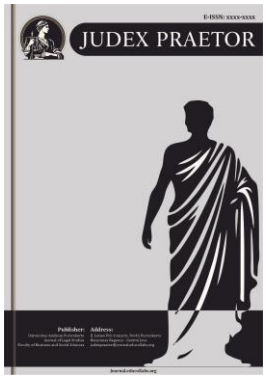
**JOURNAL OF LEGAL STUDIES JUDEX PRAETOR**
Volume 2 Issue 1 July 2026, ISSN: 3124-6419

# Law Enforcement Against Cybercrime in Indonesia: Analysis of Regulatory Effectiveness and Digital Forensic Challenges

**Ni Kadek Satriani** [1]
[1] Satria Consulting, Bali, Indonesia

## ARTICLE INFO




**History :**

Submit on 3 July 2026
Review on 17 July 2026
Accepted on 31 July 2026

**Keyword :**

Cybercrime, Law Enforcement, Cyber Regulations, Digital Forensics, Legal System.

## ABSTRACT

This research aims to analyze the effectiveness of regulations in law enforcement against cybercrime in Indonesia and to examine the role and challenges of digital forensics in the process of proving cybercrime. The research uses the socio-legal method by integrating normative studies of legislation and empirical studies obtained thru various literature on the practice of cybercrime law enforcement in Indonesia. The approaches used include the statute approach and the conceptual approach. The research data consists of secondary data, including primary, secondary, and tertiary legal materials, which are qualitatively analyzed using Lawrence M. Friedman's Legal System Theory, encompassing legal substance, legal structure, and legal culture. The research results show that Indonesia has a sufficient legal foundation thru the Electronic Information and Transactions Law and its amendments in regulating various forms of cybercrime and recognizing electronic evidence as valid evidence. However, the effectiveness of law enforcement still faces various obstacles, including legal provisions that are still open to multiple interpretations, a lack of human resources with digital forensics competence, suboptimal supporting facilities and infrastructure, and weak coordination among law enforcement agencies. In addition, technological developments such as encryption, cryptocurrency, artificial intelligence, and anonymous networks further complicate the process of identifying perpetrators and proving cybercrimes. Therefore, there is a need for more adaptive regulations, an increase in the capacity of law enforcement officers, standardization of digital forensics, and strengthening international cooperation to enhance the effectiveness of law enforcement against cybercrime in Indonesia.



**Corresponding Author:** kadeksatriani@yahoo.com

**JOURNAL OF LEGAL STUDIES JUDEX PRAETOR**
Volume 2 Issue 1 July 2026, ISSN: 3124-6419

## INTRODUCTION

The development of information and communication technology in the last two decades has brought significant changes in various aspects of human life.[1] The increasingly massive digitalization not only facilitates social, economic, and governmental activities but also opens up new spaces for the emergence of various forms of crime conducted thru electronic media. This phenomenon is known as cybercrime, which is a criminal act that utilizing computer systems, internet networks, or digital devices as means or targets of crime.[2] Cybercrime evolves dynamically along with technological advancements, creating new challenges for the conventional law enforcement system.

Globally, the increase in the number of internet users is directly proportional to the rising potential for cybercrime.[3] In Indonesia, the continuously increasing internet penetration year after year has created a vast digital ecosystem, but it has not yet been fully matched by the readiness of security systems and the legal awareness of the public. Various forms of cybercrime such as online fraud, identity theft, system hacking, malware dissemination, and ransomware attacks are becoming more frequent and causing significant losses, both materially and immaterially. In addition, cybercrime also has the characteristic of being borderless, making the law enforcement process, which relies on territorial jurisdiction, more difficult.

In the context of national law, Indonesia has legal instruments regulating cybercrime, among others thru Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016. Several provisions regulating cybercrimes include Articles 27 to 37 of the ITE Law, which govern the distribution of illegal content, illegal access to electronic systems, illegal interception, disruption of electronic systems, manipulation of electronic data, and misuse of devices used to commit cybercrimes. The criminal provisions are regulated in Articles 45 to 52 of the ITE Law. Nevertheless, the implementation of these regulations still faces various obstacles, both in terms of legal substance, law enforcement structure, and the legal culture of society.[4] Substantially, the rapid development of technology is often not followed by adequate regulatory updates, resulting in a legal gap in regulating new forms of cybercrime, such as artificial intelligence-based crimes, deepfakes, and increasingly complex digital data manipulation.

---

[1] Indra Wahyudi, Yoga Lorenza Z, Satria Sakban, Abdul Hadi Rohmadin, dan Syaiful Al Fahrezi, "Peran Teknologi Digital dalam Perubahan Pola Komunikasi dan Gaya Bahasa Generasi Muda," *Linggau Journal of Technology and Computer Science*, Vol. 1, No. 5, (2025), p. 34.

[2] Sihombing, Alfies. Mobilisasi Hukum Pidana di Era Teknologi. Bandung: CV Widina Media Utama, 2025.

[3] *Ibid.*

[4] Muhammad Akbar Bintang, Rena Yulia, and Muhamad Romdoni, "Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana," *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol. 4, No. 2, (2026), p. 57.

From the law enforcement perspective, law enforcement officers face quite serious technical challenges, especially in terms of proving evidence. Unlike conventional crimes, cybercrimes require a special approach in the collection and analysis of evidence, namely thru digital forensics. Digital evidence is susceptible to alteration, deletion, and manipulation, necessitating strict handling procedures to ensure its validity in court.[5] The limited human resources with expertise in digital forensics, as well as the lack of adequate technological infrastructure, are factors that hinder the law enforcement process against cybercrime.

In addition, coordination among law enforcement agencies is also an important issue in handling cybercrime. Given its complex and cross-sector nature, handling cybercrime requires synergy between the police, prosecutors, judicial institutions, and other related agencies, including international cooperation. However, in practice, that coordination has not been functioning optimally, which affects the effectiveness of case handling. On the other hand, the low level of digital literacy among the public also exacerbates the situation, as many internet users do not yet understand the risks and legal aspects of using digital technology.

The phenomenon shows that cybercrime is not just a technical issue, but also a complex and multidimensional legal problem. Therefore, a comprehensive approach is needed to examine this issue, not only from a normative perspective but also thru an empirical approach that can depict the real conditions on the ground. Research that integrates regulatory analysis with empirical data related to law enforcement practices and the use of digital forensics becomes very important to produce effective and evidence-based policy recommendations. Moreover, social factors and the legal culture of society also influence the effectiveness of combating cybercrime in Indonesia. The low level of digital literacy, lack of public awareness regarding personal data security, and the tendency not to report cybercrime to law enforcement pose unique challenges in the law enforcement process. On the other hand, the rapid development of technology compared to the public's ability to adapt to digital risks also increases vulnerability to various forms of cybercrime. These conditions indicate that the success of law enforcement does not only depend on the quality of regulations and the capacity of law enforcement agencies, but also on the level of awareness, compliance, and participation of the community in creating a legal culture that supports cybersecurity.

According to the research, studies on cybercrime in Indonesia are still dominated by a normative approach that focuses on the analysis of legislation.[6] Although important, this approach is not sufficient to address the issues occurring in practice, particularly regarding the effectiveness of law enforcement and the challenges faced by law enforcement officers. Research that examines empirical aspects, such as the

[5] San Putra, Tegar, Sigit Sapto Nugroho, and Meirza Aulia Chairani. "Keabsahan Alat Bukti Digital dalam Pembuktian Kasus Phantom Hacker Scam." *Jurnal Hukum Lex Generalis*, Vol. 7, No. 7, (2026), p. 6.

[6] Mulyana, Indra, Yayan Muhamad Royani, and Tia Ludiana. "Kekosongan Hukum mengenai tindak pidana penipuan deepfake dalam UU ITE Nomor 1 tahun 2024 menurut persfektif Hukum Pidana Islam." *Jurnal Ilmiah Galuh Justisi*, Vol. 14, No. 1, (2026), p. 225-240.

perceptions of law enforcement officers, the success rate of case handling, and the use of digital forensics technology, is still relatively limited. This indicates a research gap that needs to be filled thru more comprehensive studies.

Based on the description, this research becomes relevant and important to conduct in order to provide a more comprehensive picture of law enforcement against cybercrime in Indonesia. This research not only examines the regulations governing cybercrime as part of legal substance but also analyzes how these regulations are implemented by law enforcement agencies as part of the legal structure, as well as the level of public awareness and compliance with the law in the digital space as part of legal culture. Using a socio-legal approach, this research aims to understand the relationship between applicable legal norms and the social realities that occur in the practice of law enforcement against cybercrime. In addition, this research also highlights the role of digital forensics as an important instrument in the process of proving cybercrime. The development of information technology has made electronic evidence a crucial element in uncovering cybercrime. Therefore, this research also examines the readiness of law enforcement officers in utilizing digital forensic technology, including various obstacles faced in the processes of investigation, evidence collection, and law enforcement against cybercrime perpetrators.

Thus, this research is expected to provide contributions both theoretically and practically. Theoretically, this research can enrich the development of legal science, particularly in the study of cyber law, thru an analysis that integrates aspects of legal substance, legal structure, and legal culture based on Lawrence M. Friedman's Legal System Theory. Practically, the results of this research are expected to serve as evaluation and consideration materials for policymakers, law enforcement agencies, and other stakeholders in formulating more effective strategies to prevent and combat cybercrime in Indonesia. Based on this background, the formulation of the problem in this research is how the effectiveness of regulations in regulating cybercrime in Indonesia is viewed from the aspect of legal substance, the role and constraints of law enforcement agencies in handling cybercrime viewed from the aspect of legal structure, as well as the influence of public awareness and compliance with the enforcement of cybercrime laws viewed from the aspect of legal culture.

## METHOD

This research uses the socio-legal method, which is a research approach that combines normative legal studies with an analysis of the social realities related to the application of law in society. This approach is used to understand the law not only as a set of norms enshrined in legislation (law in books), but also as a social phenomenon that is applied and functions in practice (law in action). The choice of the socio-legal method is based on the research objective of not only analyzing the legal regulations regarding cybercrime but also examining the effectiveness of the implementation of these regulations in law enforcement practice. The analysis is conducted using

Lawrence M. Friedman's Legal System Theory, which includes legal substance, legal structure, and legal culture.[7]

This research uses a statute approach and a conceptual approach. The legislative approach is carried out by examining various regulations related to cybercrime, particularly Law Number 11 of 2008 on Electronic Information and Transactions as last amended by Law Number 1 of 2024, the Criminal Code, and other relevant regulations. Meanwhile, a conceptual approach is used to examine the theories, concepts, and legal doctrines related to cybercrime, digital forensics, law enforcement, and Lawrence M. Friedman's Legal System Theory. The data used are secondary data obtained thru library research.

The data includes primary legal materials such as regulations and court decisions, secondary legal materials such as books, scientific journals, research results, and academic articles, as well as tertiary legal materials such as legal dictionaries, legal encyclopedias, and other supporting sources. The collected data is analyzed qualitatively by linking normative provisions and empirical facts found in various literature on the practice of cybercrime law enforcement in Indonesia. The analysis is conducted based on Lawrence M. Friedman's Legal System theory framework to obtain a comprehensive picture of the effectiveness of regulations, the performance of law enforcement officers, and the legal awareness of the community in combating cybercrime.

## RESULT & DISCUSSION

This research found that law enforcement against cybercrime in Indonesia has experienced significant development thru the establishment of various regulations, particularly Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) along with its amendments thru Law Number 19 of 2016 and Law Number 1 of 2024 on Electronic Information and Transactions (ITE Law).[8] These regulatory changes indicate the state's efforts to align national law with the advancements in information technology and the increasingly complex patterns of digital crime. Based on normative analysis, it was found that the ITE Law has provided a legal basis for various forms of cybercrime. In addition, the recognition of electronic evidence as valid legal evidence is a form of modernization of criminal procedural law in Indonesia.[9] These provisions strengthen the position of digital forensics in the process of proving cybercrimes.

Theoretically, the existence of the ITE Law is a form of implementing the principle of legality in modern criminal law. The state strives to provide legal certainty

[7] Al Kautsar, Izzy, and Danang Wahyu Muhammad. "Sistem hukum modern Lawrance M. Friedman: Budaya hukum dan perubahan sosial masyarakat dari industrial ke digital." *Sapientia Et Virtus*, Vol. 7, No. 2, (2022), p.93.

[8] Gladys, W., & Bella, O. Peretasan dan Pelanggaran Data. *Jurnal Review Pendidikan Dan Pengajaran, V*, Vol. 8, No. 4, (2025).

[9] Audina, W. Al-Zayn: Jurnal Ilmu Sosial & Hukum. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, Vol. 4, No. 2 (2026), p.7379.

for actions that were previously unregulated in the conventional legal system.[10] In the perspective of progressive legal theory, the formation of cyber regulations is a response to the rapidly evolving dynamics of the digital society. However, the effectiveness of regulations is not only determined by the existence of legal norms but also by the clarity of the norm formulations and their implementation. Based on Soerjono Soekanto's theory of legal effectiveness, the success of law enforcement is influenced by five factors: the substance of the law, law enforcement officials, means and facilities, society, and legal culture. In the context of cybercrime in Indonesia, these five factors have not yet been functioning optimally.[11] From the aspect of legal substance, several provisions in the ITE Law still lead to multiple interpretations. For example, the provisions regarding content that violates decency as regulated in Article 27 paragraph (1), insults and/or defamation in Article 27A (previously Article 27 paragraph (3) before the amendment of the ITE Law), as well as the dissemination of information that causes public unrest in Article 28 paragraph (3). Some phrases in those provisions are considered to have a wide room for interpretation, potentially leading to legal uncertainty and misuse in their application. That condition contradicts the principles of lex certa and lex stricta in criminal law, which require that the formulation of norms be clear, firm, and unambiguous to avoid different interpretations. The ambiguity of the norm can lead to differences in law enforcement and potentially reduce the protection of citizens' rights in the digital space. Therefore, a more precise formulation of norms and clearer interpretation guidelines are needed to ensure legal certainty in combating cybercrime.[12]

The second amendment to the ITE Law thru Law Number 1 of 2024 indeed shows the government's effort to clarify several provisions that have long been controversial. However, the revision has not fully resolved the fundamental issues related to the potential criminalization in the digital space. In cybercrime, digital evidence holds a central position because almost all criminal activities are conducted thru electronic systems. Therefore, digital forensics becomes an important instrument in the process of criminal law evidence. Digital forensics is essentially a scientific process for obtaining, securing, analyzing, and presenting digital evidence so that it can be used in judicial proceedings. In the perspective of criminal procedural law, the validity of electronic evidence must meet the principles of integrity, authenticity, and chain of custody in order to have legitimate evidentiary power. Moreover, the capability of law enforcement officers in the field of digital forensics is still uneven. Most investigators still rely on information technology experts to perform the

[10] Aryawan, I. Putu Gede. "Kekosongan Norma Hukum dalam Penanganan Deepfake sebagai Alat Kejahatan Siber: Studi Yuridis di Wilayah Polri Klungkung." *Menulis: Jurnal Penelitian Nusantara* 2, no. 4 (2026), p .297.

[11] Handoyo, S., & Fakhriza, M. Efektivitas Hukum Terhadap Kepatuhan Perusahaan Dalam Kepesertaan BPJS Kesehatan. Journal De Facto, Vol. 5, No. 1, (2018), p. 1-19.

[12] Yacob, C. Y. Problematika Penerapan Pasal 28 Ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Hukum Legalita*, Vol. 6, No. 2, (2022), p. 163-170.

extraction and analysis of electronic data.[13] This dependence often causes the proofing process to take a long time and incur high costs.

Another issue arises due to the characteristics of digital evidence, which can be easily deleted, modified, or transferred across countries in a short period of time. This condition necessitates that the investigation process be conducted quickly and precisely. However, in practice, the limitations of digital forensics tools and the bureaucracy of law enforcement often hinder the effectiveness of investigations. Cybercrime has the character of a borderless crime. Perpetrators can commit crimes from other countries using virtual servers and anonymous identities. This condition causes national legal jurisdictions to often face limitations in the enforcement process. Indonesia has not yet become a party to the Budapest Convention on Cybercrime, which is an important international instrument in combating transnational cybercrime.[14] As a result, international cooperation related to the exchange of electronic data and the extradition of perpetrators still faces procedural obstacles. In addition, technological developments such as virtual private networks (VPNs), the dark web, cryptocurrency, and artificial intelligence make it increasingly difficult to identify perpetrators. This indicates that conventional law enforcement approaches are no longer adequate to tackle modern digital crimes. Based on the analysis results, there are several strategic steps that need to be taken to enhance the effectiveness of law enforcement against cybercrime in Indonesia.

In the perspective of Lawrence M. Friedman's legal system theory, the effectiveness of combating cybercrime in Indonesia can be analyzed thru three main elements, namely legal substance, legal structure, and legal culture. From the legal substance aspect, the regulation of cybercrime in Indonesia has been accommodated in Law Number 11 of 2008 concerning Information and Electronic Transactions, as last amended by Law Number 1 of 2024. The provisions regarding prohibited acts are regulated in Articles 27 to 37 of the ITE Law, which include the distribution of content that violates decency, gambling, insults or defamation, extortion and threats, the spread of false news and hate speech, illegal access to electronic systems, illegal interception, interference with electronic data or electronic systems, and manipulation of electronic information. Meanwhile, the criminal provisions are regulated in Articles 45 to 52 of the ITE Law. However, some provisions still lead to multiple interpretations, such as Article 27 paragraph (1), Article 27A, and Article 28 paragraph (3), which potentially create legal uncertainty and contradict the principles of lex certa and lex stricta.

In terms of legal substance, Indonesia essentially already has a sufficiently adequate legal foundation to regulate various forms of cybercrime thru the Electronic Information and Transactions Law and its amendments. The regulation provides legal

[13] Mubarok, A. Peranan Alat Bukti Elektronik Dalam Meningkatkan Efektivitas Pembuktian Tindak Pidana Korupsi. Al-Zayn: Jurnal Ilmu Sosial & Hukum, Vol. 4, No. 1, (2026), 572-579.

[14] Susilowati, A. Penegakan Hukum Internasional terhadap Serangan Siber terhadap Infrastruktur Kritis di Indonesia. Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora, Vol. 2, No. 5, (2025), p. 122-141.

certainty for various acts categorized as cybercrimes and accommodates electronic evidence as valid evidence in judicial processes.[15] Nevertheless, the effectiveness of the legal substance still faces several obstacles. Some provisions in the ITE Law still contain relatively broad normative formulations, which have the potential to cause multiple interpretations in their application. This condition causes law enforcement not to always proceed uniformly and has the potential to create legal uncertainty for the public. Moreover, the rapid development of information technology is often not accompanied by adequate regulatory updates. As a result, a legal gap has emerged in anticipating various forms of new cybercrimes, such as the misuse of artificial intelligence, deepfakes, and cryptocurrency-based crimes.

From the aspect of legal structure, the effectiveness of law enforcement against cybercrime heavily depends on the capacity of law enforcement agencies in handling cases based on information technology.[16] Although the Police, Prosecutor's Office, and judicial institutions have special units that handle cybercrime, the capacity of human resources and the availability of digital forensic support facilities are still uneven. The limited number of investigators with expertise in digital forensics often causes the investigation process to rely on the assistance of information technology experts. This condition affects the length of the investigation and proof process, especially in cases involving large amounts of electronic data or having cross-border dimensions. Therefore, periodic regulatory updates have become an urgent necessity so that the substance of the law can keep pace with technological developments and provide more effective legal protection to the public.

In the aspect of legal culture, the effectiveness of law enforcement against cybercrime is not only determined by the quality of regulations and the performance of law enforcement officers but also by the level of legal awareness in society. The low level of digital literacy causes some members of the community to not yet understand the risks of using information technology or the legal consequences of activities conducted in cyberspace. The phenomenon of spreading false information, hate speech, online scams, and privacy violations indicates that there is still a gap between the existence of legal norms and societal behavior in the digital space. Moreover, many victims of cybercrime choose not to report the incidents they experience because they find the legal process complicated or doubt the effectiveness of its handling. This condition indicates that the development of a legal culture that supports cybersecurity needs to be carried out thru the enhancement of digital literacy, legal education, and continuous information security awareness campaigns. With the increasing legal awareness of the community, efforts to prevent and combat cybercrime can be more effective.

[15] Khaidir, A., Kurnia, M. P., & Erawaty, R. Perlindungan Hukum Terhadap Korban Kejahatan Siber di Indonesia Dalam Perspektif Hukum Internasional. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, Vol. 3, No. 6, (2025), p. 10563–10573.

[16] Dinda, Adinda Lola Sariani. "Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia." *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum*, Vol. 2, No. 2, (2024), p.70.

**JOURNAL OF LEGAL STUDIES JUDEX PRAETOR**
Volume 2 Issue 1 July 2026, ISSN: 3124-6419

## CONCLUTIONS

Law enforcement against cybercrime in Indonesia has experienced significant development thru the formation and renewal of regulations, particularly the Electronic Information and Transactions Law and its amendments. The existence of these regulations demonstrates the state's efforts to provide legal certainty for various forms of cybercrime while also accommodating electronic evidence as legitimate evidence in the criminal justice process. From the perspective of Lawrence M. Friedman's Legal System Theory, the effectiveness of law enforcement against cybercrime still faces various obstacles. From the aspect of legal substance, there are still several provisions that have the potential to cause multiple interpretations and legal uncertainty. From the aspect of legal structure, the limited human resources with digital forensics competence, the uneven distribution of supporting technological facilities, and the suboptimal coordination between law enforcement agencies remain obstacles in the law enforcement process. Meanwhile, from the aspect of legal culture, the low level of digital literacy and legal awareness among the public still affects the effectiveness of efforts to prevent and combat cybercrime.

Digital forensics plays a very important role in the process of proving cybercrime because electronic evidence is the main element in uncovering digital crimes. However, technological developments such as encryption, cryptocurrency, artificial intelligence, virtual private networks (VPN), and anonymous networks are increasingly complicating the process of identifying perpetrators and collecting electronic evidence. Therefore, there is a need to strengthen regulations that are more adaptive to technological developments, enhance the capacity of law enforcement officers in the field of digital forensics, establish national standards in handling electronic evidence, and strengthen international cooperation to improve the effectiveness of law enforcement against cybercrime in Indonesia.

## REFERENCE

Al Kautsar, Izzy, and Danang Wahyu Muhammad. "Sistem hukum modern Lawrance M. Friedman: Budaya hukum dan perubahan sosial masyarakat dari industrial ke digital." *Sapientia Et Virtus*, Vol. 7, No. 2, (2022), 84-93.

Aryawan, I. Putu Gede. "Kekosongan Norma Hukum dalam Penanganan Deepfake sebagai Alat Kejahatan Siber: Studi Yuridis di Wilayah Polri Klungkung." *Menulis: Jurnal Penelitian Nusantara* 2, no. 4 (2026), 295-307.

Audina, W. Al-Zayn: Jurnal Ilmu Sosial & Hukum. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, Vol. 4, No. 2 (2026), 7374-7386.

Dinda, Adinda Lola Sariani. "Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia." *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum*, Vol. 2, No. 2, (2024), 69-77.

Gladys, W., & Bella, O. Peretasan dan Pelanggaran Data. *Jurnal Review Pendidikan Dan Pengajaran, V*, Vol. 8, No. 4, (2025).

Handoyo, S., & Fakhriza, M. Efektivitas Hukum Terhadap Kepatuhan Perusahaan Dalam Kepesertaan BPJS Kesehatan. Journal De Facto, Vol. 5, No. 1, (2018), p. 1-19.

Indra Wahyudi, Yoga Lorenza Z, Satria Sakban, Abdul Hadi Rohmadin, dan Syaiful Al Fahrezi, "Peran Teknologi Digital dalam Perubahan Pola Komunikasi dan Gaya Bahasa Generasi Muda," *Linggau Journal of Technology and Computer Science*, Vol. 1, No. 5, (2025).

Khaidir, A., Kurnia, M. P., & Erawaty, R. Perlindungan Hukum Terhadap Korban Kejahatan Siber di Indonesia Dalam Perspektif Hukum Internasional. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, Vol. 3, No. 6, (2025), p. 10563–10573.

Mubarok, A. Peranan Alat Bukti Elektronik Dalam Meningkatkan Efektivitas Pembuktian Tindak Pidana Korupsi. Al-Zayn: Jurnal Ilmu Sosial & Hukum, Vol. 4, No. 1, (2026), 572-579.

Muhammad Akbar Bintang, Rena Yulia, and Muhamad Romdoni, "Urgensi Reformulasi Undang-Undang Informasi dan Transaksi Elektronik terhadap Penyalahgunaan Kecerdasan Buatan Deepfake dalam Perspektif Pembaharuan Hukum Pidana," *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol. 4, No. 2, (2026), p. 57.

Mulyana, Indra, Yayan Muhamad Royani, and Tia Ludiana. "Kekosongan Hukum mengenai tindak pidana penipuan deepfake dalam UU ITE Nomor 1 tahun 2024 menurut persfektif Hukum Pidana Islam." *Jurnal Ilmiah Galuh Justisi*, Vol. 14, No. 1, (2026), p. 225-240.

San Putra, Tegar, Sigit Sapto Nugroho, and Meirza Aulia Chairani. "Keabsahan Alat Bukti Digital dalam Pembuktian Kasus Phantom Hacker Scam." *Jurnal Hukum Lex Generalis*, Vol. 7, No. 7, (2026), p. 6.

Sihombing, Alfies. Mobilisasi Hukum Pidana di Era Teknologi. Bandung: CV Widina Media Utama, 2025.

Susilowati, A. Penegakan Hukum Internasional terhadap Serangan Siber terhadap Infrastruktur Kritis di Indonesia. Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora, Vol. 2, No. 5, (2025), p. 122-141.

Yacob, C. Y. Problematika Penerapan Pasal 28 Ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Hukum Legalita*, Vol. 6, No. 2, (2022), p. 163-170.