JGSP
Jurnal Greenation Sosial dan Politik
+62 81210467572 https://greenationpublisher.org/JGSP greenation.info@gmail.com
GREENATION PUBLISHER

DOI: https://doi.org/10.38035/jgsp.v3i4

Problems of Cyber Law Enforcement Against Cyber Crimes Using Virtual Private Network Technology in Indonesia

Teguh Nugroho[1], Bambang Soesatyo[2]
[1]Universitas Borobudur, Jakarta, Indonesia, teguhnugroho2104@gmail.com
[2]Universitas Borobudur, Jakarta, Indonesia, bambang_soesatyo@borobudur.ac.id

Corresponding Author: teguhnugroho2104@gmail.com[1]

Abstract: The development of information technology has brought significant changes in digital activities, including the use of Virtual Private Networks (VPNs), which, on the one hand, are used to protect user privacy but, on the other hand, have significant potential for misuse in cybercrime. VPNs allow perpetrators to disguise their identities, obscure their digital footprints, and illegally access systems using encryption and IP masking techniques, complicating law enforcement. This study aims to examine the issues of law enforcement against cybercrime using VPNs in Indonesia, highlighting aspects of substance, structure, and legal culture. From a substantive aspect, existing regulations such as Law Number 1 of 2024 concerning the Second Amendment to the ITE Law, Law Number 27 of 2022 concerning Personal Data Protection, and the new Criminal Code (Law Number 1 of 2023) do not explicitly regulate the use of VPNs, creating a legal vacuum. From a structural aspect, law enforcement officials face limited technical capacity and digital forensic equipment, as well as suboptimal coordination between institutions such as the Indonesian National Police (Polri), the National Cyber and Information Technology Agency (BSSN), and the Ministry of Communication and Informatics. From a cultural perspective, low public awareness of the risks of VPN misuse and the dilemma between privacy protection and national security pose particular challenges. This study emphasizes the importance of regulatory revisions, increased law enforcement capacity, international cooperation, and public education so that VPNs can be used for their intended purpose without becoming a vehicle for cybercrime.

Keyword: Law Enforcement, Cybercrime, Virtual Private Network.

INTRODUCTION

The development of information technology has brought about significant changes in the lives of modern society (Wiryany, et al., 2022). Digital technology is now the primary means of communication, transactions, and even sensitive data storage (Aksenta, et al., 2023). Virtual Private Networks, or VPNs, have emerged as an innovation used by the public to maintain privacy and access internet services without geographical restrictions (Andini, et al., 2020). On the positive side, VPNs provide greater security when accessing public internet

networks because they protect data from eavesdropping. However, VPN use also poses the potential for misuse, which can hinder law enforcement efforts (Wulandari, 2024).

VPNs are often used to commit cybercrimes because they can disguise the user's true IP address. It makes perpetrators more difficult for law enforcement to track and identify (Wigrhalia, 2025). Illegal access to electronic systems, carding, and online fraud are some forms of crime often committed using VPNs (Alamsyah, et al., 2025). Hiding one's identity using a VPN gives perpetrators a technical advantage over law enforcement officials conducting investigations (Nur, 2025). This situation poses serious challenges for the Indonesian legal system in maintaining cybersecurity.

Cyber law has emerged as a legal discipline that regulates public behavior in the digital space. Cyber law encompasses not only regulations related to computer crime but also the protection of personal data, electronic transactions, and the validity of electronic evidence (Indarta, 2025). Unlike conventional law, which primarily regulates physical interactions, cyber law emphasizes regulating activities occurring in cyberspace. Key principles inherent in cyber law include cross-border jurisdiction, the validity of electronic evidence, and digital justice for all parties (Pahrudin, et al., 2025). These aspects form the basis for assessing the extent to which Indonesian law can prevent criminal acts with the help of VPNs.

VPNs technically work through data encryption, tunneling, and IP address masking. Encryption ensures that transmitted data cannot be easily accessed by third parties, tunneling creates a secure path for internet traffic, while IP masking disguises the user's true identity (Zakaria, et al., 2022). These functions make VPNs highly useful for individuals who want to maintain data confidentiality or access geographically restricted digital content. From a legal perspective, VPNs are not necessarily prohibited, as their use also supports freedom of expression and digital privacy protection. However, when used to conceal the identity of cybercriminals, VPNs pose a significant challenge for law enforcement.

The legal function of VPNs cannot be ignored as they are widely used by both companies and individuals to protect confidential data. International corporations utilize VPNs to allow their employees to securely access internal systems even when working from different locations (Suhendi & Nugraha, 2025). Individuals use VPNs to avoid hacking of personal data when accessing public networks. VPNs provide a layer of protection that aligns with information security principles (Pratama, 2023). However, the dark side of this technology remains when used to evade legal detection, ultimately creating regulatory dilemmas.

VPN misuse often goes unnoticed by the general public, who view it simply as a convenient way to access blocked websites. In reality, VPNs can be used to access the dark web, which is rife with illegal activity (Amelia, 2025). Crimes such as the sale of personal data, drug trafficking, and digital money laundering often utilize VPNs to avoid being easily detected (Bego, et al., 2025). Law enforcement officers face challenges because the digital traces left by perpetrators are encrypted or routed through overseas servers. These technical obstacles complicate investigations compared to conventional criminal cases.

Lawrence M. Friedman's law enforcement theory is highly relevant to understanding the VPN phenomenon in cybercrime. Friedman emphasizes three critical aspects: legal structure, legal substance, and legal culture. Legal structure relates to law enforcement officials and institutions, legal substance concerns applicable regulations, and legal culture reflects public legal awareness (DM, et al., 2025). When VPNs are used for cybercrime, these three aspects are tested simultaneously. Law enforcement will be effective if there is a balance between legal instruments, legal resources, and public awareness of the risks of technology abuse (Dinda, 2024).

The legal substance related to VPNs in Indonesia is reflected in several key regulations. The Electronic Information and Transactions Law, most recently updated

through Law No. 1 of 2024, regulates crimes involving illegal access, interception, and manipulation of electronic data. The 2022 Personal Data Protection Law emphasizes the importance of maintaining data security from misuse, including those related to identity theft technology (Asherli & Wiraguna, 2025). The new 2023 Criminal Code also includes provisions regarding computer crimes, strengthening the legal framework for cyber activity. All these regulations provide a legal basis for prosecuting perpetrators of crimes, even those using VPNs.

Indonesia's legal structure has established several key institutions for cyber law enforcement. The Indonesian National Police, through the Directorate of Cyber Crimes, is primarily responsible for investigating and prosecuting digital crimes (Ismail, 2023). The National Cyber and Crypto Agency (BSSN) plays a role in maintaining national network security and supporting technical investigations (Haryanto & Sutra, 2023). The Ministry of Communication and Informatics is responsible for regulating and controlling internet traffic. Collaboration between institutions is essential because cybercrime often involves international networks. The effectiveness of legal structures depends heavily on the synergy between law enforcement actors.

The legal culture of Indonesian society regarding VPN use exhibits its own dynamics. Many users are unaware of the difference between using VPNs for legal and illegal purposes. Legal awareness regarding personal data security remains low, while the drive for unlimited internet access is even higher (Arief, et al., 2024). The societal paradigm often emphasizes digital freedom without understanding the potential legal risks. This situation demonstrates that the success of law enforcement is determined not only by regulations but also by the level of public awareness as legal subjects.

A conceptual framework for research on VPNs and cybercrime needs to integrate the relationship between Friedman's three aspects. VPNs, as a technological instrument, are positioned as a crucial variable influencing cybercrime patterns. Indonesian positive law, consisting of the 2024 ITE Law, the 2022 PDP Law, and the 2023 Criminal Code, serves as the normative basis for assessing the legitimacy and enforcement of these acts. Law enforcement officials must utilize this framework to identify regulatory weaknesses and develop effective enforcement strategies. Thus, this conceptual framework is not only descriptive but also analytical in offering solutions to the challenges of VPN in cybercrime.

METHOD

The research method in this paper is normative legal research with a statutory and conceptual approach. Normative legal research focuses on the study of applicable positive legal norms, both in the form of laws, implementing regulations, and international legal instruments relevant to the issue of VPNs and cybercrime. The regulatory approach is conducted by examining Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law, Law Number 27 of 2022 concerning Personal Data Protection, and the new Criminal Code through Law Number 1 of 2023, which is the main legal framework for regulating and prosecuting the misuse of digital technology, including VPNs. The analysis also includes regulations related to the authority of institutions such as the National Police, the National Cyber and Crypto Agency, and the Ministry of Communication and Information Technology in enforcing cyber law. Meanwhile, the conceptual approach is used to understand the concept of cyber law, the function of VPN, and Lawrence M. Friedman's law enforcement theory, which emphasizes the importance of harmony between substance, structure, and legal culture. By combining these two approaches, this study seeks to provide a comprehensive overview of the legal problems arising from VPN misuse while also offering theoretical and normative solutions to strengthen cyber law enforcement in Indonesia.

RESULTS AND DISCUSSION

Legal Regulations Regarding the Use of Virtual Private Network Technology in the Context of Cybercrime in Indonesia

The Electronic Information and Transactions Law, amended by Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008, is the primary legal basis for regulating cybercrime. Article 30, paragraph (1) states that any person who intentionally and without authority or unlawfully accesses another person's computer or electronic system is prohibited. Article 32, paragraph (1) prohibits unauthorized alteration, addition, reduction, transmission, damage, removal, or transfer of electronic information. Article 35 prohibits any person from intentionally and without authority manipulating, creating, changing, deleting, damaging, or eliminating electronic information with the aim of making it appear as if the data is authentic. This provision explicitly provides a basis for prosecuting perpetrators who use VPNs to conceal illegal access to electronic systems.

Law No. 27 of 2022 concerning Personal Data Protection strengthens the cyber legal regime in Indonesia. Article 2, paragraph (1) states that personal data protection is a human right that must be protected by the state. Article 65 paragraph (1) states that every person is prohibited from unlawfully obtaining or collecting personal data that does not belong to him or her with the intention of benefiting himself or another party. Article 67 imposes criminal sanctions of up to 5 years' imprisonment and/or a maximum fine of IDR 5,000,000,000 on any party who unlawfully discloses another person's personal data. VPNs can be a means of concealment when perpetrators obtain or trade personal data, making the provisions of the PDP Law highly relevant.

The New Criminal Code, enacted through Law No. 1 of 2023 concerning the Criminal Code, also contains articles related to computer and cybercrimes. Article 263 prohibits illegal access to electronic systems owned by others. Article 264 contains criminal provisions for unauthorized interception or tapping of electronic information. Article 267 emphasizes the prohibition on destroying or altering data that could harm another party. These articles provide additional legal instruments for cyber law enforcement, while also strengthening Indonesia's position in facing the challenge of using VPNs for criminal acts. With the enactment of the new Criminal Code, synchronization with the ITE Law and the PDP Law is increasingly necessary to avoid overlap.

The Indonesian National Police (Polri) play a crucial role through the Cyber Crime Directorate of the National Police's Criminal Investigation Agency (Bareskrim Polri). This unit is authorized to conduct investigations, indictments, and take action against various cybercrimes, including those involving VPNs. This authority is based on Law Number 2 of 2002 concerning the Indonesian National Police. Article 13 of this law states that the police's duties include maintaining public order and security, enforcing the law, and providing protection, guidance, and services to the public. In cybercrime cases, the Indonesian National Police's Cyber Crime Directorate plays a leading role in facing technical challenges in penetrating VPN protection.

The National Cyber and Crypto Agency (BSSN) also plays a strategic role in national cybersecurity. Based on Presidential Regulation Number 28 of 2021 concerning the BSSN, this agency is authorized to implement cybersecurity to support law enforcement and safeguard Indonesia's digital sovereignty. Article 3 of the Presidential Regulation emphasizes that the National Cyber and Cyber Security Agency (BSSN) has the function of detecting, preventing, handling, and recovering from cyber incidents. VPNs, as a technology that complicates the identification of cyber perpetrators, must be addressed through technical collaboration between BSSN and law enforcement. This collaboration demonstrates that

handling cybercrime requires cross-institutional synergy with adequate technological capacity.

The Ministry of Communication and Informatics has the authority to regulate internet access and digital services, including VPNs. Based on Law No. 36 of 1999 concerning Telecommunications and Law No. 11 of 2008 in conjunction with Law No. 1 of 2024 concerning the Electronic Information and Transactions (ITE), the Ministry of Communication and Informatics (Kominfo) has the authority to supervise and control the use of telecommunications networks. Article 40 of the ITE Law states that the government must prevent the dissemination of prohibited electronic information. Kominfo also plays a role in blocking illegal sites and regulating policies on the use of internet-based applications. This regulation intersects with the use of VPNs, which are often used to access blocked websites, making coordination with law enforcement crucial.

The 2001 Budapest Convention on Cybercrime was the first international legal instrument to comprehensively regulate cybercrime. This convention emphasizes the criminalization of illegal access, illegal interception, data manipulation, and crimes related to computer systems. Article 2 of the Convention regulates illegal access to computer systems, Article 3 prohibits unauthorized interception, and Article 4 regulates data manipulation. Although Indonesia has not ratified this Convention, its principles are often used as a reference in updating national regulations. VPNs, as an instrument that can disguise illegal access, are highly relevant to the norms established in the Budapest Convention.

China is known for its strict regulations on VPN use. The government requires all VPN service providers to obtain official permits, and unauthorized VPN use is considered a violation of the law. Russia has implemented a similar policy, prohibiting the use of VPNs to access state-blocked websites. The United States, on the other hand, allows widespread VPN use but still imposes strict penalties for its use in cybercrime. These differing approaches demonstrate that VPN regulation is heavily influenced by each country's national policies on digital freedom and national security.

Indonesia faces a dilemma in regulating VPNs because it must balance the right to privacy with national security interests. On the one hand, VPNs are needed by individuals and companies to protect personal data. On the other hand, VPNs are often used by criminals to escape the clutches of the law. Harmonizing national regulations with international legal principles is crucial to ensure Indonesia remains on the right track in combating cross-border crime. Participation in international legal regimes such as the Budapest Convention could be a strategic option to strengthen Indonesia's legal standing.

The implications for Indonesia in its legal harmonization efforts lie in the importance of regulatory consistency with international practices. If Indonesia can strengthen VPN regulations through the ITE Law, the PDP Law, and the new Criminal Code by adding specific provisions, legal certainty will be enhanced. Harmonization will also enable more effective international cooperation, particularly in the extradition of cybercriminals who use VPNs across borders. Clarity in national regulations will provide a strong foundation for enhancing Indonesia's credibility in the global legal arena. This awareness must be accompanied by a commitment to building the technological capacity of law enforcement officers to keep pace with developments in digital crime.

Challenges and Obstacles to Cyber Law Enforcement Against Cyber Crime Through the Use of Virtual Private Network Technology in Indonesia

The substantive aspects of the law regarding the use of VPNs in cybercrimes reveal significant regulatory gaps. Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016, does not explicitly regulate VPN technology as a means of digital identity obfuscation. Existing regulations only address unlawful acts in the realm of illegal access, data manipulation, or distribution of prohibited content. This situation allows cybercriminals to utilize VPNs without being subject to articles that explicitly qualify the use of such tools as criminal acts.

Substantive weaknesses in the law are also evident in the evidentiary aspect. VPNs create a layer of encryption and anonymity that makes the perpetrator's true Internet Protocol (IP) address difficult to detect. The ITE Law regulates electronic evidence but does not provide detailed provisions regarding the validity of digital evidence that passes through anonymous networks. This has given rise to debate in judicial practice regarding whether searched data can be considered valid and have full evidentiary force. Without clear regulations, judges have room for interpretation, which can lead to disparate decisions.

Technological developments that outpace legal reforms also raise substantive issues. VPNs not only serve as a disguise tool for crime but are also used legally by companies and individuals to protect personal data. The lack of a clear distinction between legitimate use and misuse of VPNs in the law leaves law enforcement vulnerable to violating the rights of well-intentioned users. Law Number 27 of 2022 concerning Personal Data Protection strengthens the right to privacy but does not provide concrete answers on how to distinguish between legitimate privacy and criminal anonymity.

The legal structure presents serious obstacles. Law enforcement officials still face limited technical capacity to track perpetrators who use VPNs. Cybercrime demands high digital analytical skills, while improvements in the technical competence of officers do not always keep pace with the dynamics of technology-based crime. A special cybercrime unit within the police has been established, but the limited number of personnel with a thorough understanding of digital forensics limits the effectiveness of law enforcement.

Coordination between law enforcement agencies and technical institutions is also suboptimal. The Indonesian National Police (Polri) as the main investigator, the Ministry of Communication and Information Technology (Kominfo) as the telecommunications regulator, and the National Cyber Security Agency (BSSN) as the cybersecurity authority often work in a fragmented manner. The lack of a standard protocol integrating the authority of these three agencies leads to lengthy processing times for handling cyber cases. In situations where perpetrators use VPNs that can switch servers across countries, weak coordination actually widens the gap for perpetrators to escape the clutches of the law.

Lack of technological infrastructure exacerbates weaknesses in the legal structure. Law enforcement officials still have limited digital forensic equipment, both in quantity and sophistication. Premium VPNs with high-level encryption systems can penetrate the analytical capabilities of outdated forensic software. The state budget has indeed allocated funds to increase the digital capacity of the apparatus, but the realization of technology procurement is often not in line with the ever-growing needs of real investigations.

The legal culture of society also presents significant challenges. VPNs are often viewed merely as a means to access restricted websites without considering the potential for misuse. Low public awareness of the criminal risks that can be perpetrated through VPNs creates a permissive environment for digital identity disguises. This view makes law enforcement confront not only criminals but also a public opinion that remains ambiguous regarding VPN use.

Paradigms regarding privacy and security complicate the issue of legal culture. VPNs are often promoted as a tool to protect personal data from commercial tracking and state surveillance. However, when VPNs are used to commit crimes, countries face a dilemma in maintaining a balance between the right to digital freedom and the obligation to ensure public security. The PDP Law recognizes citizens' rights to personal data protection, but does not provide practical guidelines to distinguish between the use of VPNs as a legitimate form of protection or as a modus operandi for criminal acts.

In cases of online fraud and carding, VPNs are used by perpetrators to conceal their true location, making the tracing process take months. Investigators often have to work with international service providers who are not always cooperative. These technical obstacles demonstrate that national legal instruments are often inadequate in the face of global, cross-jurisdictional technology.

Evaluations of the effectiveness of criminal sanctions reveal another weakness. The ITE Law provides criminal penalties for acts committed through electronic networks, but does not address the increased penalties for crimes committed using digital disguises such as VPNs. As a result, perpetrators are only charged with general articles without any increased penalties, even though their actions are more difficult to uncover and have the potential to cause greater losses. This raises questions about whether the existing legal framework is truly capable of providing a deterrent effect or is instead a blunt instrument in the face of modern cybercrime.

CONCLUSION

VPNs, as a technology, are inherently neutral and have a positive function in protecting privacy and data security. However, in practice, they are often exploited to facilitate cybercrime. Existing regulations, such as the updated Law No. 11 of 2008 concerning Electronic Information and Transactions, Law No. 27 of 2022 concerning Personal Data Protection, and the new Criminal Code enacted through Law No. 1 of 2023, still demonstrate a clear legal gap in specific provisions regarding VPN use. This gap leaves law enforcement officials limited to general articles that are sometimes ineffective when dealing with the modus operandi of identity-stealing technology-based crimes. Law enforcement challenges, then, extend beyond the substantive aspects of the law, encompassing structural aspects such as the limited capacity of officers and infrastructure, as well as cultural aspects related to low public awareness and the tension between privacy and security.

Future improvements require systematic steps emphasizing regulatory strengthening to ensure VPNs are placed proportionally within national law, either through revisions to the ITE Law or synchronization with the PDP Law. The capacity of law enforcement officers in digital forensics needs to be enhanced through education, training, and the procurement of state-of-the-art equipment to penetrate the layers of anonymity of cyber technology. International cooperation must also be expanded, as cybercrimes involving VPNs often involve cross-jurisdictional means, necessitating synergy between countries. Furthermore, public education is crucial to raise awareness about the safe and legal use of VPNs, so that the public can enjoy their benefits without allowing them to become a loophole for cybercriminals.

REFERENCE

Aksenta, A., Irmawati, I., Ridwan, A., Hayati, N., Sepriano, S., Herlinah, H., & Ginting, T. W. (2023). *Literasi Digital: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 dan Sociaty 5.0.* Jambi: PT. Sonpedia Publishing Indonesia.

Alamsyah, A., Santoso, E., & Pranadita, N. (2025). Kajian Terhadap Kejahatan Carding Sebagai Bentuk Cybercrime Di Indonesia. *Iustitia Omnibus: Jurnal Ilmu Hukum, 6*(2), 60-68.

Amelia, R. (2025). ANALISIS HUKUM PIDANA TERHADAP PENYALAHGUNAAN AKSES DIGITAL DALAM TINDAK PIDANA SIBER. *JURNAL MAHASISWA HUKUM, 2*(2), 90-95.

Andini, M. D., Amirullah, M., & Muchtar, H. N. (2020). Penggunaan Aplikasi Virtual Private Network (VPN) Point To Point Tunneling Protocol (PPTP) Dalam Mengakses Situs Terblokir. *Supremasi Hukum: Jurnal Penelitian Hukum, 29*(2).

Arief, M. H., Fitri, K. A., & Sakti, E. M. (2024). Analisis kesadaran cyber crime di kalangan masyarakat menengah kebawah. *Jurnal Ilmiah Teknik Informatika (TEKINFO), 25*(2), 24-39.

Asherli, B. F., & Wiraguna, S. A. (2025). Perlindungan Keamanan Data Pribadi di Era Digital Menghadapi Serangan Phishing Ditinjau dari Undang-Undang Pelindungan Data Pribadi Nomor 27 Tahun 2022. *Jurnal Hukum, Administrasi Publik dan Negara, 2*(4), 1-14.

Bego, K. C., Aziz, F. R., Rahmad, R. A., & Budianto, H. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya. *Jurnal Kolaboratif Sains, 8*(1), 506-511.

Dinda, A. L. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum, 2*(2), 69-77.

DM, M. Y., Saragih, G. M., Setiawan, F., Sitompul, H. I., & Berson, H. (2025). ANALISIS FAKTOR PENGHAMBAT PENEGAKAN HUKUM PIDANA DI INDONESIA DALAM PERSPEKTIF TEORI LAWRENCE FRIEDMAN. *JURNAL ILMIAH ADVOKASI, 13*(2), 711-725.

Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal, 7*(1), 56-69.

Indarta, Y. (2025). *Cyber Law: Dimensi Hukum dalam Era Digital.* Padang: Pustaka Galeri Mandiri.

Ismail, M. (2023). Digital Policing; Studi Pemanfaatan Teknologi Dalam Pelaksanaan Tugas Intelijen Kepolisian untuk Mencegah Kejahatan Siber (Cybercrime). *Jurnal Ilmu Kepolisian, 17*(3), 15-15.

Nur, F. (2025). Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Penipuan Online Dengan Modus Social Engineering. *Innovative: Journal Of Social Science Research, 5*(4), 342-355.

Pahrudin, e. a. (2025). *Hukum Siber: Menyikapi Tantangan Hukum Di Era Digital.* Jambi: PT. Nawala Gama Education.

Pratama, R. (2023). A Literature Review: Network Security Menggunakan Virtual Private Network L2tp/Ipsec, Port Knocking, Port Forwarding, Honeypot Dan Pfsense. *Jurnal Jaringan Komputer dan Keamanan, 4*(3), 11-18.

Suhendi, H., & Nugraha, R. (2025). Perancangan Jaringan WAN Menggunakan VPN DI PT. WMI (Wide Band Media Indonesia). *Journal of Innovation Research and Knowledge, 4*(12), 9291-9300.

Wigrhalia, D. (2025). Penegakan Hukum Siber Bagi Pelaku Tindak Pidana Kesusilaan Melalui Media Elektronik (Studi Kasus: Putusan No. 196/Pid. Sus/2022/Pn. Pbr). *Jurnal Sains Riset, 15*(1), 132-142.

Wiryany, D., Natasha, S., & Kurniawan, R. (2022). Perkembangan teknologi informasi dan komunikasi terhadap perubahan sistem komunikasi Indonesia. *Jurnal Nomosleca, 8*(2), 242-252.

Wulandari, S. (2024). Integrasi VPN (Virtual Private Network) dalam Sistem Jaringan Komputer untuk Keamanan Akses Data Jarak Jauh. *Journal Of Information Technology, 3*(1), 137-147.

Zakaria, M. I., Norizan, M. N., Isa, M. M., Jamlos, M. F., & Mustapa, M. (2022). Comparative analysis on virtual private network in the internet of things gateways. *Indonesian Journal of Electrical Engineering and Computer Science, 28*(1), 488-497. doi:doi: 10.11591/ijeecs. v28.i1.pp488-497