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

DOI: https://doi.org/10.38035/gijlss.v3i3

Evaluation of the Legal Framework for Personal Data Protection and Cybersecurity in the Digital Age in the Context of the Urgency of Reform and the Formulation of a National Digital Security Law in Indonesia

Jon Rudol Manungkalit[1], Wieke Dewi Suryandari[2], Hono Sejati[3]
[1]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia,
jonrudol471918@gmail.com
[2]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia,
wiekedewi11@gmail.com
[3]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia,
sejatihono@gmail.com

Corresponding Author: jonrudol471918@gmail.com[1]

Abstract: Rapid developments in information technology have driven digital transformation in various aspects of life, from the government and economic sectors to social life. Amidst this progress, significant new challenges have also emerged, one of which is the threat to personal data protection and cybersecurity. The misuse of personal data, leaks of sensitive information, and the prevalence of cyber attacks have become urgent legal issues that must be addressed comprehensively. The protection of personal data is no longer merely a technical issue, but has become part of the fulfillment of human rights, particularly the right to privacy and security in digital life. The state, as the legal duty bearer, has the responsibility to formulate and implement adequate regulations to guarantee these rights. In this context, this study aims to examine in depth the urgency of personal data protection and cyber security in the digital era, analyze the effectiveness of existing regulations, and highlight the need to formulate a Cyber Security and Resilience Law as a strategic step to deal with the complexity of digital threats. This study uses a normative juridical method with a legislative and conceptual approach, which is based on a study of written legal norms and a conceptual understanding of the right to privacy, legal protection, and cybersecurity principles. The research data sources consist of primary legal materials such as legislation, as well as secondary legal materials in the form of legal literature, academic journals, and opinions from legal experts. With this framework, this research is expected to contribute theoretically to strengthening the legal basis for data protection and cybersecurity in Indonesia.

Keywords: Personal data protection, cybersecurity, digital transformation, privacy rights

INTRODUCTION

Digital transformation has become an inseparable part of modern human life (Ayu, 2022). Previously, conventional social activities have now shifted to the digital space, from social interactions and financial services to education and healthcare (Judijanto, 2024). This digitalization process has brought about efficiency and convenience, but at the same time, it has created new consequences in the form of an increasing volume of personal data spread across various digital platforms (Aksenta, 2023). As data becomes a high-value commodity, personal data protection has become a fundamental necessity to guarantee individual rights amidst the unstoppable flow of technological development (Daeng, 2023).

With society's growing reliance on digital systems, threats to personal data security are more prevalent (Yamin, 2024). Data leaks, misuse of information, and cybercrimes like phishing, identity theft, and hacking are increasingly complex (Ariyaningsih, 2023). Not only are individuals harmed, but institutions also risk public trust and system integrity. Thus, personal data protection and cybersecurity must be coordinated to build a safe, sustainable digital ecosystem (Huda, 2024).

This situation underscores the urgent need for the law to adapt quickly and effectively to the ever-evolving digital landscape. Regulatory frameworks must not only offer protection but also proactively anticipate and address technological advancements. Therefore, building an adaptive and comprehensive legal system becomes essential—a system designed to enforce sanctions, enhance prevention, and provide legal certainty for all digital stakeholders.

To understand personal data protection, it is important to first outline the definition of personal data itself. According to various doctrines and regulations, personal data includes any information that can identify an individual, either directly or indirectly (Suari, 2023). In Indonesia, Law No. The 2022 Law on Personal Data Protection has clarified this definition, while also affirming the rights of data subjects and the obligations of data controllers and processors (Alfitri, 2024). Meanwhile, cybersecurity refers to systematic efforts to protect digital systems and data from attacks, disruptions, or unauthorized access. In a legal context, cybersecurity is viewed not only from a technical perspective but also from the perspective of protecting human rights in the digital space (Soesanto, 2023).

The theory of legal protection provides a normative foundation for explaining the role of the state in protecting its citizens, including in the digital context (Darnia, 2023). The state is responsible for providing legal instruments capable of guaranteeing a sense of security and delivering justice for victims of data breaches or cyberattacks (Arrasuli, 2023). This legal protection is not solely aimed at responding to crime, but also at preventing it through proactive policies and comprehensive regulations. This theory reinforces the argument that the law must act as a shield against unequal relations between data owners and those who control data management systems.

Furthermore, the theory of the right to privacy positions personal data as a fundamental human right (Mutiara, 2020). The right to privacy is at the heart of the concept of privacy, and in the digital world, interference with personal data constitutes a violation of that right (Argiansyah, 2024). Therefore, legal regulations that guarantee the confidentiality and control of personal data are part of respect for human dignity. Through this theory, data protection is not merely seen as a technical or administrative necessity, but as part of the recognition of human existence in the digital space.

The rule of law theory also serves as an important framework for discussing this issue. In a rule of law state, every action of the government and citizens must be based on applicable law (Srilaksmi, 2020). In the digital era, this principle demands that the state not remain silent about the new risks facing its citizens. A rule of law state must be able to accommodate changing times by continuously updating its legal instruments to remain relevant and effective. In the context of data protection and cybersecurity, this means the

need for regulations that not only regulate but also affirm the state's position as a protector of the public interest in facing digital threats (Ajamalus, 2024).

As a consequence of this theoretical framework, various legal principles have emerged that serve as guidelines for building a data protection and cybersecurity system. The principle of legality, for example, requires that all forms of data collection, processing, and dissemination must have a clear legal basis (Satrio, 2020). Meanwhile, the principles of proportionality and transparency require that data be used openly and in accordance with legitimate purposes (Satria, 2024). The principle of accountability also plays a central role in ensuring that parties processing data are fully responsible for protecting the information they manage (Pradana, 2024).

In terms of cybersecurity, the applicable principles also reflect the spirit of digital resilience. Terms like "cyber resilience" refer to the ability of a system or country to prevent, detect, and respond to cyberattacks effectively (Linkov, 2019). This principle encompasses technical, institutional, and integrated policy aspects to create a resilient digital system. At the legal level, national cybersecurity principles require cross-sector coordination, strengthening institutional capacity, and developing flexible legal norms that still maintain human rights protection.

A comprehensive understanding of personal data protection and cybersecurity highlights one central argument: the law must continuously transform in step with technological progress. Legal adaptation is necessary not only to address new risks but to ensure the protection of human rights and values in digital life. The law’s evolution is therefore essential to safeguarding individuals and institutions in the digital era.

METHOD

This research employs a normative juridical method, a legal research approach that involves a literature review and analysis of applicable legal norms. The primary focus of this method is to examine law as written norms in legislation and relevant legal doctrines. This research does not rely on empirical data from the field, but rather focuses on the study of primary legal materials such as Law No. 27 of 2022 concerning Personal Data Protection, the Electronic Information and Transactions (ITE) Law, and various regulations related to cybersecurity at both the national and international levels. Secondary legal materials are also used, including legal literature, academic journals, expert opinions, and studies by official institutions to support the theoretical and conceptual understanding of personal data protection and cybersecurity. The approach used in this research is a statutory approach, which aims to analyze the substance of positive law related to data protection and cybersecurity, and a conceptual approach, which is used to explore and understand legal concepts such as the right to privacy, legal protection of personal data, and cyber resilience from the perspective of a state based on the rule of law. Through this approach, the author aims to assess the effectiveness of existing regulations in providing adequate protection for personal data and addressing digital security challenges in the modern era. This research is descriptive-analytical, describing the current legal situation and providing a critical analysis of its strengths and weaknesses. It also formulates the urgency of strengthening the law through the establishment of a Cyber Security and Resilience Law in Indonesia.

RESULT AND DISCUSSION

The Urgency of Personal Data Protection and Cybersecurity in the Digital Age

The development of digital technology has fundamentally changed patterns of human interaction. Activities previously conducted conventionally have now migrated to the digital space, from financial transactions and government services to education and daily communication. In this process, personal data has become the primary fuel for digital

systems, where information about an individual's identity, location, consumption habits, and preferences is collected, processed, and stored in large quantities by various parties. While the integration of personal data into information technology provides efficiency and convenience, it also creates a vulnerable space for data misuse, leaks, and manipulation that can threaten citizens' fundamental rights.

In Indonesia, the trend of data leaks and cybercrime is increasingly in the public spotlight. Cases such as hacking of government agency accounts, selling digital platform user data on the black market, and the unauthorized dissemination of personal information illustrate the weakness of the current protection system. Cybercrime is no longer simple or carried out sporadically by individuals, but has evolved into a transnational organized crime, with complex technology and strategies. This indicates that Indonesia's digital system is facing serious challenges that require attention not only from a technical perspective but also from a more robust legal and public policy perspective.

The risks of personal data breaches are widespread and have profound impacts, especially for individuals. When personal data falls into the wrong hands, individuals can experience financial losses due to account breaches, identity theft, and even fraud involving third parties. Furthermore, the damage to a digital reputation caused by the dissemination of sensitive information can also impact a person's social and professional life. In many cases, victims are unaware that their data has been used illegally until the consequences arise, at which point it is often too late to fully repair.

The impact on public and private entities is equally significant. Public trust in institutions relies heavily on assurances that the information they provide will be managed securely. When institutions fail to protect their users' data, not only their reputations are damaged, but also their business stability and established public relations. The private sector can experience significant economic losses, both from lost customers and lawsuits. In the public sector, data breaches can undermine the government's legitimacy in managing public affairs transparently and accountably.

From a constitutional perspective, personal data protection is closely linked to human rights, particularly the right to privacy and security. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees that everyone has the right to personal protection and security from threats. In the digital era, these threats are no longer just physical but also digital, where personal information can be infiltrated, monitored, and misused without the owner's knowledge. Therefore, protecting personal data is part of the state's responsibility to safeguard and fulfill the constitutional rights of every citizen.

Furthermore, the importance of cybersecurity is not only related to individual protection but also to national resilience. Digital infrastructure is now an integral part of the defense system, public services, and the national economy. If cybersecurity is weak, the potential for disruption to national stability becomes tangible. Cyberattacks on logistics systems, health services, and even election systems can become tools to undermine public trust and create social chaos. In this context, cybersecurity must be interpreted as part of a cross-sectoral and multidimensional national strategy.

Building a safe and fair digital ecosystem requires a legal framework that is not only repressive but also preventive and adaptive. The law must be able to provide real protection to all parties interacting in the digital space, and encourage accountability of electronic system administrators in managing user data. This also means providing sufficient space for the public to understand their rights and encouraging active participation in shaping a responsible digital culture. When the public feels protected, trust in the digital ecosystem will naturally grow.

Ensuring security and fairness in the digital space is not solely the government's responsibility, but also a shared responsibility between regulators, the private sector,

academics, and civil society. However, this initiative still requires a strong legal foundation as a basis for collaborative work. Personal data protection and cybersecurity are not merely a matter of developing new regulations, but rather a new paradigm for viewing data as a human right and a strategic national asset. With the right legal approach, digitalization will not be a threat, but rather an opportunity to create a more inclusive, secure, and digitally sovereign society.

Evaluation of Applicable Regulations and Implementation Barriers

An evaluation of personal data protection and cybersecurity regulations in Indonesia reflects significant progress in the national legal framework, particularly with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law is a significant milestone in guaranteeing individuals' right to privacy in the digital space, comprehensively regulating the principles of data processing, the obligations of data controllers and processors, and sanctions for violations. The PDP Law contains basic principles of data protection, such as the lawfulness of processing, purpose limitation, transparency, accountability, and data subject rights. Furthermore, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments and derivative regulations, which, while focusing more on digital communications and transactions, also provide a legal basis for cyber issues through regulations on illegal access, system disruption, and unauthorized data dissemination.

However, in practice, harmonization between laws and regulations has not been fully realized. Overlapping norms and authorities between regulatory agencies create legal uncertainty, especially when personal data is located in sectors that already have their own regulations. For example, the banking sector is regulated by OJK Regulation Number 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector, and the healthcare sector through Minister of Health Regulation Number 24 of 2022 concerning Medical Records. The lack of substance in each regulation results in inconsistent data protection across sectors and, to some extent, weakens the position of data subjects as parties who should be comprehensively protected.

In addition to differences in substance, weak oversight and weak law enforcement are highlighted. In the Personal Data Protection Law, for example, Article 58 stipulates the establishment of an independent supervisory authority as an implementing agency for personal data protection, but to date, there has been no adequate institutional and operational certainty to carry out this function. This hampers effective monitoring and enforcement of data protection violations. Furthermore, the reporting and investigation system for data breach incidents does not yet have standardized procedures that are easily accessible to the public, resulting in weak transparency in handling violations.

The lack of standardized technical regulations also hinders regulatory implementation. Many electronic system administrators (ESEs), both government and private, do not clearly understand the technical and procedural security standards for processing personal data. The PDP Law mandates adequate data protection, but does not specifically specify the cybersecurity standards that must be implemented in the context of ever-evolving technology. This often results in businesses being unaware of the technical obligations they need to fulfill, or simply implementing them minimally to meet formal obligations.

Implementation in the field also faces serious obstacles due to low digital literacy, both among the general public and businesses. Many individuals do not understand the value and vulnerability of their own personal data, leading to careless digital behavior that is easily exploited. Furthermore, small and medium-sized businesses often do not consider data security a top priority due to limited knowledge and costs, often ignoring protection

standards. As a result, the digital space remains vulnerable to various forms of data crime and manipulation.

The problem of inter-agency coordination is an unresolved structural challenge. Cybersecurity and data protection management fall under various ministries and institutions, such as the Ministry of Communication and Informatics, the National Cyber and Crypto Agency (BSSN), and other sectoral agencies. Without a clear coordination system, responses to cyber incidents are slow and unintegrated. This exacerbates the challenges of handling violations, which are cross-sectoral and often require multi-stakeholder involvement. The absence of an efficient coordination mechanism makes regulations that are sound on paper ineffective in their implementation on the ground.

Furthermore, limited human resources in the cybersecurity sector remain a significant obstacle. Indonesia still lacks experts with technical competencies in cyber risk management, digital forensics, and the development of AI-based security systems. This lack of adequate human resources has resulted in the weak capacity of public institutions and the private sector to prevent and respond to cyberattacks. The PDP Law requires the establishment of a Data Protection Officer in certain institutions, but this policy will not be implemented optimally if the labor market is not ready to supply the required skills.

Uneven technological infrastructure exacerbates the disparity in regulatory implementation. Regions with limited access to technology and networks cannot build reliable data protection systems. This situation not only creates a digital divide between regions but also opens up security gaps that can be exploited by irresponsible parties. When basic infrastructure is inadequate, the hope of implementing high data protection standards becomes difficult to achieve, ultimately placing communities in underdeveloped regions most vulnerable to personal data exploitation.

The Urgency of Legal Framework Reform and the Need for Cyber Security and Resilience Legislation

Challenges in the cyber realm are increasingly demonstrating extraordinary complexity. One rapidly evolving threat is Advanced Persistent Threat (APT) attacks, which are stealthy, sustained, and targeted cyberattacks targeting specific infrastructure, often involving state actors. These attacks are not only economically damaging but also jeopardize data integrity and a nation's digital sovereignty. Ransomware-based attacks pose a real threat to both public and private institutions, locking systems or stealing data that is only unlocked after a ransom is paid. Even more concerning is the potential for digital espionage, where foreign actors use technology to steal strategic information from government agencies or critical companies without easily traceable traces.

More broadly, the world has witnessed an increase in cyberwarfare as part of geopolitical conflicts. Attacks on power systems, communication networks, and even population data can disrupt national stability without even a single shot being fired. Critical national infrastructure, such as airports, ports, financial systems, and healthcare systems are particularly vulnerable targets. Without a robust and well-structured legal framework, the state will find itself in a fragile defensive position. This situation demands more than just a technical response—it requires a comprehensive reformation of the legal system to provide strategic and systemic protection.

Legal reform efforts must begin with the development of a framework capable of integrating aspects of personal data protection, individual privacy, and national security in a balanced manner. The sectoral approach must be transformed into a holistic legal system, encompassing not only protection against individual violations but also addressing the broader dimensions of national security. The legal framework should not merely impose sanctions on violations, but should also be able to map potential threats, facilitate

coordination between institutions, and promote a culture of cyber awareness from an early age.

This legal reform also requires alignment with international standards, both in terms of substance and implementation mechanisms. The European Union's General Data Protection Regulation (GDPR), for example, serves as a global benchmark for personal data protection that balances individual rights and the needs of the digital economy. Similarly, technical standards such as the NIST Cybersecurity Framework from the United States emphasize systematic risk management. Within the regional context, the ASEAN Cybersecurity Cooperation Strategy encourages collaboration among member countries to strengthen cybersecurity capabilities. Indonesia, as an ASEAN member country, must adapt its domestic regulations to be compatible with regional and global frameworks.

One urgent matter that cannot be postponed is the creation of a Cybersecurity and Resilience Law. To date, Indonesia does not have a specific law that explicitly regulates all aspects of cybersecurity. Existing regulations are scattered across various sectoral regulations and are unable to address the complexity of today's threats. This law is expected to provide a solid legal foundation, encompassing strategies for prevention, detection, mitigation, and recovery from cyber incidents. This is not simply a matter of creating new laws, but rather how those laws are designed to remain relevant in the face of evolving threats.

The position of the National Cyber and Crypto Agency (BSSN) as the primary institution in cybersecurity management needs to be strengthened legally and institutionally. BSSN has played a crucial role in addressing national cyber issues, but currently lacks a legal umbrella in the form of legislation that provides legitimacy and broad authority. The Cybersecurity and Resilience Law will serve as a framework that clarifies the BSSN's functions, limits gray areas of authority, and opens up opportunities for more effective coordination with other agencies. This is crucial to avoid overlapping roles or even conflicts between agencies in the field.

As a legal product, the desired law should not simply contain repressive norms, but rather should be designed with a preventative, adaptive, and responsive approach. Preventive means prioritizing prevention through education, technical standards, and clear security protocols. Adaptive refers to the flexibility of legal norms that can adapt to technological developments without losing effectiveness. Meanwhile, responsive means the law must be able to respond quickly and decisively to cyber incidents, through an adequate reporting system, investigations, and sanctions. In this regard, the law must think like technology: moving quickly, measurably, and not stagnating in bureaucracy.

The formation of this law will also have a positive impact on the national digital economic ecosystem. Legal certainty that guarantees data security and digital infrastructure will increase investor confidence and ensure business actors' comfort. Furthermore, the public will feel safer interacting and transacting in the digital space. When the legal framework provides comprehensive protection, the public is encouraged to actively safeguard their own data security, creating a healthy collaboration between the state, the private sector, and individuals in addressing cyber challenges.

CONCLUSION

Personal data protection and cybersecurity have become issues that are no longer optional, but rather fundamental necessities in facing the dynamics of the digital era. The digital transformation that has penetrated almost every aspect of life demands a legal system capable of addressing the challenges and risks that accompany it. As dependence on information technology increases, the potential for threats to personal data and digital infrastructure also increases. Unfortunately, current regulations, such as Law No. 27 of 2022 concerning Personal Data Protection and several provisions in the Electronic Information and

Transactions Law (UU ITE), have not demonstrated optimal effectiveness. Numerous gaps remain, including harmonization between regulations, weak oversight and enforcement, and the absence of legal instruments specifically addressing cybersecurity and resilience in an integrated manner. In this context, the need for a stronger, more integrated, and more comprehensive national legal framework is becoming increasingly urgent.

To encounter this situation, several strategic steps must be taken immediately. First, accelerating the formation of the Cybersecurity and Resilience Law is a priority that cannot be postponed any longer, to ensure the country has a legal framework capable of protecting the public and critical infrastructure from cyberattacks. Second, institutional strengthening—particularly the National Cyber and Cyber Security Agency (BSSN)—needs to be encouraged, along with increasing digital literacy among the public and business actors, so that collective awareness of the importance of cybersecurity can grow from the ground up. Third, harmonizing national regulations with international standards, such as GDPR, NIST, and the ASEAN regional framework is a crucial step to maintain competitiveness and safeguard the sustainability of Indonesia's digital ecosystem. Cross-sector collaboration, openness to innovation, and flexible yet firm legal policies will be the main foundations for facing an increasingly digitalized future safely, fairly, and sustainably.

REFERENCES

Ajamalus, H. &. (2024). Perkembangan Hukum Cyber di Indonesia: Tantangan dan Peluang. *Bulletin of Community Engagement, 4(3)*, 109-116.

Aksenta, A. I. (2023). *LITERASI DIGITAL: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 dan Sociaty 5.0.* Jambi: PT. Sonpedia Publishing Indonesia.

Alfitri, N. A. (2024). Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Journal Social Society, 4(2)*, 92-111.

Argiansyah, H. Y. (2024). Perlindungan Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia. *Jurnal Hukum Pelita, 5(1)*, 61-75.

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

Arrasuli, B. K. (2023). Perlindungan hukum positif Indonesia terhadap kejahatan penyalahgunaan data pribadi. *UNES Journal of Swara Justisia, 7(2)*, 369-392.

Ayu, I. W. (2022). Budaya digital dalam transformasi digital menghadapi era society 5.0. *Jurnal Pengembangan Masyarakat Lokal, 5(1)*, 20-25.

Daeng, Y. L. (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. *Innovative: Journal Of Social Science Research, 3(6)*, 2898-2905.

Darnia, M. E. (2023). Strategi Penguatan Hukum Perlindungan Konsumen Dalam Era Digital. *Perkara: Jurnal Ilmu Hukum Dan Politik, 1(4)*, 44-58.

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

Judijanto, L. S. (2024). *Literasi Digital di Era Society 5.0: Panduan Cerdas Menghadapi Transformasi Digital.* Jambi: PT. Sonpedia Publishing Indonesia.

Linkov, I. &. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, 1-25.

Mutiara, U. &. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Indonesian Journal of Law and Policy Studies, 1(1)*, 42-54.

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

Satria, M. K. (2024). Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Intelek Dan Cendikiawan Nusantara, 1(2)*, 2442-2456.

Satrio, M. B. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia). *JCA of Law, 1(1).*

Soesanto, E. R. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, 1(2)*, 172-191.

Srilaksmi, N. K. (2020). Fungsi Kebijakan Dalam Negara Hukum. *Pariksa: Jurnal Hukum Agama Hindu, 4(1)*, 30-38.

Suari, K. R. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum, 6(1)*, 132-142.

Yamin, A. F. (2024). Perlindungan Data Pribadi Dalam Era Digital: Tantangan Dan Solusi. *Meraja journal, 7(2)*, 138-155.