GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i2
https://creativecommons.org/licenses/by/4.0/

Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption

Endro Satoto[1], Faisal Santiago[2]
[1]Universitas Borobudur, Jakarta, Indonesia, endro91@gmail.com
[2]Universitas Borobudur, Jakarta, Indonesia, faisalsantiago@borobudur.ac.id

Corresponding Author: endro91@gmail.com[1]

Abstract. The rapid development of information and communication technology has given rise to increasingly complex cybercrime phenomena that cross territorial, legal, and national jurisdiction boundaries. In Indonesia, the cyber law system still shows various weaknesses in terms of regulation, law enforcement, and protection of victims. Although there are several legal instruments such as the Electronic Information and Transactions Law (Law No. 1 of 2024) and the Personal Data Protection Law (Law No. 27 of 2022), these regulations have not fully addressed the dynamic digital threats that continue to evolve, such as AI-based crimes, ransomware, and misuse of personal data. Law enforcement also faces challenges due to limited human resource competencies, constraints in digital forensic technology, and weak inter-agency coordination. This situation is exacerbated by regulatory disharmony, resulting in legal vacuums and overlapping authorities among institutions. This study proposes the reconstruction of Indonesia's cyber law system to be adaptive and integrated by promoting the formation of a National Cyber Law, strengthening the role of the National Cyber and Crypto Agency or *Badan Siber dan Sandi Negara* (BSSN), and establishing a unified task force to respond to cross-sector digital crimes. Using a normative juridical approach, this paper analyzes the urgency of developing a legal system that is not only responsive to technological developments but also ensures legal certainty and justice for all citizens in the digital space.

Keywords: Cyber Law, Digital Crime, Legal Reconstruction, BSSN, Technological Disruption.

INTRODUCTION

The development of information and communication technology in the era of disruption has brought significant impacts on human life across various fields, including legal aspects (Saputra, 2023). The rapidly evolving digital technology creates a new ecosystem full of both potential and risks, one of which is the emergence of various forms of cybercrime (Kusnanto, 2024). These cybercrimes do not only occur within local digital spaces but also cross-national borders and become a global threat (Maskun, 2022). The boundless cyber space allows

perpetrators to carry out actions across jurisdictional territories, making it difficult for law enforcement to identify, trace, and prosecute offenders (Pamungkas, 2024). In this context, a legal system that does not quickly adapt will fall far behind the continuously evolving dynamics of crime.

The threat to digital security becomes more tangible when considering various forms of cyberattacks targeting personal data, critical infrastructure, and government systems (Kristalia, 2024). Crimes such as data theft, ransomware, online fraud, and hacking of government agency websites demonstrate how vulnerable Indonesia is amid technological disruption (Hapsari, 2023). This situation is worsened by the fact that cybercrime is dynamic, difficult to predict, and utilizes sophisticated technology that law enforcement often lacks (Andriyani, 2023). The rapid pace of digital transformation is not matched by the readiness of regulations or human resources capable of responding appropriately to these threats. Consequently, a gap emerges between the legal reality and technological development, hindering the effectiveness of law enforcement (Ariyaningsih, 2023).

This disparity becomes even sharper when the national legal system fails to anticipate new forms of crime that are not yet recognized in positive legal norms. AI-based crimes, the spread of deepfakes, and exploitation of software security loopholes are threats that have not been specifically addressed in existing regulations (Subekti, 2024). Legal norms are often general and outdated, while technology continues to evolve daily. This situation creates a real legal vacuum, especially in the enforcement against highly technical and complex types of digital crime. A non-adaptive legal system becomes a gap exploited by criminals to avoid legal accountability.

A review of cybercrime as a legal phenomenon requires a comprehensive understanding of its definition and characteristics. Cybercrime is a form of criminal act carried out through or against computer systems, internet networks, and digital data (Habibi, 2020). The main characteristics of this crime are the anonymity of the perpetrators, the speed of action, and its cross-border reach, which make it very different from conventional crimes (Budiyanto, 2025). Furthermore, cybercrime can occur in various forms, ranging from online fraud, data manipulation, to system sabotage (Bahri, 2023). Its complexity demands legal thinking that is not only normative but also technological and multidisciplinary.

The classification of cybercrime according to the Budapest Convention of 2001 provides an important framework for understanding the scope of cyber threats internationally (Muchamad, 2023). This convention divides cybercrime into four main categories: violations of the confidentiality, integrity, and availability of computer systems; crimes related to illegal content; crimes related to copyright infringement; and crimes related to financial information systems (Febrian, 2024). Interpol also categorizes cyber threats based on the level of risk and the methods used by perpetrators in carrying out their actions, such as social engineering, malware attacks, and account takeovers (Chandra, 2025). These concepts are important references for formulating a national legal system that is harmonious with international norms, so that efforts to combat cybercrime are not insular.

In understanding the challenges of cyber law, a theoretical approach is an indispensable foundation. The responsive legal theory from Philippe Nonet and Philip Selznick shows that the law should be adaptive to social and technological changes (Gussela, 2025). In the context of cybercrime, this responsive approach encourages the state to create laws that can accurately and flexibly capture the dynamics of the digital space. The law must not be rigid and overly textual because the nature of cybercrime itself changes very quickly and requires innovative legal interpretation (Ferryanto, 2024). Strengthening responsive legal norms will create a judicial system capable of acting swiftly and fairly.

The legal protection theory developed by Satjipto Rahardjo emphasizes the importance of the state's presence in protecting its citizens from all forms of threats, including in the digital

space (Huda, 2024). Cybercrime causes real harm to individuals and institutions alike, ranging from identity theft, financial damage, to psychological trauma (Malian, 2024). Within the framework of legal protection, the state is not only obligated to prosecute perpetrators of crimes but also to ensure preventive measures and effective recovery systems for victims. If the legal system cannot provide a sense of security in the digital world, then the state has failed to fulfill its constitutional responsibilities.

The principles of legality and legal certainty become extremely important in cyber-criminal law. In many cases, law enforcement faces difficulties when existing legal norms do not explicitly regulate certain forms of cybercrime. This situation can create uncertainty during prosecution, as perpetrators may argue that their actions are not regulated by existing law. Legal certainty is not only about the existence of norms but also about the clarity, consistency, and the ability of those norms to address societal needs. This principle forms the foundation so that the law is not arbitrary and continues to provide protection for all parties in the digital space (Panggabean, 2025).

Current regulations have made efforts to address some of the challenges of cyber law in Indonesia. Law No. 1 of 2024, as the second amendment to the Electronic Information and Transactions Law (UU ITE), demonstrates a commitment to adjust legal regulations to technological developments. Several articles were updated to accommodate new issues such as digital defamation and the dissemination of illegal content. Law No. 27 of 2022 on Personal Data Protection also marks an important milestone in safeguarding citizens' digital rights. However, the harmonization between the UU ITE, UU PDP, and other regulations remains suboptimal, as each adopts different approaches to the definitions and sanctions related to cybercrime.

The government has also issued Presidential Regulation No. 82 of 2022 concerning the Protection of Vital Information Infrastructure, which emphasizes the importance of safeguarding digital systems that serve as the backbone of public services and the national economy. In addition, the National Cyber and Crypto Agency or *Badan Siber dan Sandi Negara* (BSSN) Regulation No. 4 of 2021 on Cybersecurity Governance provides technical guidelines for institutions and organizations to maintain the integrity of their digital systems. These regulations reflect the government's efforts to strengthen the institutional foundation of cybersecurity, although their implementation still faces various challenges. Limitations in budget, human resources, and digital awareness pose serious obstacles to the effective and equitable application of these regulations across all sectors.

Indonesia's cyber legal system has a reasonably solid initial foundation but still requires significant refinement to become adaptive, firm, and integrated. Law must not only regulate but also prevent and protect society from invisible threats that have major impacts. The reconstruction of the legal system is an inevitability, not only in terms of substantive regulations but also in building synergy among institutions, technological readiness, and digital legal literacy among the public. Cybercrime will not wait for the law to catch up, so legal measures must be more progressive and sensitive to every technological development that occurs. If the law wants to remain relevant, it must move as fast as the digital world itself.

METHOD

This research employs a normative juridical method, which is a legal research approach that relies on the analysis of applicable written legal norms as the basis for explaining legal phenomena, particularly in the context of combating cybercrime in Indonesia. The primary focus of this study lies in the examination of legislation, legal doctrines, and general legal principles relevant to the cyber legal system. The primary legal materials analyzed include Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (ITE Law), Law Number 27 of 2022 concerning Personal Data Protection,

as well as derivative regulations such as Presidential Regulation Number 82 of 2022 and BSSN Regulation Number 4 of 2021. In addition, this study also utilizes secondary legal materials in the form of scientific literature, journal articles, academic studies, and opinions from cyber law experts. The analysis is conducted descriptively and analytically to elaborate the current condition of Indonesia's cyber legal system and to identify substantial and structural weaknesses faced in addressing increasingly complex digital crimes. Through this approach, the study aims to formulate a reconstruction model of the law that is more adaptive, integrative, and aligned with the needs of legal protection in the era of digital technology disruption. This method also enables the researcher to develop strong and systematic legal arguments in recommending the formation of a new comprehensive legal framework.

RESULT AND DISCUSSION

Existing Condition of the Cyber Legal System in Indonesia

Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as last amended by Law Number 1 of 2024, remains the primary legal foundation for addressing cybercrime in Indonesia. However, this law has not fully been able to meet the challenges posed by the highly dynamic development of digital technology. The norms within the ITE Law tend to be general and less comprehensive in covering new, more complex forms of cybercrime such as cyberattacks on critical infrastructure and AI exploitation. The 2024 regulatory amendments corrected several ambiguous articles but have not substantively expanded the legal scope to adequately address modern cybercrime. The regulation does not yet comprehensively provide a strong legal framework for prevention, enforcement, and recovery related to cyber offenses.

Law Number 27 of 2022 on Personal Data Protection (PDP Law) serves as an important legal instrument in safeguarding citizens' digital rights, especially in the management and protection of data. Although the PDP Law imposes criminal and administrative sanctions on violators, its effectiveness is still hindered because not all implementing provisions have been fully enacted. Furthermore, challenges in inter-agency coordination during the implementation of data protection remain significant, especially in cases of large-scale data breaches. The misalignment in definitions and approaches between the PDP Law and the ITE Law creates ambiguity in responsibility for handling cyber incidents. This leads to uncertainty in law enforcement processes because agency authorities have not been systemically coordinated.

A major weakness in Indonesia's current cyber legal system is the lack of synchronization among the related laws. The ITE Law, the PDP Law, and other regulations such as Presidential Regulation Number 82 of 2022 and BSSN regulations have yet to be integrated into a solid national cyber legal framework. Each regulation stands alone with its own objectives and approaches, without normative bridges that unify the handling of cybercrime from upstream to downstream processes. As a result, legal enforcement tends to be sporadic and lacks a unified strategic reference. When large-scale cyber incidents occur, legal responses are often slow due to limited coordination among agencies and overlapping authorities.

Law enforcement against cybercrime in Indonesia involves several main institutions such as the Indonesian National Police (Polri), the Prosecutor's Office, and the National Cyber and Crypto Agency (BSSN). However, the division of roles, which is not comprehensively structured, often causes confusion in case handling. The Police are responsible for investigation and arresting suspects but frequently face limitations in collecting and interpreting complex digital evidence. The Prosecutor's Office, as the party that prosecutes, does not always possess deep technical expertise regarding the digital aspects of these crimes. Meanwhile, BSSN, which should serve as the central command for cybersecurity, does not yet have executive authority to take direct action against cybercrime perpetrators.

The technology used by cybercriminals is increasingly sophisticated and covert, while digital tracking tools and forensic expertise in Indonesia remain very limited. Tracking digital footprints, such as identifying IP addresses manipulated via VPN, proxy, or other anonymizer methods, requires high-level equipment and expertise that are not yet uniformly available among law enforcement personnel. Furthermore, the collection of digital evidence must be conducted carefully so as not to violate principles of legality and data integrity, which are often overlooked due to a lack of specialized training. Digital forensics, which forms the backbone of legal proof in cybercrime cases, has not become a standard competency for investigators and law enforcement officers. This causes law enforcement to be slow and results in inaccurate investigation outcomes.

The quality of human resources involved in cyber law enforcement remains a major obstacle. Not all law enforcement officers have an in-depth understanding of the characteristics and modus operandi of cybercrime. Many officers have never received specialized training in cybersecurity, digital investigation techniques, or introduction to information systems and networks. The shortage of experts in law and technology causes investigation processes to be frequently delayed and often misunderstood. The gap between legal understanding and technological developments creates loopholes exploited by digital criminals to evade legal sanctions technically.

Victims of cybercrime in Indonesia often do not receive adequate legal protection. Preventive measures to protect the public from digital crimes have not been well structured, whether in the form of digital education or early warning systems. When attacks occur, mechanisms for victim protection and recovery are not yet clearly available or integrated. Reports from victims are often not promptly followed up because they are considered low priority, especially if the losses are small, despite having significant social impact. The unpreparedness of the protection system for victims leads to a sense of insecurity and public distrust in the existing legal system.

The National Cyber and Crypto Agency (BSSN) in practice only functions as a passive intelligence agency without repressive authority. Its status as a negative intelligence agency means that BSSN cannot take direct action when indications of a cyberattack are found but can only convey information to other law enforcement agencies. This limitation results in the absence of a rapid follow-up response in emergency situations that require an instant reaction. In a complex state structure like Indonesia, the existence of an agency with reactive authority is crucial to ensure a quick and effective digital security response. Without an executive function, BSSN's role becomes very limited and symbolic.

The lack of regulation granting executive authority to BSSN causes Indonesia's cyber defense system to be fragmented and ineffective. Although BSSN is the agency with the most adequate technical expertise in the field of cybersecurity, it cannot take legal steps without going through other law enforcement bodies. This makes the reaction time to attacks too slow and creates opportunities for perpetrators to escape or erase digital traces. Dependence on other institutions to take legal action makes BSSN's work inefficient, even though intelligence data and information are fully available. Institutional reform and granting direct authority based on law are urgent in building a strong and integrated cyber legal system.

The current structure of the cyber legal system is far from ideal. The absence of effective coordination mechanisms between regulations, law enforcement, and victim protection makes this system unable to respond comprehensively to cybercrime challenges. In such conditions, Indonesia's digital society becomes highly vulnerable to exploitation and crime. The need for reconstructing the cyber legal system is not merely a normative reform but concerns institutional design, strengthening human resources, and synergistic cross-sector integration. Combating cybercrime will not be effective if the legal system supporting it remains partial, slow, and disconnected from the realities of global technological development.

Problems and the Need for Reconstruction of Cyber Law in the Era of Technological Disruption

The emergence of new forms of cybercrime such as deepfake, ransomware, and AI-based phishing reveals a significant substantive legal vacuum within Indonesia's legal system. The existing legal instruments do not yet have specific provisions that directly address crimes utilizing such advanced technologies. For example, the use of deepfake to spread false information or conduct extortion lacks explicit legal articles that appropriately sanction perpetrators. Consequently, law enforcement tends to rely on broad interpretations of general norms, which can trigger legal uncertainty. Without substantive regulations that are responsive to technological innovations, the law will always lag behind and fail to effectively protect society.

In addition to the substantive legal gaps, Indonesia faces overlapping and disharmonized regulations in the cybersecurity sector. Various laws and regulations operate independently without clear normative coordination or legal hierarchy, causing ambiguity in enforcement. A single act can be regulated by multiple regulations with different, even conflicting legal consequences. In practice, law enforcement officers often struggle to determine the most appropriate legal basis when handling cases. This situation not only hampers the effectiveness of law enforcement but also increases the risk of human rights violations due to inconsistent norms.

As technology continues to advance, the absence of sophisticated digital forensic tools becomes a major obstacle in uncovering cybercrimes. Investigations cannot rely solely on conventional tools because the digital footprints left by perpetrators are increasingly hidden, encrypted, and transnational. Many law enforcement institutions lack access to advanced tracking technologies, even for basic tasks like extracting data from locked devices. Dependence on foreign technology also raises unresolved issues of digital sovereignty. Without adequate forensic capabilities, cybercrimes risk not being legally proven in court.

Law enforcement institutions still face major obstacles regarding the availability of special cyber teams with technical expertise and experience. Many investigators still work using conventional methods that are no longer suitable for the nature and character of today's digital crimes. Specialized training and education in cybersecurity have not yet become a national standard implemented evenly, so individual capabilities heavily depend on the initiative of each institution. On the other hand, the attractiveness of the private sector offering higher salaries makes many cyber talents reluctant to join government agencies. Without planned and competitive human resource development, strengthening the legal system will always remain theoretical.

Coordination among institutions in handling cybercrime is still far from ideal. There is no integrated system capable of consolidating information, resources, and investigative processes from various agencies such as the Police, BSSN, Prosecutor's Office, and Ministry of Communication and Informatics. Each institution operates with its own internal procedures which are often disconnected. When a cyber-attack occurs, response time is slow due to complicated bureaucracy between agencies. This lack of integration is highly detrimental in the context of cybercrime, which is dynamic and requires real-time response.

This complex condition marks an urgent need for a comprehensive reconstruction of Indonesia's cyber law. The establishment of a National Cyber Law Act is a very important step to unify norms, clarify institutional structures, and formulate procedures for case handling from prevention to recovery. This law must be designed not only to fill substantive legal gaps but also to anticipate digital technological developments in an adaptive manner. With a single comprehensive legal instrument, cyber law enforcement can be more directed, efficient, and

guarantee legal certainty for all involved parties. The new regulation must also be based on human rights and ensure public participation in its formation process.

One important element in this reconstruction is the strengthening of positive legal authority for BSSN. As the institution that technically understands the landscape of digital threats best, BSSN needs to be granted legal legitimacy to carry out limited executive actions in emergency situations. It is not enough to function merely as an analyst and warning provider; this institution must be able to take direct steps to prevent or mitigate cyber-attacks. Such authority needs to be regulated strictly and proportionally to prevent abuse of power, yet remain flexible enough to respond swiftly during cyber crises. With a strong position within national law, BSSN can become the frontline defense in the country's digital security.

In operational terms, the establishment of a cross-agency Cybercrime Response Task Force is a strategically urgent need. This team must consist of personnel from various agencies such as the Police, BSSN, Prosecutor's Office, and Ministry of Communication and Informatics who are specially trained to handle various forms of cyber-attacks. With an integrated command system and standardized response procedures, this team can respond to incidents with greater speed and accuracy. Moreover, the presence of this task force will foster a culture of collaboration among institutions that have tended to work in silos. The availability of a trained emergency response unit also provides a sense of security for the public and digital industry players.

Integration between the personal data protection system and the national digital infrastructure is an important element in creating a resilient cyber legal system. Data protection cannot stand alone without being linked to the digital ecosystem used by both government and private institutions. A national system needs to be built that not only guarantees data security but also ensures the resilience of infrastructure such as data centers, government networks, and digital-based public services. This integration will reduce system fragmentation and facilitate supervision as well as law enforcement in case of violations. When data protection and infrastructure security work in harmony, the stability of the national cyber space can be better assured.

Realizing an ideal cyber legal system requires an approach that is not only legalistic but also transformative. Regulatory updates must be followed by simultaneous institutional and technological capacity building. The needs of an increasingly digitalized society demand that the state be present not only as a regulator but also as a protector and facilitator in the digital space. The challenges of the disruption era cannot be answered with old legal systems that are rigid and slow. Indonesia's cyber law must reflect the courage to adapt and think forward, not merely patching up past shortcomings.

CONCLUSION

Indonesia's cyber legal system until now has not been able to effectively keep pace with the rapid disruption of digital technology. This lag is clearly visible in the weak regulations that have yet to cover the evolving types of cybercrime, as well as the lack of synchronization among several regulations which instead cause confusion in law enforcement. Obstacles also arise from limited human resources in law enforcement institutions, especially regarding expertise in digital forensics, data analysis, and technology-based investigations. Coupled with inadequate technological support, the process of cyber law enforcement often hits a dead end, which ultimately reduces public trust in legal protection within the digital space. In this situation, the need for legal reconstruction becomes imperative, with an approach that is not only repressive but also preventive and adaptive to technological developments as well as cross-border and dynamic cyber risks.

It is crucial for the government and policymakers to promptly draft and enact a comprehensive Cyber Law that can unify various legal norms into one clear and operational

framework. Enhancing human resource capacity in digital forensics and cyber investigation must be a priority agenda, through continuous training, the establishment of specialized curricula, and the recruitment of experts in these fields. Collaboration among domestic agencies as well as international cooperation must also be strengthened, considering the transnational nature of cybercrime which requires cross-border coordination. Furthermore, the position and authority of the National Cyber and Crypto Agency (BSSN) must be legally strengthened so that this institution can play a more strategic role in prevention, mitigation, and handling of national cyber incidents. With these concrete steps, Indonesia can build a cyber legal system that is not only responsive to today's challenges but also resilient in facing future challenges.

REFERENCES

Andriyani, W. S. (2023). *Technology, Law And Society.* Makassar: Tohar Media.

Ariyaningsih, S. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum, 1(1)*, 1-11.

Bahri, I. S. (2023). *Cyber Crime dalam Sorotan Hukum Pidana (Edisi 2023).* Bahasa Rakyat.

Budiyanto, S. H. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia.* Banten: Sada Kurnia Pustaka.

Chandra, J. T. (2025). Peran Interpol dalam Menangani dan Menanggulangi Kejahatan Siber di Indonesia. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora, 4(3)*, 4710-4719.

Febrian, W. R. (2024). PERAN HUKUM INTERNASIONAL DALAM MENANGANI KASUS CYBER CRIME. *JURNAL SAHID DA'WATII, 3(02)*, 1-7.

Ferryanto, J. T. (2024). Komersialisasi Data dalam Politik Hukum Keamanan Siber. *Barelang Journal of Legal Studies, 2(1)*, 73-87.

Gussela, M. D. (2025). Fenomena "No Viral No Justice" Perspektif Teori Penegakkan Hukum. *Ranah Research: Journal of Multidisciplinary Research and Development, 7(2)*, 792-800.

Habibi, M. R. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam, 23(2)*, 400-426.

Hapsari, R. D. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen, 5(1)*, 1-17.

Huda, H. U. (2024). *DATA PRIBADI, HAK WARGA, DAN NEGARA HUKUM: MENJAGA PRIVASI DI TENGAH ANCAMAN DIGITAL.* Bandung: Penerbit Widina.

Kristalia, B. Y. (2024). Ancaman Siber dan Penguatan Kedaulatan Digital Indonesia dari Perspektif Geopolitik Digital. *Jurnal Ilmiah Multidisiplin, 3(02)*, 83-93.

Kusnanto, S. P. (2024). *Transformasi Era Digitalisasi Masyarakat Kontemporer.* Ponorogo: Uwais Inspirasi Indonesia.

Malian, D. (2024). Penanganan Dan Tantangan Cybercrime Di Era Digital Perspektif Kriminologi. *Innovative: Journal Of Social Science Research, 4(6)*, 7048-7056.

Maskun, S. H. (2022). *Kejahatan Siber (Cyber Crime): Suatu Pengantar.* Jakarta: Prenada Media.

Muchamad, M. K. (2023). *Kejahatan Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia.* Banda Aceh: Syiah Kuala University Press.

Pamungkas, A. T. (2024). Tracing Legal Regulations in Dealing with Cybercrime in Indonesia: Examining Obstacles and Solutions. *DELICTUM : Jurnal Hukum Pidana Islam, 2(2)*.

Panggabean, E. &. (2025). KEBIJAKAN HUKUM PIDANA TERKAIT SANKSI PIDANA BAGI PELAKU KEJAHATAN SIBER DI INDONESIA. *SCIENTIA JOURNAL: Jurnal Ilmiah Mahasiswa, 7(1)*.

Saputra, A. M. (2023). *TEKNOLOGI INFORMASI: Peranan TI dalam berbagai bidang.* Jambi: PT. Sonpedia Publishing Indonesia.

Subekti, I. S. (2024). Reformulasi Kebijakan Kriminal Dalam Penanggulangan Kejahatan Berbasis Teknologi Kecerdasan Buatan. *SETARA: Jurnal Ilmu Hukum, 5(2)*, 60-74.