JOURNAL LA SOCIALE

VOL. 06, ISSUE 03 (842-859), 2025
DOI:10.37899/journal-la-sociale.v6i3.1702

Implications of Government Policy on Digitalization of Public Services in Realizing Smart Government

Lutfi Pratama Adi Subarkah[1], Basri Mulyani[1], Muammar Alay Idrus[1]

[1]*Universitas Gunung Rinjani, NTB*

**Corresponding Author: Lutfi Pratama Adi Subarkah*
E-mail: luhtfipratam1976@gmail.com

Article Info

Article history:
Received 12 October 2024
Received in revised form 9 February 2025
Accepted 24 March 2024

Keywords:
Law No. 27 of 2022
Personal Data
SIAK Digitalization
Personal Data Violations

Abstract

Digitization of public services has become one of the main focuses of the Indonesian government in an effort to improve the efficiency, transparency, and accessibility of services to the public. This digitalization policy, especially in the context of the Population Administration System (SIAK), has significant legal implications. This study aims to analyze the legal impact of government policies related to SIAK digitalization by highlighting aspects of personal data protection, the validity of electronic documents, and the accessibility of services for all citizens. This study uses a qualitative research method with the type of Normative Juridical research. In this study, the Approach used is the Statute Approach. The analysis focuses on the legal framework that regulates personal data protection, including Law Number 27 of 2022 concerning Personal Data Protection, as well as regulations related to electronic documents regulated in the Electronic Information and Transaction Law (UU ITE). The results of the study show that although SIAK digitalization has succeeded in increasing efficiency and facilitating access to services, there are still several legal challenges that need to be overcome. These challenges include the risk of personal data breaches, the digital divide that can hinder access to services for people in remote areas, and the issue of the validity of electronic documents that still cause uncertainty among the public. This study concludes that to achieve effective and equitable implementation of digitalization, further adjustments to existing regulations are needed, increasing people's digital literacy and strengthening information technology infrastructure.

Introduction

Advances in information and communication technology have made many things easier in various aspects of life (Ahadiyah, 2023; Cholik, 2021; Mukhsin, 2020), including the management of personal data. However, these advancements also bring new challenges, especially related to the security and privacy of personal data. Personal data is a valuable asset and is vulnerable to various threats, such as misuse, theft, or hacking (Fad, 2021; Saputra et al., 2024; Nusantara et al., 2024). Therefore, personal data protection is an increasingly important issue to address, especially in today's digital era (Suari & Sarjana, 2023).

To support the protection of personal data in Indonesia, Law Number 27 of 2022 concerning Personal Data Protection regulates various important aspects, ranging from the rights of data subjects to the obligations of data controllers, and establishes sanctions for violations (Disemadi et al., 2023; Yudistira & Ramadhan, 2023). In addition, regulations made by the Electronic Information and Transaction Law (UU ITE) for electronic documents support this protection effort (Rosadi, 2023).

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

The government is making efforts to implement these regulations as part of efforts to build a smart government that is responsive and reliable. Smart Government's focus is not only on efficient and accessible public services but also on the security and privacy of citizens. The government seeks to create a secure digital environment by strengthening the protection of personal data and electronic documents (Mahran & Sebyar, 2023; Masri & Hirwansyah, 2023). This will increase public trust in technology and public services. The success of smart government is highly dependent on the government's ability to protect personal data and ensure the security of electronic transactions (Multazam & Widiarto, 2023). Therefore, strong laws and strict supervision are essential to ensure Smart Government works properly and meets the expectations of the Community (Kwak & Lee, 2023; Singh et al., 2022). Through these steps, the government shows its commitment to building digital infrastructure that is safe, reliable, and able to face challenges in the information technology era (Wirawan, 2020).

The concept of Smart Government is very important in efforts to modernize and optimize the performance of government institutions through the use of information technology (Adenekan et al., 2024; Anthopoulos et al., 2021; Criado & Gil-Garcia, 2019). Smart Government focuses on improving the quality of public services that are fast, precise, and responsive to the needs of the community (Adventy et al., 2024; Budiono & Mukhlis, 2024). However, in its implementation, several problems hinder the assessment of the success of smart government, especially in terms of the ideal quality of public services.

The government's unpreparedness to integrate public services with the e-government system as a whole is a major problem (Amalia, 2019; Reis et al., 2019). One of the various elements of this unpreparedness is the failure to ensure the security of digital data in the digitization of public services (Multazam & Widiarto, 2023). Data security is essential in the digital age because digitally stored public data is vulnerable to threats such as hacking, misuse, and data leakage (Keshta & Odeh, 2021; Perwej et al., 2021). If the government is not fully prepared to manage and protect this digital data, public trust, and service performance will be threatened.

In addition to data security issues, the shift toward smart government is also influenced by changes in the life models of people, countries, and states (Aldabbas et al., 2020; Grinin et al., 2022; Ismagilova et al., 2022). Currently, society is growing because of the needs and expectations that continue to change along with technological advances. Public services can become irrelevant or even detrimental if the government is unable to adapt to these changes (Dunlop et al., 2020; Valle-Cruz et al., 2019; Kurniawan, 2022).

This research focuses on the analysis of the legal implications of the public service digitization policy in the context of SIAK. With a case study on SIAK, this study will explore how these policies are implemented and their impact on citizens' rights. In addition, this study will also review the readiness of existing regulations to face challenges arising from digitalization, as well as provide recommendations for future policy improvements.

Methods

In this study, several relevant approaches should be considered. This type of normative juridical research is used. This study will concentrate on laws and regulations related to public service digitalization policies and how they are applied to the concept of smart government. The purpose of this research is to gain an understanding of the basic legal, policy, and legal consequences of the application of technology in public services. The Statute Approach is an approach that analyzes laws, government regulations, and policies related to the digitization of public services, such as the Presidential Regulation on Electronic-Based Government Systems and the Law on Information and Electronic Transactions. Conceptual Approach: Analyzing concepts and theories about smart government and public service digitalization to understand

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

the theoretical foundation and academic perspective related to digital transformation in public services (Marzuki, 2016).

The primary data in this study is Law Number 27 of 2022 concerning Personal Data Protection (abbreviated as the Personal Data Protection Law), which is analyzed in depth by relating it to data and supporting theories. Meanwhile, secondary data includes literature, academic journals, books, government reports, and legal documents related to research topics. Through qualitative analysis techniques, the collected data will be processed by examining the relationship between legal policies and the implementation of public service digitalization and its impact on smart governance.

With the right methods and approaches that are in line with the needs of the research, it is hoped that the research can provide outputs, including producing recommendations related to the ideal legal framework to support the digitization of public services, identifying legal obstacles faced in the implementation of Smart Government and providing feasible solutions to be implemented, providing insight into how government policies in digitizing public services can run more effective in the existing legal order (Alkotsar, 2018). This method helps to understand the legal implications in the context of the digitization of public services so that it can make a significant contribution to the legal literature and Smart Government practices in Indonesia.

Results and Discussion

Research on the digitization of public services has been carried out in the context of efforts to realize smart government. According to Winarno, the digitization of public services is an important step in accelerating transparency, accountability, and government efficiency. The success of this digitalization is highly dependent on a supporting legal framework, especially related to data protection and information security (Winarno, 2020). On the other hand, a study conducted by Pertiwi discusses regulatory barriers to the digitization of public services in Indonesia. Pratama found that despite significant efforts in adopting digital technology, the lack of harmonization between central and regional regulations is often a major obstacle. This research highlights the need for more integrated and consistent regulations to ensure the effective implementation of Smart Government (Pertiwi, 2023).

Personal data protection is a critical aspect in the digitization of public services, as regulated in Law No. 27 of 2022. The legal implications of this law on public policy, especially in the context of smart government, as quoted by Annisa et al. Yulianti concluded that although this law provides stronger protection for personal data, its implementation still faces various challenges, including inadequate technological infrastructure and low digital literacy among government officials (Rosadi, 2023).

Another research by Rahman examines the impact of Law No. 27 of 2022 on the private sector involved in the provision of public services. Rahman found that the law presents new challenges for the private sector in managing personal data, especially related to compliance with strict security standards. However, Rahman also emphasized that this regulation can encourage an improvement in overall data protection standards in Indonesia (Mahameru et al., 2023).

The validity aspect of electronic documents is also the focus of several previous studies. For example, a study by Suryani (2020) discusses the validity of electronic documents in the Indonesian judicial system. Suryani emphasized that although the ITE Law provides a legal basis for electronic documents, there are still doubts among legal practitioners about the authenticity and security of the documents as evidence in court. This shows the need for regulatory adjustments and increased legal understanding of the use of electronic documents.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

The study by Prayitno examines legal challenges in the implementation of public service digitalization policies in Indonesia. Prayitno identified several key obstacles, including a lack of coordination between government agencies, unclear regulations related to data sharing between agencies, and the readiness of technology infrastructure that varies in different regions. This study recommends the need for more focused regulatory and policy improvements to overcome these obstacles (Prayitno, 2023). In comparison, Lee's research reviews the implementation of Smart Government in South Korea and the accompanying legal implications. Lee pointed out that strict regulations and strong infrastructure support are the keys to the successful implementation of Smart Government in the country. This study provides insight into the importance of regulatory integration, data security, and technology readiness in supporting.

Personal Data Theft and the Role of the Minister of Communication and Information

Didik M. Arief Mansur and Elisatris Gultom highlighted the positive and negative impacts of information technology advancements, especially the increase in internet use. They identified cybercrime as one of the serious negative impacts, often caused by a lack of ability or knowledge of law enforcement officials in handling cases in cyberspace. With the advancement of information technology, humans can now carry out activities not only in the real world but also in the virtual world. In cyberspace, humans can live a second life that is almost similar to real life, complete with different challenges and threats. One of the biggest threats is cybercrime, which can damage real life in a variety of ways (Yudistira & Ramadhan, 2023).

While computer technology provides many advantages, such as access to information, job opportunities, political participation, and entertainment, it also carries significant risks. The threat of cybercrime is a serious problem for individuals and organizations, especially governments, that have to deal with the various crimes that arise from these technological advancements. The public doesn't know much about internet crime and how to protect their data, which exacerbates the problem. Cybercrime, which includes various forms of lawlessness, such as data theft, hacking, and online fraud, has become a threat to the wider community. One of the causes is the lack of additional resources and equipment needed to deal with the problem. As a result, in order to effectively tackle cybercrime, stronger efforts are needed, such as improved security infrastructure and better training for law enforcement. These efforts will not only reduce the adverse effects of information technology but will also strengthen the protection of personal data and the integrity of information systems (Mutiara & Maulana, 2020).

Due to the large number of cases of personal data leaks that occurred in Indonesia before the Personal Data Protection Law, some previous laws partially regulated personal data protection. Still, there were no specific laws that regulated the rights and responsibilities of the parties managing the data. This condition allows for uncontrolled leakage of personal data.

The Personal Data Protection Law was drafted to meet the need for more effective protection of the personal data of Indonesian citizens. This law aims to strengthen individuals' rights to their data, increase awareness of the importance of data protection, and provide better legal certainty for individuals regarding data management by various parties. This initiative is in line with global trends in data security and privacy, which are reflected in regulations such as the General Data Protection Regulation (GDPR) in the European Union (Fauzi & Shandy, 2022).

One of the crucial elements of this law is the application of administrative sanctions for violations related to personal data protection. Although administrative sanctions are not always clearly defined in the law, in general, they are seen as a form of punishment aimed at ensuring compliance with administrative provisions. In the context of the Personal Data Protection Law,

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

administrative sanctions are applied to deal with violations of the norms set in the management of personal data. The goal is to enforce the law, provide a deterrent effect, and prevent the recurrence of violations in the future.

The application of administrative sanctions regulated in Chapter VIII Article 57 of the Personal Data Protection Law provides a legal basis for the authorities to take firm action against violations that occur. These sanctions include several forms, such as administrative fines, warnings, and revocation of business licenses for entities proven to have committed serious violations of data protection provisions. The goal is not only to punish violators but also to restore order and ensure legal certainty in protecting the community's data (Bahtiyar, 2023).

The Personal Data Protection Law was passed on October 17, 2022, in response to the challenges of data protection in the digital era. This law aims to address the problem of personal data leakage that is often managed by Electronic System Operators (PSEs), including the Ministry of Communication and Information Technology and private entities.

One of the main objectives of this law is to prevent the misuse of personal data by irresponsible parties, who often take advantage of loopholes in data security systems. With the advancement of technology and the rapid development of the internet, cybercrime, including data leaks, is becoming increasingly difficult to avoid. Cases such as identity theft, fraud, and illegal access to personal information have become a real threat. Hence, the protection of personal data is no longer just an individual right but a collective need to create a sense of security in interacting with technology.

The importance of handling this data leak cannot be underestimated, considering its significant impact on various aspects of life. In the realm of individuals, personal data leaks can lead to financial losses, privacy violations, and identity misuse. For groups or institutions, data leaks can damage reputations, lower levels of public trust, and cause operational disruptions. On a broader scale, countries can also be adversely affected by cyberattacks, especially if sensitive data related to national security or politics is leaked to irresponsible parties (Vania et al., 2023).

This is where the Personal Data Protection Law is very important because it provides certainty for individuals and organizations about their rights and obligations regarding personal data. The law also requires PSEs to implement adequate security measures if a breach is committed. This effort is made to reduce the possibility of data leakage and to guarantee that electronic system operators are fully responsible for the management of the personal data they collect. However, the implementation of this law must be accompanied by strict supervision and cooperation between the government, the private sector, and the community. In addition to strong regulations, increasing public awareness of the importance of safeguarding personal data is also key. A definitive and secure solution to the problem of data leakage must include a multi-sectoral approach involving advanced technology, increased digital literacy, and strict law enforcement. Only with these measures can optimal personal data protection be achieved, creating a safer and more reliable digital environment for all parties.

Based on Indonesia's cybersecurity report from 2020 to 2022, there was a significant increase in the number of personal data leak cases. Some important points related to data leakage during this period are as follows (Najwa, 2024): 1) One of the biggest cases of data leaks in Indonesia occurred in 2020 when data from 91 million Tokopedia users was reportedly leaked and sold on dark web forums. This case has come to the attention of the public and highlighted vulnerabilities in data security managed by large platforms; 2) Leaks also occurred in the health sector, where data on 230 thousand COVID-19 patients was leaked from government applications that manage health information; 3) The total number of cyber incidents reported by the State Cyber and Cryptography Agency (BSSN) reached 290 million attacks, mostly

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

related to malware, phishing, and hacking; 4) In 2021, various government agencies also experienced data leaks. One of the most striking is the leak of personal data from the KPU (General Election Commission), where the data of around 2.3 million Indonesians was leaked and circulated on online forums; 5) The BPJS Kesehatan data leak case involving 279 million personal data is in the main spotlight. The leaked data includes sensitive information such as NIK, name, address, and phone number; 6) Cyberattacks in Indonesia have increased this year, with BSSN recording more than 1.6 billion cyber incidents, which include malware attacks, data theft, and network compromise; 7) In 2022, attacks on the government sector continued. One of the major cases is the leak of National Police data, where around 28 million personal data of National Police members was reported to have been leaked; 8) Other institutions, including the Ministry of Home Affairs and several private platforms, also experienced data leaks that resulted in the leakage of NIK, KK, and other personal information; 10)BSSN reported a further increase in cyberattacks, with more than 2 billion threats recorded during the year. These attacks are dominated by the exploitation of security gaps in digital systems that have not yet been updated.

From this data, it is clear that Indonesia faces major challenges in cybersecurity and personal data protection. The increase in the frequency of data leaks indicates the need for stronger regulations, the implementation of better security standards, and a wider awareness of the importance of data protection.

Legal Implications of Law No. 27 of 2022 concerning Personal Data Protection

The purpose of the Personal Data Protection Law is to provide a clear and comprehensive legal framework for protecting personal data. Personal data includes information such as name, address, phone number, and biometric data that can be used to identify a person. With the increasing use of digital technology and data collection in various industries, the protection of personal data has become very important.

Protection of Personal Data

The digitization of the Population Administration Information System (SIAK) in Indonesia is an important step in the modernization of public services, enabling the management of citizens' data more efficiently and transparently. However, this large-scale data management poses significant challenges related to personal data protection. With the risk of data leaks increasing along with technological developments and cyberattacks, SIAK needs special attention in terms of data security (Irwandi et al., 2021).

The Personal Data Protection Law has been passed in Indonesia to provide a legal basis for protecting personal data. This law establishes the rights and obligations of all related parties as well as sanctions for violators. However, in the context of the Population Administration Information System (SIAK), further adjustments are needed to manage population data involving millions of people. SIAK stores sensitive data, including NICs, addresses, and other demographic information, so vulnerability to cyberattacks must be minimized with advanced security technology. Electronic system operators are also fully responsible for the management of the personal data they collect. Some important steps to take to overcome these challenges include (Rahman et al., 2023):

High Safety Standards

SIAK must be equipped with strong encryption technology to protect data in transmission and storage. Encrypted data is difficult for unauthorized parties to access, even in the event of a leak. Multi-factor authentication (MFA) needs to be implemented to ensure that only authorized users, both government officials and public users, can access the system.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

System Supervision and Audit

Strict monitoring mechanisms must be implemented to ensure that all access and activities within the system are monitored and recorded. Periodic audits of the system also need to be carried out to detect potential weaknesses and proactively improve security. The use of blockchain-based technology can be considered to create a system that is more transparent and difficult to manipulate, especially when it comes to data tracking.

Law Enforcement and Sanctions

The government must strictly enforce the Personal Data Protection Law in the context of SIAK, including applying administrative and criminal sanctions for parties proven to have committed violations. Cooperation between institutions, such as Kominfo and BSSN, is needed to ensure the security of digital systems on a national scale.

Community Education

In addition to technology, people must also be educated about the importance of safeguarding their data. They need to understand the risks that exist in the digital ecosystem as well as ways to protect their information, such as through strong passwords, avoiding phishing links, and being aware of data protection practices. Awareness campaigns on data privacy and security should be part of the government's agenda to create a safer digital ecosystem.

In conclusion, the implementation of the Personal Data Protection Law requires a layered security strategy and strong law enforcement. The digitization of population administration is a great opportunity for Indonesia to improve the efficiency of public services. Still, it must be supported by adequate measures to protect the personal data of its citizens. With good security standards and continuous public education, SIAK can run more safely and reduce the risk of data breaches.

Validity of Electronic Documents

With the digitization of the Population Administration Information System (SIAK), the transition from physical documents to electronic documents brings convenience and efficiency to the community but also brings challenges related to public trust in the security and validity of electronic documents. Since the Electronic Information and Transaction Law (UU ITE) stipulates that electronic documents have the same legal force as physical documents, electronic documents must meet certain conditions, such as using a valid electronic signature to verify the identity of the signer and maintaining the integrity of the document so that it cannot be altered or forged. However, uncertainty among the public regarding the workings and validity of electronic signatures, as well as trust in this technology, is an issue that requires special attention (Jayasinga & Triono, 2023).

Some of the challenges faced in the implementation of electronic documents in SIAK include (Christine & Kansil, 2023): 1) Lack of public understanding. There are still many people who do not fully understand the concept of electronic signatures and how electronic documents can be guaranteed to be authentic. They often doubt that digital documents can be used as valid evidence in legal or administrative proceedings. Socialization of regulations related to electronic documents and electronic signatures needs to be increased so that the public is more familiar with the use of digital documents and understands the legal protections inherent in these documents; 2) Trust in Safety. Concerns about the security of electronic documents often arise, especially when it comes to potential forgery or manipulation. The security of the encryption system used in the management of electronic documents must be continuously monitored and improved to ensure the integrity of the documents. The implementation of technologies that can provide security guarantees, such as blockchain or digital certificates,

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

needs to be strengthened. This will increase public confidence that documents generated from SIAK cannot be altered or forged after they have been issued; 3) Validity of Documents in Legal Process. Although the ITE Law recognizes electronic documents as valid legal evidence, there are concerns about how courts or government agencies will verify the authenticity of documents in dispute cases. The development of national standards related to electronic document verification is essential to ensure consistency and clarity in legal processes; 4) Infrastructure and Supporting Technology. To ensure that electronic documents can be widely used, an adequate technological infrastructure is required, including a secure digital platform for data and document management. The government must ensure that SIAK systems are supported by cutting-edge technology and have good reserves in place to deal with possible cyberattacks; 5) Clear Legal and Policy Guarantees. The government must provide clearer and more convincing legal guarantees to the public regarding the validity and protection of electronic documents. This can be done by issuing more detailed technical guidelines on the use of electronic signatures and the recognition of digital documents in various agencies.

To address these challenges, the steps that need to be taken include 1) Extensive public education on the regulation and validity of electronic documents, including the use of electronic signatures; 2) Development of a stronger legal framework to ensure electronic documents are acceptable in all aspects of law and administration; 3) Improvement of security technology in the SIAK system to guarantee that electronic documents cannot be manipulated and remain secure; and 4) Training for law enforcement and bureaucracy related to the management, validation, and recognition of electronic documents.

With these efforts, public trust in electronic documents can be increased so that they have more confidence in the legitimacy of documents issued through SIAK. This will facilitate the transition to broader and more effective digital services in Indonesia.

Service Accessibility

The digitization of the Population Administration Information System (SIAK) has the potential to increase the efficiency and accessibility of public services for all citizens. However, as you mentioned, the main challenge facing these policies is the significant digital divide at different levels of society. People who live in remote areas or have limited digital literacy may not have adequate access to information and communication technology, which can hinder their ability to make optimal use of digital services (Marfu'ah, 2024).

Some of the main challenges related to the digital divide in the implementation of SIAK digitalization are (Manurung & Thalib, 2022): 1) Limited Access to Technology in Remote Areas. In many remote areas, technological infrastructure, such as internet access and communication networks, are still inadequate. This makes it difficult for residents in these areas to access digital services, including SIAK. The availability of devices such as computers or smartphones is also an obstacle. Many families do not have the devices needed to access digital services independently; 2) Low Digital Literacy. Many citizens, especially older people or those living in rural areas, have low digital literacy. They may not be used to using technological devices to access online services or even feel unconfident in the face of new digital platforms. The lack of understanding of cybersecurity is also a problem, where people are vulnerable to phishing attacks or other digital scams; 3) Social and Economic Inequality. Socioeconomic disparities play a role in access to technology. Low-income communities often do not have the financial means to get quality internet access, adequate devices, or digital literacy training. Those in the lower middle economic group also often do not have the knowledge or opportunity to learn about digital technologies that continue to develop; 4) Uneven Infrastructure. Another challenge is uneven technological infrastructure. In many

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

regions, especially in eastern Indonesia, telecommunications infrastructure is inadequate, so internet speed and signal coverage are very limited.

To address these challenges and prevent SIAK digitalization from exacerbating inequality, the government needs to formulate several comprehensive strategies (Rachmatullah & Purwani, 2022): 1) Technological Infrastructure Improvement. The government must work with telecommunications service providers to expand the reach of internet access and telecommunication networks in remote areas. Programs such as Village BTS (Base Transceiver Stations) or the expansion of fiber optic networks can help improve internet access in underserved areas. Additional infrastructure, such as digital service centers in villages, could also be built to provide access to technology for people who do not have personal devices; 2) Digital Literacy Training. Digital literacy training must be the government's main focus in bridging the digital divide. Free training organized by the government or NGOs in remote areas can improve people's ability to use technological devices and access digital services. Education about digital security is also very important so that people can understand how to protect their data when using digital platforms such as SIAK; 3) Hybrid Solution. In areas with limited access to technology, the government can consider a hybrid approach, where public services remain physically accessible in government offices but with the integration of technology that allows data to be digitized and stored centrally through SIAK. Officers in villages or sub-districts can be provided with digital tools so that they can help residents who do not have internet access to register their data online; 4) Subsidies and Financial Support. For underprivileged families, the government can provide internet subsidies or cheap digital devices. Programs like this have been implemented in various countries to help address inequality in access to technology. Device loan initiatives or technology assistance programs can also be considered, where people can borrow devices such as laptops or tablets for the purpose of accessing digital public services; 5) Building cooperation with the private sector and international institutions. CSR (Corporate Social Responsibility) programs from telecommunications or technology companies can be used to improve internet access in remote areas.

With this effort, SIAK digitalization can truly support digital inclusion and provide benefits for all citizens without exception. Governments must commit to bridging this digital divide so that all communities, both urban and rural, can benefit from easier, faster, and more transparent public services.

Challenges and Potential

The digitization policy of the Population Administration Information System (SIAK) brings great potential to improve the administrative system in Indonesia, especially in terms of efficiency, transparency, and accessibility of public services. By using digital technology, the process of managing population documents such as ID cards, birth certificates, or family cards can be carried out faster, reducing waiting times and administrative costs that are often complaints of the community (Hisbulloh, 2021). However, in order for this potential to be fully realized, several important aspects need to be considered:

Efficiency and Ease of Access to Services

Process Speed. Digitalization allows for faster and more efficient administrative services. Citizens can take care of population documents online without the need to visit the service office physically. This can save time and effort, especially for those who live far from government service centers.

Reduced Administrative Costs. With a digital system, the cost of procurement, filing, and management of physical documents can be reduced. An integrated system can reduce the need

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

to print and store documents in physical format, as well as simplify the audit and data tracking process.

Transparency and Accountability. Digital systems allow for more accurate and transparent record-keeping. With data recorded automatically, the possibility of corruption or administrative errors can be minimized, thereby increasing public trust in public services.

Regulatory Updates in Accordance with Technological Developments

Dynamic Regulatory Needs. Along with the rapid development of technology, regulations related to SIAK must be constantly updated. For example, data encryption technology, biometric-based authentication, or the use of blockchain in population data management can be an important part of a more modern policy.

Alignment with Laws and Regulations. Law Number 27 of 2022 concerning Personal Data Protection and the ITE Law must continue to be adjusted to innovations in the field of technology. This regulation must clearly regulate the rights and obligations of all parties related to personal data protection and sanctions for violations, including in the context of SIAK (Suryawijaya, 2023).

Strengthening System Security

Security of Personal Data. One of the biggest challenges in digitalization is cybersecurity. Personal data managed at scale by SIAKs must be protected with high-security mechanisms, such as encryption, multi-factor authentication, and real-time monitoring of cyber activities.

Precautions against cyberattacks. Potential cyberattacks, such as hacking or data theft, are a major concern. The government must invest in sophisticated security systems and continue to increase awareness and capabilities in handling cyber incidents across all sectors involved in SIAK (Ali & Nurhayati, 2020).

Collaboration Between Stakeholders

Public-Private Cooperation. To create a safe and inclusive digital ecosystem, the government needs to work with the private sector, such as technology companies, internet service providers, and cybersecurity institutions. The private sector can contribute to providing technological infrastructure and sharing expertise in terms of innovation and security.

Civil Society and Public Education. In addition to the private sector, civil society also plays an important role in overseeing the implementation of policies and voicing the interests of the community. Public education on digital literacy and citizens' rights in the context of personal data is essential to ensure broader and sustainable participation in the digital ecosystem.

International Collaboration: Given that data security and management is a global issue, collaboration with international institutions is also necessary to share best practices, obtain international certifications, and participate in global forums related to data protection and privacy (Katharina, 2021).

Inclusivity of Digital Services

Access for All Walks of Life. Digitalization must not create new gaps in terms of access to public services. The government needs to ensure that all levels of society, including those living in remote areas or having limited access to technology, can take advantage of these services. The digital device subsidy program and the improvement of internet infrastructure in remote areas are concrete steps that need to be taken.

Facilities for vulnerable groups. For vulnerable groups, such as people with disabilities or people who are not tech-savvy, the government needs to provide special facilities, such as

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

digital service centers, that can be physically accessed with the help of trained officers (Nurlaila et al., 2024).

Supervision and Law Enforcement Mechanism

Audit and Supervision of SIAK Services: To ensure that population data is managed correctly and safely, a strict monitoring mechanism needs to be implemented. The use of automated audit technology can help monitor any changes or access to data, as well as detect potential abuse.

Strict Sanctions for Data Breaches: In the event of a data breach, both by individuals and agencies, the government must enforce sanctions in accordance with applicable laws and regulations. The Personal Data Protection Law already provides an adequate legal framework, but its implementation must be strengthened through cooperation with law enforcement agencies and regulators in the technology sector (Kosegeran, 2022).

By overcoming existing challenges and maximizing the potential brought by SIAK's digitalization, Indonesia can create a more modern, efficient, and inclusive administrative system. Governments need to develop dynamic regulations to adapt quickly to technological changes and ensure that all citizens can benefit from these policies.

The Urgency of Law No. 27 of 2022 in Meeting Public Demands in Technological Development and Personal Data Theft

The Ministry of Communication and Information Technology stated that, in the midst of the advancement of the digital economy and information technology, the Personal Data Protection Law (PDP Law) plays an important role in protecting the personal data of Indonesians. There are 18 chapters and 78 articles in this law that regulate data transfer, sanctions, illegal use, and dispute resolution. Most human rights, especially the right to privacy, include the protection of personal data. Many countries around the world see the protection of personal data as a constitutional right or use data habeas mechanisms to correct misused data. In this case, the dignity and freedom of the individual are related to the right to the protection of personal data. Effective protection of personal data serves as a solid foundation to ensure political, spiritual, and religious freedom, all of which are part of basic human rights (Bintarawati, 2024).

With the PDP Law, Indonesia has decisively opened a new era in personal data management, presenting clear legal standards to maintain public privacy. The law also has the potential to increase public confidence in the use of technology, both in the government and private sectors, as it provides a legal framework that protects against the threat of data misuse. Along with the increasing digitalization in various aspects of life, the implementation of this law is expected to answer the challenges and risks faced by society while supporting responsible innovation in the digital sector. The protection of personal data under the PDP Law is also an important foundation for creating a safe and sustainable digital climate where people can feel more protected in maintaining their privacy rights without hindering technological advancement.

Frequent personal data protection failures, as outlined, indicate serious weaknesses in response mechanisms to data breaches. One of the main problems is that personal data controllers are often too late to realize that there is unauthorized access or hacking of the data they manage, so the response to protect or save the data is less than optimal. In fact, some data controllers may tend to deny the existence of such a breach even though public evidence has clearly shown a data leak. This phenomenon risks damaging public trust in the data protection system and the reputation of data controllers (Humairah, 2023).

Every sector needs a unique approach to implementing data security and cybersecurity. All organizations have different needs and goals related to personal data protection, so they should conduct a gap assessment, also known as a gap assessment, to find out how well their data is

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

currently secured. This assessment helps determine the strengths and weaknesses that must be maintained. Once this assessment is complete, organizations can create a roadmap to protect personal data. This roadmap includes several important steps: 1) Implementation of Consent Management. Manage the consent of the individuals whose data is collected, ensuring that they understand and consent to how the data will be used; 2) Records of Processing Activities (ROPA). Logs all personal data processing activities carried out by the organization to ensure transparency and regulatory compliance; 3) Conduct privacy impact assessments before processing personal data at scale, which can identify risks and provide mitigation before a privacy breach occurs; 4) Drafting a privacy policy that is easy for users or clients to understand, explaining how their data will be processed protected, and the rights they have; 5) Appointment of Data Protection Officer (DPO). Appoint a data protection officer who is responsible for the organization's compliance with personal data protection laws and manages all aspects related to privacy.

This roadmap is designed for two to five years, depending on the needs of the organization. Organizations must monitor changes in laws and regulations relating to the protection of personal data at the national and international levels. To implement comprehensive data protection, departments such as leadership, IT, finance, and legal must work together. Additionally, the roadmap should include employee training on privacy and cybersecurity to increase their awareness of the importance of maintaining data privacy and best practices in managing personal data.

It is essential to establish clear rights and obligations for legal entities that manage personal data in order to keep personal data safe. By using the Personal Data Protection Law (PDP Law), several basic principles can be applied to comprehensively maintain the security and privacy of personal data (Mahameru et al., 2023):

Limited and Specific Data Processing. Personal data must be processed in accordance with the purposes for which it has been specifically determined and on a legitimate legal basis. Data processing must not be carried out carelessly or outside the scope of the purpose agreed upon by the personal data subject. This aims to limit the misuse of personal data.

Openness and Transparency. Legal entities that manage personal data must exercise transparency in every stage of data processing. Data subjects have the right to know how their data is processed, who has access to it, and how long it will be stored. This openness is important to build trust and maintain the integrity of data managers.

Subject Rights. Personal data subjects must be granted their rights, including the right to access, correct, or delete their data. To fulfill this right, the personal data management agency must have a sophisticated and reliable system.

Deletion or Destruction of Data. Personal data must be securely deleted or destroyed after the retention or data processing period is complete. However, there are specific regulations that may require longer storage, such as laws or regulations of related sectors.

Use of Data Processing Tools in Public Facilities. The use of data processing tools in public facilities, such as for security, traffic management, and disaster prevention, is an important step in protecting personal data. In situations like these, in order to maintain transparency and ensure that the appliance is being used for a clear purpose, information about the installation location of the appliance must be made available to the public.

Management Code of Ethics. Both individuals and legal entities that manage personal data must have a code of ethics that governs how to manage personal data properly. This code of

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

conduct can be established through professional associations or at the request of relevant institutions, so there are clear standards for managing personal data.

By establishing clear rights for data subjects and strict obligations for data controllers, Smart Government systems can be built in a more secure, transparent, and structured manner. In this digital era, Smart Government requires effective management of personal data to support efficient and responsive public services while maintaining citizens' right to privacy. Legal entities that manage data in the Smart Government ecosystem must continue to innovate in terms of data security. Technologies such as encryption, multi-factor authentication, and threat monitoring and detection need to be adopted to ensure that personal data is processed and stored securely. By referring to the Personal Data Protection Law (PDP Law), data managers have clear guidelines for designing systems that minimize the risk of data security breaches. Every technological innovation implemented in Smart Government must always refer to existing regulations. Fulfilling legal obligations for data controllers, such as granting access to data subjects, applying transparency principles, and deleting data after the retention period has expired, is key to ensuring the security and privacy of personal data.

The implementation of optimal personal data protection in Smart Government also requires cross-sectoral collaboration between government agencies, the private sector, and the community. Organizational leaders and IT, legal, and information security departments must work together to create a holistic data protection policy. Engaging all stakeholders can create a safer digital ecosystem and ensure that each party understands their roles and responsibilities in protecting personal data. This effort provides stronger privacy guarantees for data subjects. By managing personal data securely and in compliance with the law, citizens can have more confidence in the public services provided through the Smart Government system. This will encourage wider adoption of the technology and increase public trust in the government. Ultimately, the proper implementation of data subject rights and data controller obligations not only improves government efficiency but also plays a role in building security, privacy, and legal compliance in the digital ecosystem, which is essential for achieving a reliable Smart Government.

Conclusion

The conclusion of this study shows that the digitization of the Population Administration Information System (SIAK) has made a positive contribution to improving the efficiency and ease of access to public services. However, several legal challenges still need to be faced to ensure a more optimal and fairer implementation. These challenges include, first, the Risk of Personal Data Breach: Digitalization raises concerns about the protection of personal data, which requires strengthening regulations related to cybersecurity and privacy; second, the Digital Divide: People in remote areas face limited access to digital services due to uneven technological infrastructure, which has the potential to exacerbate the gap in public services; Third, Validity of Electronic Documents: There is still uncertainty regarding the recognition and validity of electronic documents in legal transactions, which raises doubts among the public. Therefore, this study recommends that there are first, regulatory adjustments to ensure data protection and clear legal recognition of electronic documents; second, Increasing digital literacy in the community so that they are better prepared to access and utilize digital services; third, strengthening information technology infrastructure to overcome the digital divide and ensure equitable access to public services throughout the region. With these steps, it is hoped that the implementation of digitization of public services can run more effectively, safely, and fairly for all levels of society.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

References

Adenekan, O. A., Ezeigweneme, C., & Chukwurah, E. G. (2024). The evolution of smart cities: Integrating technology, governance, and sustainable development. *International Journal of Applied Research in Social Sciences*, *6*(5), 891–902. https://doi.org/10.51594/ijarss.v6i5.1131

Ahadiyah, F. N. (2023). Perkembangan Teknologi Infomasi Terhadap Peningkatan Bisnis Online. *INTERDISIPLIN: Journal of Qualitative and Quantitative Research*, *1*(1), 41–49. https://doi.org/10.61166/interdisiplin.v1i1.5

Aldabbas, M., Xie, X., Teufel, B., & Teufel, S. (2020). Future Security Challenges for Smart Societies: Overview from Technical and Societal Perspectives. *2020 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, 103–111. https://doi.org/10.1109/ICSGCE49177.2020.9275630

Ali, M. & Nurhayati, D. (2020). Perlindungan Data Pribadi dalam Era Digital di Indonesia: Tantangan dan Solusi. *Jurnal Hukum & Pembangunan*, *50*(1), 25–39.

Alkotsar, A. (2018). *Metode Penelitian Hukum Profetik*.

Amalia, E. (2019). Backend Challenges and Issues for E-Government in Indonesia seen through the Perspective of Infrastructure of E-Government Components Cube. *Global Business and Management Research*, *11*(1), 110–119.

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Anthopoulos, L., Sirakoulis, K., & Reddick, C. G. (2021). Conceptualizing Smart Government: Interrelations and Reciprocities with Smart City. *Digital Government: Research and Practice*, *2*(4), 1–28. https://doi.org/10.1145/3465061

Bahtiyar, A. (2023). *Implikasi Hukum Pidana Dalam Perlindungan Data Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*.

Bintarawati, F. (2024). The Influence Of The Personal Data Protection Law (Uu Pdp) On Law Enforcement In The Digital Era. *Anayasa : Journal of Legal Studies*, *1*(2), 135–143. https://doi.org/10.61397/ays.v1i2.92

Cholik, C. A. (2021). Perkembangan Teknologi Informasi Komunikasi / Ict Dalam Berbagai Bidang. *Industry and Higher Education*, *2*(1), 1689–1699.

Christine, B., & Kansil, C. S. T. (2023). Hambatan Penerapan Perlindungan Data Pribadi di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *7*(9), 16331–16339. https://doi.org/10.36418/syntax-literate.v7i9.13936

Criado, J. I., & Gil-Garcia, J. R. (2019). Creating public value through smart technologies and strategies. *International Journal of Public Sector Management*, *32*(5), 438–450. https://doi.org/10.1108/IJPSM-07-2019-0178

Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, M. (2023). Perlindungan Data Pribadi di Era Digital : Mengapa Kita Perlu Peduli ? *Sang Sewagati Journal*, *1*(2), 67–90. https://doi.org/https://doi.org/10.37253/sasenal.v1i2.8579

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Dunlop, C. A., Ongaro, E., & Baker, K. (2020). Researching COVID-19: A research agenda for public policy and administration scholars. *Public Policy and Administration*, *35*(4), 365–383. https://doi.org/10.1177/0952076720939631

Fad, M. F. (2021). Perlindungan Data Pribadi Dalam Perspektif Sadd Dzari'ah. *MUAMALATUNA*, *13*(1), 33. https://doi.org/10.37035/mua.v13i1.4674

Fauzi, E., & Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Lex Renaissance*, *7*(3), 445–461. https://doi.org/10.20885/JLR.vol7.iss3.art1

Grinin, L., Grinin, A., & Korotayev, A. (2022). COVID-19 pandemic as a trigger for the acceleration of the cybernetic revolution, transition from e-government to e-state, and change in social relations. *Technological Forecasting and Social Change*, *175*, 121348. https://doi.org/10.1016/j.techfore.2021.121348

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, *37*(2), 119. https://doi.org/10.26532/jh.v37i2.16272

Humairah, S. A. (2023). Upaya Penanggulangan Kebocoran Data Pribadi pada Aplikasi Lacak Pasien Corona Melalui Pemberlakuan UU PDP dan Pendayagunaan Anonymity/Pseudonymity 355. *Jurnal Hukum Lex Generalis*, *4*(4), 354–368. https://doi.org/10.56370/jhlg.v4i4.118

Adventy, M. I. Y., Tarizah, D. A., & Rafinzar, R. (2024). Tren Penelitian Pada Kualitas Layanan Publik Di Dunia: Blibliometric Analysis. *Jurnal Borneo Akcaya*, *10*(1), 111-121. https://doi.org/10.51266/jba.v10i1.397

Irwandi, M., Said, M. R., & Basri, B. (2021). Sistem Digitalisasi Administrasi Kependudukan Pada Kantor Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Polewali Mandar. *Journal Peqguruang: Conference Series*, *3*(2), 592. https://doi.org/10.35329/jp.v3i2.2400

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers*, *24*(2), 393–414. https://doi.org/10.1007/s10796-020-10044-1

Jayasinga, I. P. A., & Triono, A. (2023). Digitalization of Population Administration to Facilitate Public Services in the Era of Regional Autonomy. *International Journal of Multicultural and Multireligious Understanding*, *10*(5), 484. https://doi.org/10.18415/ijmmu.v10i5.4725

Katharina, R. (2021). *Pelayanan publik & pemerintahan digital Indonesia*.

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Kosegeran, G. (2022). Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin. *Lex Privatum*.

Kurniawan, T. (2022). Urgensi Pengesahan Rancangan Undang Undang Perlindungan Data Pribadi Dalam Digitalisasi Pelayanan Publik Guna Mewujudkan Smart Government. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *2*(2), 264–281. https://doi.org/10.15294/ipmhi.v2i2.55032

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Kwak, Y. H., & Lee, J. (2023). Toward Sustainable Smart City: Lessons From 20 Years of Korean Programs. *IEEE Transactions on Engineering Management*, *70*(2), 740–754. https://doi.org/10.1109/TEM.2021.3060956

Mahameru, D., Nurhalizah, A., Wildan, A., Badjeber, M., & Rahmadia, M. (2023). Implementasi Uu Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia. *Jurnal ESENSI HUKUM*, *November*.

Mahran, Z. A., & Sebyar, M. H. (2023). Pengaruh Peraturan Menteri Perdagangan (PERMENDAG) Nomor 31 Tahun 2023 terhadap Perkembangan E-commerce di Indonesia. *Jurnal Ilmu Hukum Dan Sosial*, *1*(4), 51–67. https://doi.org/10.51903/hakim.v1i4.1440

Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati (JHS)*, *4*(2), 139–148.

Marfu'ah, S. (2024). Digitalisasi Pelayanan Publik : Ketidaksiapan Masyarakat Dalam Penggunaan Aplikasi Identitas Kependudukan Digital Di Bojonegoro. *Jomantara: Indonesian Journal of Art and Culture*, *Volume 15 No. 02 Juni 2024*. https://doi.org/10.23969/kebijakan.v15i02.12309

Marzuki, P. M. (2016). *Penelitian Hukum*. Kencana.

Masri, E., & Hirwansyah. (2023). Kebijakan Penerbitan Sertipikat Elektronik Pada Sistem Pendaftaran Tanah di Indonesia Untuk Mewujudkan Kepastian Hukum. *Krtha Bhayangkara*, *17*(1), 157–174. https://doi.org/10.31599/krtha.v17i1.2109

Mukhsin, M. (2020). Peranan Teknologi Informasi Dan Komunikasi Menerapkan Sistem Informasi Desa Dalam Publikasi Informasi Desa Di Era Globalisasi. *Teknokom*, *3*(1), 7–15. https://doi.org/10.31943/teknokom.v3i1.43

Multazam, M. T., & Widiarto, A. E. (2023). Digitalization of the Legal System: Opportunities and Challenges for Indonesia. *Rechtsidee*, *11*(2). https://doi.org/10.21070/jihr.v12i2.1014

Mutiara, U., & Maulana, R. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Indonesian Journal of Law and Policy Studies*, *1*(1), 42. https://doi.org/10.31000/ijlp.v1i1.2648

Nurlaila, N., Zuriatin, Z., & Nurhasanah, N. (2024). Transformasi Digital Pelayanan Publik: Tantangan dan Prospek dalam Implementasi E-Government di Kabupaten Bima. *Public Service and Governance Journal*, *5*(2), 21–37. https://doi.org/10.56444/psgj.v5i2.1468

Pertiwi. (2023). Mewujudkan good governance melalui pelayanan publik responsif gender. *Journal of Gender Equality Disability Social Inclusion and Children*, *1*(1). https://doi.org/10.61511/jgedsic.v1i1.2023.170

Perwej, D. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, D. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Prayitno, A. (2023). Technological Innovation in Public Administration Transformation: Case Study of e-Government Implementation in Indonesia. *Journal of Governance*, *8*(4). https://doi.org/10.31506/jog.v8i4.23017

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Rachmatullah, N., & Purwani, F. (2022). Analisis Pentingnya Digitalisasi & Infrastruktur Teknologi Informasi Dalam Institusi Pemerintahan : E-Government. *JURNAL FASILKOM*, *12*(1), 14–19. https://doi.org/10.37859/jf.v12i1.3512

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, *2*(1), 8-16. https://doi.org/10.32520/albahts.v2i1.3044

Rahman, Y. M., Haora, A., & Sutansi, E. N. (2023). Personal Data Protection In The Era Of Globalization (Indonesia Perspective). *Tirtayasa Journal of International Law*, *2*(1), 15. https://doi.org/10.51825/tjil.v2i1.19603

Reis, J., Santo, P. E., & Melão, N. (2019). *Artificial Intelligence in Government Services: A Systematic Literature Review* (pp. 241–252). https://doi.org/10.1007/978-3-030-16181-1_23

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi*. https://books.google.com/books?hl=en%5C&lr=%5C&id=-y7dEAAAQBAJ%5C&oi=fnd%5C&pg=PP1%5C&dq=privasi+personal+health+record+dalam+tindakan+pelanggaran+ham%5C&ots=Uw8O72qPzT%5C&sig=ikcBd2neGB9zOi4MKnkReyBlfSM

Saputra, B. A., Kurnia, E., Rahmah, M., & Sumarni, T. (2024). Penerapan Privasi Dan Etika Di Era Digital Dalam Perlindungan Data Pribadi. *Musytari: Neraca Manajemen, Akuntansi, Dan Ekonomi*, *5*(9), 55–65. https://doi.org/https://doi.org/10.8734/musytari.v5i9.3570

Nusantara, A. H. S., Umam, I. K., & Lubis, M. (2024). Jaminan Informasi dan Keamanan yang Lebih Baik: Studi Kasus BPJS Kesehatan. *Nuansa Informatika*, *18*(2), 120-127. https://doi.org/10.25134/ilkom.v18i2.202

Singh, T., Solanki, A., Sharma, S. K., Nayyar, A., & Paul, A. (2022). A Decade Review on Smart Cities: Paradigms, Challenges and Opportunities. *IEEE Access*, *10*, 68319–68364. https://doi.org/10.1109/ACCESS.2022.3184710

Budiono, P., & Mukhlis, M. (2024). Peran Krusial Manajemen Strategi Dalam Meningkatkan Kinerja Organisasi Publik. *Journal Publicuho*, *7*(3), 1183-1189. https://doi.org/10.35817/publicuho.v7i3.476

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68. https://doi.org/10.21787/jskp.2.2023.55-68

Valle-Cruz, D., Alejandro Ruvalcaba-Gomez, E., Sandoval-Almazan, R., & Ignacio Criado, J. (2019). A Review of Artificial Intelligence in Government and its Potential from a Public Policy Perspective. *Proceedings of the 20th Annual International Conference on Digital Government Research*, 91–99. https://doi.org/10.1145/3325112.3325242

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, *2*(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157

Winarno, B. (2020). *Digitalisasi Layanan Publik: Transparansi, Akuntabilitas, Dan Efisiensi Pemerintahan. Jakarta: Pustaka Pemerintahan*. Pustaka Pemerintahan.

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)

Wirawan, V. (2020). Penerapan E-Government dalam Menyongsong Era Revolusi Industri 4.0 Kontemporer di Indonesia. *Jurnal Penegakan Hukum Dan Keadilan*, *1*(1). https://doi.org/10.18196/jphk.1101

Yudistira, M., & Ramadhan. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo. *Unes Law Review*, *5*(4), 3802–3815. https://doi.org/https://doi.org/10.31933/unesrev.v5i4.698

ISSN 2721-0960 (Print), ISSN 2721-0847 (online)