E-ISSN : 2963-4946
Vol. 4 No. 8 May 2026
https://ajosh.org/

Asian Journal of Social and Humanities

Reconstruction of Legal Policy in Handling Ransomware Attacks on National Critical Infrastructure in Indonesia

Teguh Nugroho*, Hidayati
Universitas Borobudur, Indonesia
Email: teguhnugroho2104@gmail.com*, hidayati@borobudur.ac.id

Keywords:
ransomware; cybercrime; legal policy; national critical infrastructure.

Abstract

This study aims to analyze and reconstruct legal policies in addressing ransomware attacks on national critical infrastructure in Indonesia using normative juridical methods through legislative and conceptual approaches. The results show that the legal provisions contained in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection do not specifically regulate ransomware as a separate crime and do not provide comprehensive protection for national critical infrastructure. Furthermore, there are weaknesses in both normative and implementation aspects, including the absence of a legal definition of ransomware, weak cybersecurity standards, institutional fragmentation, and obstacles in digital evidence management and cross-border law enforcement. Therefore, legal policy reconstruction is needed through the establishment of specific norms related to ransomware, the strengthening of regulations for critical infrastructure protection based on a risk approach, the implementation of mandatory cybersecurity standards, as well as institutional integration and the enhancement of law enforcement capacity. This study contributes to the development of a legal policy model that is preventive, repressive, and adaptive to technological developments to ensure national security and Indonesia's digital sovereignty.

INTRODUCTION

The development of digital transformation has led to a very high dependence on national critical infrastructure, including the energy, banking, health, transportation, and telecommunications sectors, as the backbone of national life (Erwin, 2023). In Indonesia, the acceleration of digitalization through the implementation of e-government, digital financial systems (fintech), and the integration of smart systems in public services has created both efficiencies and new systemic vulnerabilities (Irfan, 2023). This dependence has the consequence that disruptions to one digital subsystem can have a cascading impact on economic stability, national security, and the continuity of public services (Chowdhury, 2022; Desouza et al., 2025). Normatively, the protection of electronic systems is currently regulated in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, specifically Article 30 concerning illegal access and Article 33 concerning disruptions to electronic systems. However, these regulations are still general in nature and do not explicitly regulate the protection of national critical infrastructure as a vital digitalized state object (Harahap, 2022).Globally, cybercrime has

escalated significantly, with ransomware being one of the most dominant and complex forms of threat (Apollyus, 2022). Technically, ransomware is malicious software that encrypts a victim's system or data for the purpose of extortion, but legally, it can be classified as a combination of the crimes of illegal access, data manipulation, and extortion. The evolution of ransomware from crypto-ransomware to the ransomware-as-a-service model demonstrates the industrialization of organized, transnational cybercrime (Jubhari, 2022). From the perspective of Indonesian positive law, the provisions of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, through Articles 32 and 48, can indeed be used to prosecute acts of destroying or transferring electronic data. However, the construction of these norms remains implicit and is therefore unable to accommodate the complex nature of ransomware as a modern cybercrime (Ramadhan, 2023).The characteristics of ransomware attacks on critical infrastructure indicate that their impact is not limited to financial losses but also includes operational disruption and threats to national security (Kurniawan, 2021). Ransomware's modus operandi, which includes data encryption, data exfiltration, and the threat of publishing sensitive data, has the potential to paralyze vital state systems such as healthcare, energy, and transportation (Simorangkir, 2024). From a legal perspective, this situation should be classified as a threat to the public interest, as reflected in Article 33 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. However, this norm does not explicitly regulate the classification of attacks on critical infrastructure as a form of crime with national strategic impact (Wildan, 2025). This is exacerbated by the low level of institutional cyber resilience, indicating that the existing legal approach is still predominantly repressive and does not comprehensively regulate preventive obligations. Several ransomware cases demonstrate a systematic attack pattern that exploits security system weaknesses and a lack of adequate digital protection standards both internationally and nationally (Tus, 2021). This situation indicates that Indonesia's legal framework is not fully prepared to address this threat, despite the existence of Law Number 27 of 2022 concerning Personal Data Protection, which, in Article 35, requires personal data controllers to ensure data security, and Article 46, which regulates sanctions for data protection violations (Nabila, 2024). However, this law focuses more on protecting data subjects rather than comprehensively protecting critical systems and infrastructure, making it an ineffective legal instrument for combating ransomware.The weaknesses of legal policy in combating ransomware in Indonesia are increasingly evident in the absence of an explicit legal definition of ransomware in legislation, weak regulations regarding critical infrastructure protection, and institutional fragmentation in national cybersecurity governance. Furthermore, the lack of mandatory cybersecurity standards and an integrated incident response mechanism demonstrates that Indonesian positive law remains ill-adapted to technological developments (Stone, 2025). In terms of law enforcement, the use of encryption technology, the anonymity of perpetrators through the dark web, and the use of cryptocurrency create serious evidentiary difficulties that have not been fully accommodated in the criminal procedural law system or in the electronic evidence provisions in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (Sulubara, 2024).From a comparative perspective, several countries have developed more advanced legal frameworks for protecting critical infrastructure and countering ransomware

through a risk-based approach, system security obligations, and integration between the public and private sectors. This indicates that Indonesia still faces a normative lag in responding to increasingly complex cyber threats. Therefore, the reconstruction of legal policy is urgent, emphasizing a shift from a reactive approach to a preventive and systemic approach that integrates aspects of national security, digital sovereignty, and public protection, thereby establishing a cyber legal regime that is responsive, adaptive, and oriented toward protecting national critical infrastructure.The novelty of this research lies in its comprehensive legal policy reconstruction model that integrates four key dimensions: (1) explicit criminalization of ransomware as a standalone offense with aggravated penalties for attacks on critical infrastructure; (2) risk-based critical infrastructure protection regulations with binding cybersecurity standards; (3) institutional integration through a single national cybersecurity authority; and (4) enhanced international cooperation mechanisms for cross-border ransomware cases. Unlike previous studies that focused on single aspects such as criminal liability or technical mitigation, this research provides a holistic legal framework that connects normative, institutional, and enforcement dimensions. The purpose of this study is to analyze current legal provisions on ransomware and formulate a legal policy reconstruction model applicable to national critical infrastructure protection. The contribution of this research is to provide concrete recommendations for legislators, policymakers, law enforcement agencies, and critical infrastructure operators. The benefits include enhanced legal certainty, improved national cybersecurity posture, better victim protection, and strengthened digital sovereignty for Indonesia in the face of evolving cyber threats.

METHOD

This research is a normative juridical study that examines positive legal norms as a basis for analyzing legal issues related to ransomware countermeasures against national critical infrastructure in Indonesia, using both a legislative and a conceptual approach. The legislative approach is carried out by examining various relevant laws and regulations, particularly Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection, as well as other related regulations, to identify normative gaps, inconsistencies, and regulatory weaknesses in dealing with ransomware crimes. Meanwhile, the conceptual approach is used to examine developing legal doctrines, theories, and concepts, such as the concepts of cybercrime, cybersecurity, critical infrastructure protection, and criminal law policy from the perspective of legal reform, in order to build comprehensive and systematic legal arguments. The legal materials used include primary legal materials in the form of statutory regulations, secondary legal materials in the form of scientific literature, journals, and previous research results, as well as tertiary legal materials as supporting references, which are then analyzed qualitatively using legal interpretation methods to produce prescriptions in the form of recommendations for the reconstruction of legal policies that are responsive to technological developments and cyber threats.

RESULT AND DISCUSSION

Positive Legal Regulations for Countering Ransomware in the Indonesian Legal System

Positive legal regulations for countering ransomware in the Indonesian legal system are still primarily based on the cyber law regime stipulated in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, the latest amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. In its normative construction, the ITE Law regulates various forms of conduct related to illegal access, system disruption, and electronic data manipulation. However, ransomware, as a form of modern cybercrime, has not been explicitly regulated as a separate offense but must be constructed through the interpretation of existing norms, thus raising issues of legal certainty and the effectiveness of law enforcement (Robbi, 2025).More specifically, Article 30 paragraphs (1), (2), and (3) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions prohibit illegal access to electronic systems at various levels of severity, ranging from unauthorized access to access for the purpose of obtaining electronic information. This provision is relevant to the initial stages of a ransomware attack, which generally begins with unauthorized access through the exploitation of system security vulnerabilities (Anbiyaa, 2025). However, this norm does not specifically regulate the subsequent goal of controlling and locking data for extortion, thus leaving a normative gap in qualifying ransomware as a complete crime. Article 32 paragraphs (1), (2), and (3) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions prohibit the unauthorized alteration, addition, reduction, transmission, destruction, removal, transfer, or concealment of electronic information. This provision can be used to prosecute ransomware perpetrators who encrypt or lock victim data, which can be viewed as a form of eliminating access to electronic information. Furthermore, Article 33 prohibits acts that disrupt electronic systems, which is relevant to the operational impact of ransomware attacks on critical infrastructure (Afifah, 2023).However, it is again apparent that these norms do not explicitly accommodate the characteristics of ransomware, which are not only destructive or disruptive but also contain elements of data-based extortion. The criminal sanctions for these acts are regulated in Articles 46 and 48 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, which provide criminal penalties for perpetrators of illegal access and manipulation of electronic data. However, these sanctions still follow the basic crime structure without considering the level of complexity and broad impact of ransomware attacks, especially on national critical infrastructure (Farisin, 2025). In this regard, the absence of criminal aggravation based on strategic impact indicates that positive law has not adopted the risk-based regulatory approach commonly used in protecting vital sectors.On the other hand, the link with Law Number 27 of 2022 concerning Personal Data Protection is also crucial, particularly Article 35, which requires personal data controllers to protect and ensure the security of personal data from unauthorized access, and Articles 65 and 67, which regulate criminal sanctions for the misuse of personal data. In the context of ransomware, the exfiltration and threatened publication of personal data can be classified as violations of these provisions. However, this law focuses more on protecting data subjects

rather than on comprehensive system or infrastructure protection, and therefore fails to address the dimensions of ransomware as a threat to national security (Novita, 2023).From a general criminal law perspective, ransomware acts can also be linked to provisions in the Indonesian Criminal Code, specifically Article 368 concerning extortion and Article 406 concerning destruction of property. However, the application of these provisions to cybercrime faces challenges due to the intangible nature of the protected object, which is electronic data. This raises issues in the construction of the offense and the burden of proof, thus emphasizing that ransomware in the current Indonesian legal system remains an implicit offense scattered across various norms, rather than a specifically and comprehensively formulated offense (Praptono, 2024). Therefore, although there is a legal basis for prosecuting ransomware perpetrators, these regulations remain partial and unable to accommodate the complexity and development of ransomware as a modern cybercrime with a widespread impact on national critical infrastructure.

Weaknesses and Challenges of Legal Policy in Countering Ransomware against National Critical Infrastructure

A fundamental weakness in Indonesian legal policy in countering ransomware lies in the lack of an explicit legal definition of ransomware in legislation. In Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, although there are provisions regarding illegal access in Article 30 and manipulation and interference with data in Articles 32 and 33, there is no single provision that expressly qualifies ransomware as a separate crime. Empirically, this situation makes it difficult for law enforcement officials to construct a comprehensive charge, as ransomware is a multi-layered crime involving illegal access, data control, and extortion. As a result, cases are often handled in a piecemeal manner, combining several articles that do not necessarily reflect the full nature of the crime, thus impairing legal certainty.

Furthermore, the absence of specific regulations governing the protection of national critical infrastructure indicates a significant gap in the Indonesian legal system. Although Article 33 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions prohibits acts that disrupt electronic systems, this provision fails to distinguish between ordinary systems and systems of national strategic value. Empirically, various sectors such as healthcare, energy, and transportation still lack specific legal protection standards against cyber threats. Therefore, when a ransomware attack occurs, the impact is not only technical but also disrupts public services and may even endanger public safety. This shows that positive law has not adopted a risk-based approach to protecting vital state assets.

Another significant weakness is the institutional fragmentation of national cybersecurity governance, which leads to suboptimal coordination between agencies. Normatively, cybersecurity-related authority is spread across various institutions without a unified legal framework. Although Law Number 27 of 2022 concerning Personal Data Protection, through Article 58, regulates the establishment of a personal data protection supervisory agency, this regulation is limited to the personal data aspect and does not cover overall system security. Empirically, this situation often leads to overlapping authority and slow responses to cyber incidents, including ransomware, due to the lack of a clear command and coordination mechanism for handling national-scale incidents.

From a preventive perspective, the weakness of mandatory cybersecurity standards also poses a serious challenge. Although Article 16 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions requires electronic system operators to maintain reliable and secure systems, this norm remains general in nature and is not accompanied by binding technical standards. Empirically, many institutions, including those managing critical infrastructure, lack adequate cybersecurity preparedness, leaving them vulnerable to ransomware attacks. Furthermore, the limited availability of rapid and integrated incident response mechanisms often results in reactive and ineffective attempts to mitigate their impact.

From a law enforcement perspective, digital evidence collection is a major challenge, primarily due to the use of encryption technology, the anonymity of perpetrators through the dark web, and the use of cryptocurrency for transactions. Although Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions recognizes electronic information and documents as valid evidence, in practice, digital forensics still faces various technical and legal challenges. Empirically, law enforcement officials often struggle to track perpetrators, identify the flow of funds, and prove the causal relationship between their actions and the resulting losses, resulting in low resolution rates for ransomware cases.

Another significant challenge is the nature of ransomware as a cross-border crime that requires effective international cooperation. In practice, ransomware perpetrators often operate from different jurisdictions, posing challenges to national law enforcement. Although Indonesia has an international cooperation framework for combating cybercrime, its implementation remains suboptimal. Empirically, extradition processes, data exchange, and coordination between countries are often time-consuming and ineffective in dealing with fast-paced and dynamic crimes such as ransomware. This situation is further exacerbated by the limited capacity of law enforcement officials to address technological developments, thus highlighting the gap between legal norms — a legal gap — and law enforcement implementation — an enforcement gap — underpinning the urgent need for legal policy reconstruction in this area.

Reconstruction of Legal Policy in Countering Ransomware Attacks on National Critical Infrastructure in Indonesia

Reconstruction of legal policy in countering ransomware attacks on national critical infrastructure in Indonesia must begin with the establishment of legal norms that explicitly regulate ransomware as a separate criminal offense within the national legal system. In this context, lawmakers need to revise existing laws or enact new ones that complement the regime of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions by including a legal definition of ransomware, elements of the offense that encompass illegal access, data encryption or locking, and electronic system-based extortion, as well as increased criminal penalties for attacks targeting national critical infrastructure. Concrete actions that can be taken include the development of academic papers and a special bill on advanced cybercrime that accommodates evolving ransomware modus operandi and harmonizes them with provisions in general criminal law.

Strengthening regulations for protecting national critical infrastructure needs to be implemented through a risk-based approach that classifies strategic sectors based on their level of vulnerability to cyberattacks. In this regard, the government needs to establish binding derivative regulations requiring every critical infrastructure operator to meet specific cybersecurity standards, including mandatory periodic security audits, the implementation of intrusion detection systems, and mandatory reporting of cyber incidents. Concrete actions that can be taken include the creation of government regulations or presidential regulations on protecting national critical infrastructure that integrate technical and legal aspects and align with the data protection obligations stipulated in Law Number 27 of 2022 concerning Personal Data Protection.

Legal policy reform must also include the establishment of mandatory and measurable cybersecurity standards. The provisions in Article 16 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, which regulate the obligation of electronic system operators to provide reliable and secure systems, need to be translated into concrete and binding operational standards. Concrete actions in this regard include the development of national cybersecurity standards that adhere to international practices, such as ISO/IEC 27001, which are mandatory for all critical infrastructure sectors, along with certification mechanisms and administrative sanctions for those who fail to meet these standards.

Furthermore, institutional integration within the national cybersecurity system is needed to address the fragmentation of authority that has been a significant obstacle. This reconstruction can be achieved through the establishment of a single national cybersecurity authority with coordinating and operational authority for the prevention, detection, and handling of cyberattacks, including ransomware. Concrete actions include strengthening existing institutional mandates through new regulations that clearly define the division of authority, and establishing a national cyber incident response command center that operates in real time to handle attacks on critical infrastructure.

In terms of law enforcement, reconstruction must also be directed at reformulating the digital evidence system in criminal procedure law to make it more adaptable to technological developments. The provisions regarding electronic evidence in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions need to be strengthened with technical regulations regarding digital forensics, cryptocurrency transaction tracking, and collaboration with global digital service providers. Concrete actions that can be taken include increasing the capacity of law enforcement officers through specialized training in digital forensics, establishing a dedicated integrated cybercrime handling unit, and developing a digital tracking system based on the latest technology.

Legal policy reconstruction must be supported by the strengthening of international cooperation and the adoption of best practices from other countries that have successfully addressed ransomware. Indonesia needs to develop more effective cross-border cooperation mechanisms for data exchange, extradition, and digital asset tracing. Concrete actions include ratifying international conventions on cybercrime, expanding cooperation networks with international law enforcement agencies, and establishing a national legal framework aligned with global standards. This will ensure that the resulting legal policy reconstruction is not only

normative but also operational and implementable, addressing the real challenges of countering ransomware against national critical infrastructure.

CONCLUSION

Based on the discussion, it can be concluded that Indonesia's positive legal regulations for dealing with ransomware attacks on national critical infrastructure essentially have a normative basis through Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection. However, these regulations remain partial, implicit, and unable to accommodate the complexity of ransomware as a modern cybercrime. The absence of a legal definition of ransomware, the absence of specific regulations regarding the protection of national critical infrastructure, and weak cybersecurity standards indicate a legal gap. Furthermore, law enforcement challenges such as limited digital evidence, perpetrator anonymity, and the transnational nature of ransomware create an enforcement gap. This situation indicates that the existing legal system remains reactive and unable to provide comprehensive protection against threats that have broad impacts on national security, economic stability, and public safety.

Therefore, it is recommended that legal policy be reconstructed to be comprehensive, adaptive, and risk-based in dealing with ransomware in Indonesia. Concrete steps that can be taken include the creation of specific legal norms that explicitly regulate ransomware as a separate crime with increased penalties for attacks on critical infrastructure, the development of specific regulations regarding the protection of national critical infrastructure, and the implementation of mandatory and measurable cybersecurity standards. Moreover, institutional strengthening is needed through the integration of national cybersecurity systems, increasing the capacity of law enforcement officers in the field of digital forensics, and optimizing international cooperation in handling cross-border cybercrime. This is expected to construct a cyber legal system that is not only repressive but also preventive and responsive to technological developments, thereby ensuring Indonesia's digital sovereignty and national security in a sustainable manner.

REFERENCE

Afifah, D. (2023). Perlindungan Konsumen Di Sektor Jasa Keuangan Pada Kasus Serangan Siber Ransomware Yang Menimpa Perbankan. Jiip-Jurnal Ilmiah Ilmu Pendidikan, 9318-9323.

Anbiyaa, F. (2025). Model Pemolisian Siber: Pendekatan Community Policing Dan E-Policing Dalam Penanggulangan Kejahatan Ransomware. Cerdika: Jurnal Ilmiah Indonesia, 53.

Apollyus, E. (2022). Eskalasi Reproduksi Cybercrime Pada Masa Pandemi Covid-19. Nusantara: Jurnal Ilmu Pengetahuan Sosial, 2063-2069.

Chowdhury, R. H. (2022). Digital government initiatives and national resilience: How digital governance frameworks were transformed post-COVID to maintain national services. *World Journal of Advanced Engineering Technology and Sciences*, *7*(1), 224–240.

Desouza, K., Watson, R. T., & Xie, Y. (2025). *Managing Digital Dependencies in a Connected Society: Policy Options for Ecosystem Transitivity*.

Erwin, E. P. (2023). Transformasi Digital. Jambi: Pt. Sonpedia Publishing Indonesia.

Farisin, M. S. (2025). Menjaga Keamanan Digital Strategi Serta Kebijakan Swiss Dalam Mengatasi Ancaman Ransomware. Interdependence Journal Of International Studies, 69-80.

Harahap, A. R. (2022). Perlindungan Hukum Terhadap Sistem Pembayaran Transaksi Elektronik Lintas Batas Negara. Pekalongan: Nem.

Irfan, B. A. (2023). Pelayanan Publik Era Digital: Studi Literatur. Indonesian Journal Of Intellectual Publication, 23-31.

Jubhari, A. R. (2022). Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus Ransomware Wannacry Di Indonesia. Makassar: Universitas Hasanuddin.

Kurniawan, I. A. (2021). Penyebaran Virus Ransomware Wannacry Berdasarkan Undang-Undang No. 11 Tahun 2008. Penyebaran Virus Ransomware Wannacry Berdasarkan Undang-Undang No. 11 Tahun 2008, 427-432.

Nabila, F. I. (2024). Evaluasi Terhadap Kebocoran Data Dalam Sistem Perbankan Di Indonesia (Studi Kasus Ransomware Pada Bank Syariah Indonesia). Al-Qisth Law Review, 295-310.

Novita, A. P. (2023). Cyber Security Threats; Analisis Dan Mitigasi Resiko Ransomware Di Indonesia. Jurnal Ilmiah Sistem Informasi, 160-169.

Praptono, A. A. (2024). Tinjauan Kriminologi Terhadap Pelaku Kejahatan Pemerasan Dengan Menggunakan Virus, Ransomware Wannacry Sebagai Suatu Kejahatan Modern. Jurnal Intelek Dan Cendikiawan Nusantara, 1660-1669.

Ramadhan, G. (2023). Perlidungan Hukum Bagi Korban Ransomware Wannacry. Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat, 102.

Robbi, S. W. (2025). Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Ransomware Dalam Perspektif Peraturan Perundang-Undangan. Pampas: Journal Of Criminal Law, 282-295.

Simorangkir, A. S. (2024). Ransomware Pada Data Pdn Implikasi Etis Dan Tanggung Jawab Profesional Dalam Pengelolaan Keamanan Siber. Journal Sains Student Research, 324-331.

Sulubara, S. M. (2024). Perlindungan Data Pribadi Dalam Kasus Ransomware: Apa Kata Hukum? Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara, 426-434.

Tus, D. S. (2021). Perlindungan Hukum Bagi Korban Serangan Ransomware. Vyavahara Duta, 126-136.

Wildan, A. A. (2025). Analisis Dan Evaluasi Peraturan Pemerintah No. 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (Pste) Dalam Menanggulangi Kejahatan Ransomware Di Indonesia. Academos Jurnal Hukum Dan Tatanan Sosial, 41.