JIHAD : Jurnal Ilmu Hukum dan Administrasi
Vol. 7 No. 3 September 2025
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v7i3.9460/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Legal Aspects of Personal Data Protection in the Implementation of Regional E-Government

Beverly Evangelista[1], R. Fahmi Natigor Daulay[2]
Fakultas Hukum, Ilmu Sosial dan Ilmu Politik
Universitas Mataram, Indonesia

Article Info
Article history:
Received: 17 September 2025
Publish: 27 September 2025

Keywords:
E-Government;
Personal Data Protection;
Normative Weakness.

Abstract
The transformation of government services from manual systems to digital platforms through e-government in Indonesia is a response to the advancement of information and communication technology (ICT) and the demand for bureaucratic efficiency. Presidential Instruction No. 3 of 2003 marked the initial milestone in e-government development, which has since evolved into various digital public services such as OSS, SatuSehat, and Satu Data Indonesia. This study employs a normative legal method using statutory, conceptual, and normative gap analysis approaches. The focus of the research is directed at two main aspects: the regulation of personal data protection within regional e-government systems and the normative weaknesses in ensuring the security and confidentiality of citizens' data. The discussion reveals that despite the enactment of the Personal Data Protection Law (PDP Law), its implementation at the regional level faces significant challenges, including overlapping regulations, lack of technical standards, weak oversight, and ineffective sanctions. Regional governments often lack clear operational guidelines, resulting in disparities in data protection across regions. The study concludes that personal data protection must be an integral part of digital governance system design. Regulatory reform, institutional capacity building at the regional level, and the establishment of effective oversight mechanisms are strategic steps to ensure comprehensive protection of citizens' privacy rights in the digital era.

Corresponding Author:
Beverly Evangelista
Fakultas Hukum, Ilmu Sosial dan Ilmu Politik
Universitas Mataram, Indonesia.
Email: beverly@staff.unram.ac.id

1. BACKGROUND

The transformation of government services from manual to electronic systems marked the beginning of e-government in Indonesia. This change not only reflects increased bureaucratic efficiency but also demonstrates a paradigm shift in public services that are more responsive and adaptive to public needs. Improved performance of state officials has also driven changes in mental attitudes and behaviors that are more service-oriented, in line with the development of Information and Communication Technology (ICT), which has transformed the mindset and lifestyle of society at large. Presidential Instruction Number 3 of 2003 concerning "National Policy and Strategy for e-Government Development" became an important milestone that affirmed the state's commitment to utilizing ICT as a primary instrument for effective and efficient governance. The government recognizes that ICT has great potential to bridge communication between the state and citizens, as well as address various complex public service challenges (Amrozi, Y. et al., 2022). From a global

perspective, the World Bank defines e-government as "the use of information technology by government agencies to improve services to citizens, businesses, and also support collaboration with other government agencies," emphasizing the importance of community empowerment through broad access to information (Lenak, S.C. et al., 2021). This definition emphasizes that e-government does not only concern internal bureaucracy, but also external relations with work partners and the public as service subjects.

The implementation of e-government in Indonesia has been realized in various forms of digital services, such as the Peduli Lindungi application (now integrated with SatuSehat) in response to the health crisis, the Online Single Submission (OSS) System for businesses, and the Satu Data Indonesia initiative that encourages information integration between government agencies. These achievements demonstrate the government's digital readiness in various sectors and have even received international recognition through the 2022 United Nations E-Government Survey, in which Indonesia ranked 77th out of 193 countries. However, behind these achievements lie fundamental challenges that have not been fully addressed, particularly related to the digital divide in the 3T (frontier, outermost, and least developed) regions, as well as the suboptimal protection of people's personal data in the e-government system (UN E-Government, 2022). Two key issues highlighted are the weakness of legal regulations that specifically and operationally guarantee the security and confidentiality of personal data, and the lack of uniform technical standards at the regional level. Despite the existence of the Personal Data Protection Law (UU PDP), its implementation still faces serious challenges in terms of devolution of authority, oversight, and enforcement of sanctions. Local governments often face overlapping, undetailed regulations with minimal technical guidance, creating disparities in data protection across regions.

Therefore, this background not only highlights the evolution of e-government as a form of bureaucratic modernization but also draws attention to the urgency of regulatory and institutional reforms to guarantee citizens' digital rights. Personal data protection regulations must be an integral part of e-government system design, not merely an administrative complement. Furthermore, the normative weaknesses still rooted in the national legal system need to be addressed through more operational regulatory reforms, strengthening regional capacity, and establishing effective oversight mechanisms. Thus, e-government becomes not only a symbol of technological progress but also an instrument for protecting human rights in the digital era.

2. RESEARCH METHOD

This research uses a normative legal research method which is based on a study of written legal norms that regulate the protection of personal data in the context of the implementation of *e-government* in the regions. The approach used is a combination of a statutory approach, a conceptual approach, and a normative gap analysis. The statutory approach is used to examine various relevant regulations, such as Law Number 27 of 2022 concerning Personal Data Protection, Law Number 23 of 2014 concerning Regional Government, the Electronic Information and Transactions Law, and other sectoral regulations containing personal data protection norms. The conceptual approach is used to understand legal principles such as accountability, privacy, and information security, and how these principles are translated into the technical practices of providing electronic-based public services.

3. RESEARCH RESULTS AND DISCUSSION

1. Personal Data Protection Settings in the *E-Government* System District According to Laws and Regulations in Force

The development of information and communication technology has driven the transformation of government systems towards digitalization through the concept of Electronic-Based Government Systems (EBS). Presidential Regulation Number 95 of 2018 defines EBS as "government administration that utilizes information and communication technology to provide services to EBS users" (Presidential Regulation No. 95 of 2018, Article 1 paragraph 1). In this context, system security is a fundamental element, as emphasized in Article 2 paragraph (8) that security includes "confidentiality, integrity, availability, authenticity, and non-repudiation of resources supporting EBS" (Iswandari, B. A.: 2021). This means that the confidentiality of personal data of citizens involved in e-government services must be guaranteed and must not be misused. This is an important starting point in examining how regulations in Indonesia regulate the protection of personal data in digital government systems, especially at the regional level.

Law No. 23 of 2014 concerning Regional Government provides the legal basis for the implementation of e-government at the provincial and district/city levels. Although it does not explicitly regulate personal data protection, this law emphasizes that every authority delegated to regions must be accompanied by a responsibility to protect the resources entrusted to them by the public, including their personal data. Regional governments, as providers of public services, have a legal responsibility to ensure data security, use data legally and in a limited manner, and implement the principle of transparency. Therefore, regional heads and their staff bear full responsibility for data management in the e-government system, and any negligence that results in data leakage can be held accountable under the Regional Government Law and strengthened by the Personal Data Protection Law (Law No. 27 of 2022).

In addition to the Regional Government Law, a number of sectoral regulations also strengthen the personal data protection framework. Law Number 36 of 2009 concerning Health states that everyone has the right to privacy and protection of personal data, and Article 57 paragraph (1) requires recognition of everyone's right to confidentiality of their personal health condition. Law Number 23 of 2006 concerning Population Administration also emphasizes that personal data must be protected and may not be used for unauthorized purposes. Article 2 letters C and F state that everyone is obliged to protect the personal data of others and may not misuse it. These provisions indicate that personal data protection has become an integral part of various public service sectors, although it was not systematically integrated before the introduction of the PDP Law.

Other regulations that also govern the protection of personal data include the Banking Law (Law No. 10 of 1998), the Telecommunications Law (Law No. 36 of 1999), the Consumer Protection Law (Law No. 8 of 1999), and the Human Rights Law (Law No. 39 of 1999). The Banking Law requires banks to maintain the confidentiality of customer information, while the Telecommunications Law prohibits illegal access to telecommunications networks. The Consumer Protection Law emphasizes the principles of security and safety, and the Human Rights Law guarantees the right to personal protection and the confidentiality of electronic communications. The Electronic Information and Transactions Law (Law No. 11 of 2008) is also relevant, as Article 26 paragraph (1) states that the use of personal data through electronic media must be carried out with the consent of the data owner. In the context of e-government, this provision is very important because electronic systems are the main medium for collecting and processing citizen data.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and Government Regulation Number 80 of 2019

concerning Commerce Through Electronic Systems emphasize that personal data is an individual's property that must be protected by business actors and electronic system providers. Minister of Communication and Information Regulation Number 20 of 2016 also requires every electronic system provider to have internal rules for protecting personal data. Article 5 paragraph (1) states that "every Electronic System Provider must have internal rules for protecting Personal Data" (Minister of Communication and Information Regulation No. 20 of 2016). In addition, Article 17 paragraph (3) of Minister of Communication and Information Regulation No. 12 of 2016 emphasizes that telecommunications companies are required to maintain the confidentiality of user information and identities. This regulation gives data owners the right to access, delete, and resolve disputes related to their data, and requires the implementation of a protection system that is appropriate to the available technology and human resources.

The pinnacle of personal data protection regulations in Indonesia was the enactment of Law Number 27 of 2022 concerning Personal Data Protection. This law is a significant milestone because it explicitly regulates the right to privacy as part of the human rights guaranteed by the constitution. Article 28G of the 1945 Constitution of the Republic of Indonesia states that "everyone has the right to protection of themselves, their families, their honor, their dignity, and their property under their control." Therefore, personal data protection is not merely a technical administrative issue but also an integral part of respect for human dignity. The Personal Data Protection Law regulates the principles of data processing, the rights of data subjects, the obligations of data controllers, and sanctions for violations. In the context of regional e-government, this law provides a strong legal foundation for local governments to build a system that is secure, accountable, and oriented towards protecting citizens' rights (Mahameru, D. E., et al.: 2023).

Overall, the regulation of personal data protection in Indonesia's regional e-government system is the result of an integration of various complementary regulations. While previously scattered across various sectoral laws, the introduction of the Personal Data Protection Law provides stronger consolidation and legal certainty. Regional governments are required not only to comply with legal provisions but also to develop systems capable of ensuring data security technically and administratively. In the increasingly complex digital era, a holistic approach to personal data protection is essential, and existing regulations must continually adapt to technological developments and public needs for privacy and information security.

2. **Normative Weaknesses in Guaranteeing the Security and Confidentiality of Community Data in Implementation of *E-Government* in the area**

In an increasingly complex digital era, the implementation of e-government in regional governments is inevitable to improve the efficiency and transparency of public services. However, behind this progress lies a fundamental problem that has not been fully resolved: the weak normative guarantees for the security and confidentiality of public personal data. This weakness stems not only from the lack of comprehensive regulations prior to the enactment of the Personal Data Protection Law (PDP Law), but also from overlapping and substantive inaccuracies within various existing regulations. Before the PDP Law was passed, regional governments had to refer to several regulations, such as the Electronic Information and Transactions Law (ITE Law) and the Public Information Disclosure Law, each of which has a different perspective on personal data. This disharmony has led to confusion in implementation at the grassroots level and created legal uncertainty that directly impacts the protection of public rights (Suvil et al., 2024).

The main problem with existing regulations is their overly general and non-operational nature. Many provisions simply state that data must be secured, without providing clear and standardized technical instructions. For example, there is no explanation of the type of encryption that must be used, the security protocols that must be implemented, or the audit mechanisms that must be implemented. As a result, the level of data security depends heavily on the technical capacity and budget of each region, creating significant disparities between regions. Regions with limited resources tend to have more vulnerable security systems, while more developed regions can implement higher standards. The weak mandate for regular and independent audits and oversight within the regulations also creates a significant loophole. Without mandatory regular audits, system vulnerabilities can go undetected until data leaks occur. Furthermore, the lack of clear and firm rules establishing responsibility and accountability in the event of a data breach complicates the process of tracing and redressing the rights of affected communities. In this context, a weak and undetailed legal framework is the root of the problem, making guarantees of public data security and confidentiality in regional e-government highly vulnerable (Suvil et al., 2024).

These normative weaknesses lie not only in the absence of regulations, but also in the depth, coherence, and binding force of existing norms. While the Personal Data Protection Law (PDP) has been established as an umbrella legal framework, its implementation at the regional level still faces serious challenges. There is ambiguity and a lack of specificity in the devolution of authority from the PDP Law to regional governments. Ideally, the PDP Law should be accompanied by implementing regulations in the form of Regional Regulations (Perda) or Regent/Mayor Regulations that technically govern the implementation of personal data protection. However, to date, there are no standard guidelines from the central government explaining how general principles such as privacy by design, data minimization, or security safeguards should be translated into the technical practices of e-government service delivery. Without such guidelines, each region interprets and implements these principles differently, creating a regulatory patchwork that is inconsistent and vulnerable to legal loopholes. For example, encryption standards for health data in regional healthcare applications can be very different from those applied to tax data, even though the data sensitivity may be equivalent (Carlo & Hirawan, 2022).

The provisions in the PDP Law and the ITE Law generally only outline general principles without providing detailed technical guidance. Norms such as "Electronic System Operators are required to guarantee the security of Personal Data" are too vague and non-operational for direct implementation by local governments. Consequently, there are no clear, standard guidelines regarding technical security standards, such as the level of encryption required for sensitive data or security specifications for cloud versus on-premise data storage. Furthermore, there are no concrete data breach handling protocols, such as steps to be taken in the event of a data breach, who must be notified, and reporting deadlines. Human resource certification and competency are also not explicitly regulated, even though system operators handling personal data are supposed to have specific security certifications. This lack of clarity causes data security levels to depend heavily on the capacity and awareness of each region, creating unequal security gaps and potentially compromising people's privacy rights (Kriswandaru et al., 2024).

Existing regulations tend to focus on "what must be done" and are very limited in addressing "how to monitor" and "what sanctions will be imposed for negligence." Although the Personal Data Protection Law has established a Personal Data Protection Authority, internal oversight mechanisms at the regional level remain weak. The lack of mandatory periodic audits is a key indicator of weak oversight. There are no norms

mandating regular and independent data security audits of all regional e-government systems. The sanctions that are in place are often ineffective. Violations committed by State Civil Apparatus (ASN) are usually only subject to internal administrative sanctions such as warnings, which have no deterrent effect. Public reporting mechanisms are also unclear, inaccessible, and often complicated. This indicates that the oversight and law enforcement system has not been comprehensively designed to guarantee comprehensive personal data protection (Meldrum, 2003).

Sanctions stipulated in various regulations are often disproportionate and do not focus on redressing victims' rights. Imprisonment for data breach perpetrators, for example, does not automatically redress immaterial losses such as embarrassment, stress, or reputational damage suffered by data owners. Norms regarding adequate compensation for victims are also difficult to enforce and implement in practice, so victims often do not receive adequate remediation. Furthermore, the criminal sanctions imposed often fail to create a lasting deterrent effect for business entities, particularly corporations that perpetrate data breaches. Financial fines or imprisonment for specific individuals within a company do not necessarily force structural changes in the organization's data security system. Ideal sanctions should be not only retributive (punitive) but also reformative, requiring perpetrators to conduct comprehensive security audits, implement stricter protocols, and provide ongoing training for their employees. This approach can address the root cause and prevent similar violations in the future (Burdon, 2010).

Overall, the normative weaknesses in ensuring the security and confidentiality of public data in the implementation of e-government in the regions constitute a structural issue that requires comprehensive improvement. Existing regulations must be strengthened with clear technical provisions, effective oversight mechanisms, and proportionate sanctions oriented toward restoring victims' rights. The central government needs to provide standard guidelines that can be adopted uniformly by all regions to prevent disparities in personal data protection. Furthermore, institutional capacity at the regional level must be strengthened through training, certification, and adequate budget allocation. Without these measures, e-government, which should be an instrument for improving public services, has the potential to become a new source of vulnerabilities for the public's basic rights.

4. CONCLUSION

1. Personal data protection regulations in Indonesia's regional e-government systems are regulated through various complementary regulations, both sectoral and general. While previously scattered and unintegrated, the PDP Law provides a stronger and more comprehensive legal basis. Regional governments have full responsibility for maintaining the security and confidentiality of public data and ensuring that digital innovation does not compromise the right to privacy. Personal data protection is now part of respect for human rights and must be implemented through a secure, transparent, and accountable system.
2. Normative weaknesses in ensuring the security and confidentiality of public data in regional e-government lie in substantive inaccuracies, a lack of technical guidance, and weak oversight. Existing regulations tend to be abstract and non-operational, creating disparities in protection across regions. Without technical standards, regular audits, and effective sanctions, the system is vulnerable to violations. The PDP Law does not fully address implementation needs in the regions. Therefore, more detailed and reformative regulatory reforms are needed, oriented toward restoring victims' rights and increasing institutional capacity at the local level.

5. BIBLIOGRAPHY

Books and Journals

Amrozi, Y., dkk. (2022). *Kebijakan dan Strategi Nasional Pengembangan e-Government*. Jakarta: Pustaka Pemerintah.

Burdon, M. (2010). *Privacy and Data Protection in the Digital Age*. Oxford: Oxford University Press.

Carlo, R., & Hirawan, F. (2022). *Regulatory Patchwork dalam Implementasi E-Government Daerah*. Jakarta: CSIS Press.

Kriswandaru, A., et al. (2024). *Standar Teknis Keamanan Data dalam Sistem Pemerintahan Digital*. Yogyakarta: UGM Press.

Lenak, S. C., dkk. (2021). *E-Government dan Transformasi Digital Pelayanan Publik*. Bandung: Pustaka Administrasi.

Meldrum, D. (2003). *Accountability and Oversight in Public Sector Data Governance*. London: Routledge.

Suvil, T., et al. (2024). *Kelemahan Normatif dalam Perlindungan Data Pribadi di Pemerintahan Daerah*. Bandung: Pustaka Hukum Indonesia.

Legislation

The 1945 Constitution of the Republic of Indonesia.

Law Number 27 of 2022 concerning Personal Data Protection

Law Number 23 of 2014 concerning Regional Government.

Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 14 of 2008 concerning Public Information Disclosure.

Presidential Instruction Number 3 of 2003 concerning National Policy and Strategy for the Development of e-Government.