E-NISN : 2614-2643
P-NISN : 2541-7037
Journal Equitable
Vol 11 No 3
2026

WEAKNESSES OF THE DIGITAL SURVEILLANCE SYSTEM AT BPJS KESEHATAN WHICH RESULT IN POTENTIAL ABUSE OF POWER

Haya Kahilah Rahmah
Esa Unggul University, Indonesia, rahmahhaya@student.esaunggul.ac.id

Adhining Prabawati Rahmahani
Esa Unggul University, Indonesia, adhining.pr@esaunggul.ac.id

Abstract

The development of information technology has encouraged the state to utilize digital systems. This study aims to analyze why the weakness of digital surveillance has the potential to cause abuse of power by the state and have an impact on the shift in the principle of Rechtsstaat in Indonesia, as well as examine the implementation of state power restrictions in the implementation of digital surveillance to ensure the protection of citizens' privacy rights. The research uses normative juridical methods with a statutory approach and a conceptual approach. The legal materials used consist of primary legal materials in the form of "the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, and Government Regulation Number 71 of 2019, as well as relevant secondary and tertiary legal materials." The analysis was carried out qualitatively by drawing conclusions deductively. The results of the study show that weak digital surveillance can open up opportunities for abuse of authority and abuse of access to citizens' personal data. This condition is contrary to the principles of Modern Constitutionalism and Rechtsstaat which places the law as an instrument limiting state power. The BPJS Kesehatan data leak case shows weaknesses in information security governance and supervision mechanisms for personal data management that have the potential to threaten people's privacy rights. Therefore, it is necessary to strengthen supervision, transparency, accountability, and cybersecurity to ensure that digital surveillance practices remain in line with the principles of the rule of law and the protection.

Keywords: digital surveillance, abuse of power, privacy rights, rule of law, protection of personal data.

A. Introduction

The practice of collecting, storing, and utilizing personal data by the state has the potential to cause violations of constitutional rights if it is not regulated in a transparent, proportionate, and accountable manner. Digital surveillance is a legal and ethical issue that is closely related to the principle of the rule of law. Digital surveillance without effective control mechanisms, as well as without adequate accountability, causes the relationship between the state and citizens to become unbalanced. This inequality has the potential to encourage abuse of power, namely the use of authority that exceeds the

limits set by law or is not in accordance with the purpose of granting the authority. As a result of these conditions, there is a significant risk to the protection of the right to privacy. Weak surveillance can encourage abuse of power in digital surveillance practices, which ultimately threatens citizens' civil liberties. "In addition, the protection of the right to privacy also serves to limit the abuse of power by the government." [1]

Weak supervision in the management of personal data causes data controlled by the government and authorities to experience leaks. Personal data that was leaked included NIK, full name, address, cellphone number, email, date of birth, and even payslip information and personal photos. In addition, the impact of personal data leakage is also experienced by the public in the form of repeated calls from foreign numbers, contacts of close people contacted by unknown numbers, to the registration of illegal loans by parties who hold personal data information. Privacy violations can also appear in various forms, such as wiretapping without legal basis, dissemination of personal data without consent, use of facial recognition technology without permission, to falsification of personal data. "The right to privacy is one of the fundamental rights that has the potential to be violated if supervision is carried out without a clear, proportionate, and accountable legal basis." [2]

The case of data leakage in the BPJS Kesehatan system is one of the clear examples of weak digital supervision of personal data management by institutions

[1] Kurniawan Tri Wibowo, *DIGITAL LAW AND DATA PRIVACY*, ed. Muhammad Syaukani (CV. Al-Haramain Lombok, 2025), 10.
[2] M Rizki Ananda and Akhmad Ikraam, "JURNAL LOCUS : Research & Service of Human Rights Protection in the Era of Digital Surveillance by the State: Legal Analysis on Privacy Vs Security," *LOCUS JOURNAL: Research & Devotion* 5, no. 01 (2026): 512.

that provide public services. The leak allegedly involved data belonging to millions to hundreds of millions of Indonesian citizens which was then traded through internet forums. The leaked data includes important information, such as Population Identification Number (NIK), BPJS membership number, residential address, telephone number, and various other population administration data. The large amount of data affected shows weaknesses in the information security system, access control, and supervision mechanisms for the management of personal data that are under the control of public service providers. This incident reflects the lack of optimal state governance and supervision of digital systems that collect public data on a large scale. From the perspective of personal data protection, the state is not only obliged to collect and manage citizens' data, but also ensures the security, confidentiality, and integrity of such data through an effective surveillance system. The BPJS Kesehatan data leak shows a failure in carrying out these obligations, especially in the aspects of prevention, early detection, and cyber security risk mitigation.

In addition, indications that there are parties who trade personal data from the leak indicate the misuse of access to information that should be protected. However, academically, it is necessary to distinguish between data leaks that occur due to weak security systems and abuse of power which requires an abuse of authority by those who have authority. Therefore, in the absence of an official verdict or findings regarding the perpetrators and the mechanism of the leak, it is more appropriate to state that this case shows the weak supervision and protection of personal data that opens up opportunities for data misuse by unauthorized parties. As a result of these leaks, people lose control over their

personal data and face various risks of loss, such as identity theft, digital fraud, phishing, misuse of data for illegal online loans, and various other forms of cybercrime. This condition shows that the protection of personal data is not only related to the technical aspects of system security, but is also part of the fulfillment of citizens' constitutional rights to privacy and legal protection in the digital era.

The right to privacy is interpreted as the right of every individual to protect and control his or her personal information, personal life, and personal space from interference, surveillance, or dissemination without consent. This right gives everyone the authority to determine how data and information about themselves are collected, used, stored, or disseminated by other parties. The protection of the right to privacy is constitutionally guaranteed in the "Constitution of the Republic of Indonesia of 1945, especially Article 28G paragraph (1) which includes the right to personal protection, family, honor, and dignity." The PDP Law also provides for heavier sanctions for certain forms of violations, such as "falsification of personal data punishable by imprisonment of up to 6 years and/or a maximum fine of Rp60 billion, as well as illegal access to personal data for certain benefits punishable by up to 5 years in prison and a fine of Rp5 billion."

To overcome these problems, it is necessary to strengthen the legal framework that expressly regulates the practice of digital surveillance in line with the principles of modern constitutionalism. "The government needs to increase transparency by providing clear information about the objectives, methods, and scope of supervision to the public. Internal accountability mechanisms should be strengthened to ensure that any oversight

measures are carried out in accordance with applicable laws and procedures." [3]

Most research still focuses on the protection of personal data sectorally, such as in the context of digital banking, social media, or health services, without comprehensively examining the practice of digital surveillance by the state as a form of exercise of power. There has not been much research that explicitly links digital surveillance practices to potential abuse of power. Therefore, this study is here to fill this gap by analyzing digital surveillance in the framework of limiting power and protecting citizens' constitutional rights.

B. Problem Formulation

1. Why does the weakness of digital supervision have the potential to cause abuse of power by the state and have an impact on the shift in the principle of rechtstaat in Indonesia?
2. How is the implementation of state power restrictions in the implementation of digital surveillance to ensure the protection of citizens' privacy rights in Indonesia?

C. Research Objectives

This study aims to analyze the factors that cause weaknesses in digital supervision to potentially cause abuse of power by the state and its implications for the shift in the principle of rechtstaat in Indonesia. In addition, this study aims to examine the implementation of state power restrictions in the implementation of digital surveillance as an effort to ensure the protection of citizens' privacy rights in accordance with the principles of the state of law, human rights, and the provisions of

[3] Ridho Pakina and Mohammad Solekhan, "The Influence of Information Technology on Privacy Laws and Control in Indonesia: Balance Between Security And," *Journal of Scientech Research and Development* 6, no. 1 (2024): 281.

applicable laws and regulations in Indonesia. Through this analysis, this research is expected to make a conceptual contribution to the development of constitutional law and produce recommendations on strengthening digital supervision mechanisms that are accountable, proportionate, and in line with the principles of rechtstaat.

D. Research Methods

This study uses a normative juridical method with a descriptive-analytical nature. This method is used to examine positive legal norms that govern digital surveillance by the state. "Normative legal research methods are approaches that focus on the study of legal norms contained in laws and regulations, court decisions and legal doctrines, this method is often referred to as doctrinal methods or literature methods, because the research is through the analysis of written legal materials" [4]. "Normative legal research will start from legal events and then will search for references to legal norms such as laws and regulations, legal principles, and legal doctrines taught by legal experts to seek legal construction and legal relations." [5]

The research approach includes a statutory approach to analyze regulations related to personal data protection and digital surveillance, as well as a conceptual approach to examine the concepts of privacy, digital surveillance, and abuse of power in the perspective of modern constitutionalism. The legal materials used consist of primary legal materials in the form of "the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning the Protection of Personal Data, Government Regulation Number 71 of 2019, and other relevant regulations".

[4] Agus Satory et al., *Legal Research Methods*, vol. 2 (Tahta Media Group, 2024), 73.
[5] Vicky Srivastava, *Legal Research Methods Textbook*, *Published by Global Media*, 2024, 35, http://repository.uki.ac.id/14688/1/BukuAjarMetodePenelitianHukum.pdf.

Secondary legal materials in the form of books, scientific journals, and the results of previous research; as well as tertiary legal materials in the form of legal dictionaries and encyclopedias.

Data collection is carried out through library research by examining and inventorying various relevant legal materials. This method is the main technique in normative legal research because it relies on written legal materials as the main source of data. Data analysis is carried out qualitatively through the interpretation and assessment of the relationship between legal norms and digital surveillance practices by the state. Conclusions are drawn deductively, namely from general legal norms to more specific conclusions, so as to allow the preparation of logical, systematic, and comprehensive legal arguments related to the protection of privacy rights and the potential for abuse of power in digital surveillance.

The development of modern legal thought shows a shift from a rigid legal approach to a more responsive approach to the needs of society. "Overall, the application of responsive legal principles in regulatory formation allows for harmonization between formal legal certainty and substantive justice." [6] This approach is reinforced by the view that the law functions not only as a means of control over power, but also as a means to achieve broader social goals, including effective legal protection of citizens' personal data. "So that all of them meet the sense of justice according to the formulation of the Pancasila precept and also realize the existence of legal protection for the community". [7] "In this context, the state constitution plays a very important role in

[6] Joemarthine Chandra and Zainal Arifin Hoesein, "The Application of Responsive Legal Theory in the Formation of Regulations in Indonesia," *Judge : Legal Journal* 6, no. 05 (2025): 1495, https://journal.cattleyadf.org/index.php/Judge/article/view/1898.

[7] Dani Habibi and Nuruzzaman MS, "FUNCTIONALIZATION OF LAW

regulating governance, setting limits on government power, and protecting the rights of individuals." [8] Within this framework, the ethical principles of state administrators are important to ensure that the use of authority in digital supervision does not deviate from the legal purpose. "With strict supervision, it is hoped that the risk of data leakage can be significantly minimized, while encouraging a corporate culture that better respects consumers' privacy rights as an asset that must be optimally protected." [9] Thus, in the context of digital supervision, law enforcement should not only focus on the formal legality aspect, but must also consider the balance between legal certainty, fairness, and utility, as well as pay attention to the ethical dimension as an integral part of good governance.

Modern Constitutionalism Theory

John Locke stated that "the social contract that gives birth to the state does not by itself eliminate the individual rights of the people to participate in the decision-making process of the state". [10] The main principles in this theory include the rule of law, the limitation of power, and the existence of a monitoring mechanism (checks and balances) between state institutions. In the context of digital surveillance, this theory demands that any form of collection, processing, and utilization of personal data by the state must have a clear legal basis, a legitimate purpose, and be carried out proportionately, transparently, and accountably. It is

RESPONSIVE TO THE IMPLEMENTATION OF PERATUN JUDGMENTS AS A FORM OF LEGAL PROTECTION IN THE FRAMEWORK OF NATIONAL LEGAL SYSTEM REFORM," *Jotika Research in Business Law* 2, no. 2 (2023): 80.

[8] Muhamad Zaky Djauzie, "Pancasila as a Grundnorm According to Pure Legal Theory and Responsive Legal Theory," *To-Ra Law Journal* 11, no. 1 (2025): 241.

[9] Johanes Maruli Burju, "Analysis of the Role of Cyber Law in Maintaining User Privacy in Indonesia in the Digital Era," *Innovative Law : Journal of Social Law and Humanities* 3, no. 1 (2026): 33, https://doi.org/https://doi.org/10.62383/humif.v3i1.2781.

[10] Jimly Asshiddiqie, *The Constitution and Constitutionalism of Indonesia*, 2021, 172.

important to ensure that the use of technology does not violate the constitutional rights of citizens, especially the right to privacy guaranteed in the Constitution of the Republic of Indonesia of 1945). Modern constitutionalism serves as a normative framework for assessing whether the practice of digital surveillance by the state is still within the bounds of legitimate authority or has exceeded the principle of limitation of power.

The Theory of the State of Law (Rechtsstaat)

"The purpose of the state of law (Rechtsstaat) is to achieve justice, welfare and prosperity and to protect the rights of the people". [11] In this perspective, the law functions as an instrument of controlling power so that the state does not act arbitrarily against citizens. In the context of digital surveillance, the application of the Rechtsstaat principle requires the state to carry out surveillance practices based on clear legal provisions, as well as ensuring accountability in every use of citizens' personal data. As state power becomes more dominant than law, this shift can occur when digital surveillance is carried out without adequate oversight, without transparency, or without clear accountability [12]mechanisms. The law no longer functions as a limitation of power, but has the potential to be a tool of legitimacy for state actions. As a result, digital surveillance practices that should aim to protect the public interest have the potential to become a means of abuse of power that threatens citizens' privacy rights[13].

E. Results of Research and Discussion

[11] John Kenedi, *Penal Policy in the Law Enforcement System in Indonesia*, 2017, 4.
[12] Jimly Asshiddiqie, *The Constitution and Constitutionalism of Indonesia*; Satjipto Rahardjo, *Law in the Universe of Order*, 2006.
[13] Alisha Elvis, Lita Estyawati, and Lutfiah Nafi'ah Sholikhatun, "Ethics and Law in the Use of Digital Surveillance Technology by the State," *BUNK BEDS* 2, no. 4 (2025): 510–16, https://litera-academica.com/ojs/litera/.

Analysis of the weaknesses of digital supervision has the potential to cause abuse of power by the state and have an impact on shifting the principle of rechtstaat in Indonesia

The weakness of digital surveillance has the potential to cause abuse of power because the control of large amounts of data by the state is not always balanced with effective, transparent, and accountable control mechanisms. The main problem in digital surveillance in Indonesia does not lie in the use of digital technology by the state, but in the weak supervision mechanism for the processing of personal data. The state has broad authority to collect and manage public data through various electronic systems, but this authority has not been fully balanced by independent, transparent, and accountable oversight [14]mechanisms. This condition poses a risk of abuse of power, violation of privacy rights, and weakening of the principle of the rule of law.

In the perspective of the Modern Theory of Constitutionalism put forward by John Locke, the power of the state must be limited by the constitution to prevent abuse of authority and ensure the protection of the basic rights of citizens. Digital surveillance that allows the state to collect, store, and manage people's personal data can only be justified if it is implemented based on the principles of legality, proportionality, transparency, and accountability. When the mechanism for monitoring the use of digital technology does not run optimally, there is an imbalance in the relationship between the state and citizens which opens up space for abuse of authority. This condition is contrary to the principle of checks and balances that is at the core of modern

[14] Predderics Hockop Simanjuntak, "Legal Protection of Personal Data in the Era in Indonesia: A Study of the Personal Data Law and General Data Protection (GDPR)," *Journal of Legal Essence* 6, no. 2 (December 2024): 61.

constitutionalism because the state gains enormous access to citizen data without adequate supervision.

In the perspective of the Theory of the State of Law (Rechtsstaat), all government actions must be subject to the law and guarantee the protection of human rights. According to Hans Kelsen, the law functions as an instrument of limiting power so that the state does not act arbitrarily against citizens. Therefore, digital surveillance that is not accompanied by a clear accountability mechanism has the potential to shift the principle of the Rechtsstaat towards the dominance of state power over the law. This shift occurs when the law no longer functions as a tool of controlling power, but only becomes a formal legitimacy for state actions that have the potential to ignore people's privacy rights. Under such conditions, digital surveillance is no longer oriented to the public interest, but has the potential to become an instrument that expands state control over citizens without clear boundaries.

Normatively, the protection of the right to privacy has been guaranteed in "Article 28G paragraph (1) of the Constitution of the Republic of Indonesia of 1945 which states that everyone has the right to the protection of personal self, family, honor, dignity, and security from threats against himself." "Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia" not only provides recognition of the right to personal personal protection, but also creates a constitutional obligation for the state to prevent violations of citizens' privacy rights. Thus, when the state collects personal data through a digital surveillance system, the state is obliged to ensure that the collection, storage, and use of data is carried out in a secure manner and does not pose a risk of misuse. If the state fails to meet these

obligations, the constitutional protection of the right to privacy becomes ineffective.

The constitutional guarantee is strengthened through "Law Number 27 of 2022 concerning Personal Data Protection" which requires every personal data controller to maintain the security and confidentiality of the data it manages. In addition, "Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions" also requires electronic system operators to implement a reliable and responsible security system in protecting user data. Thus, the state not only has the authority to manage citizens' personal data, but also has a legal obligation to ensure the security, integrity, and confidentiality of such data. Failure to fulfill these obligations shows the weak implementation of the principle of the rule of law in digital governance. From the perspective of the Personal Data Protection Law, government agencies that process personal data are positioned as controllers of personal data so that they have the obligation to apply the principles of accountability, processing security, purpose limitation, and protection of the rights of data subjects. Therefore, large amounts of data leakage indicate that data protection obligations have not been carried out optimally, although assessments of violations of the law must still be proven through applicable supervision and law enforcement mechanisms.

This condition can be seen in the case of BPJS Kesehatan data leak which allegedly involves data of millions to hundreds of millions of Indonesians. The leaked data includes Population Identification Number (NIK), BPJS membership number, address, phone number, and various other population administration information which is then traded through internet forums. The large amount of data affected shows weaknesses

in information security systems, access control, and monitoring mechanisms for the management of personal data by public service providers. From the perspective of constitutional law, this case cannot automatically be qualified as an abuse of power because there has been no official decision or finding proving the abuse of authority by the authorized officials. However, the leak shows a failure of the state to carry out its constitutional obligation to protect citizens' privacy rights. Weak digital surveillance has created opportunities for unauthorized parties to illegally access and utilize people's personal data.

The impact of BPJS Kesehatan data leaks is not only in the form of individual losses such as identity theft, digital fraud, phishing, and data misuse for illegal online loans, but also has broader implications for the principle of the rule of law. When the state is unable to guarantee the security of the data it collects itself, public trust in state institutions declines. This condition shows that there is a gap between the legal norms that guarantee the protection of personal data and its implementation in practice. As a result, the principle of the Rechtsstaat, which requires the protection of human rights and the limitation of state power, is reduced because the state gains the authority to access public data without being accompanied by a balanced responsibility in ensuring its security.

Based on this description, it can be concluded that the weakness of digital supervision has the potential to cause abuse of power because it opens up space for abuse of authority and abuse of access to citizens' personal data. From the perspective of Modern Constitutionalism and Rechtsstaat Theory, digital surveillance practices must be implemented based on the principles of legality, transparency, proportionality, accountability, and

effective supervision. The BPJS Kesehatan data leak case shows that weak digital governance and supervision have threatened the protection of citizens' privacy rights and has the potential to shift the principle of the rule of law from the rule of law to the dominance of state power in the management of people's digital data.

Although the BPJS Kesehatan data leak cannot be qualified as an abuse of power in the sense of abuse of authority by state officials because there has been no decision stating this, the case shows the potential for structural abuse of power. This potential arises when the state has very broad access to people's personal data without an effective monitoring mechanism for the use of this authority. In other words, the weaknesses of digital surveillance create conditions that allow the abuse of authority if it is not accompanied by adequate restrictions and supervision.

The shift in the principle of Rechtsstaat does not mean that Indonesia has stopped being a state of law, but rather shows a tendency to weaken the function of law as an instrument limiting state power in the digital space. As states gain increasingly broad authority to access personal data without effective surveillance mechanisms, the law risks serving only as a formal legal basis for the expansion of that authority, rather than as an instrument that provides effective protection of citizens' rights. This shift is one of the main challenges in the implementation of digital-based government.

Analysis of the implementation of state power restrictions in the implementation of digital surveillance to ensure the protection of citizens' privacy rights in Indonesia

The development of information technology has encouraged the country to utilize digital systems in the

implementation of public services, national security, population administration, and various forms of electronic-based governance. However, the widespread use of digital technology by the state also increases the risk of violations of privacy rights if it is not accompanied by an adequate power restriction mechanism[15]. In a democratic legal country, digital surveillance cannot be carried out solely based on administrative needs or security interests, but must be limited by law to prevent abuse of power and ensure the protection of human rights. The main problem in the implementation of state power restrictions in the field of digital supervision lies in the lack of optimal supervision mechanisms for the use of state authority in collecting, processing, and utilizing citizens' personal data. Although the regulatory framework is available, its implementation still faces various obstacles so that the protection of privacy rights has not been implemented effectively[16].

In the perspective of Modern Constitutionalism Theory, the limitation of power is the main instrument to prevent the state from acting beyond its authority. According to John Locke, state power must be exercised according to the constitution and supervised through a mechanism of checks and balances so that the basic rights of citizens are protected. In the context of digital surveillance, the principle requires that every action of collection, storage, processing, and use of personal data is carried out based on a clear legal basis, legitimate purposes, and accountable supervisory mechanisms. The state cannot use digital technology indefinitely because the right to privacy is part of a constitutional right that must be respected and protected.

[15] Jeane Neltje Saly and et.al, "ANALYSIS OF RELATED PERSONAL DATA PROTECTION NO.27 OF 2022," *Serina Journal of Social Humanities* 1, no. 3 (2023).

[16] Rendy Pratama Putra et al., "Personal Data Protection in the Digital Era: A Review of the Framework," *INNOVATIVE: Journal Of Social Science Research* 3, no. 6 (2023).

The implementation of state power restrictions in the Indonesian legal system has obtained a constitutional basis through "Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia which affirms that Indonesia is a state of law." The affirmation of Indonesia as a state of law has the consequence that the use of digital technology by the government should not be based solely on considerations of administrative efficiency, but must meet the principles of legality, due process of law, and respect for human rights. As such, any form of digital surveillance must have a clear legal basis, a legitimate purpose, and a legally testable limit of authority. Consequently, all government actions, including digital surveillance, must be subject to the principle of the rule of law and must not be carried out arbitrarily. In addition, "Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia provides guarantees to everyone for the protection of their personal self, family, honor, dignity, and security from threats against themselves." These provisions show that the right to privacy is part of the constitutional right that must be protected by the state, including in the implementation of digital systems and the management of personal data. "The right to personal protection as guaranteed by Article 28G paragraph (1) not only prohibits arbitrary actions against citizens' privacy, but also creates a positive obligation for the state to build an effective data protection system." Therefore, the state's failure to ensure the security of personal data can be seen as a form of non-optimal fulfillment of these constitutional obligations.

Strengthening the limits on state power in digital surveillance is also realized through "Law Number 27 of 2022 concerning Personal Data Protection." This law stipulates that the processing of

personal data must be carried out in a lawful, limited, specific, transparent and accountable manner. Personal data controllers, including government agencies, have an obligation to maintain the security of the data they manage as well as be responsible for any breaches that cause harm to the data subject. The presence of the Personal Data Protection Law is a concrete form of restricting state authority because the collection and use of personal data can no longer be done without paying attention to the rights of data owners. Thus, the state not only plays a role as a holder of authority, but also as a party that has a legal responsibility in protecting data under its control. The provisions in the Personal Data Protection Law show that the state's authority as a data controller is not absolute. The state remains bound by the principles of purpose limitation, data minimization, accountability, and processing security. As such, any data collection action that goes beyond the set goals or is not accompanied by adequate safeguards has the potential to be contrary to those principles.

In addition, "Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions" requires every electronic system operator to implement a reliable, secure, and responsible security system. This provision emphasizes that the use of digital technology by the government must be accompanied by efforts to prevent the risk of data leakage, illegal access, and misuse of personal information. Within the framework of the state of law, these obligations are a form of implementation of the principle of accountability which aims to ensure that the power of the state in managing digital data is not used excessively or unsupervised. The obligation of electronic system operators to implement a reliable security system shows that the protection of personal data is a legal

obligation that must be fulfilled from the design, operation, to maintenance stage of electronic systems. Therefore, the occurrence of large-scale data leaks shows that the implementation of these obligations still faces weaknesses in terms of governance and supervision.

However, the implementation of state power restrictions in the practice of digital surveillance still faces various challenges. The BPJS Kesehatan data leak case shows that the mechanism for protecting and supervising personal data has not run optimally. Data leaks involving millions to hundreds of millions of population data show weaknesses in information security governance, access control, and supervision of digital systems managed by public service providers. This condition indicates that the existence of regulations has not been fully followed by effective implementation. As a result, citizens' privacy rights, which have been normatively guaranteed by the constitution and laws and regulations, are still vulnerable to violations. When linked to the provisions of the "1945 Constitution of the Republic of Indonesia, the Personal Data Protection Law, and Government Regulation Number 71 of 2019", the BPJS Kesehatan data leak case shows that there is a gap between legal norms and implementation. Normatively, the state already has an obligation to protect personal data, but in practice this obligation has not been carried out optimally so that citizens' privacy rights are still vulnerable to violations.

In the perspective of the Rechtsstaat Theory, the effectiveness of the limitation of state power is determined not only by the existence of legal norms, but also by the state's ability to implement and enforce those norms consistently. If digital surveillance is carried out without transparency, without an effective

complaint mechanism, and without clear accountability when violations occur, then the function of law as a limiting power becomes weakened. Under such conditions, digital surveillance has the potential to change from an instrument of public service to an instrument of state domination that threatens civil liberties and people's right to privacy. In the perspective of modern constitutionalism, the limitation of power is not enough to be realized through the formation of regulations, but also requires an effective checks and balances mechanism. Supervision of the management of personal data by government agencies needs to be carried out through an independent mechanism so that control over the use of authority does not depend only on internal government supervision.

In addition to the principle of legality, the implementation of state power restrictions must also meet the principle of proportionality. The collection and processing of personal data may only be carried out for as long as it is absolutely necessary to achieve a legitimate purpose and must not exceed such needs. This principle serves to prevent the state from excessive data collection (mass surveillance) that has the potential to interfere with citizens' privacy rights. The existence of the "1945 Constitution of the Republic of Indonesia, the Personal Data Protection Law, and Government Regulation Number 71 of 2019" shows that Indonesia normatively already has a relatively adequate legal framework. However, the effectiveness of restricting state power still depends more on the quality of implementation than the completeness of regulations. In other words, the main challenge is no longer a legal vacuum, but the consistency of implementation, institutional capacity, and the effectiveness of oversight mechanisms.

Therefore, the implementation of restrictions on state power in digital supervision needs to be strengthened through several steps. First, increasing transparency in the collection and use of personal data by government agencies. Second, strengthening the independent supervision mechanism for the management of personal data by state institutions. Third, the application of strict accountability principles through the provision of administrative, civil, and criminal sanctions for every violation of personal data protection. Fourth, strengthening cybersecurity and risk management systems to prevent data leaks that can harm society. Thus, the implementation of restrictions on state power in digital surveillance has basically obtained an adequate legal basis through the "1945 Constitution of the Republic of Indonesia, the Personal Data Protection Law, and Government Regulation Number 71 of 2019." However, the effectiveness of protecting citizens' privacy rights still depends on the consistency of implementing the principles of legality, transparency, accountability, and effective supervision. Limiting state power in the digital space is an important requirement to maintain a balance between state interests in utilizing technology and citizens' constitutional rights to privacy in the Indonesian legal state.

F. Conclusion/Conclusion

Digital supervision is a consequence of the development of information technology used by the state in the implementation of public services and governance. However, weak supervision of personal data management has the potential to cause abuse of power and threaten citizens' privacy rights. Based on the Theory of Modern Constitutionalism and the Theory of the State of Law (Rechtsstaat), any use of state authority in

the digital space must be limited by law, carried out proportionately, and supervised through effective accountability mechanisms. The BPJS Kesehatan data leak case shows that weaknesses in the digital surveillance system and personal data protection can open up opportunities for misuse of access to public data and cause various losses, such as identity theft, digital fraud, and other cybercrimes. This condition shows that the protection of the right to privacy is not only a technical issue of system security, but also part of the fulfillment of citizens' constitutional rights.

The implementation of restrictions on state power in digital surveillance basically has a legal basis through "Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions." However, the existence of these regulations has not been fully followed by effective implementation in practice. The persistence of data leaks shows that there is a gap between legal norms and their implementation. Therefore, to maintain the principle of Rechtsstaat in Indonesia, it is necessary to strengthen the mechanism of supervision, transparency, and accountability in every digital surveillance practice so that the use of technology by the state remains within the legal corridor and does not threaten citizens' privacy rights.

The government needs to strengthen digital surveillance governance through improving cybersecurity, strengthening independent supervision mechanisms for personal data management, and applying the principles of transparency and accountability in every data processing by state agencies. In addition, the enforcement of the Personal Data Protection Law must

be carried out consistently through the provision of strict sanctions for any violations or omissions that result in data leaks. Strengthening coordination between agencies and increasing the capacity of human resources in the field of information security is also needed so that personal data protection standards can be implemented effectively and sustainably.

In addition, the mechanism for regular monitoring and evaluation of the digital surveillance system needs to be optimized to ensure that any use of state authority remains within the limits of the law, respects citizens' privacy rights, and meets the principle of checks and balances. This step is important to ensure the protection of citizens' privacy rights, increase public trust in the government's digital system, and keep the implementation of digital surveillance in line with the principles of the state of law and modern constitutionalism.

Bibliography

1. Books

Jimly Asshiddiqie. Indonesian Constitution and Constitutionalism, 2021.

John Kenedi. Penal Policy in the Law Enforcement System in Indonesia, 2017.

Kurniawan Tri Wibowo. DIGITAL LAW AND DATA PRIVACY. Edited by Muhammad Syaukani. CV. Al-Haramain Lombok, 2025.

Rahardjo, Satjipto. Law in the Universe of Order, 2006.

2. Journal Articles

Ananda, M Rizki, and Akhmad Ikraam. "JURNAL LOCUS : Research & Service of Human Rights Protection in the Era of Digital Surveillance by the State: Legal Analysis on Privacy Vs Security." LOCUS JOURNAL: Research & Devotion 5, no. 01 (2026): 511–20.

Burju, Johanes Maruli. "Analysis of the Role of Cyber Law in Maintaining User Privacy in Indonesia in the Digital Era." Innovative Law: Journal of Social Law and Humanities 3, no. 1 (2026): 25–37. https://doi.org/https://doi.org/10.62383/humif.v3i1.2781.

Chandra, Joemarthine, and Zainal Arifin Hoesein. "The Application of Responsive Legal Theory in the Formation of Regulations in Indonesia." Judge : Journal of Law 6, no. 05 (2025): 1483–99. https://journal.cattleyadf.org/index.php/Judge/article/view/1898.

Dani Habibi, and Nuruzzaman MS. "LEGAL FUNCTIONALIZATION RESPONSIVE TO THE IMPLEMENTATION OF PERATUN JUDGMENTS AS A FORM OF LEGAL PROTECTION IN THE FRAMEWORK OF THE REFORM OF THE NATIONAL LEGAL SYSTEM." Jotika Research in Business Law 2, no. 2 (2023): 66–82.

Djauzie, Muhamad Zaky. "Pancasila as a Grundnorm according to the theory of pure law and the theory of responsive law." To-Ra Law Journal 11, no. 1 (2025): 14.

Elvis, Alisha, Lita Estyawati, and Lutfiah Nafi'ah Sholikhatun. "Ethics and Law in the Use of Digital Surveillance Technology by the State." VOL. 2, no. 4 (2025): 510–16. https://litera-academica.com/ojs/litera/.

Jeane Neltje Saly, and et.al. "ANALYSIS OF PERSONAL DATA PROTECTION RELATED TO NO.27 OF 2022." Journal of Social Humanities 1, no. 3 (2023).

Jimly Asshiddiqie. Indonesian Constitution and Constitutionalism, 2021.

John Kenedi. Penal Policy in the Law Enforcement System in Indonesia, 2017.

Pakina, Ridho, and Mohammad Solekhan. "The Influence of Information Technology on Privacy Laws and Control in Indonesia : Balance Between Security and." Journal of Scientech Research and Development 6, no. 1 (2024): 273–86.

Pratama Putra, Rendy, Hendi Saputra, Privacy Protection Law Yusuf Daeng, Nasri Linra, Atan Darham, Derry Handrianto, Risky Risandy Sianturi, and Denny Martin. "Personal Data Protection in the Digital Age: A Review

of the Framework." INNOVATIVE: Journal Of Social Science Research 3, no. 6 (2023).

Predderics Hockop Simanjuntak. "Legal Protection of Personal Data in the Era in Indonesia: A Study of the Personal Data Law and General Data Protection (GDPR)." Journal of Legal Essence 6, no. 2 (December 2024): 61.

Rahardjo, Satjipto. Law in the Universe of Order, 2006.

Satory, Agus, Yenny Febrianty, Widiyanti Rahayu Budi Astuti, and Aditya Fajri Kurnia Pradana. Legal Research Methods. Vol. 2. Tahta Media Group, 2024.

By Vicky Sri. Textbook of Legal Research Methods. Published by Global Media, 2024. http://repository.uki.ac.id/14688/1/BukuAjarMetodePenelitianHukum.pdf.