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
https://creativecommons.org/licenses/by/4.0/

Cybersecurity and Personal Data Protection Challenges in the 5G Era as a Basis for Legal Regulatory Reform

Cepi Hendrayani[1], Richard[2]
[1]Universitas Borobudur, Jakarta, Indonesia, cepihendrayani@gmail.com
[2]Universitas Borobudur, Jakarta, Indonesia, richard@borobudur.ac.id

Corresponding Author: cepihendrayani@gmail.com[1]

Abstract: The development of 5G technology has brought about a significant transformation in digital connectivity with high speed, low latency, and extensive network capacity. However, it also poses serious challenges to cybersecurity and personal data protection. Although Indonesia has passed Law No. 27 of 2022 concerning Personal Data Protection, its implementation still faces significant obstacles, primarily due to the lack of an effective independent supervisory body as stipulated in Article 59. The weakens oversight of personal data processing and increases the risk of data exploitation by irresponsible parties. This situation is exacerbated by the increasing number of IoT devices connected via 5G networks, which opens up opportunities for more complex and widespread cyber threats. This research uses a normative juridical method with a statutory and conceptual approach to analyze existing regulatory gaps and the need for legal reforms that can address the challenges of the digital era. The research findings show that legal regulatory reforms, including strengthening the role of regulatory bodies and adjusting legal provisions related to personal data protection, are crucial for ensuring cybersecurity in the 5G era and providing effective protection for the public and critical digital infrastructure. Thus, this research is expected to form the basis for recommendations for adaptive and responsive legal policies to technological dynamics, particularly in the context of personal data protection and cyber risk mitigation.

Keyword: 5G, Cybersecurity, Personal Data Protection.

INTRODUCTION

The development of communications technology has reached a new milestone with the arrival of 5G networks, which offer data transmission speeds up to tens of times faster than previous generations (Sugiyatno et al., 2023). This technology not only accelerates human connectivity to the internet but also enables massive integration between devices on a global scale (Putra, Riski, Yahya, & Ramadhan, 2023). Sectors from industry, healthcare, transportation, and even government are shifting toward digital-based systems with a high dependence on 5G networks (Judijanto et al., 2025). This transformation demonstrates a new

direction for the development of digital civilization, transforming work patterns, economic systems, and social interactions (Junaedi et al., 2023). However, this massive technological advancement carries significant consequences for digital security governance and individual privacy. The expansion of 5G networks has fueled the explosion in the use of the Internet of Things (IoT), enabling various devices to connect and exchange data automatically (Ruseno et al., 2025). This phenomenon has increased the volume of personal data collected, stored, and processed by various parties, from technology corporations to government agencies. The openness of these systems widens the opportunity for cyberattacks that could potentially compromise data security and the integrity of user information (Sofyan et al., 2025). The risk of data breaches increases significantly because traditional security systems are no longer able to keep up with the complexity of 5G network architecture and the widespread distribution of IoT devices (Angellia et al., 2024). Failure to anticipate these threats could lead to mass privacy breaches and a decline in public trust in the national digital infrastructure.

The Indonesian government has responded to this technological development by enacting Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) as the legal basis for protecting citizens' privacy rights. This regulation marks a significant milestone because it provides, for the first time, explicit recognition of personal data as a legal object that must be systematically protected. This law establishes the basic principles of data processing, the rights of data subjects, the obligations of data controllers and processors, and administrative and criminal sanctions for violations (Sidik & Wiraguna, 2025). However, its implementation remains far from optimal because the oversight mechanism is not yet operating independently. Article 59 of the PDP Law mandates the establishment of an independent supervisory body, but to date, this has not been concretely realized, leaving oversight dependent on existing bureaucratic structures.

Cybersecurity is generally defined as a systematic effort to protect digital infrastructure, communication networks, and data from all forms of attack or unauthorized access. This term encompasses technical, legal, and administrative measures designed to maintain the integrity, confidentiality, and availability of digital information (Kurniawan, 2025). In the context of national policy, cybersecurity is an integral part of national resilience because it is directly related to the protection of the country's strategic information assets. Cybersecurity also demands cross-agency coordination and international collaboration, given that digital threats often cross borders and involve actors from multiple jurisdictions (Tobing et al., 2024). Therefore, a cybersecurity approach cannot be solely technology-based; it must also have a solid legal foundation.

The scope of cybersecurity encompasses the protection of personal data, electronic government systems, financial networks, and critical infrastructure such as energy and transportation. Its complexity increases with the convergence of the physical and digital worlds, where disruptions to digital systems can have direct implications for public safety (Syah et al., 2025). International standards such as ISO/IEC 27001 emphasize that cybersecurity must be managed as part of integrated organizational governance (Ramadhanty, 2024). At the national level, institutions such as the National Cyber and Crypto Agency (BSSN) play a role in establishing technical policies and strategic coordination. However, without strong regulatory support and effective legal protection mechanisms, cybersecurity has the potential to become little more than policy jargon without real implementation power.

The three main principles that underpin cybersecurity are confidentiality, integrity, and availability. The principle of confidentiality requires that information be accessible only to authorized parties, while integrity ensures that data is not altered without authorization (Pratama, Syaiful, & Rahman, 2024). The principle of availability ensures that systems and data can be used whenever needed without interruption (Munawar et al., 2023). These three

principles form the basic framework for designing information security systems worldwide. Failure to uphold any one of these principles can cause systemic damage that has a broad impact on public trust.

Personal data protection has a strong philosophical and constitutional basis because it relates to the right to privacy as a fundamental human right. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia affirms that everyone has the right to protection of themselves, their families, their honor, their dignity, and their property under their control. This provision serves as the constitutional basis for recognizing the right to personal data protection. In the realm of international law, similar rights are also regulated in the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17), which strengthens the position of privacy protection as a universal right that must be guaranteed by the state (Megantara et al., 2025).

Law Number 27 of 2022 affirms the legal status of personal data as a right that cannot be violated without a valid legal basis. This law regulates various data processing principles, including lawfulness, transparency, purpose limitation, and accountability (Pradana & Saragih, 2024). These principles are designed to ensure that every party processing data is responsible for the security and use of the data they collect. Data controllers' obligations include notifying data subjects in the event of a breach and ensuring that data is used for the agreed purposes (Salsabila & Wiraguna, 2025). These principles align with data protection practices in developed countries, which emphasize a balance between technological innovation and individual privacy rights.

Implementing personal data protection requires a strong commitment from the government, the private sector, and the public. These three elements must work together to ensure that all digital activities comply with applicable legal principles. The application of technology without due regard for ethical and legal aspects can have widespread negative impacts, including data misuse, algorithmic discrimination, and privacy violations (Nirwan & Sampurna, 2025). Public awareness of the importance of safeguarding personal data is also a crucial factor in strengthening legal protection. The higher the public's digital literacy, the stronger the legal resistance to privacy violations in cyberspace.

The Indonesian legal system already has several regulations related to cybersecurity and personal data protection, although they are not yet fully integrated. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments serve as the initial legal basis governing the use of information technology. Articles in the ITE Law address aspects of electronic system security and the responsibility of system administrators to maintain the confidentiality of user data. However, these provisions are still general and do not explicitly provide adequate protection for personal data. The introduction of the PDP Law complements and refines Indonesia's digital legal framework.

National cybersecurity policy is implemented through the role of the National Cyber and Crypto Agency (BSSN), which has the mandate to safeguard Indonesia's cyberspace sovereignty. This institution is tasked with coordinating digital infrastructure security and providing technical guidance against cyber threats (Maharani & Atman, 2025). Furthermore, there are a number of derivative regulations from ministries and agencies that govern data governance in specific sectors, such as finance, health, and education. This fragmentation of regulations often leads to overlapping authority and gaps in protection standards between sectors. Standardizing norms and establishing a coordinating framework is a strategic step to prevent partial implementation of national regulations.

International regulations, such as the European Union's General Data Protection Regulation (GDPR), served as the primary reference in the drafting of the Data Protection Law in Indonesia. The GDPR details data subject rights, consent mechanisms, and sanctions for violators, and its success has been used as a model for many other countries (Rinjani &

Firmansyah, 2025). Comparison with the GDPR shows that Indonesia still needs improvement, particularly in terms of independent supervisory institutions and law enforcement. Harmonization with global standards will strengthen international trust in the national data protection system, particularly in cross-border digital trade, which relies on the security and reliability of data exchange.

Satjipto Rahardjo's legal protection theory emphasizes that the law must function to provide justice and a sense of security for individuals whose rights are threatened. This principle is relevant to explaining why the state is obliged to protect personal data as part of citizens' rights. Legal protection does not solely take the form of sanctions, but also prevention of violations through clear regulations and effective institutions (Samin, 2024). This perspective positions the law not as a repressive instrument, but rather as a means of ensuring society's digital security.

The responsive legal theory developed by Philippe Nonet and Philip Selznick suggests that the law must adapt to social and technological changes (Djauzie, 2025). In the 5G era, this theory demonstrates the importance of flexible regulations to keep pace with the rapid dynamics of digital development. Overly normative regulations risk losing relevance as technology constantly changes. A responsive approach requires the state to continually adapt regulations to protect the public interest without stifling innovation. Thus, legal reform is a continuous need in line with developments in communication and information technology.

The cyber law and digital rights approach provide a new conceptual framework for human rights protection in the technological era. Digital rights encompass the rights to privacy, data security, access to information, and freedom of expression in cyberspace (Rif'at & Dompak, 2025). The approach emphasizes that digital space is not a lawless zone but rather needs to be regulated based on legal principles that guarantee justice and a balance between freedom and security. In the Indonesian context, strengthening the cyber law and digital rights paradigm can serve as a foundation for building a comprehensive regulatory system oriented toward human protection amidst technological advancements.

METHOD

This research employs a normative juridical method, a legal research method that focuses on analyzing applicable positive legal norms and the legal principles underlying their regulation. The approaches employed include a statutory and a conceptual approach. The statutory and regulatory approach examines legal provisions related to cybersecurity and personal data protection, such as Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, and various national policies regarding cybersecurity regulated by the National Cyber and Crypto Agency. Through this approach, the research assesses the effectiveness and appropriateness of applicable regulations in addressing the challenges of 5G technology and the threat of personal data leaks. The conceptual approach is used to examine relevant legal ideas, principles, and theories, such as the theory of legal protection, responsive legal theory, and the concept of the right to privacy as part of human rights. The method enables a broader understanding of how laws should be designed and implemented to adapt to technological advances. Through a combination of these two approaches, this study seeks to produce a comprehensive and argumentative analysis regarding the need for legal regulatory reform to strengthen personal data protection and cybersecurity in the digital era.

RESULTS AND DISCUSSION

Cybersecurity and Data Protection Challenges in the 5G Era

5G technology is the fifth generation of cellular network systems, delivering significant improvements in network capacity, speed, and efficiency compared to previous generations. 5G architecture is designed around the concept of network slicing, the ability to divide a single physical network into multiple virtual networks that can be used separately as needed. This technology also enables the implementation of edge computing, which moves data processing closer to the source, such as IoT devices and smart sensors. This change accelerates data delivery and reduces latency but also creates new points of vulnerability to cyberattacks. The complexity of 5G network structures increases the risk of data breaches and makes it difficult to control access to digital systems.

The 5G ecosystem massively expands inter-device connectivity through the Internet of Things (IoT), where millions of devices are connected to share data in real time. This system improves efficiency in various sectors such as transportation, healthcare, and manufacturing, but each connected device is a potential entry point for cyberattacks. Security threats arise because not all devices have strong encryption and authentication systems. Furthermore, decentralized data processing complicates oversight, especially for authorities responsible for maintaining information security. The combination of high connectivity and distributed architecture makes it increasingly difficult to comprehensively control personal data.

Innovations such as network slicing open up significant opportunities for more efficient digital services but also present new challenges in maintaining data security. Each virtual network created poses a different risk of exploitation, depending on the security level and policies implemented by the operator. Attacks on one virtual network have the potential to impact other networks if their isolation systems are not well designed. Reliance on network service providers to maintain data integrity raises legal liability issues in the event of a breach. Weaknesses in technical and institutional arrangements could threaten the stability of national cybersecurity in the future.

The use of edge computing in 5G systems shortens the communication path between users and data centers, increasing efficiency but posing risks to control and privacy. Data is no longer processed solely at the central server center, but also at various local nodes scattered throughout the network. This model makes traditional security mechanisms difficult to implement because encryption and authentication processes must be decentralized. Attacks on edge nodes can lead to data manipulation, eavesdropping, and even surreptitious system takeover. This situation demonstrates that increased network performance often comes with increased complexity of risks that must be anticipated.

Security threats in the 5G era are increasingly diverse and sophisticated, encompassing attacks targeting individuals, organizations, and even national infrastructure. One of the most common threats is data breaches, the leakage of personal data due to security system failures. Such incidents can be caused by weak encryption, misconfigurations, or attacks from external parties exploiting system vulnerabilities. Furthermore, phishing and malware attacks are increasingly being used to steal user credentials and access network systems without authorization. The widespread deployment of IoT devices expands the attack surface, making each device a potential weak point in the larger system.

Ransomware attacks are a serious threat that is increasing rapidly with the advancement of network technology. Attackers can encrypt the entire data of a company or public institution and demand a ransom to recover it. The impact of such attacks not only causes financial losses but also disrupts the operation of public services such as hospitals, transportation, and government agencies. The digital infrastructure that forms the backbone of public services can be paralyzed if its security system is not strengthened. This risk is

exacerbated when 5G systems are used to support critical services such as smart cities or smart energy grids, which rely heavily on real-time connectivity.

Public privacy is also threatened by increased monitoring and data collection by various parties utilizing 5G networks. The use of technologies such as sensors, smart cameras, and location-based applications generates vast volumes of personal data. Without transparent management mechanisms and strict legal restrictions, this data can be exploited for commercial or political purposes, violating citizens' privacy rights. Cyberattacks on personal data not only result in material losses but can also undermine the dignity and sense of security of individuals as legal subjects. Strengthening cybersecurity systems is a fundamental need to prevent the public's right to privacy from being further eroded by the tide of digitalization.

The implementation of Law Number 27 of 2022 concerning Personal Data Protection faces serious obstacles during its implementation, particularly related to institutional weaknesses as stipulated in Article 59. This article mandates the establishment of an independent supervisory agency tasked with monitoring, law enforcement, and dispute resolution related to personal data breaches. However, to date, such an agency has not been established, and oversight is still carried out by the Ministry of Communication and Informatics, which falls within the executive branch. This inseparable relationship between policymakers and supervisors creates potential conflicts of interest and diminishes the objectivity of law enforcement. This structural weakness is one of the main causes of weak data protection in Indonesia.

Law enforcement against personal data breaches also faces coordination issues between agencies such as the National Agency for National Security (BSSN), the Ministry of Communication and Informatics (Kominfo), and law enforcement officials. Lack of synchronization in authority and reporting mechanisms often hampers the investigation and prosecution of violations. The lack of uniform procedural standards results in overlapping responsibilities between institutions. This situation slows the state's response to data breach incidents, which should be handled quickly and measurably. Furthermore, the lack of human resources with expertise in digital forensics and cyber law undermines the effectiveness of the law enforcement system in this sector.

Industry players' compliance with data protection principles remains low. Many companies have not implemented data management policies that comply with the security standards stipulated in the Data Protection Law. Most businesses view data protection as an administrative burden, rather than a legal and ethical responsibility. The lack of public awareness and oversight means that obligations such as data breach notification, the appointment of a data protection officer, and secure data storage have not been fully implemented. The private sector's unpreparedness in implementing these legal principles has the potential to create legal risks in the future when enforcement systems begin to tighten.

Indonesia's cybersecurity legal framework remains fragmented and scattered across various sectoral regulations. Regulations in the public and private sectors are not yet coordinated, resulting in differing security standards across institutions. This disharmony creates difficulties in building a comprehensive data protection system. Government agencies have their own security protocols, while the private sector tends to use global standards that do not always align with national regulations. This discrepancy indicates the absence of a national cybersecurity framework capable of unifying various policies under a single, consistent legal system.

The absence of a unified cybersecurity framework hampers effective responses to cross-sectoral cyber threats. Each agency tends to work independently without clear coordination, often delaying mitigation measures. Developed countries have developed national cybersecurity strategies that serve as a single guideline for addressing digital threats,

while Indonesia still relies on sectoral regulations. The lack of coordination raises the risk of legal loopholes that can be exploited by cybercriminals. The development of a national policy that unifies security standards across agencies is an urgent need for national digital security.

National data security standards are also not fully aligned with global practices such as the European Union's GDPR or the United States' NIST Cybersecurity Framework. These differences in standards complicate international cooperation and cross-border data exchange, which require equivalent levels of protection. This inconsistency has the potential to hinder digital investment and global technology collaboration. Strengthening national standards that adhere to international principles is necessary for Indonesia's legal system to be accepted within the interconnected global network. Regulatory harmonization efforts are an important step in building digital trust both domestically and internationally.

Legal Analysis and the Urgency of Legal Regulatory Reform

The effectiveness of Law Number 27 of 2022 concerning Personal Data Protection still faces several fundamental issues related to its implementation. The norms contained in this law are largely declarative and do not fully guarantee the operational protection of personal data. While some provisions, such as those governing data subject rights, data controller obligations, and processing mechanisms, are regulated, they are not supported by adequate legal instruments for their implementation. Criminal and administrative provisions remain general in nature without clear technical guidance. This situation creates uncertainty for businesses and public institutions in interpreting the limits of their authority and legal liability for personal data breaches.

Another fundamental weakness is the absence of an effective independent oversight body, as mandated by Article 59 of the Personal Data Protection Law. This provision does not comprehensively explain the structure, authority, and working mechanisms of the oversight body, resulting in suboptimal oversight. It contrasts with countries with independent data protection authorities, such as the European Union's Data Protection Authority, which has strong investigative and sanctioning powers. Indonesia still relies on coordination between institutions, such as the Ministry of Communication and Informatics and the National Agency for the Protection of Personal Data (BSSN), which have overlapping authorities. This situation has led to weak oversight of personal data processors in both the public and private sectors.

The establishment of an independent supervisory body is an urgent need to ensure fair and transparent law enforcement. Such an institution functions as both a regulator and an oversight body, mandated to ensure compliance by all entities with data protection principles. Experience in other countries demonstrates that the existence of such an authority is a key factor in the successful implementation of data protection laws. For example, the GDPR grants the Supervisory Authority broad authority to impose sanctions of up to four percent of the total annual revenue of violating companies. The ideal institutional model for Indonesia is an independent body directly responsible to the president but with a public accountability mechanism, with a structure that includes investigation units, dispute resolution, and regulatory policy development.

An effective supervisory body must be supported by competent human resources with high integrity. Oversight of data controllers and processors requires not only legal capacity but also technical understanding of cybersecurity systems, encryption, and risk management. Furthermore, the public also needs access to complaints and legal protection when their privacy rights are violated. The role of a supervisory body should not be limited to law enforcement but also encompass public education, data security certification, and guidance for digital industry players. The performance of this institution will significantly determine the extent to which the PDP Law can provide real protection for citizens.

Harmonization between cybersecurity regulations and personal data protection is key to creating a comprehensive legal system. To date, the national cybersecurity policy, as regulated by the Presidential Regulation on the National Cyber Security Agency (BSSN), has not been integrated with the personal data protection policy. As a result, a gap remains between efforts to maintain system security and the protection of individual privacy rights. Developed countries have developed integrated legal frameworks that regulate the technical, governance, and procedural aspects of data security. Indonesia needs to adopt a similar approach by integrating digital security and privacy principles into a single national legal policy.

The drafting of the National Cybersecurity Law is a strategic step in strengthening synergy between institutions and clarifying the state's role in addressing cyber threats. This regulation needs to establish mechanisms for preventing, mitigating, and responding to cyberattacks against critical digital infrastructure, including financial, energy, and government systems. Within the national legal framework, this law can serve as an umbrella for sectoral regulations to prevent overlapping issues. Coordination between institutions such as the National Cyber and Cyberspace Agency (BSSN), the Ministry of Communication and Information Technology (Kominfo), the Indonesian National Police (Polri), and the private sector will also be easier when there is an explicit and hierarchical legal basis. This harmonization will create a stronger and more sustainable cyber law ecosystem.

Legal regulatory reform must be directed at establishing a data protection system that adapts to developments in digital technology, particularly 5G and artificial intelligence. Rapid technological change demands laws that are flexible while still ensuring certainty. Regulations that are too rigid can stifle innovation, while those that are too lax can open the door to data misuse. Indonesia needs to design legal policies that balance innovation and human rights protection. The adaptive principle here means that laws can adapt to technological advances without losing their fundamental value in protecting the public interest.

Legal sanctions also need to be strengthened to provide a deterrent effect for perpetrators. The sanctions provisions in the PDP Law still lack strong enforcement because they are not balanced by effective enforcement mechanisms. Criminal and administrative provisions need to be updated to be proportionate to the severity of the violation, as well as to include a fair compensation system for victims of data breaches. Providing compensation and restoring victims' reputations is an essential part of substantive justice that should be guaranteed by the state. Sanctions reform must consider international best practices to provide optimal protection.

Aligning regulations with global standards such as the GDPR and the OECD Privacy Guidelines will strengthen Indonesia's position in international data governance. This harmonization is crucial to ensure legal interoperability between countries, particularly in digital trade and cross-border data exchange. International standards emphasize transparency, accountability, and public participation in data management, which are also relevant in Indonesia. Implementing these standards will increase global trust in the national legal system and support a safe digital investment climate. Legal policies aligned with global norms also demonstrate Indonesia's commitment to protecting human rights in the digital realm.

Legal transformation towards an adaptive data protection system must involve all stakeholders, including government, the private sector, academia, and civil society. Reform is not simply achieved through normative reforms, but also through building a legal culture that respects privacy and digital security. Cyber law education and public awareness of the importance of personal data protection need to be expanded to enable the public to become active participants in the digital legal system. Collaboration across sectors will produce more

realistic and sustainable policies. Comprehensive regulatory reform will be the primary foundation for building a safe, fair, and socially just digital ecosystem.

CONCLUSION

Cybersecurity challenges in the 5G era demonstrate that existing legal regulations are not yet fully capable of ensuring effective personal data protection. The complexity of 5G technology, with its high-speed networks, massive connectivity, and IoT device integration, increases the potential risk of data breaches and cyberattacks. Weak implementation of Law Number 27 of 2022 concerning Personal Data Protection, particularly the lack of a supervisory institution, has created a vacuum in oversight and legal uncertainty. This situation hinders the enforcement of basic data protection principles such as accountability, transparency, and information security. Legal reform is urgently needed to ensure Indonesia's data protection system can adapt to digital dynamics and sustainably safeguard people's privacy rights.

Improving the effectiveness of personal data protection requires concrete steps, including the establishment of an independent supervisory body with full authority to audit, investigate, and enforce the law on data breaches. The government needs to immediately draft a specific law on national cybersecurity that regulates the governance, prevention, and response to attacks on critical digital infrastructure. Strengthening international cooperation is also crucial to addressing the increasingly complex transnational threats in cyberspace. On the other hand, improving digital literacy and the capacity of law enforcement in cyber law enforcement must be a priority so that all elements of society and state officials have equal awareness and capability to face the challenges of the 5G era. An adaptive, participatory, and technology-based legal approach is the main foundation for a resilient and equitable national cybersecurity system.

REFERENCE

Angellia, F.,et al., (2024). *Internet of Things: Membangun Dunia yang Terkoneksi.* Jambi: PT. Sonpedia Publishing Indonesia.

Djauzie, M. Z. (2025). PANCASILA SEBAGAI GRUNDNORM MENURUT TEORI HUKUM MURNI HANS KELSEN DAN TEORI HUKUM RESPONSIF OLEH PHILIPPE NONET DAN PHILIP SELZNICK. *Jurnal Hukum to-ra: Hukum Untuk Mengatur dan Melindungi Masyarakat, 11*(1), 239-252.

Judijanto, L., Rustiyana, R., Indrayani, N., Juwita, R., & Yusuf, M. (2025). *Teknologi Masa Depan dan Revolusi Industri.* Yogyakarta: PT. Sonpedia Publishing Indonesia.

Junaedi, D., Supriyatna, R. K., & Arsyad, M. R. (2023). Era Baru Perkembangan Peradaban Ekonomi Digital. *Sci-Tech Journal, 2*(1), 32-46.

Kurniawan, Y. (2025). Urgensi Penataan Keamanan Siber yang Demokratis di Indonesia. In *Gagasan Akademisi Maroon Untuk Negeri* (s. 8). Jakarta: Universitas Bakrie Press.

Maharani, M. A., & Atman, W. (2025). Evaluasi Strategi Nasional Keamanan Siber Indonesia dalam Menanggapi Ancaman Digital Indonesia. *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik, 2*(3), 344-354.

Megantara, D., Arianti, R., & Mutiawati, A. I. (2025). Analisis Yuridis Perlindungan Data Pribadi Sebagai Hak Privasi dalam Transaksi E-Commerce di Indonesia. *Jurnal Hukum Indonesia, 1*(1).

Munawar, Z., Putri, N. I., Kharisma, I. L., Sid, S. S., Insany, G. P., Mogi, I. K., . . . Barus, O. P. (2023). *Keamanan Sistem Informasi: Prinsip Dasar, Teori, dan Rekayasa Penerapan Konsep.* Bandung: Kaizen Media Publishing.

Nirwan, D., & Sampurna, A. (2025). MENYELARASKAN TEKNOLOGI DENGAN PERLINDUNGAN HAK PRIVASI. *Juris Prudentia: Jurnal Hukum Ekselen, 7*(2).

Pradana, M. A., & Saragih, H. (2024). Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya. *Innovative: Journal Of Social Science Research, 4*(4), 3412-3425.

Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). *Keamanan Data dan Informasi.* Bandung: Kaizen Media Publishing.

Putra, F. P., Riski, M., Yahya, M. S., & Ramadhan, M. H. (2023). Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G. *Jurnal Sistim Informasi dan Teknologi, 5*(2), 167-174.

Ramadhanty, N. (2024). Implementasi Kerangka Keamanan NIST Dan ISO/IEC 27001 Dalam Menghadapi Ancaman Risiko Siber. *Journal of Indonesian Management, 4*(4).

Rif'at, E. M., & Dompak, T. (2025). Hak asasi manusia di era digital: Tantangan dan peluang dalam mengatasi kejahatan siber. *Jurnal Ilmu Multidisiplin, 3*(1), 86-98.

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum, 8*(1), 70-83.

Ruseno, N., Rantina, M., & Santoso, G. (2025). Analisis Automation, Keamanan, dan Kecepatan Jaringan 5G dalam Implementasi Internet of Things (IoT). *Jurnal PASTI: Jurnal Publikasi Artikel Sistem Teknologi Informasi, 1*(1), 34-43.

Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi, 2*(2), 145-157.

Samin, H. H. (2024). Perlindungan hukum terhadap kebocoran data pribadi oleh pengendali data melalui pendekatan hukum progresif. *Jurnal Ilmiah Research Student, 1*(3), 1-15.

Sidik, B. P., & Wiraguna, S. A. (2025). Tinjauan Hukum terhadap Aplikasi Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora, 2*(2), 219-232.

Sofyan, R., Sriwidodo, J., & Hasibuan, E. S. (2025). Reformasi Tata Kelola Intelijen di Era Digital: Adaptasi Terhadap Ancaman Siber. *Jurnal sosial dan sains, 5*(9), 7251-7260.

Sugiyatno, S., Sidiq, P., & Edrisy, I. F. (2023). The Influence of 5G Technology on the Evolution of Communication: A Study of Developments and Implications in the Field of Science. *NUCLEUS, 4*(2), 115-120.

Syah, E., Weharima, H., Susilo, T., Basuki, T., & Akad, A. M. (2025). Serangan Siber terhadap Infrastruktur Kritis: Ancaman Bagi Keamanan dan Kesejahteraan Masyarakat. *JURNAL SYNTAX IMPERATIF: Jurnal Ilmu Sosial dan Pendidikan, 6*(2), 145-154.

Tobing, C., Surya, T., Selvias, L., Girsang, S., Azzahra, P., Purba, L., . . . Rusmana, N. (2024). Globalisasi Digital Dan Cybercrime: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas. *Jurnal Hukum Sasana, 10*(2), 105-123. doi: https://doi.org/10.31599/sasana.v10i2.3170