Aliansi : Jurnal Hukum, Pendidikan dan Sosial Humaniora
Volume. 2, Nomor.5 September 2025
e- ISSN: 3031-9706; p- ISSN: 3031-9684, Hal 240-249
DOI: https://doi.org/10.62383/aliansi.v2i5.1234
Available online at: https://journal.appihi.or.id/index.php/Aliansi

.

Legal Protection Against Cybercrime from Ransomware Attacks and Evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's Defense

Seri Mughni Sulubara[1*], Virdyra Tasril [2], Nurkhalisah [3]
[1,3] Muhammadiyah Mahakarya Aceh University, Bireun, Indonesia
[2] Medan State Polytechnic, Medan, Indonesia

*Author Correspondence: serimughni@ummah.ac.id**

Abstract. *This research examines in-depth legal protection against cybercrime in Indonesia, with a specific focus on ransomware attacks. It also evaluates the 2025 Draft Cyber Security and Resilience Law (RUU KKS) as a measure to strengthen the national cyber defense system. The increase in ransomware cases targeting personal data, public institutions, and vital infrastructure has posed a serious threat to information security and national stability. Although the 2008 Electronic Information and Transactions Law (UU ITE) and the 2022 Personal Data Protection Law (UU PDP) serve as the legal basis, these two regulations do not yet specifically and comprehensively regulate ransomware. This results in challenges in law enforcement and victim protection, both in technical aspects, coordination, and human rights protection. The research method used is normative legal with a qualitative approach, which includes analysis of primary and secondary legal materials, as well as comparisons with regulations in several countries that have more mature ransomware handling mechanisms. The analysis of the 2025 Cyber Security Bill (RUU KKS) indicates that this draft regulation has the potential to strengthen the authority of cyber authorities, mandate reporting of cyber incidents, and impose stricter sanctions on perpetrators. However, implementing this policy requires effective cross-agency coordination, transparent oversight, and synergy between the public and private sectors. This study concludes that the 2025 Cyber Security Bill (RUU KKS) represents a strategic step in building a national cybersecurity system that is adaptive, integrated, and responsive to evolving cyber threats. However, its success will depend heavily on improving public digital security literacy, multi-sectoral collaboration, investment in detection and prevention technology, and guaranteeing human rights protection. These findings are expected to provide input for policymakers in formulating comprehensive and sustainable cybersecurity regulations as a bulwark of national defense in the digital era.*

Keyword: *Cybercrime, Evaluation, Indonesia's Defense, Legal Protection, Ransomware Attack.*

1. INTRODUCTION

Cybercrime is a crime committed using information and communication technology. In a legal context, cybercrime is not only related to criminal offenses but also raises civil issues, particularly concerning the protection of rights and the losses suffered by victims (I. Seri Mughni Sulubara, 2024). The ITE Law serves as the primary legal framework for addressing cybercrime in Indonesia, regulating various cybercrimes such as unauthorized access, the dissemination of negative content, and electronic fraud. Additionally, civil law governs disputes over electronic contracts and the protection of intellectual property rights, which often become the subject of disputes in the digital (Sulubara, Fauzi, et al., 2025). Cybercrime not only causes criminal losses but also material and immaterial losses that impact civil rights such as the right to personal data, intellectual property rights, and consumer rights (Sulubara, 2024). Civil law studies are needed to provide legal protection against such losses and to provide compensation mechanisms for victims. Many cybercrime cases, such as online fraud or

Received: Juni 23, 2025; Revised: Juli 19, 2025; Accepted: Agustus 05, 2025; Online Available: Agustus 08, 2025

defamation in the virtual world, can be resolved through civil channels, such as compensation claims or demands for the cessation of unlawful acts (A. A. Seri Mughni Sulubara, 2024).

The development of digital technology has had a major impact on the lives of Indonesians. In this era of rapid digital transformation, cybercrime threats including ransomware attacks continue to increase, threatening the security of individuals, state institutions, and even vital national infrastructure. Ransomware has become one of the most prominent types of cybercrime, in which perpetrators lock victims' data and demand a ransom to return it. Statistics for 2024 show that Indonesia has the highest number of ransomware attacks in Southeast Asia, with thousands of cases involving public institutions and the private sector, including major attacks on the National Data Center and leading banks (I. Seri Mughni Sulubara, 2024). As a result, various public services have been disrupted, and citizens' personal data is at risk of being leaked and exploited by irresponsible parties. Amidst this situation, legal protection against cybercrime in Indonesia still faces various challenges. The main legal basis currently in force, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and the Personal Data Protection Law of 2022, has regulated various aspects of crime and data protection (Azrica & Sulubara, 2023). However, the increasingly complex nature of cybercrime demands adaptive and integrated legal regulations and systems. Some studies even suggest that protection for victims remains inadequate, with penalties and recovery mechanisms not commensurate with the scale of losses caused by cybercrime, particularly ransomware (Sulubara et al., 2024).

The Indonesian government also recognizes the urgency of strengthening the national cyber defense and security system. One strategic step is to include the Cyber Security and Resilience Bill (RUU KKS) as a top priority in the 2025 National Legislation Program (Prolegnas). This bill is expected to not only serve as a solid foundation for handling cyber incidents at the national level, but also to strengthen multi-sector coordination in protecting digital infrastructure, enforcing effective law enforcement, and increasing public awareness and education. The RUU KKS is designed to address the need for up-to-date regulations, regulate the obligations of all relevant parties, and impose strict sanctions for violations, whether by individuals or corporations. The transformation of Indonesia's cyber defense system also requires integration between legal, technological, educational, and international cooperation aspects to create a safe and resilient digital space (Sulubara & Tasril, 2025). Therefore, a critical evaluation of the 2025 Cyber Security and Resilience Bill is crucial to producing effective regulations to protect the nation from cybercrime, particularly ransomware attacks, which continue to pose a real threat to national resilience and public welfare (Sulubara et al., 2024).

Legally, efforts to protect against ransomware crimes in Indonesia are currently based on the Electronic Information and Transaction Law (ITE Law) of 2008 and the Personal Data Protection Law (PDP Law) of 2022. The UU ITE includes provisions criminalizing extortion in the digital realm, while the UU PDP regulates obligations for securing personal data and reporting data breaches. However, neither regulation specifically or comprehensively addresses ransomware as a distinct criminal offense, leaving law enforcement and victim protection facing various challenges (Botchkovar et al., 2025). To address this issue, the Indonesian government has initiated the 2025 Cyber Security and Resilience Bill (RUU KKS) as a strategic step to strengthen the national cyber defense system. This bill aims to provide a more holistic and adaptive legal framework by regulating the authority of the National Cyber Agency as the main authority, incident handling mechanisms, reporting obligations, and imposing stricter sanctions on cybercriminals, including ransomware. The RUU KKS also encourages multisectoral collaboration to create a more resilient and sustainable digital security ecosystem (Bhunia et al., 2025). Cybercrime is transnational and dynamic in nature, so national regulations must be balanced with international cooperation and increased capacity for surveillance, education, and digital security literacy among the public. This research supports the development of an integrated and sustainable cyber defense strategy in Indonesia. Therefore, this research is crucial to ensure that Indonesia has responsive, effective legal systems and cybersecurity policies capable of protecting the nation and its people from ransomware attacks that could significantly undermine national resilience (Botchkovar et al., 2025).

2. RESEARCH METHOD

The research titled “Legal Protection Against Cybercrime from Ransomware Attacks and Evaluation of the 2025 Cyber Security and Resilience Bill in Indonesia's Defense” uses a normative legal research method with a qualitative-descriptive approach (Zainuddin & Karina, 2023). The following is a detailed description of the methods that can be used, namely legal research that examines primary and secondary legal materials, as well as analyzing concepts, regulations, and literature related to legal protection against cybercrime and the 2025 Cyber Security and Resilience Bill to describe the phenomenon of ransomware attacks, legal responses, and the effectiveness of regulations in depth. The primary legal materials include:

1) Law No. 11 of 2008 on ITE.
2) Personal Data Protection Law of 2022.

3) Draft/Bill on Cyber Security and Resilience 2025.
4) Official government documents related to cyber security.

Secondary legal materials include journals, books, research reports, and relevant news articles on ransomware cases, cybercrime trends, and evaluations of cybersecurity regulations in Indonesia and other countries. Data collection techniques include library research, as well as searching digital documents and legal databases. Data analysis techniques involve descriptive analysis by interpreting legislation, legal concepts, and comparing the applicable legal logic (Soekanto, 2019). The research will focus on case studies of cyber attacks in Indonesia during the period 2024–2025, with a scope covering strategic government institutions and national public data. This method provides a systematic framework for assessing the effectiveness of legal protection against ransomware threats and evaluating the readiness of cybersecurity regulations to strengthen national defense in the digital age.

3. RESULT AND DISCUSSION

From 2024 to mid-2025, Indonesia experienced a surge in ransomware cases, making it the country with the most incidents in Southeast Asia. Many strategic government agencies, hospitals, and financial institutions were targeted, including the hacking of important data at the National Data Center and a number of major banks. The impacts include the disruption of public services, the leakage of personal data, and significant financial and reputational losses for the victims. The 2008 ITE Law and the 2022 Personal Data Protection Law serve as the primary legal framework for protecting against cybercrime and ransomware in Indonesia. However, both regulations are deemed to have loopholes (Li & Liu, 2021). The ITE Law focuses more on criminalizing actions and does not detail mechanisms for compensating ransomware victims. Meanwhile, the PDP Law is still new, and the challenge lies in its implementation and enforcement, which are not yet optimal, particularly in terms of preventive sanctions and aspects of victim compensation. The 2025 KKS Bill was drafted to address the escalating cyber threats, including ransomware, and is a key focus in the 2025 National Legislation Program (Sarkar & Shukla, 2023).

The draft bill proposes expanded regulations: from incident handling authorities, attack reporting obligations, strategic asset protection, to heavier sanctions against cyber attackers. The bill also encourages multisector collaboration government, private sector, and community in improving national digital defense (Alshehri, 2025). However, there are critical concerns regarding inter-agency coordination, overlapping authorities, and the potential weakening of individual data protection if there is no strict oversight of cyber authorities. Ransomware threats are one of the most concerning forms of cybercrime, posing a risk to the security of the country's data and critical infrastructure. In Indonesia, legal protection against such cybercrimes currently relies on several key legal frameworks, such as the 2008 Electronic Information and Transactions Law (EIT Law) and the 2022 Personal Data Protection Law (Dafoe et al., 2024). However, both regulations face several limitations, for example, the ITE Law focuses more on criminalization without regulating detailed victim recovery mechanisms, and the Personal Data Protection Law still needs to be strengthened, especially in terms of preventive sanctions and protection of ransomware victims' data (Almotiri, 2025).

Countries such as Singapore and South Korea have adopted integrated and responsive cyber legislation models, and regularly conduct incident simulations and policy updates. Indonesia still needs to strengthen regulatory synergy and improve its rapid response capabilities (incident response), education, and national cyber surveillance. Indonesia needs adaptive and effective cyber regulations to deal with ransomware threats (Tubaishat & Alaleeli, 2024). The 2025 Cyber Security and Resilience Bill is an important step, but its implementation must be accompanied by strengthening the legal, technological, and educational ecosystems, as well as cross-sectoral and international cooperation. Continuous evaluation and oversight are needed to ensure that legal protection can truly shield society and the state from cybercrime. Legal protection against ransomware crimes under Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) is primarily regulated through several articles that criminalize actions related to ransomware as a form of extortion and cybercrime. The key points are as follows (Sulubara, Tasril, et al., 2025):

1. Article 27 paragraph (4) of the ITE Law regulates the prohibition of disseminating electronic information that contains extortion. Ransomware is considered a criminal act of extortion because the perpetrator threatens the victim by locking or holding the victim's electronic data hostage and demanding a ransom to unlock it. This article serves as the legal basis for prosecuting ransomware perpetrators in Indonesia with criminal penalties.
2. Linkage with Article 368 paragraph (1) of the Criminal Code concerning extortion as the main criminal offense in ransomware cases, where ransomware fulfills the elements of extortion carried out by threatening or blocking access to the victim's data.
3. Article 27B paragraph (1), Article 30 paragraphs (1) & (2), and Article 32 paragraph (1) of the ITE Law are also referred to as the legal framework for ransomware perpetrators. However, there is still ambiguity in the norms and there is no article in the ITE Law that explicitly regulates ransomware crimes as a separate legal threat. This

creates difficulties in proving and enforcing the law in ransomware cases.

4. Criminal sanctions in the form of imprisonment and/or fines are imposed on ransomware perpetrators as a form of criminal liability under these provisions. Cases that have been handled use the ITE Law together with the Criminal Code as the legal basis for prosecution (Seri Mughni Sulubara, Hidayati Purnama Lubis, Nanci Yosepin Simbolon, 2024).

Protection for victims is also recommended in the form of strengthening cyber defense and cooperation between the government and the public. However, the legal mechanisms for compensation or recovery for ransomware victims are still lacking in detail in the ITE Law, so revisions and further regulatory strengthening are needed (Achuthan et al., 2025). Legal protection against ransomware crimes in Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia focuses on the regulation of the collection, processing, and storage of personal data, as well as the rights of personal data subjects who are vulnerable to ransomware attacks. The PDP Law serves as a legal framework that provides comprehensive protection for personal data, including in situations of violations caused by ransomware that result in the leakage and illegal use of personal data. The PDP Law regulates the obligations of personal data controllers and processors to maintain data security, including anticipating the risk of ransomware attacks that could result in the loss of control over personal data (Alzakari et al., 2025). The PDP Law imposes strict sanctions on parties who intentionally and unlawfully obtain, disclose, use, or falsify personal data that is not their right, which can be exploited in the context of ransomware crimes. For example, someone who illegally discloses the personal data of a ransomware victim can be sentenced to 4-5 years in prison and/or fined billions of rupiah (Article 67 of the PDP Law) (Yan & Khoei, 2025). Personal data managers who experience data breaches due to ransomware are required to report to the competent authorities and to the subjects of personal data in accordance with the provisions of the PDP Law and its implementing regulations. This is important for further mitigation and protection of victims (Afraji et al., 2025). The PDP Law strengthens the protection of ransomware victims, which has not been detailed in the ITE Law, particularly regarding the rights of data subjects, compensation mechanisms, and prevention of data misuse after the incident. Although the PDP Law provides a clearer legal framework, its implementation still requires strengthened oversight, education, and coordination among institutions, as ransomware is a complex crime involving both technological and legal aspects (Hossain et al., 2025). Thus, the 2022 Personal Data Protection Law strengthens Indonesia's legal protection system against ransomware attacks by providing a legal framework to safeguard personal data security, imposing sanctions on data violators, and mandating the reporting of data breach incidents. The existence of this law complements the ITE Law in providing a more adaptive and protective legal framework for victims of cyber ransomware crimes in Indonesia (Onwuadiamu, 2025).

4. CONCLUSION

Legal protection against ransomware crimes in Indonesia is currently primarily based on the Electronic Information and Transactions Law (ITE Law) of 2008 and the Personal Data Protection Law (PDP Law) of 2022 (Seri Mughni Sulubara, 2024). The ITE Law criminalizes ransomware as part of extortion offenses (Article 27(4) of the ITE Law and Article 368 of the Criminal Code), with penalties including imprisonment and fines. However, the ITE Law does not explicitly address ransomware specifically, leading to legal ambiguity that complicates enforcement. The PDP Law provides a more comprehensive legal framework for personal data protection, including data security obligations, incident reporting requirements, and stringent penalties for data breaches, thereby strengthening the protection of ransomware victims from a personal data perspective (Sulubara, Fauzi, et al., 2025). The 2025 Cyber Security and Resilience Bill (RUU KKS) is a strategic step by the Indonesian government to strengthen the national cyber defense system and provide a more comprehensive and integrated legal basis for dealing with ransomware threats and other cyber crimes. This bill regulates the authority of the main cyber authority (National Cyber Agency), incident reporting obligations, protection of strategic assets, and stricter law enforcement mechanisms (Sulubara, 2024). A multi-sector approach and inter-agency collaboration, including public participation and independent oversight, are designed to enhance the effectiveness of national cyber security protection and response. However, greater attention is needed on inter-agency synergy, human rights protection, and improving public cyber literacy as part of a resilient cyber defense ecosystem (A. A. Seri Mughni Sulubara, 2024).

Overall, Indonesia already has an initial legal framework to prosecute ransomware perpetrators and protect victims through the ITE Law and the PDP Law, but it still requires more adaptive and comprehensive regulations and implementation. The 2025 Cyber Security Bill is expected to serve as an instrument capable of addressing the complexities of modern cyber threats by providing more effective legal protection and a robust national defense system. Continuous monitoring, education, international cooperation, and transparency are key factors in ensuring the success of such legal protection and Indonesia's resilience in facing the growing and increasingly damaging ransomware attacks.

REFERENCE

Journals/Proceedings :

Achuthan, K., Khobragade, S., & Kowalski, R. (2025). Cybercrime through the public lens: A longitudinal analysis. *Humanities and Social Sciences Communications*, 1–16. https://doi.org/10.1057/s41599-025-04459-x

Afraji, D. M. A. A., Lloret, J., & Peñalver, L. (2025). Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments. *Cyber Security and Applications, 3*(September 2024), 100085. https://doi.org/10.1016/j.csa.2025.100085

Almotiri, S. H. (2025). AI driven IoMT security framework for advanced malware and ransomware detection in SDN. *Journal of Cloud Computing*, *14*(1). https://doi.org/10.1186/s13677-025-00745-w

Alshehri, A. (2025). Developing a multi-layer agent framework to enhance AI-generated educational questions for cybersecurity. *Journal of Umm Al-Qura University for Engineering and Architecture*. https://doi.org/10.1007/s43995-025-00136-x

Alzakari, S. A., Aljebreen, M., Ahmad, N., Alhashmi, A. A., Alahmari, S., Alrusaini, O., Al-Sharafi, A. M., & Almukadi, W. S. (2025). An intelligent ransomware-based cyberthreat detection model using multi-head attention-based recurrent neural networks with optimization algorithm in IoT environment. *Scientific Reports*, *15*(1), 1–21. https://doi.org/10.1038/s41598-025-92711-4

Azrica, H., & Sulubara, S. M. (2023). Legalitas transaksi e-commerce dalam platform Shopee ditinjau dalam Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek), Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan perspektif fiqih muamalah. *Hakim: Jurnal Ilmu Hukum dan Sosial*, *1*(3), 1–23. https://doi.org/10.51903/hakim.v1i3.1305

Bhunia, S., Blackert, M., Deal, H., DePero, A., & Patra, A. (2025). Analyzing the 2021 Kaseya ransomware attack: Combined spearphishing through SonicWall SSLVPN vulnerability. *IET Information Security*. https://doi.org/10.1049/ise2/1655307

Botchkovar, E., Cui, K., Antonaccio, O., Perkins, R., & Maimon, D. (2025). The organized activities of ransomware groups: A social network approach. *Technology in Society*, *82*(February), 102873. https://doi.org/10.1016/j.techsoc.2025.102873

Dafoe, J., Chen, N., Chen, B., & Wang, Z. (2024). Enabling per-file data recovery from ransomware attacks via file system forensics and flash translation layer data extraction. *Cybersecurity*, *7*(1). https://doi.org/10.1186/s42400-024-00287-9

Hossain, M. A., Hasan, T., Ahmed, F., Cheragee, S. H., Kanchan, M. H., & Haque, M. A. (2025). Towards superior Android ransomware detection: An ensemble machine learning perspective. *Cyber Security and Applications*, *3*(July 2024), 100076. https://doi.org/10.1016/j.csa.2024.100076

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cybersecurity: Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Oh, D. B., Kim, D., & Kim, H. K. (2024). volGPT: Evaluation on triaging ransomware process in memory forensics with large language model. *Forensic Science International: Digital Investigation*, *49*(S), 301756. https://doi.org/10.1016/j.fsidi.2024.301756

Onwuadiamu, G. (2025). Cybercrime in criminology: A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*(February), 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*(September), 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Seri Mughni Sulubara, A. A. (2024). Legalitas fintech peer-to-peer lending pinjaman online dalam aspek hukum konvensional. *MANDUB: Jurnal Politik, Sosial, Hukum dan Humaniora*, *2*(2), 177–187. https://doi.org/10.59059/mandub.v2i2.1184

Seri Mughni Sulubara, H. P. L., Simbolon, N. Y., & F. R. (2024). *Teori hukum perdata (Studi kasus: Transaksi e-commerce Shopee Paylater)* (Edisi pertama). Tahta Media Group.

Seri Mughni Sulubara, I. (2024). Regulasi dan lisensi mengenai perlindungan hukum investor di platform fintech peer-to-peer lending dalam hukum konvensional. *Jurnal Hukum, Politik dan Ilmu Sosial*, *3*(4), 431–442. https://doi.org/10.55606/jhpis.v3i4.4499

Seri Mughni Sulubara. (2024). Perlindungan data pribadi dalam kasus ransomware: Apa kata hukum? *Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara*, *2*(November), 426–434. https://doi.org/10.55606/eksekusi.v2i4.1823

Soekanto, S. (2019). Penelitian hukum normatif. *Hukum*, *1*(1), 4.

Sulubara, S. M. (2024). Menyajikan berbagai insiden cybercrime yang terjadi di Indonesia, termasuk pencurian data dan peretasan situs web pemerintah. *Konsensus: Jurnal Ilmu Politik dan Komunikasi*, *1*(6), 199–206. https://doi.org/10.62383/konsensus.v1i6.692

Sulubara, S. M., & Tasril, V. (2025). Legal protection of cybercrime crimes from ransomware attacks and evaluation of the Cyber Security and Resilience Bill 2025 in Indonesia's defense. *De Lega Lata: Jurnal Ilmu Hukum*, *10*(December), 287–297. https://doi.org/10.30596/dll.v10i2.25786

Sulubara, S. M., Fauzi, H., Muslim, B., Ferdiansyah, M. F., & Musmulyadi, M. (2025). Judi online sebagai cybercrime serta tantangan penegakan hukum pidana di era digital: Antara regulasi, pembuktian, dan ancaman cybercrime. *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora*, *4*(2), 539–552. https://doi.org/10.55606/jurrish.v4i2.4990

Sulubara, S. M., Lubis, H. P., & Simbolon, N. Y. (2024a). Legal review of electronic commerce-based buying and selling on the Shopee platform against consumers using Shopee PayLater. *Proceeding of IROFONIC 2024, Proceeding*(02), 392–402.

Sulubara, S. M., Lubis, H. P., & Simbolon, N. Y. (2024b). Legality of Shopee PayLater payments for Shopee platform e-commerce transactions in conventional law. *DELEGALATA Jurnal Ilmu Hukum*, *9*(2), 247–256. https://doi.org/10.30596/dll.v9i2.20414

Sulubara, S. M., Tasril, V., & Nurkhalisah. (2025). *Perlindungan hukum tindak pidana cybercrime dalam cyberlaw di Indonesia: Perkembangan teknologi dan tantangan hukum dalam mewujudkan cybersecurity* (Edisi pertama). Tahta Media.

Tubaishat, A., & Alaleeli, H. (2024). A framework to prevent cybercrime in the UAE. *Procedia Computer Science, 238*, 558–565. https://doi.org/10.1016/j.procs.2024.06.060

Yan, P., & Khoei, T. T. (2025). Securing the Internet of Things: A comprehensive review of ransomware attacks, detection, countermeasures, and future prospects. *Franklin Open*, 100256. https://doi.org/10.1016/j.fraope.2025.100256

Zainuddin, M., & Karina, A. D. (2023). Penggunaan metode yuridis normatif dalam membuktikan kebenaran pada penelitian hukum. *Smart Law Journal, 2*(2), 114–123. https://journal.unkaha.com/index.php/slj/article/view/26

Books:

Sulubara, S. M., Tasril, V., & Nurkhalisah. (2025). *Perlindungan hukum tindak pidana cybercrime dalam cyberlaw di Indonesia: Perkembangan teknologi dan tantangan hukum dalam mewujudkan cybersecurity* (Edisi pertama). Tahta Media.

Sulubara, S. M., Lubis, H. P., Simbolon, N. Y., & Razi, F. (2024). *Teori hukum perdata (Studi kasus: Transaksi e-commerce Shopee Paylater*; Edisi pertama; Tahta Media, Ed.). CV Tahta Media Group.

Legislation:

Criminal Code (KUHP).

Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2024).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (2022).

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. (1999).