Jurnal Komunikasi
Vol. 3 No. 2 2025, hal. 288-298 e-ISSN: 2988-1331

WIRETAPPING IN THE DIGITAL AGE: SURVEILLANCE CHALLENGES TO PERSONAL DATA PROTECTION IN INDONESIA

Gunawan Widjaja
Faculty of Law Universitas 17 Agustus 1945 Jakarta, Indonesia
widjaja_gunawan@yahoo.com

Adrian Bima Putra
Faculty of Law Universitas 17 Agustus 1945 Jakarta, Indonesia

Abstract

The development of digital technology has brought convenience in information exchange, but also increased the risk of wiretapping and violation of personal data in Indonesia. This research aims to examine the challenges of monitoring wiretapping practices in the context of personal data protection in Indonesia through a literature study of relevant regulations, cases, and literature. The results of the study show that regulatory fragmentation, the absence of independent oversight institutions, weak oversight mechanisms, and low public digital literacy are the main obstacles in protecting personal data from the threat of wiretapping. In addition, the rapid development of technology and cross-border jurisdictional issues complicate monitoring efforts. Regulatory harmonisation, the establishment of effective supervisory institutions, and multi-sector collaboration are needed to strengthen personal data protection in the digital era. This research recommends surveillance system reform, public education, and technical capacity building as strategic steps to create a safe and trusted digital ecosystem in Indonesia.

Keywords: Wiretapping, Personal Data Protection, Surveillance, Digital Age, Regulation, Indonesia.

Abstrak

Perkembangan teknologi digital telah membawa kemudahan dalam pertukaran informasi, namun juga meningkatkan risiko penyadapan dan pelanggaran terhadap data pribadi di Indonesia. Penelitian ini bertujuan untuk mengkaji tantangan pengawasan terhadap praktik penyadapan dalam konteks perlindungan data pribadi di Indonesia melalui studi literatur terhadap regulasi, kasus, dan literatur terkait. Hasil kajian menunjukkan bahwa fragmentasi regulasi, absennya lembaga pengawas independen, lemahnya mekanisme pengawasan, serta rendahnya literasi digital masyarakat menjadi hambatan utama dalam perlindungan data pribadi dari ancaman penyadapan. Selain itu, perkembangan teknologi yang pesat dan isu yurisdiksi lintas negara memperumit upaya pengawasan. Diperlukan harmonisasi regulasi, pembentukan lembaga pengawas yang efektif, serta kolaborasi multisektor untuk memperkuat perlindungan data pribadi di era digital. Penelitian ini merekomendasikan reformasi sistem pengawasan, edukasi publik, dan penguatan kapasitas teknis sebagai langkah strategis untuk menciptakan ekosistem digital yang aman dan terpercaya di Indonesia.

Kata Kunci: Penyadapan, Perlindungan Data Pribadi, Pengawasan, Era Digital, Regulasi, Indonesia.

Introduction

The development of information and communication technology in the digital era has brought major changes in various aspects of human life, from how to communicate, work, to social interaction. Digitalisation is a hallmark of the 21st century, where almost all human activities are now connected to digital devices and internet networks. The ease of access to information and real-time data exchange is one of the main advantages of this era, but on the other hand it also raises new complex challenges, especially related to the security and privacy of personal data (Institute for Criminal Justice Reform, 2020) .

One of the crucial issues that has emerged is wiretapping or interception of personal data. Wiretapping in the digital era is no longer limited to conventional telephone conversations, but has penetrated into various digital communication platforms, such as email, social media, and instant messaging applications. These wiretapping activities can be carried out by state and non-state actors with various motives, ranging from political, economic, to cybercrime interests (Mabruri ., 2025)

In Indonesia, wiretapping cases have become a national issue when it was revealed that there was an attempt to wiretap high-ranking state officials, including the President and First Lady, by foreign parties. This case shows how vulnerable personal data and important communications are to the threat of wiretapping in the midst of rapid technological development (Sukartara, 2024) . In addition, wiretapping can also target the general public , especially through mobile devices that have become an integral part of everyday life (D. Pratama ., 2023)

The threat of eavesdropping is increasingly realised as society's reliance on digital services increases. Personal data stored or transmitted over the internet has the potential to be accessed, used, and even misused by unauthorised parties. This raises concerns regarding the protection of individual privacy rights and the security of personal data that should be guaranteed by the state (Vernando, 2022) .

In terms of regulation, Indonesia has responded to this challenge by passing Law No. 27 of 2022 on Personal Data Protection (PDP Law), as well as several other regulations such as the ITE Law and Telecommunications Law. However, the implementation of supervision and law enforcement against wiretapping practices still faces various obstacles, ranging from overlapping regulations, weak coordination between institutions, to limited human resources and technology (R. Pratama ., 2023)

In addition to regulatory challenges, technical aspects are also a major concern. Wiretapping in the digital era utilises sophisticated technology that continues to evolve, so detection and prevention efforts require adequate capabilities and infrastructure. The lack of digital literacy among the public also exacerbates the situation, as many

individuals do not understand the risks and how to protect their personal data in cyberspace (Yusuf, 2025) .

The phenomenon of wiretapping is not only a domestic issue, but also a transnational one. In the context of globalisation and borderless society, personal data of Indonesian citizens can be accessed from abroad, so data monitoring and protection requires international cooperation and harmonisation of regulations with global standards. This is a challenge for Indonesia in maintaining digital sovereignty and national security (Nugroho, 2025) .

Strengthening personal data protection is becoming increasingly urgent, given the increasing trend of eavesdropping and data leaks. Strong protection is needed not only to maintain individual privacy, but also to build public trust in the national digital ecosystem. Without effective oversight, wiretapping can undermine the integrity of government systems, the business world, and people's social lives (Dynasty, 2022) .

The role of the government, oversight institutions, and cross-sector collaboration is crucial in facing this challenge. The government needs to strengthen the legal framework, improve law enforcement capacity, and encourage education and digital literacy in the community. On the other hand, the private sector must also improve data security standards and transparency in managing users' personal data (Syaifudin, 2020) . In addition, the public as data subjects need to be given adequate understanding of their rights and how to protect personal data from the threat of eavesdropping. This collective awareness is an important foundation in building a strong personal data protection culture in Indonesia (D. Sari Pratama, R., 2021) .

Thus, wiretapping in the digital era is a serious challenge that requires comprehensive surveillance and protection of personal data. This research will examine in depth the challenges of monitoring wiretapping practices in the context of personal data protection in Indonesia, highlighting relevant regulatory, technical, social and jurisdictional aspects. It is hoped that the results of this study can make a real contribution to strengthening the personal data protection system and encouraging the creation of a safe and reliable digital ecosystem in Indonesia.

Research Methods

The research method used in this study is normative legal research with a normative juridical approach, which examines and analyses relevant laws and regulations, literature, scientific journals, and legal documents related to wiretapping and personal data protection in Indonesia. The data used is secondary data consisting of primary legal materials (such as Law No. 27 of 2022 on Personal Data Protection, ITE Law, and Telecommunications Law), secondary legal materials (literature, journals, and international guidelines), and tertiary legal materials (legal dictionaries and encyclopedias). The analysis is carried out qualitatively and descriptively analytically to

describe, connect, and describe problems and solutions based on legal theory and applicable norms systematically (Rothstein et al., 2006) ; (Kitchenham, 2020) .

Results and Discussion

Wiretapping and Personal Data Protection in Indonesia

Wiretapping and personal data protection in Indonesia are two contradictory issues in the digital era. On the one hand, technological advances facilitate the exchange of information, but on the other hand, the risk of data misuse through wiretapping practices has increased significantly. Wiretapping, or the interception of digital communications, is now not only done through conventional telephony but extends to platforms such as email, social media, and instant messaging applications like WhatsApp, often using *malware* software or hacking techniques. These activities involve both state and non-state actors, with motives ranging from legal surveillance to cybercrime (E. Sari et al., 2025) .

Legally, Indonesia already has several regulations in place to govern this practice. The Telecommunications Law (Law No. 36/1999) expressly prohibits wiretapping, except for the purposes of the criminal justice process at the request of law enforcement officials such as the KPK, the Police, or the Attorney General's Office. Meanwhile, the Personal Data Protection Law (PDP Law No. 27/2022) affirms an individual's right to data confidentiality and requires government and private institutions to protect user information. However, overlapping authority between agencies and lack of clarity on legal wiretapping procedures often lead to legal loopholes (N. Sari, 2023) .

Cases of wiretapping in Indonesia have occurred since the reform era, such as the wiretapping of President BJ Habibie's conversations in 1998 and the 2009 incident of wiretapping of the Presidential Palace circle by Australian intelligence agents revealed by Edward Snowden. This phenomenon shows the vulnerability of Indonesia's digital security system, even at the highest levels of government. Ironically, the response of state leaders is often minimal, such as President Jokowi's joke that "there is nothing to wiretap" from him (D. Sari, 2022) .

From a technical perspective, wiretapping in the digital era utilises telecommunications and internet infrastructure. Internet service providers (ISPs) are required to comply with a Ministerial Regulation that requires monitoring of data traffic, including in internet cafes, to anticipate cybercrime. However, this practice has the potential to violate privacy as it is often done without a court-authorised letter. Technologies such as *deep packet inspection* (DPI) used to monitor internet traffic are also prone to abuse for mass surveillance (Rahmawati, 2023) .

The main challenge lies in weak law enforcement. Although the PDP Law has been passed, there is no effective independent oversight authority. Law enforcement officials often lack the technical capacity to investigate data leakage cases, while

criminal sanctions and fines have not had a deterrent effect. A clear example can be seen from the rampant WhatsApp wiretapping cases, where perpetrators can be sentenced to 5 years in prison under the PDP Law, but implementation is still rare (Budiyanto ., 2025)

Social aspects exacerbate the problem, especially the low level of digital literacy. Many internet users do not understand the risks of sharing personal data or how to activate security features such as two-step verification in messaging apps. On the other hand, the culture of transparency in the private sector is also still low, with many companies reluctant to report data leaks for fear of reputation (Prabowo, 2023) .

Cross-border jurisdictional issues are increasingly complex. Leaks of Indonesian citizens' data stored on global servers, such as the case of the wiretapping of 1.8 million Telkomsel and Indosat subscribers by the US NSA in 2014, demonstrate the need for international regulatory harmonisation. However, Indonesia has not fully adopted global standards such as the European Union's *General Data Protection Regulation* (GDPR) (Wulandari, 2022) .

Government efforts are beginning to show with the establishment of systems such as the Indonesia Data Protection System (IDPS) and collaboration with international organisations. However, this step is still hampered by limited budget and resistance from interested parties. Public education through digital literacy campaigns and socialisation of the PDP Law also needs to be improved. The WhatsApp wiretapping case is a clear example of system vulnerability. Perpetrators often utilise application security loopholes or *phishing* techniques to access victims' accounts. Although the ITE Law and PDP Law provide a legal basis for prosecution, victims still have difficulty proving immaterial losses due to privacy violations (Putra, 2023) .

Prevention requires multi-sector synergy. Individuals should actively use end-to-end encryption and avoid sharing sensitive information through insecure platforms. Companies need to implement *privacy by design* in system development, while the government should accelerate the establishment of the Personal Data Protection Agency (BPDP) as an independent watchdog (Hidayat, 2024) .

Going forward, Indonesia needs to revise the Telecommunications Law and ITE Law to align with the PDP Law, and ratify international conventions such as the Budapest Convention on Cybercrime. Strengthening human resource capacity in cybersecurity and budget allocation for ethical surveillance technology research are also crucial. Given the complexity of these challenges, the balance between national security and citizens' privacy rights must be prioritised. Lawful wiretapping for legal purposes is still necessary, but it must be accompanied by a transparent and accountable oversight mechanism. Only with comprehensive reform can Indonesia become an example of a democratic country that can protect personal data without compromising digital progress.

Challenges in Monitoring Wiretapping Practices in the Context of Personal Data Protection in Indonesia

Wiretapping in the context of personal data protection in Indonesia faces multidimensional and interrelated monitoring challenges. Existing regulations such as the Telecommunications Law, ITE Law, and PDP Law have not been harmoniously integrated, creating legal loopholes that are exploited for illegal wiretapping. This lack of synchronisation has led to ambiguity in the authority of law enforcement agencies, telecommunications operators and the private sector in overseeing data interception practices (Prasetyo ., 2021)

The weakness of the wiretapping licence mechanism is a crucial problem. Although the Telecommunications Law requires court permission, in practice institutions such as the KPK have conducted wiretaps with only internal approval, a dangerous precedent that ignores the principle of *checks and balances*. The Constitutional Court's decision to allow notification of wiretapping after the act has been committed further undermines accountability. The absence of an independent oversight body such as the Personal Data Protection Agency (BPDP) mandated by the PDP Law exacerbates the situation. Without a dedicated authority, oversight of legal versus illegal wiretapping overlaps between the police, Kominfo, and BSSN, while the public has no effective channels for complaints (Kurniawan, 2021) .

The technical aspects of surveillance face serious obstacles. The *deep packet inspection* (DPI) technology used by ISPs to monitor data traffic is often operated without a court order, potentially becoming a tool of mass surveillance. On the other hand, the lack of experienced human resources in the field of digital forensics means that investigations into wiretapping cases often stagnate at the investigation level. Vulnerable cybersecurity infrastructure magnifies the risks. A SAFEnet report (2024) revealed that 78% of government agencies do not have data leakage emergency response protocols, while private companies are reluctant to invest in advanced encryption systems due to high costs and lack of regulatory incentives (Santoso, 2021) .

From a social perspective, people's low digital literacy is an opening for exploitation. Many users do not understand how to enable basic security features such as two-step verification, making them easy victims of *phishing* or eavesdropping *malware*. At the same time, there is a lack of transparency in the private sector about data collection practices. Cross-border jurisdictional issues add to the complexity. Many digital platforms store data on overseas servers, making eavesdropping by foreign entities difficult to prosecute. The PDP Law, which does not comprehensively regulate *cross-border data transfer*, weakens Indonesia's bargaining position in international cooperation (Wibowo, 2021) .

Selective law enforcement undermines the legitimacy of the regulation. Although the PDP Law promises fines of up to IDR 72 billion, large data leak cases such as BPJS Health 2021 are only responded to with apologies without criminal sanctions.

This lack of deterrent effect creates the perception that privacy violations are not serious crimes (Ramadhan, 2022) .

Institutional resistance to external oversight is a systemic barrier. Polri and KPK often resist intervention under the pretext of "law enforcement effectiveness", even though the Constitutional Court has affirmed that unsupervised wiretapping violates citizens' constitutional rights. The *cyber patrol* programme that monitors 200+ social media accounts without any legal basis is a clear example of abuse of power. The lag between regulations and technological developments widens the surveillance gap. Wiretapping through *artificial intelligence* (AI) or *Internet of Things* (IoT) devices has not been anticipated by existing laws, while *smart home devices* can be misused to spy on private activities without permission (T. Suryani Nugroho, W., 2022) .

Overlapping authority between agencies creates a *legal vacuum*. Coordination between MOCI, MOLHR and BSSN is weak, as evidenced by data leak reporting that is not followed by legal action. The private sector is also confused about complying with sectoral regulations that often contradict the PDP Law (N. Suryani, 2024) .

The misuse of intercepted data for political purposes threatens democracy. The case of the tapping of palace circles by foreign intelligence agencies (2009) and the leak of data on 1.8 million Telkomsel customers by the NSA (2014) show how strategic data can become a commodity for illicit transactions. Without a post-tapping data deletion mechanism, sensitive information risks being misused for intimidation or black campaigns (Lestari, 2023) . The lack of public education on digital rights exacerbates the situation. People are unaware that they can file class action lawsuits for data breaches, while victims of illegal wiretapping struggle to prove immaterial losses in court. The limited socialisation of the PDP Law makes data protection merely a normative discourse (Anwar, 2024) .

Going forward, strengthening the surveillance system requires revising the Telecommunications Law and ITE Law to align with the PDP Law, establishing an independent BPDP, and allocating a budget for research into ethical surveillance technology. Without comprehensive reform, illegal wiretapping will continue to erode public confidence in the state's commitment to protecting citizens' privacy (Dewi, 2023).

Furthermore, efforts to monitor wiretapping practices in Indonesia continue to be a hot and complex issue. Various parties, ranging from the government, the House of Representatives, to oversight institutions such as the Judicial Commission and Komnas HAM, have provided input regarding the need for firmer, more transparent and accountable arrangements in the wiretapping mechanism (Setiawan, 2024) . The bills being discussed, such as the KUHAP Bill and the Polri Bill, are expected to strengthen the external oversight system of law enforcement officials, instead of expanding their authority without adequate control. However, until now, many regulations governing wiretapping are still scattered in various sectoral laws, resulting in overlapping rules,

differences in procedures between institutions, and unclear procedures for licensing and supervision (Sitorus ., 2024)

In practice, wiretapping mechanisms carried out by law enforcement agencies such as the KPK, the Police, and the BNN often vary because they refer to their respective internal regulations. For example, the KPK was required to obtain permission from the Supervisory Board before conducting wiretapping, but after the Constitutional Court decision, the mechanism changed to notification to the Dewas no later than 14 working days after the wiretapping was carried out (Hutabarat, 2023) . This difference in mechanism raises the risk of abuse of power and violation of privacy rights, especially if there are no standardised standards and strict supervision. In addition, internal supervision conducted by the same institution as the perpetrator of the wiretapping is often considered unobjective and ineffective, so an independent external supervisory institution is needed (Bahtiar ., 2022)

Another issue that has emerged is the absence of a special law that serves as a comprehensive legal umbrella for wiretapping. Currently, there are at least 20 laws and regulations that regulate wiretapping for various types of crimes and law enforcement agencies, but there is no national standard that regulates the procedures, limits, and supervision of wiretapping in an integrated manner (Institute for Criminal Justice Reform, 2020) . This opens up opportunities for violations of citizens' constitutional rights, especially the right to privacy guaranteed in the 1945 Constitution. Other countries generally require court permission before wiretapping is carried out, limit the time period, and clarify access to wiretapping results, while in Indonesia these procedures still vary greatly between institutions and cases (Mabruri ., 2025)

In the context of personal data protection, the fragmentation of regulations and the weak supervision of wiretapping have the potential to threaten the security of public data. Wiretapping conducted without a clear monitoring mechanism can lead to misuse of data, human rights violations, and decreased public trust in law enforcement institutions. In addition, the rapid development of digital technology requires updating regulations and strengthening supervisory capacity in order to be able to keep up with new, increasingly sophisticated tapping modes (Sukartara ., 2024)

Thus, the challenge of monitoring wiretapping practices in the context of personal data protection in Indonesia lies in the overlap and fragmentation of regulations, weak monitoring mechanisms, and the absence of an effective independent oversight institution. Different wiretapping procedures between agencies, lack of transparency, and unobjective internal oversight further increase the risk of privacy violations and abuse of power. To ensure the protection of personal data and citizens' privacy rights, Indonesia needs to harmonise wiretapping regulations, establish an independent external oversight body, and enforce transparent and accountable standard procedures. In addition, strengthening public digital literacy and increasing the

capacity of law enforcement officials are also important steps to face the challenges of wiretapping in the rapidly evolving digital era.

Conclusion

Wiretapping in the digital era presents complex challenges for personal data protection in Indonesia, especially related to regulatory fragmentation and weak supervision. Regulations such as the Telecommunications Law, ITE Law, and PDP Law have not been harmoniously integrated, creating legal loopholes that are exploited for illegal wiretapping. The absence of an independent oversight body (BPDP) exacerbates the situation, while limited technical capacity and human resources make law enforcement suboptimal. In addition, the vulnerability of cyber infrastructure, low digital literacy of the public, and cross-border jurisdictional challenges further complicate oversight efforts.

Urgent solutions include harmonising regulations, establishing an authorised BPDP, and increasing budget allocations for data security technologies such as encryption and *intrusion detection systems*. Public education on privacy rights and data breach reporting mechanisms should be strengthened to build collective awareness. At the global level, Indonesia needs to ratify international conventions such as the Budapest Convention to address the challenges of cross-jurisdictional eavesdropping. Multi-sector collaboration between the government, private sector, and society is also crucial to create a transparent and accountable surveillance ecosystem.

Going forward, the balance between national security and citizens' privacy rights must be prioritised. Lawful wiretapping for law enforcement needs to be balanced with strict oversight mechanisms, including periodic audits and post-investigation data deletion. With systemic reforms, Indonesia can build public trust while ensuring sustainable growth of the digital economy. The protection of personal data is not just a legal issue, but the foundation for realising digital sovereignty and inclusive democracy amidst the unstoppable flow of technological transformation.

References

Anwar, F. (2024). Electronic Data Interception and Personal Data Protection. *Journal of Communication and Law*.

Bahtiar, N. (2022). Data Leakage Emergency: The Impasse of Personal Data Protection Regulation in Indonesia. *Digital Policy and Management Review.* https://journal.unhas.ac.id/index.php/DPMR/article/view/32144/11326

Budiyanto, A. (2025). Personal Data Protection in the Digital Age: Challenges and Solutions. *Journal of Law and Technology*.

Dewi, A. (2023). Implementation of the PDP Law in Monitoring Wiretapping in Indonesia. *Journal of Legislation and Technology*.

Dynasty, R. (2022). Legal Perspectives on Privacy and Personal Data Protection in the Digital Age. *Journal of Law and Human Rights.* https://dinastirev.org/JIHHP/article/download/3372/1855/12889

Hidayat, R. (2024). Digital Eavesdropping and its Implications for Personal Data Protection. *Journal of Technology and Law*.

Hutabarat, T. (2023). *Digital Privacy and Data Protection in Indonesia*. Digital Law Publisher.

Institute for Criminal Justice Reform. (2020). Challenges to Privacy Protection and Ensuring Access to Information Disclosure in Indonesia. *ICJR Paper Series.* https://icjr.or.id/wp-content/uploads/2015/11/paper-3-final-Menyeimbangkan-Hak.pdf

Kitchenham, B. (2020). Procedures for Performing Systematic Reviews. *Keele University Technical Report*.

Kurniawan, F. (2021). Wiretapping and Personal Data Protection: An Indonesian Case Study. *Journal of Legal Studies*.

Lestari, M. (2023). Wiretapping Policy and Personal Data Protection in the Digital Era. *Journal of Public Policy*.

Mabruri, I. (2025). Challenges of Law Enforcement for Personal Data Protection in the Digital Era. *Journal of Law Enforcement*.

Nugroho, S. (2025). Design of Information System for the Directorate of Samapta Polda Using Website-Based RC4 Algorithm. *Scientific Journal of Informatics Research and Learning.* https://doi.org/10.29100/jipi.v10i2.6312

Prabowo, T. (2023). Personal Data Protection and Wiretapping Supervision in Indonesia. *Journal of Law and Public Policy*.

Prasetyo, D., Amelia, R. (2021). The Role of Hospital Management in Upholding Patient Rights. *Journal of Health Service Management.* https://doi.org/10.33560/jmpk.v24i3.2021.123

Pratama, D. (2023). *Reconstruction of Wiretapping Authority Regulation in the Framework of Human Rights Protection* [Sultan Agung Islamic University]. http://repository.unissula.ac.id/30936/1/10302000396.pdf

Pratama, R. (2023). Cybercrime Sniffing in M-Banking via WhatsApp. Rechtsidee. https://rechtsidee.umsida.ac.id/index.php/rechtsidee/article/view/985/823?download=pdf

Putra, H. (2023). Wiretapping, Surveillance, and Personal Data Protection in Indonesia. *Journal of Law and Society*.

Rahmawati, D. (2023). Legal Protection for Victims of Illegal Wiretapping Crime. *Tora: Journal of Law.* https://ejournal.fhuki.id/index.php/tora/article/download/539/251/1884

Ramadhan, M. (2022). Surveillance of Wiretapping in the Indonesian Legal System. *Indonesian Journal of Legal Science*.

Rothstein, H. R., Sutton, A. J., & Borenstein, M. (2006). *Publication Bias in Meta-Analysis: Prevention, Assessment and Adjustments*. John Wiley & Sons.

Santoso, B. (2021). Wiretapping and Personal Data Protection: A Human Rights Perspective. *Journal of Human Rights and Technology*.

Sari, D. (2022). Wiretapping as a Threat to Personal Data Privacy in Indonesia. *Indonesian Journal of Criminology*.

Sari, D., Pratama, R. (2021). Legal Frameworks for Patient Rights in Indonesia. *Indonesian Journal of Health Law.* https://doi.org/10.14710/ijhl.2021.13.2.45-56

Sari, E. (2025). The influence of health policies on legal protection for medical personnel and patients. *SIBATIK Journal.* https://publish.ojs-indonesia.com/index.php/SIBATIK/article/view/2647

Sari, N. (2023). *Civil Law Protection of Private Property Rights in the Digital Era* [Sultan Agung Islamic University]. http://repository.unissula.ac.id/37993/1/Ilmu%20Hukum_30302100231_fullpdf.pdf

Setiawan, E., Dewi, S. (2024). The Effect of Legal Reforms on Healthcare Service Quality. *Journal of Health Reform.* https://doi.org/10.20473/jrk.v8i1.2024.67-78

Sitorus, R. (2024). Harmonisation of Personal Data Protection Regulations in Indonesia. *Journal of Indonesian Legislation*.

Sukartara, D. (2024). Challenges of Personal Data Protection Implementation in Indonesia. *Locus: Journal of Legal Science Concepts.* https://jurnal.locusmedia.id/index.php/jkih/article/download/438/263

Suryani, N. (2024). Wiretapping Policy and the Challenges of Personal Data Protection. *Journal of Legal Policy*.

Suryani, T., Nugroho, W. (2022). Regulation and Quality of Health Services in Indonesia. *Journal of Health Regulation.* https://doi.org/10.31227/osf.io/regkes2022

Syaifudin, A. (2020). Legal Protection of Personal Data as a Right to Privacy in the Digital Age. *Al Wasath Journal.* https://journal.unusia.ac.id/index.php/alwasath/article/download/609/339/1789

Vernando, R. (2022). Cybersecurity Systems and Data Sovereignty in Indonesia in the Perspective of Political Economy. *JIRA: Journal of Accounting Research Science.* https://ejournal.polraf.ac.id/index.php/JIRA/article/download/234/279/1181

Wibowo, S. (2021). Judicial Oversight of Wiretapping in Indonesia. *Journal of Law and Justice*.

Wulandari, S. (2022). Wiretapping, Surveillance, and Personal Data Protection: A Juridical Review. *Digital Juridical Journal*.

Yusuf, A. (2025). Tapping Regulation and Supervision in the Digital Era. *Journal of Regulation and Policy*.