

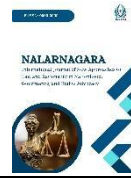


International Journal of New Approaches to Law and Rationality in
Nationhood, Governance, and Rights Advocacy

Nalarnagara Journal

Vol. 1, No. 2, April 2026 pp. 1-13

Journal Page is available at: <https://internationaljournal.lppmunsaka.ac.id/index.php/nalarnagara>



Constitutional Control Of State Digital Surveillance: Protecting Citizens' Constitutional Rights Through An Indonesian Model

Ramelan

Salakanagara University, Ramelan@unsaka.ac.id

ABSTRACT

The development of digital technology has expanded the capacity of the state to collect, process, analyze, and monitor information concerning citizens through various instruments, including communications interception, metadata collection, biometric systems, algorithmic surveillance, and database integration. On the one hand, digital surveillance is necessary to support law enforcement, national security, and the protection of public interests. On the other hand, the expansion of surveillance capabilities potentially places citizens in a vulnerable position with regard to violations of constitutional rights, particularly the rights to personal protection, privacy, freedom of communication, and informational autonomy. This study aims to analyze the construction of constitutional protection for citizens against state digital surveillance, identify the constitutional limits of state authority in conducting digital surveillance, and formulate an ideal model of constitutional control. This study employs normative legal research using statutory, conceptual, case, and comparative approaches. The findings indicate that the principal problem concerning digital surveillance does not lie merely in the legitimacy of surveillance technology, but rather in the absence of an integrated mechanism for limiting state power that is preventive, independent, and accountable. The protection of constitutional rights cannot rely solely on the principle of proportionality; it requires a control architecture capable of operating before, during, and after surveillance activities are conducted. This study proposes the Constitutional Digital Surveillance Control Model, a constitutional control model for digital surveillance consisting of five layers of protection: legality, legitimate purpose, necessity, independent authorization, and accountability and effective remedy. The model is expected to establish a balance between state security interests and the protection of citizens' constitutional rights while preventing the transformation of state digital power into practices characteristic of a surveillance state.

Keywords: Constitutional Rights; Digital Surveillance; Privacy; State Power; Digital Constitutionalism.

INTRODUCTION

The transformation of information and communication technology has fundamentally changed the way the state exercises its power. Digitalization is no longer merely an instrument for improving the efficiency of public services but has developed into an infrastructure through which the state can collect, process, analyze, and utilize information concerning its citizens. The development of big data, artificial intelligence, biometric systems, facial recognition, electronic communications interception, location tracking, and database integration has significantly expanded the state's capacity to conduct surveillance systematically, automatically, and on a scale that was previously difficult to imagine.

Digital surveillance provides important benefits for the state. Such technology can support law enforcement, crime prevention, the eradication of cybercrime, national security, counter-terrorism efforts, and the maintenance of public order. Because threats to security have also shifted into the digital sphere, the state cannot entirely abandon the use of surveillance technologies. Therefore, the constitutional issue is not simply whether the state may conduct digital surveillance, but rather the extent to which such authority may be granted and how that power must be limited.

The issue becomes increasingly complex because the characteristics of digital surveillance differ significantly from conventional surveillance. Technology enables the automatic and large-scale collection of communications metadata, online activities, geographic

locations, biometric records, electronic transactions, and behavioral patterns. The data collected can subsequently be linked and analyzed to generate profiles, classifications, and even predictions concerning individuals. Digital surveillance therefore provides the state not only with the ability to determine what an individual has done, but also with the ability to map and predict citizens' behavior.

The expansion of such capabilities creates risks for a democratic state governed by the rule of law. Surveillance initially intended as a security instrument may develop into excessive surveillance, mass surveillance, or surveillance conducted without clear individual suspicion. Under such conditions, technology may encourage the transformation of the state into a surveillance state, namely a condition in which the state possesses the capacity to continuously and systematically observe, record, and analyze the lives of its citizens.

These threats are directly connected to constitutional rights. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees protection of the individual, family, honor, dignity, property, and security. Article 28F guarantees the right to communicate and obtain information, while Article 28D paragraph (1) guarantees fair legal certainty. Article 28J provides a constitutional basis for restricting rights through legislation, but it cannot be interpreted as providing unlimited legitimacy for the state to interfere with citizens' private lives.

In the digital context, the protection of the individual should be interpreted dynamically so as to encompass personal data, digital identity, electronic communications, biometric data, location information, and other information that reflects an individual's life. Law Number 27 of 2022 concerning Personal Data Protection strengthens this construction by placing personal data protection within the broader protection of the individual. Nevertheless, personal data protection is not identical to the constitutional control of digital surveillance. Data protection focuses primarily on data governance, whereas digital surveillance concerns the broader exercise of state power to intervene in citizens' private spheres.

From the perspective of constitutionalism, the recognition of rights is always correlated with limitations on power. A constitution does not merely legitimize state institutions; it also restricts the excessive exercise of power. In the digital era, this principle must be expanded because threats to liberty do not always take the form of physical actions or direct prohibitions. They may also arise through covert information collection, algorithmic processing, and cross-institutional data integration.

The principal problem in Indonesia is the absence of a comprehensive constitutional-control framework governing the exercise of digital surveillance powers. Various legal instruments provide legal bases for surveillance, interception, access to electronic information, and data collection. However, these regulations have developed sectorally and therefore have not yet fully established an integrated control system. This condition may result in fragmented authority, different oversight standards, and uncertainty regarding the boundary between national security interests and the protection of citizens' private spheres.

Research on digital surveillance has developed through approaches concerning privacy, data protection, proportionality tests, due process, national security, and the need for independent oversight. However, these approaches generally remain focused on determining the limits of particular surveillance measures. There remains room for research aimed at formulating an architecture for controlling surveillance power that operates substantively, procedurally, institutionally, and remedially throughout the entire surveillance process.

This need is consistent with the development of international standards. The judgment in *Big Brother Watch and Others v. United Kingdom* demonstrates that the protection of rights in digital surveillance cannot be assessed solely on the basis of the existence of state authority, but must also take into account the quality of safeguards throughout the surveillance process.

Protection must operate before surveillance is conducted, during the collection and processing of data, and after the data have been used and retained.

On this basis, this study proposes the Constitutional Digital Surveillance Control Model, a constitutional-control model integrating five layers: legality, legitimate purpose, necessity, independent authorization, and accountability and effective remedy. These five elements constitute an interconnected control system. Legality establishes the legal basis and limits of authority; legitimate purpose restricts the purposes for which surveillance may be conducted; necessity examines the need for and minimization of interference; independent authorization prevents the concentration of power; while accountability and effective remedy ensure responsibility and redress.

The novelty of this study lies in shifting the perspective from merely examining whether a surveillance measure satisfies the principle of proportionality toward constructing an integrated architecture for the constitutional control of digital surveillance power. This model is further developed through the principle of Lifecycle Constitutional Control, namely a control mechanism that follows the entire surveillance cycle from the granting of authority to the deletion of data.

Accordingly, this study addresses three research questions. First, how is the constitutional protection of citizens against state digital surveillance constructed within the Indonesian legal system? Second, what are the limits and weaknesses of constitutional control over the state's authority to conduct digital surveillance? Third, what ideal constitutional-control model can ensure a balance between national security interests and the protection of citizens' constitutional rights?

This study aims to analyze the existing legal construction, identify weaknesses in the current control system, and formulate a constitutional-control model capable of strengthening Indonesia as a democratic state governed by the rule of law in the digital era.

METHODS

This study constitutes normative legal research oriented toward examining norms, principles, concepts, and legal constructions concerning the protection of citizens' constitutional rights against state digital surveillance. Normative legal research is employed because the focus of the study concerns the legitimacy of state authority, the constitutional limits on the exercise of such authority, and the formulation of an ideal legal construction.

The study employs a statutory approach, conceptual approach, case approach, and limited comparative approach. The statutory approach is used to analyze the 1945 Constitution of the Republic of Indonesia and legislation concerning human rights, personal data protection, electronic information, and state authority to conduct surveillance and interception. The conceptual approach is used to examine the rule of law, constitutionalism, constitutional rights, privacy, limitations on state power, digital constitutionalism, the surveillance state, and proportionality.

The case approach focuses primarily on *Big Brother Watch and Others v. United Kingdom*, while the comparative approach is used to identify relevant protection principles emerging from international legal developments.

The legal materials consist of primary, secondary, and tertiary legal materials. Primary legal materials include the 1945 Constitution of the Republic of Indonesia, legislation concerning human rights, personal data protection, electronic information, relevant judicial decisions, and relevant international legal instruments. Secondary legal materials consist of books, scholarly journals, research findings, and academic works concerning constitutionalism, privacy, data protection, digital surveillance, and digital constitutionalism.

The legal materials were collected through library research and subsequently analyzed using qualitative-prescriptive analysis through legal interpretation, systematization of norms, legal construction, and legal argumentation. The analysis is directed toward reconstructing mechanisms for controlling digital surveillance authority through the five principal elements of the Constitutional Digital Surveillance Control Model.

RESULTS AND DISCUSSION

A. The Construction Of Constitutional Rights Protection Against State Digital Surveillance

1. The Transformation of State Surveillance in the Digital Ecosystem

Digital technology has transformed the character of state surveillance. Conventional surveillance is generally constrained by space, time, human resources, and technical capabilities. Digitalization, by contrast, enables information to be collected automatically, continuously, and on a large scale. Citizens' activities through mobile phones, electronic communications, social media, digital transactions, public services, transportation systems, and surveillance cameras generate digital footprints that can be collected, stored, linked, and analyzed.

This transformation enables surveillance to develop from retrospective surveillance into predictive surveillance. Through big-data analytics and artificial intelligence, previously separate data can be combined to produce profiles, classifications, and predictions of individual behavior. Consequently, surveillance power is no longer determined solely by the state's ability to access data, but also by its ability to connect information originating from different sources.

Digital surveillance is characterized by the ability to operate without the physical presence of state officers, its often-invisible nature to the subject, its capacity to operate continuously and automatically, long-term data retention, and the use of algorithms for classification and prediction. Interference with private spheres can therefore occur invisibly through the collection, aggregation, correlation, and analysis of data.

This condition creates the risk of a surveillance state, particularly when the concentration of informational power is not accompanied by adequate control mechanisms. The state may increasingly know about its citizens, while citizens may know very little about how their data are collected and used. This creates information asymmetry and may produce asymmetrical transparency: citizens become increasingly transparent before the state, while the exercise of state power becomes increasingly difficult for citizens to observe.

Digital surveillance must therefore be understood as a transformation of state power. In the digital state, the ability to collect, connect, and control information constitutes a form of informational power that must remain subject to constitutional principles.

2. Constitutional Rights as Limits on Surveillance Power

Constitutional rights serve a dual function: they guarantee individual freedom and dignity while simultaneously limiting state power. The state has an obligation to protect security and public order, but such obligations do not confer unlimited authority to access the private lives of citizens.

Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia constitutes an important basis for privacy protection through its guarantees concerning the protection of the individual, family, honor, dignity, property, and security. Although the Constitution does not explicitly employ the term right to privacy, the protection of the individual may be interpreted as encompassing digital identity,

electronic communications, biometric data, location information, and other personal information.

Article 28F protects the right to communicate and obtain information. In a digital environment, communications that continuously take place under the shadow of surveillance may produce a chilling effect, namely a tendency for individuals to restrict their expression or communication because they perceive themselves to be under potential surveillance. Article 28D paragraph (1) also requires legal certainty concerning the limits of state authority. Meanwhile, Article 28J must be understood within the framework of the rule of law; the existence of legislation as a formal legal basis does not automatically render a restriction of constitutional rights legitimate.

Digital surveillance therefore lies at the intersection of the state's obligation to maintain security and its obligation to protect rights. The solution is not to eliminate one of these interests, but to establish mechanisms that prevent security interests from being used to eliminate constitutional rights.

3. Privacy as a Constitutional Right in the Digital Sphere

Privacy in a digital society is no longer limited to physical spaces. Activities conducted through digital devices generate information capable of revealing significant aspects of an individual's life. Privacy may at least be understood through four dimensions: informational privacy, communication privacy, spatial privacy, and decisional privacy.

Informational privacy concerns an individual's control over information about themselves; communication privacy concerns the confidentiality of communications and related information; spatial privacy concerns private living spaces; while decisional privacy concerns the freedom to make choices without unlawful state interference.

Privacy is therefore not merely a right to conceal secrets but a condition that enables individuals to develop autonomy. Awareness that communications, social relationships, and activities may be monitored can create a chilling effect that interferes with freedom of expression, association, communication, and the exercise of other constitutional rights.

4. The Shift in the Concept of State Power and Digital Constitutionalism

Technological development has generated a new form of power in the form of informational power. The state possesses advantages over private actors because it has legal authority, law-enforcement apparatuses, intelligence institutions, and access to various databases. The concentration of information within state institutions must therefore be understood as a constitutional issue.

The concept of digital constitutionalism provides a framework for adapting constitutional principles to the digital environment. Principles concerning the limitation of power, protection of rights, accountability, the rule of law, and checks and balances remain relevant, but they must be applied to new forms of power emerging through technology. Technology does not constitute a space beyond the law; surveillance technology is an instrument of power and must therefore remain subject to constitutional scrutiny.

From this perspective, citizens are not merely data subjects but constitutional subjects. Data reflecting an individual's life cannot be treated solely as an administrative resource or security instrument. The greater the state's capacity to know about its citizens, the stronger the constitutional mechanisms required to control that capacity.

B. Problems And Weaknesses In The Constitutional Control Of Digital Surveillance In Indonesia

1. Fragmentation of Legal Bases and Authority

Regulation concerning access to information, interception, data collection, electronic information processing, and intelligence activities is distributed across various legal instruments with different purposes, institutions, and procedures. Such fragmentation produces a plurality of authorities without uniform control standards. The problem becomes more complex when technology enables cross-sectoral data integration. Data initially collected for administrative services may subsequently acquire value for law enforcement, intelligence, security, or public policy. This creates the risk of function creep, namely the use of data for new purposes beyond the original purpose for which the data were collected. Accordingly, the constitutional question is not merely whether a particular institution possesses legal authority, but whether all state institutions are subject to the same constitutional protection standards.

2. Problems of Formal Legality

Legality constitutes a foundation of the rule of law. However, in the context of digital surveillance, the mere existence of a legal norm granting authority is insufficient. Quality of law requires clarity concerning the competent institution, object of surveillance, purpose, procedure, duration, categories of data, use and dissemination of data, retention, deletion, and mechanisms of accountability. Without clear boundaries, technological development may expand state authority without explicit legislative action. This creates a distinction between legal authorization and constitutional legitimacy. An action may possess a formal legal basis but still fail to satisfy constitutional standards.

3. Ambiguity of National Security and Public Interest

National security, law enforcement, public order, and interests relating to state administration may, in principle, constitute legitimate purposes. However, these concepts have broad interpretive scope and may become open-ended justifications if they are not accompanied by clear parameters. Law Number 27 of 2022 concerning Personal Data Protection provides exceptions to several data-subject rights for purposes relating to national defense and security, law enforcement, and certain public interests. Nevertheless, such exceptions remain situated within the framework of statutory implementation. Accordingly, security considerations cannot be used to justify unlimited information collection. A distinction must be made between legitimate purpose and administrative convenience. Technological efficiency cannot serve as a justification for replacing the principle of “collecting the data that are necessary” with “collecting all data that may potentially be useful.” The constitutional question is not what the state can technically do, but what the state is constitutionally permitted to do.

4. Weaknesses in Independent Authorization

Concentration of power occurs when the institution requiring information simultaneously determines the need for surveillance, grants authorization, conducts oversight, and controls the results of surveillance. Such a condition creates the risk of self-authorized surveillance. Because the level of intrusiveness varies, authorization should adopt a risk-based authorization approach. Low-risk surveillance may be subject to administrative control; medium-risk surveillance should require approval from an authorized official and auditing; while high-risk surveillance should require independent or judicial authorization.

5. Limitations of Oversight

Ex ante control is insufficient. Once data have been obtained, they may be reused, retained for long periods, or combined with other sources. Continuous oversight is therefore necessary to examine whether surveillance remains consistent with its authorized purpose, the scope of collection, access, reuse, retention periods, and the possibility of abuse. Operational secrecy may be justified under certain circumstances, but it must be distinguished from secrecy concerning accountability. Secrecy of operation must not become secrecy from accountability. The greater the confidentiality attached to a particular power, the more important it becomes for an oversight institution with sufficient access to examine its implementation.

6. Transparency and Information Asymmetry

The confidential nature of digital surveillance creates an information imbalance. Citizens may not know whether they are being monitored, what data have been collected, how long the data will be retained, or how the information is being used. Confidentiality may be justified while surveillance is ongoing, but it cannot necessarily be maintained permanently once the justification for secrecy has ended. This produces a remedial paradox: citizens theoretically possess rights to seek redress, but in practice cannot exercise those rights because they do not know that a violation has occurred. Transparency may therefore be established through clear regulations, institutional information, statistical reporting, post-surveillance notification under certain circumstances, and access through independent institutions.

7. Limitations of Effective Remedy

Constitutional rights require mechanisms of redress. However, the confidential nature of digital surveillance makes it difficult for citizens to prove that they have been monitored or that a violation has occurred. The state controls information concerning the surveillance process, whereas citizens do not. The Personal Data Protection Law recognizes the right to bring legal claims and obtain compensation and also provides for impact assessments concerning high-risk processing. Nevertheless, these protections do not by themselves establish a remedial mechanism specifically covering the entire digital-surveillance lifecycle. A distinction must therefore be made between a data protection remedy and a surveillance remedy.

8. Algorithmic and Artificial Intelligence-Based Surveillance

Artificial intelligence enables the state to identify patterns, classify individuals, assess risks, detect anomalies, map social relationships, and predict behavior. Problems arise when an individual is categorized as “high risk” based on statistical correlations without having committed any unlawful act. The use of algorithms therefore concerns not only data security but also the accountability of state power. It must be possible to determine who is responsible for erroneous classifications, how individuals may challenge such classifications, and to what extent algorithmic predictions may constitute a basis for state action. Algorithmic systems should not constitute the sole basis for actions that seriously restrict an individual's rights without human verification and oversight.

9. Constitutional Control Gap

The foregoing problems demonstrate that Indonesia's principal problem is not the absence of law. Indonesia already possesses various legal instruments concerning human rights, electronic information, personal data protection, and the authority of state institutions. The problem is the existence of a gap between digital surveillance capabilities and constitutional-control mechanisms.

Technological capabilities are developing rapidly, automatically, in an integrated and cross-institutional manner, and increasingly through algorithmic

systems. Meanwhile, control mechanisms remain largely sectoral, fragmented, institution-based, reactive, and not yet fully designed to regulate the entire surveillance lifecycle. This gap is referred to in this study as the Constitutional Control Gap. Accordingly, the solution cannot simply consist of adding further sectoral regulations. What is required is a model that connects the granting of authority, determination of purpose, assessment of necessity, independent authorization, implementation, processing, use, retention, deletion, accountability, and redress.

C. Reconstruction Of The Constitutional Digital Surveillance Control Model

1. The Urgency of Reconstruction

Technological development has created informational power, namely the state's ability to obtain, control, connect, and use information concerning citizens. In constitutionalism, every expansion of power must be accompanied by a corresponding mechanism for limiting that power. However, the preceding analysis demonstrates that digital surveillance capabilities have developed more rapidly than the mechanisms designed to control them.

Digital surveillance must therefore be understood as a process rather than as a single act. The process includes the granting of authority, determination of purpose, request and authorization, data collection, processing, analysis, retention, use, exchange, and deletion. Because surveillance constitutes a cycle of power, constitutional control must operate throughout that cycle.

On this basis, this study proposes the Constitutional Digital Surveillance Control Model, consisting of five cumulative layers:

- a. Legality
- b. Legitimate Purpose
- c. Necessity
- d. Independent Authorization
- e. Accountability and Effective Remedy

Failure to satisfy any one of these layers may cause a surveillance measure to lose its constitutional legitimacy.

2. Legality

Every digital-surveillance activity must have a legal basis that is clear, valid, predictable, and subject to constitutional review. Legality must not be understood formalistically. The legal norm must determine the competent institution, form of surveillance, target, conditions of implementation, purpose, procedure, duration, categories of data, restrictions on the use and dissemination of data, retention, deletion, and accountability.

This principle prevents technology-driven expansion of power, namely the expansion of state authority resulting from technological development rather than from the enactment of law. Authority to obtain information does not automatically imply authority to conduct mass biometric surveillance or behavioral mapping through artificial intelligence. Legality therefore performs two functions: an authorization function as a source of legitimacy and a limitation function as a boundary on power.

3. Legitimate Purpose

A legal basis does not grant the state unrestricted freedom to use surveillance for any purpose. Every surveillance measure must have a legitimate purpose and a direct relationship with a justifiable public interest. Such purposes may include national security, the prevention of serious crimes, public safety, protection of the rights of others, and law enforcement.

These purposes must not become open-ended justifications. Data collected for one purpose cannot be freely used for another purpose without a legal basis and new justification. This principle constitutes the purpose limitation of surveillance power and is an important instrument for preventing function creep. The state therefore cannot merely demonstrate that it “possesses authority”; it must also explain for what purpose that authority is being exercised.

4. Necessity and Minimal Intrusion

Surveillance may only be conducted when it is genuinely necessary. The state must demonstrate an actual need, the absence of less intrusive alternatives, a non-excessive scope, a limited duration, and the relevance of the data collected. This model rejects the principle of “collect first, justify later.” Instead, it adopts the principle: “Justify first, collect only what is necessary.” The technological ability to collect large amounts of data does not mean that all such data may legitimately be collected. The principle of necessity must be accompanied by data minimization: where a legitimate purpose can be achieved with less data, the collection of additional data cannot be justified. Accordingly, a necessity assessment must be conducted before surveillance begins. The assessment should determine whether there is a real threat, whether surveillance is necessary, whether less intrusive alternatives exist, whether the data are relevant, whether the duration is limited, and whether the scope of surveillance can be narrowed.

5. Independent Authorization

An institution with an interest in conducting surveillance should not be the sole authority determining the legitimacy of its own actions. When an institution determines the need for surveillance, approves the measure, implements it, and controls the results simultaneously, the risk of concentration of power arises.

Therefore, surveillance involving a high degree of intrusiveness must be assessed by an independent authority. Such authorization may take the form of judicial authorization, authorization by a judge or specialized judicial officer, an independent commissioner, or an oversight institution possessing structural and functional independence.

The appropriate model is risk-based authorization. The higher the risk to constitutional rights, the greater the degree of independence and authorization required.

6. Accountability and Effective Remedy

Control does not end with authorization. Every surveillance measure must be capable of being accounted for with respect to its legal basis, purpose, data, duration, use, access, retention, deletion, and potential violations. Accountability must be supported by an audit trail. Every surveillance action should leave an administrative and digital record that enables examination of who accessed the data, when the access occurred, for what purpose, and whether the action complied with the authorization. The principle is: “No surveillance without traceability.”

Meanwhile, effective remedies must be adapted to the confidential character of surveillance. Available mechanisms may include post-surveillance notification, complaints to independent institutions, confidential judicial review, the right to verification, deletion or destruction of unlawfully obtained data, compensation, and sanctions for abuse of authority.

7. Lifecycle Constitutional Control

The principal contribution of this study lies not only in the five principles but also in their integration throughout the digital-surveillance lifecycle. This concept is referred to as Lifecycle Constitutional Control.

a. Authorization Stage

At the authorization stage, legality, legitimate purpose, necessity, and the level of risk to rights must be assessed. High-risk surveillance requires independent authorization.

b. Collection Stage

At the collection stage, the principles of data minimization, purpose limitation, and scope limitation apply. The state may only collect data within the authorized scope.

c. Processing Stage

Processing must be subject to access restrictions, data-security requirements, prohibitions on processing beyond the authorized purpose, and human oversight of algorithms. Algorithmic systems must not constitute the sole basis for actions having serious consequences for rights.

d. Use and Sharing Stage

The use and exchange of data must comply with purpose limitation, necessity, and authorization. Data must not be shared with another institution merely because such sharing is technically possible.

e. Retention Stage

Data retention must have a time limit, periodic evaluation, and access restrictions. Unlimited retention may transform temporary surveillance into a permanent database concerning citizens' lives.

f. Deletion and Review Stage

Once the purpose of surveillance has been fulfilled, the relevance of the data must be evaluated, unnecessary data must be deleted, unlawfully obtained data must be destroyed, independent review must be conducted, and post-surveillance notification should be provided under certain circumstances.

Thus, constitutional control does not end when data have been successfully obtained; it continues until the data are no longer under the control of the state.

8. Reconstructing the Relationship between State Security and Constitutional Rights

Surveillance is frequently understood through the dichotomy of Security versus Privacy. This approach is inadequate because national security and the protection of constitutional rights are not necessarily mutually exclusive interests. A democratic state governed by the rule of law should instead build security through mechanisms that respect rights. Uncontrolled surveillance may generate short-term security capabilities but undermine public trust in the long term. Therefore, this study proposes a paradigm shift toward: "Constitutional Security through Rights-Based Surveillance." Under this paradigm, the protection of rights is not an obstacle to security but a condition for the legitimacy of the exercise of security powers.

9. Relevance of the Model to the Indonesian Legal System

The Constitutional Digital Surveillance Control Model is not intended to replace all existing regulations. Rather, it functions as a constitutional framework applicable to the various forms of state digital-surveillance authority. Its implementation can be pursued at three levels. First, legislative strengthening. Every regulation granting surveillance authority must establish the legal basis, purpose, necessity limits, authorization mechanism, and accountability requirements.

Second, institutional strengthening. Independent oversight mechanisms are necessary through stronger judicial involvement, specialized commissioners,

independent oversight institutions, or a combination of judicial and administrative supervision.

Third, procedural safeguards. Every surveillance measure should be subject to necessity assessment, proportionality assessment, risk classification, documentation, audit trails, periodic review, deletion mechanisms, and complaint mechanisms. The model consequently produces a form of control that is multi-layered, lifecycle-based, risk-sensitive, preventive, independent, accountable, and remedial. The approach therefore shifts from merely regulating surveillance toward constitutionally controlling surveillance power.

CONCLUSION

Digital transformation has changed the relationship between the state, technology, and citizens. The state possesses increasingly powerful capabilities to collect, store, integrate, and analyze information concerning individuals. Such capabilities generate informational power, enabling the state not only to know what citizens have done but also to map and predict their behavior. Digital surveillance may be employed for legitimate purposes such as national security, crime prevention, and law enforcement. However, without adequate limitations, such technology may threaten privacy, personal protection, freedom of communication, freedom of expression, and other constitutional rights.

This study finds that Indonesia's principal problem is not the absence of legal instruments, but rather regulatory fragmentation and the absence of an integrated constitutional-control system. This condition creates a Constitutional Control Gap, namely a gap between the development of digital-surveillance capabilities and the ability of the legal system to effectively control such power. To address this gap, the study proposes the Constitutional Digital Surveillance Control Model, consisting of five cumulative layers: legality, legitimate purpose, necessity, independent authorization, and accountability and effective remedy.

These five layers do not operate independently. Rather, they form an integrated control system ensuring that surveillance authority possesses a legal basis, serves a legitimate purpose, responds to a genuine need, receives independent authorization, and is accompanied by mechanisms of accountability and redress. The principal contribution of this model is reinforced by the concept of Lifecycle Constitutional Control. Digital surveillance must be controlled from the authorization stage through collection, processing, use and sharing, retention, deletion, and review. Constitutional protection thereby ceases to be merely reactive and becomes a preventive system that follows the entire lifecycle of surveillance power. Ultimately, the rule of law in the digital era should not be measured by how much the state is capable of knowing about its citizens, but by how effectively the Constitution is able to constrain the use of that capability. The greater the state's surveillance capacity, the stronger the constitutional protection and control mechanisms that must accompany it.

REFERENCE

A. Legislation

The 1945 Constitution of the Republic of Indonesia.

Law Number 39 of 1999 concerning Human Rights.

Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 27 of 2022 concerning Personal Data Protection.

B. Judgments and International Legal Instruments

European Court of Human Rights. *Big Brother Watch and Others v. The United Kingdom*, Applications Nos. 58170/13, 62322/14, and 24960/15, Grand Chamber Judgment, 25 May 2021.

European Court of Human Rights. *Roman Zakharov v. Russia*, Application No. 47143/06, Grand Chamber Judgment, 4 December 2015.

United Nations. *Universal Declaration of Human Rights*, 1948.

United Nations. *International Covenant on Civil and Political Rights*, 1966.

United Nations Human Rights Committee. *General Comment No. 16: Article 17 (Right to Privacy)*, 1988.

United Nations General Assembly. *The Right to Privacy in the Digital Age*, A/RES/68/167, 2013.

C. Books

Barak, Aharon. (2012). *Proportionality: Constitutional Rights and Their Limitations*. Cambridge: Cambridge University Press.

Foucault, Michel. (1995). *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Lyon, David. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, David. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Nissenbaum, Helen. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

Solove, Daniel J. (2018). *Understanding Privacy*. Cambridge, Massachusetts: Harvard University Press.

Zuboff, Shoshana. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs,

D. Journal Articles

De Gregorio, Giovanni, and Roxana Radu. (2022) "Digital Constitutionalism in the New Era of Internet Governance." *International Journal of Law and Information Technology* 30, no. 1 : 68–87.

De Gregorio, Giovanni. (2021) "The Rise of Digital Constitutionalism in the European Union." *International Journal of Constitutional Law* 19, no. 1 : 41–70.

Mann, Monique, Angela Daly, Michael Wilson, and Nicolas Suzor. (2018). "The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)balance in Australia." *International Communication Gazette* 80, no. 4 : 369–384.

Pollicino, Oreste. (2023) "The Quadrangular Shape of the Geometry of Digital Power(s) and the Move Towards a Procedural Digital Constitutionalism." *European Law Journal*

Subekti, Nanang, I Gusti Ayu Ketut Rahmi Handayani, and Arief Hidayat. (2023). "Konstitusionalisme Digital di Indonesia: Mengartikulasikan Hak dan Kekuasaan dalam Masyarakat Digital." *Peradaban Journal of Law and Society* 2, no. 1.

Yilma, Kinfe Micheal. (2017) "Digital Privacy and Virtues of Multilateral Digital Constitutionalism—Preliminary Thoughts." *International Journal of Law and Information Technology* 25, no. 2 : 115–138.

Yilma, Kinfe. (2026) "Reimagining Digital Constitutionalism." *Global Constitutionalism* 15, no. 1: 62–84.

Prayogi, Arditya, Muhammad Sobri Maulana, and Dwitia Pratiwi. (2026) "Constitutional Limits on State Digital Surveillance in Indonesia: A Proportionality Test of Privacy and Due Process." *Recht: Journal of Legal Studies* 1, no. 1 : 322–331.

- Indraswara, Dede.(2026). “Digital Constitutionalism: A Pancasila Framework in the Era of Artificial Intelligence.” *Indonesian Journal of Pancasila and Global Constitutionalism* 5, no. 1.
- European Court of Human Rights. “Q&A on the Judgment *Big Brother Watch and Others v. The United Kingdom*.” Strasbourg: ECHR.