage someone's reputation and potentially violate the law. By increasing digital literacy, it is hoped that society will be more cautious and think twice before spreading information that may defame others, thereby reducing the incidence of online defamation.

To effectively tackle the challenges surrounding legal protection for defamation victims, it is crucial to strengthen the current regulations. This can be achieved by updating the ITE Law to better align with the rapid technology advancement. The regulation should be adjusted to the increasingly complex dynamics of cyberspace, such as the evolution of social media, digital platforms, and new forms of electronic communication that can affect individual reputations. Current regulations need to be more detailed and clear in governing online defamation, clarifying definitions, evidentiary processes, and sanctions for offenders. Furthermore, strengthening the implementation of these regulations is also necessary to ensure consistent law application, reduce ambiguity in law enforcement, and provide a sense of security to victims harmed by online defamation.

Law enforcement against online defamation cases can also be enhanced by leveraging technological advancements. The digital forensic tools and tracking technology can assist law enforcement in identifying perpetrators who commit defamation online. Collaboration with digital platform providers such as social media, internet service providers, and technology companies can be a strategic step in uncovering the identities of perpetrators often hidden behind anonymity. Forensic technology can be utilized to verify digital footprints, communication records, and other evidence that can aid in investigations. By applying technology in law enforcement, perpetrators of defamation can be more easily found, thereby

creating a deterrent effect and reducing the misuse of electronic media for damaging others' reputations.

Repressive efforts in providing legal protection for defamation victims must involve the application of fair and proportional sanctions. Law enforcement should consider various aspects in each case, such as the malicious intent behind the perpetrator's actions, the impact on the victim, and the context in which the defamation occurred. It is essential to ensure that the imposed sanctions are not merely punitive but also consider the freedom of expression rights guaranteed by the Constitution. Therefore, the sanctions given should be proportional to the losses experienced by the victim and not excessive, acknowledging that freedom of expression in the online sphere is also a right that must be protected. By establishing transparent, decisive, and equitable sanctions, the aim is to foster a deterrent impact that discourages wrongdoers from engaging in similar behavior in the future while offering a sense of justice for those affected.

4 CONCLUSION

Legal protection against defamation in Indonesia, particularly in electronic media, faces significant challenges due to the absence of specific laws governing this issue. While Articles 310 to 321 of the Criminal Code (KUHP) and Article 27, paragraph (3) of the ITE Law provide a legal foundation, the lack of clear and specific definitions of defamation in the digital realm complicates the fair and transparent application of the law. Although Article 27, paragraph (3) of the ITE Law aims to protect individual reputation, it also has the potential to restrict freedom of expression if applied carelessly, given the subjective and objective elements that must be precisely proven. In the digital age, the rapid and extensive dissemination of harmful information underscores the urgent need for more adaptive and specific regulations to address the complexities of this issue. Legal protection can be divided into two aspects: preventive and repressive; the preventive aspect focuses on enhancing digital literacy to avoid misuse of social media, while the repressive aspect requires stringent law enforcement against offenders who use anonymity to tarnish others' reputations. However, despite efforts to safeguard individual rights to honor and dignity, challenges such as difficulties in proving violations and unclear definitions in regulations persist, requiring legal reforms to provide more effective and comprehensive protection.

A comprehensive approach to legal protection for victims of online defamation is essential, encompassing both preventive and repressive aspects. Preventive measures, such as enhancing digital literacy and educating the public on ethical communication in the digital

realm, are essential to curbing the spread of harmful information. At the same time, it is crucial to strengthen regulations, including updating the ITE Law, to ensure they are responsive to ongoing technological advancements. Effective law enforcement can be achieved by utilizing technology, such as digital forensic tools, and collaborating with platform providers to identify perpetrators who often operate under the veil of anonymity. Lastly, implementing fair and proportional sanctions is vital for creating a deterrent effect while respecting the right to freedom of expression. Therefore, legal protection for victims of defamation in electronic media can be made more effective, just, and reassuring for society.

REFERENCES

- A. A. Fauz, *Pemanfaatan Teknologi Informasi Di Berbagai Sektor Pada Masa Society 5.0*, Jambi: Sonpedia Publishing Indonesia, 2023.
- A. Ahmad, "Perkembangan Teknologi Komunikasi dan Informasi: Akar Revolusi dan Berbagai Standarnya," *Jurnal Dakwah Tablig*, vol. 13, no. 1, 2012
- B. Warsita, "Landasan Teori Dan Teknologi Informasi," *Jurnal Teknodik*, vol. 15, no. 1, pp. 84-96, 2011.
- D. Sarkawi, "Perubahan Sosial dan Budaya Akibat Media Sosial," *Jurnal Administrasi Kantor*, vol. 4, no. 2, pp. 307-338, 2016.
- N. A. Shidiqie and dkk, "Perubahan Sosial dan Pengaruh Media Sosial Tentang Peran Instagram dalam Membentuk Identitas Diri Remaja," *SIMPATI: Jurnal Penelitian Pendidikan dan Bahasa*, vol. 1, no. 3, pp. 98-112, 2023.
- N. N. Fauziah, S. A. Saputri and Y. T. Herlambang, "Teknologi Informasi: Dampak Media Sosial pada Perubahan Sosial Masyarakat," *Indo-MathEdu Intellectuals Journal*, vol. 5, no. 1, pp. 757-766, 2024.
- P. M. Marzuki, *Penelitian Hukum*, Jakarta: Kencana Prenada Media Group, 2006
- R. P. A. D. Ngiji, S. Suseno and B. A. Atmaja, "Penerapan Pasal 27 Ayat (3) Undang-Undang ITE Dalam Perkara Pencemaran Nama Baik Melalui Media Sosial Terhadap Kelompok Orang," *Jurnal Fundamental Justice*, vol. 3, no. 3, 2022
- Raharjo, *Cyber Crime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: PT Citra Aditya Bakti, 2002
- Rusman and F. M. S, "Tindakan pencemaran Nama Baik dan Penghinaan Melalui media Elektronik," *Jurnal Hukum Mimbar Justitia*, vol. 7, no. 2, 2021
- Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime*, Malang: Media Nusa Creative, 2018