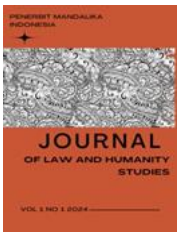

Vol 2 No 2, 2025 || E-ISSN 3032-6796 P-ISSSN 3032-4297

Journal of Law and Humanity Studies

Journal homepage:
https://journal.mediamandalika.com/index.php/jlhs

A Juridical Review of Cybercrime and Defamation under Indonesia's Law No. 1 of 2024 on Electronic Information and Transactions

Adi Darmawansyah[1], Andry Dwiarnanto[2], Irwan Putra Satriyawan[3], Istiqomah[4]
Universitas Bung Karno, Indonesia [1,2,3,4]
Email: andrydwiarnanto@yahoo.com

KEYWORDS

Cybercrime, Criminal Act ITE.

ABSTRACT

Along with technological advances, social changes will also be affected, one of which is crime in cyber crime. Existing society will always coexist with cyberspace and there are even criminal law problems in it (cybercrime). The research analyzes the provisions of criminal acts of defamation through cybercrime which are according to the provisions of positive law in Indonesia. And how the law can accommodate the position of evidence in cyberspace. Normative juridical research specifically discusses regulations in accordance with Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. Defamation in cyber crimes is regulated in the Criminal Code Articles 310 to 321 and is also regulated in Law Number 1 of 2024, Second Amendment to Law Number I1 of 2008 concerning Information and Electronic Transactions Article 27A and Article 27 B paragraph (2) Jo. Article45. The newNational Criminal Code(KUHP) also regulates provisions for defamation in relation to cybercrime. Proof of criminal acts of information and electronic transactions based on Law Number 1 of 2024, Second Amendment to Law Number I1 of 2008 Regarding ITE, it is based on valid evidence as regulated in Article 184 of the Criminal Procedure Code.

1. Introduction

The enactment of Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (the ITE Law) marks a significant development in the regulation of legal conduct related to the use of the internet. This legislation governs various forms of actions carried out through electronic media, including the imposition of criminal sanctions for violations of its provisions. One of the central issues regulated under this law is the criminalization of defamation committed through social media platforms, along with several legal breakthroughs involving the expansion of criminal law principles, evidentiary rules, and sanction mechanisms.

The amended ITE Law does not only regulate substantive criminal provisions but also introduces procedural aspects, particularly concerning the development and expansion of admissible evidence. A notable advancement is the formal recognition of electronic evidence as a legitimate means of proof in criminal proceedings. This development reflects the law's adaptive response to technological advancements and the increasing prevalence of digital-based criminal acts.

In practice, cases involving violations of electronic information and transactions are frequently prosecuted under Article 45 paragraph (1) in conjunction with Article 27 of the ITE Law. These provisions criminalize acts of defamation conducted through electronic media, emphasizing the importance of legal certainty in addressing cyber-based offenses. However, the law also acknowledges limitations to criminal liability. In relation to Article 310 paragraph (3) of the Indonesian Criminal Code, certain acts are exempted from being categorized as defamation if they are clearly carried out in the public interest or constitute legitimate self-defense.

With the implementation of Law Number 1 of 2024, the ITE Law is expected to function as a legal safeguard for society, balancing the protection of individual reputation with freedom of expression while ensuring accountability in the digital space. This legal framework aims to provide clearer boundaries and stronger legal certainty in addressing

cybercrime, particularly defamation offenses in electronic media.

Based on the foregoing discussion, this study limits its scope to the following legal issues in order to ensure a focused and systematic analysis. First, how is the regulation of the criminal offense of defamation structured under Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions? Second, what is the legal standing and evidentiary value of digital evidence in proving defamation offenses under the same legal framework?

2. Method

The scientific method in a discipline constitutes all systematic approaches employed to achieve a coherent body of knowledge. Without a scientific method, a field of knowledge cannot be regarded as a science, but merely as a collection of fragmented observations lacking an understanding of the interrelationships among phenomena. Therefore, a methodical approach is essential to ensure analytical coherence and academic validity in legal research.

This study employs legal research at the theoretical level, which is necessary for the development of a particular field of legal studies. Such research is intended to enhance and enrich legal knowledge, particularly in relation to the application of legal norms. Through an in-depth examination of criminal sanctions, this research also seeks to explore the underlying legal theories that form the basis of statutory provisions governing defamation in electronic media.

The research method applied in this study is normative legal research. Normative legal research focuses on examining the application of legal norms and principles within positive law. It emphasizes the analysis of statutory regulations, legal doctrines, and judicial concepts rather than empirical data. This approach is appropriate because the study aims to analyze the legal framework governing cybercrime, particularly defamation offenses, as regulated under Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions.

Normative legal research relies on secondary data sources obtained through library research. These data consist of primary legal materials, such as legislation and official legal documents; secondary legal materials, including legal textbooks, scholarly journals, and expert opinions; and tertiary legal materials, such as legal dictionaries and electronic resources accessed via the internet. This method enables a comprehensive and systematic analysis of existing legal norms and their theoretical foundations.

3. Result and Discussion

3.1. Regulation of the Criminal Offense of Defamation under Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions

The plenary meeting of the House of Representatives of the Republic of Indonesia (DPR RI) held on 5 December 2023 approved the Bill on the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), thereby formally enacting it into law. Since February 2023, the Government had initiated preparations for the second amendment to the ITE Law. This amendment was broadly welcomed by the public, particularly because it was intended to respond to public concerns regarding legal uncertainty arising from the application of the ITE Law.

The second amendment became the subject of intense public attention when it was revealed that the revised regulation did not repeal provisions that had long been considered controversial, including Article 27 paragraph (3) concerning defamation. The multi-interpretative nature of this article has been widely regarded as one of the main causes of legal uncertainty in the implementation of the ITE Law. The retention of this provision in the second amendment recalls the first amendment to the ITE Law, during which calls for the abolition of Article 27 paragraph (3) were also strongly voiced. Nevertheless, the provision was maintained. At that time, the Minister of Communication and Information stated that Article 27 paragraph (3) of the ITE Law could not be removed because its abolition could eliminate the deterrent effect of the law.

In 2016, Law Number 19 of 2016 concerning the Amendment to the ITE Law was enacted and promulgated. This amendment was designed as a solution to problems arising from the implementation of the ITE Law. One of the significant changes introduced was the clarification that criminal acts of insult and defamation in the field of electronic information and electronic transactions constitute complaint-based offenses (delik aduan). In addition, in order to provide legal certainty to the public, the amendment sought to harmonize the ITE Law with Indonesia's substantive criminal law system through the addition of explanatory provisions to Article 27 paragraphs (1), (3), and (4). However, the repeal of Article 27 paragraph (3) was ultimately not carried out. Following the enactment of the first amendment, instead of providing legal certainty, the number of victims prosecuted under the ITE Law

continued to increase. Amnesty International Indonesia recorded 332 victims whose freedom of expression was violated between January 2019 and May 2022.

The approval of the second amendment to the ITE Law was therefore expected to bring renewed optimism. The amendment of fourteen articles and the addition of five new provisions were believed to enhance legal certainty. One of the main sources of legal uncertainty arising from the multi-interpretative application of the ITE Law, particularly Article 27 paragraph (3), relates to limitations on the right to freedom of expression. The existence of this right within the framework of the ITE Law has thus become an important issue for analysis.

UNESCO has stated that, to date, approximately 80 percent of countries worldwide still impose criminal sanctions for defamation. Nevertheless, several countries have undertaken decriminalization of defamation offenses due to concerns that such criminalization poses a risk to the protection of freedom of expression. Through the ITE Law, Indonesia remains one of the countries that criminalizes defamation. In 2021, Indonesia came under scrutiny by the Office of the United Nations High Commissioner for Human Rights (OHCHR), which, through an official press release, urged Indonesia to halt the criminalization of freedom of expression. This raises an important question regarding how legal certainty and the protection of freedom of expression can be guaranteed under the second amendment to the ITE Law.

Several provisions of the ITE Law will operate concurrently with the new Criminal Code (KUHP), which is scheduled to take effect on 1 January 2026. However, certain provisions of the ITE Law will be repealed upon the implementation of the new KUHP. Some norms in the revised ITE Law represent an adoption of provisions contained in the new KUHP while also providing more detailed explanations than those found in the previous version of the ITE Law. The Director General of Informatics Applications at the Ministry of Communication and Information Technology cited Article 27A as an example of such normative changes. Article 27A stipulates that "Any person who intentionally attacks the honor or reputation of another person by making an allegation with the intent that such allegation be known to the public in the form of Electronic Information and/or Electronic Documents through an Electronic System" commits a criminal offense. The creation of Article 27A reflects the reclassification of defamation provisions, which will later be repealed upon the full implementation of the new KUHP.

The amendment also introduced changes to normative formulations, including the addition of phrases such as "broadcasting" and "displaying," which were adopted from definitions contained in the Criminal Code. In the previous version of the ITE Law, these terms were not comprehensively explained, leading to ambiguity. The revised ITE Law provides clearer definitions of actions such as broadcasting, distributing, and transmitting electronic information in order to prevent multiple interpretations.

Meanwhile, Article 27 paragraph (2) did not undergo substantive changes; however, additional explanations were included, adopting provisions from the new Criminal Code. This regulation refers to gambling offenses as regulated in the KUHP, including acts of offering or providing opportunities for gambling, making gambling a livelihood, and participating in gambling activities.

Changes were also made to the former Article 27 paragraph (3) of the ITE Law, which was restructured as Article 27A in the Second Amendment. This restructuring was carried out to align the grouping of offenses with the classification used in the new KUHP. Article 27A of the revised ITE Law regulates defamation as an offense distinct from morality-related and gambling-related offenses, thereby clarifying the categorization of criminal acts.

The Second Amendment to the ITE Law introduced several significant changes and additions, including provisions on foreign electronic certification, child protection in electronic systems, restructuring of defamation and coercion offenses, regulation of hate speech, removal of certain provisions on illegal access, changes to penalty enhancement provisions, government intervention in electronic systems, closure of social media accounts by investigators, and revised criminal sanctions for morality and defamation offenses, including exemptions for acts committed in the public interest or for self-defense.

Historically, regulations on insult and defamation in Indonesia were first introduced through the Criminal Code (KUHP) and the Civil Code, both inherited from the Dutch colonial legal system. The Criminal Code regulates insults, slander, and defamation under Articles 310 to 321, while the Civil Code provides remedies in the form of compensation and public apologies. According to Oemar Seno Adji, defamation or insult can be classified into two types: material insult and formal insult. Within the KUHP, defamation is regulated primarily under Articles 310 to 312.

Article 310 of the KUHP stipulates that any person who intentionally attacks the honor or reputation of another person by making an allegation with the intent that it be known to the public may be punished for defamation. If such acts are committed through writing or images disseminated, displayed, or posted publicly, they constitute written defamation. However, acts committed in the public

interest or as an act of self-defense are excluded from criminal liability.

Nevertheless, the elements contained in Article 310 of the KUHP are insufficient to address defamation committed through electronic media. Therefore, the principle of lex specialis derogat legi generali applies, allowing the ITE Law to supersede the general provisions of the Criminal Code in regulating cyber-based defamation. As technological development continues, the regulation of defamation has evolved not only in terms of form but also with respect to the media used. Since the enactment of the ITE Law in 2008, activities conducted through social media and the internet have fallen under its legal framework.

The ITE Law, which was first enacted on 21 April 2008, represents Indonesia's first comprehensive legislation in the field of information technology and electronic transactions. Despite its progressive intent, the implementation of the ITE Law has encountered numerous challenges, particularly due to vague provisions often referred to as "rubber articles." The insertion of Articles 27A and 27B in the Second Amendment aims to address these issues by providing clearer and more specific formulations.

Social media platforms provide users with significant freedom, which unfortunately has also facilitated the commission of criminal acts, including defamation. Cybercrimes committed through insulting or defamatory content can cause profound harm to victims. Therefore, the imposition of appropriate criminal sanctions is considered necessary to uphold justice and protect individuals' rights.

In determining whether content constitutes defamation, three elements must be satisfied: first, the identity of the defamed person must be clearly identifiable; second, the identity may be indicated through photographs, usernames, biographies, or other personal information; and third, even if the identity is not explicitly stated, it must be commonly understood by the public to refer to the victim.

Defamation offenses under the ITE Law are complaint-based offenses. Consequently, prosecution may only proceed upon a complaint filed by the victim. Victims may pursue both civil and criminal remedies, including imprisonment for up to six years and/or fines of up to one billion rupiah under Article 27A in conjunction with Article 45A of the ITE Law.

In practice, law enforcement agencies have emphasized the application of restorative justice in handling defamation cases. Through Circular Letters issued by the Chief of the Indonesian National Police, investigators are instructed to prioritize mediation, distinguish between criticism and criminal defamation, and apply criminal law as a last resort (ultimum remedium). Restorative justice seeks to restore relationships between offenders and victims through accountability, apology, and reparation rather than purely punitive measures.

The integration of restorative justice into the criminal justice system reflects a progressive legal approach aimed at achieving social harmony, legal certainty, and substantive justice. When implemented in an integrated manner across law enforcement institutions, restorative justice has the potential to renew conventional paradigms of criminal law enforcement and promote a more humane and socially responsive legal system.

3.2. The Legal Standing of Digital Evidence in Proving the Criminal Offense of Defamation under Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions

Evidence plays a crucial role in the examination of criminal offenses involving electronic information and transactions, as evidentiary processes constitute the primary means of obtaining information through evidence and physical exhibits in order to enable judges to reach a conviction regarding the guilt or innocence of the accused. Through the evidentiary process, the fate of the defendant is determined. If the evidence presented in court, as stipulated by law, is insufficient to prove the defendant's guilt, the defendant must be acquitted. Conversely, if the defendant's guilt can be established through legally recognized evidence, the defendant must be declared guilty and sentenced accordingly.

The evidentiary framework for criminal offenses involving electronic information and transactions under Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) is regulated in Article 5, which provides as follows:

1. Electronic Information and/or Electronic Documents and/or their printouts constitute lawful evidence.
2. Electronic Information and/or Electronic Documents and/or their printouts as referred to in paragraph (1) constitute an expansion of lawful evidence in accordance with procedural law applicable in Indonesia.
3. Electronic Information and/or Electronic Documents are deemed valid if they are generated through an Electronic System that complies with the provisions stipulated in this Law.

Based on the provisions of Article 5 of the ITE Law, it can be understood that evidence in criminal cases involving electronic information and transactions includes electronic

information, electronic documents, and their printouts. Such forms of evidence constitute an expansion of legally recognized evidence under Indonesian procedural law, namely Law Number 8 of 1981 concerning the Criminal Procedure Code (KUHAP).

According to Article 184 of the KUHAP, lawful evidence consists of: (1) witness testimony; (2) expert testimony; (3) documentary evidence; (4) indications; and (5) the statement of the defendant. These forms of evidence are essential, as judges are prohibited from imposing criminal penalties on a person unless, based on at least two lawful pieces of evidence, the judge is convinced that a criminal offense has indeed occurred and that the defendant committed the act.

The prosecution of criminal offenses involving electronic information must therefore be based on lawful evidence as regulated under Article 5 of the ITE Law and Article 184 of the KUHAP. Such evidence must correspond to factual circumstances and must not be fabricated. Pursuant to Article 5 of the ITE Law, electronic information, electronic documents, and their printouts are recognized as lawful evidence and constitute an expansion of the evidentiary system stipulated in Article 184 of the KUHAP.

The legal standing of electronic evidence in the form of electronic information, electronic transactions, and their printouts is therefore valid within the evidentiary system under Article 184 of the KUHAP. The recognition of electronic information, electronic documents, and their printouts as lawful evidence provides legal certainty in the administration of electronic systems and transactions, particularly in proving criminal offenses committed through electronic systems.

In cyberspace-related cases, law enforcement authorities often encounter difficulties in evidentiary processes, particularly in addressing cybercrime offenses such as data forgery. These difficulties arise because investigators must prove matters that are intangible and virtual in nature. The evidence involved is electronic, primarily in the form of electronic documents, which until now have not been comprehensively regulated under procedural law as formal law, although they are widely recognized and used in practice. Current regulations concerning electronic evidence remain largely within the scope of substantive law, as reflected in the ITE Law.

Electronic Information (EI) and Electronic Data (ED) stored within a Central Processing Unit (CPU), particularly on a hard disk, constitute highly important evidence capable of uncovering criminal acts. However, such data is meaningless without the ability to interpret its contents. To determine the integrity and authenticity of data stored on a hard disk, the storage medium must remain intact in its original condition, and forensic testing tools and examiners must be internationally recognized and legally accredited.

The existence of physical evidence is vital in the investigation of computer crimes and computer-related crimes. Through such evidence, investigators and forensic experts can reconstruct the chronology of offenses, trace perpetrators, and ultimately apprehend them. Given the strategic importance of evidence, investigators and forensic analysts must possess a thorough understanding of the various types of evidence. When arriving at a crime scene related to computer crime, they must be able to identify relevant evidence for further forensic examination and analysis.

Evidence refers to objects used to commit a criminal offense, objects resulting from a criminal offense, or objects that have a direct connection to a criminal act. Digital evidence can be classified into two categories: electronic evidence and digital evidence.

Electronic evidence consists of physical objects that can be visually identified. Therefore, investigators and forensic experts must be able to recognize such evidence during the search process at a crime scene. Types of electronic evidence include personal computers, laptops, notebooks, netbooks, tablets, mobile phones, smartphones, flash drives, floppy disks, hard disks, CDs and DVDs, routers, switches, hubs, video cameras, CCTV devices, digital recorders, and music or video players. These devices must undergo digital forensic testing, with particular attention paid to safeguarding electronic information and electronic data throughout the forensic process.

Digital evidence, on the other hand, refers to data extracted or recovered from electronic evidence. In the ITE Law, such evidence is referred to as electronic information and electronic documents. This type of evidence must be meticulously analyzed by forensic experts to establish the relationship between individual data files in uncovering cybercrime cases. Examples of digital evidence include logical files, deleted files, slack files, long files, encrypted files, steganographic files, office files, audio files, video files, image files, emails, user IDs, Short Message Service (SMS), Multimedia Message Service (MMS), and call logs.

According to Article 1 point 1 of the ITE Law, Electronic Information is defined as one or a set of electronic data, including but not limited to text, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegrams, telex, telecopy, letters, symbols, numbers, access codes, symbols, or perforations that have been processed to possess meaning or can be understood by individuals capable of understanding them.

Article 1 point 4 of the ITE Law defines an Electronic Document as any electronic information that is created, transmitted, sent, received, or stored in analog, digital, electromagnetic, optical, or similar forms, which can be displayed, shown, and/or heard through a computer or electronic system, including but not limited to text, sound, images, maps, designs, photographs, letters, symbols, numbers, access codes, or perforations that have meaning or can be understood by individuals capable of understanding them.

Electronic evidence is considered legally valid only if it is generated through an electronic system that complies with applicable regulations in Indonesia. Electronic evidence possesses legal force if the integrity of the information can be guaranteed, the information is accountable, accessible, and capable of being displayed to explain a particular factual condition. The Indonesian National Police, particularly the Cybercrime Unit of the Jakarta Metropolitan Police, has established procedures for handling and seizing electronic evidence, which are compiled in operational guidelines.

Due to the unique characteristics of electronic evidence—namely its electronic form, ease of duplication, and susceptibility to alteration—its handling requires extreme caution. Improper handling may render electronic evidence inadmissible and ultimately weaken the prosecution's case due to procedural errors. Therefore, the handling and seizure of electronic evidence must ensure that such evidence can be presented authentically before the court and remains intact and unaltered.

In the author's view, the existence of the ITE Law is essential to provide a clear and structured legal framework addressing the significance of cyber-related legislation, particularly in the realm of electronic information and transactions. Through the ITE Law, electronic evidence is formally recognized as lawful evidence that may be submitted before a court of law. Although the recognition of electronic evidence under the ITE Law represents a significant advancement, it remains primarily regulated at the level of substantive law. Given that judicial practice is fundamentally governed by procedural law as binding formal law, the explicit regulation of electronic evidence within the Criminal Procedure Code (KUHAP) is necessary to achieve comprehensive legal certainty.

4. Conclusion

Defamation constitutes the dissemination of false information, often in the form of slander, that harms an individual's reputation. Victims of defamation are entitled to file legal complaints against such acts. In the context of cybercrime, defamation is regulated under Articles 310 to 321 of the Indonesian Criminal Code as well as under Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, particularly Articles 27A and 27B paragraph (2) in conjunction with Article 45. Furthermore, the new Indonesian Criminal Code, which will come into force on 2 January 2026, also regulates cyber-related defamation offenses under Articles 433, 434, 435, 441, and 158. In practice, the application of defamation offenses is also guided by the restorative justice approach, as emphasized in the Circular Letter of the Chief of the Indonesian National Police Number SE/8/VII/2018 on the Implementation of Restorative Justice in the Settlement of Criminal Cases.

The evidentiary process in criminal offenses involving electronic information and transactions under Law Number 1 of 2024 is based on lawful evidence as regulated under Article 184 of the Criminal Procedure Code, including witness testimony, expert testimony, documentary evidence, indications, and the statement of the defendant. In addition, Article 5 of the ITE Law recognizes electronic information, electronic documents, and their printouts as lawful evidence. The recognition of electronic evidence as an expansion of lawful evidence provides legal certainty in the administration of electronic systems, particularly in proving cyber-related criminal offenses.

To prevent defamation offenses through social media, public legal awareness must be strengthened through continuous government-led socialization and education regarding the legal consequences of online defamation. Moreover, given the critical role of evidence in judicial proceedings, judges must carefully and prudently assess electronic evidence presented in court. It is therefore recommended that electronic evidence be explicitly regulated as lawful evidence within the Criminal Procedure Code in order to ensure greater legal certainty and consistency in the enforcement of cybercrime laws.

5. References

Ali, M. (2010). Defamation through electronic information and transaction media (A review of Constitutional Court Decision No. 2/PUU-VII/2009). *Jurnal Konstitusi, 7*(6).

Aminudin, & Zainal, A. H. (2008). *Pengantar metode penelitian hukum*. RajaGrafindo Persada.

Arief, B. N. (2002). *Bunga rampai kebijakan hukum pidana*. Citra Aditya Bakti.

Arief, B. N. (2006). *Tindak pidana perkembangan cybercrime di Indonesia*. RajaGrafindo Persada.

Awawangi, R. V. (2014). Defamation under the Criminal Code and Law No. 11 of 2008 concerning electronic information and transactions. *Lex Crimen, 3*(4).

Bakhri, S. (2008). *Dinamika hukum pembuktian*.

RajaGrafindo Persada.
Broadhurst, R. (2006). Developments in the global law enforcement of cybercrime. *International Journal of Police Strategies & Management, 29*(3).
Brown, S. D., & Cameron, S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1).
Chazawi, A., & Ferdian, A. (2014). *Tindak pidana pemalsuan: Tindak pidana yang menyerang kepentingan hukum terhadap kepercayaan masyarakat mengenai kebenaran isi tulisan dan berita yang disampaikan*. Putra Utama Offset.
Chazawi, A., & Ferdian, A. (2015). *Tindak pidana informasi dan transaksi elektronik*. Media Nusa Kreatif.
Dion, M. (2011). Corruption, fraud and cybercrime as dehumanizing phenomena. *International Journal of Social Economics, 38*(5).
Hamzah, A. (2001). *Asas-asas hukum pidana*. Rineka Cipta.
Harahap, M. Y. (2005). *Pembahasan permasalahan dan penerapan KUHAP* (Vol. II). Sarana Bakti Semesta.
Hiariej, E. O. S. (2012). *Teori dan hukum pembuktian*. Erlangga.
Ibrahim, J. (2005). *Teori dan metode penelitian hukum normatif*. Bayumedia Publishing.
Indriani, F. (2016). Juridical review of defamation through social media based on Article 27 paragraph (3) of Law No. 11 of 2008. *Jurnal Online Mahasiswa Fakultas Hukum, 3*(1).
Jaishankar, K. (2018). Cyber criminology as an academic discipline: History, contribution and impact. *International Journal of Cyber Criminology, 12*(1).
Kaligis, O. C. (2002). *Narkoba dan peradilannya di Indonesia*. Alumni.
Kaligis, O. C. (2012). *Penerapan Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik dalam praktiknya*. Yarsif Watampone.
Lamintang, P. A. F. (2004). *Dasar-dasar hukum pidana Indonesia*. Sinar Baru.
Lamintang, P. A. F., & Lamintang, T. (2013). *Delik-delik khusus kejahatan membahayakan kepercayaan umum terhadap surat, alat pembayaran, alat bukti, dan peradilan*. Sinar Grafika.
Marzuki, P. M. (2010). *Penelitian hukum*. Kencana.
Moeljatno. (2007). *Asas-asas hukum pidana*. Bina Aksara.
Muchladun, W. (2015). Juridical review of defamation crimes. *Legal Opinion, 3*(6).
Poernomo, B. (2008). *Asas-asas hukum pidana*. Ghalia Indonesia.
Prodjodikoro, W. (2005). *Hukum acara pidana di Indonesia*. Sumur.
Purbo, O. W. (2011). *Cyberlaw: Filsafat hukum di dunia maya*. Sekolah Tinggi Hukum Bandung.
Republic of Indonesia. (1945). *The 1945 Constitution of the Republic of Indonesia*.
Republic of Indonesia. (1981). *Law No. 8 of 1981 on the Criminal Procedure Code (KUHAP)*.
Republic of Indonesia. (2024). *Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions*.
Chief of the Indonesian National Police. (2018). *Circular Letter No. SE/8/VII/2018 on the implementation of restorative justice*.
Soekanto, S. (1984). *Pengantar penelitian hukum*. UI Press.
Soemitro, R. H. (1990). *Metodologi penelitian hukum dan jurimetri*. Ghalia Indonesia.
Sunggono, B. (2010). *Metodologi penelitian hukum*. RajaGrafindo Persada.
Tami, N. D. P., & Jaya, N. S. P. (2013). Comparative study of defamation regulation under criminal and civil law in Indonesia. *Law Reform, 9*(1).
Waluyo, B. (2012). *Sistem pembuktian dalam peradilan Indonesia*. Sinar Grafika.
Analisis hukum terhadap tindak pidana pencemaran nama baik pada jejaring sosial. (2023). Retrieved from http://elib.unikom.ac.id
Ancaman pencemaran nama baik mengintai. (2024). Retrieved from http://www.hukumonline.com
Etika berkomunikasi di dunia maya. (2023). Retrieved from http://pustaka.ut.ac.id
Jejaring sosial (social networking). (2023). Retrieved from http://www.ridwanforge.net